

Mastering Ethereum

Andreas M. Antonopoulos, Gavin Wood

Table of Contents

Preface	1
Intended audience	1
The bees on the book's cover	1
Conventions used in this book	2
Code examples	3
Using code examples	3
References to companies and products	4
Ethereum addresses and transactions in this book	4
O'Reilly Safari	4
How to contact us	5
Contacting the authors	5
Contacting Andreas	5
Contacting Gavin	6
Acknowledgments by Andreas	6
Acknowledgments by Gavin	6
Contributions	7
Sources	11
Quick Glossary	13
What is Ethereum?	27
Compared to Bitcoin	27
Components of a blockchain	27
Development of Ethereum	28
The Birth of Ethereum	29
Ethereum's four stages of development	31
Past transitions	31
Current state	32
Future plans	32
Ethereum: A general-purpose blockchain	32
Ethereum's components	33
Further references	34
Ethereum and Turing completeness	35
Turing completeness as a "feature"	35
Implications of Turing completeness	36
From general-purpose blockchains to Decentralized Applications (DApps)	37
The Third Age of the Internet	37

Ethereum's development culture	39
Why learn Ethereum?	40
What this book will teach you?.....	40
Ethereum Basics	41
Ether currency units	41
Choosing an Ethereum wallet.....	42
Control and responsibility.....	43
Installing MetaMask.....	45
Using MetaMask for the first time.....	45
Switching networks.....	49
Getting some test ether	50
Sending ether from MetaMask	52
Exploring the transaction history of an address.....	54
Introducing the world computer	57
Externally Owned Accounts (EOAs) and contracts	57
A simple contract: a test ether faucet	58
Compiling the faucet contract	61
Creating the contract on the blockchain	63
Interacting with the contract	67
Viewing the contract address in a block explorer.....	67
Funding the contract.....	69
Withdrawing from our contract	70
Conclusions.....	74
Ethereum Clients	77
Ethereum Networks	77
Should I run a full node?.....	78
Full Node Advantages and Disadvantages	79
Public Testnet Advantages and Disadvantages	80
Local Blockchain Simulation Advantages and Disadvantages	80
Running an Ethereum client	81
Hardware Requirements for a Full Node	81
Software Requirements for Building and Running a Client (Node)	83
Parity.....	84
Installing Parity	84
Go-Ethereum (Geth)	86
Repository Links.....	86
Cloning the repository.....	87
Building Geth from Source Code	87

The First Synchronization of Ethereum-based Blockchains	89
Running geth or parity	90
JSON-RPC Interface.....	90
Parity's Geth Compatibility Mode.....	93
Remote Ethereum Clients	93
Mobile (Smartphone) Wallets	94
Browser wallets	94
MetaMask.....	95
Jaxx.....	95
MyEtherWallet (MEW)	95
MyCrypto	96
Mist	96
Keys, Addresses	97
Introduction	97
Public key cryptography and cryptocurrency	98
Private keys.....	100
Generating a private key from a random number	101
Public keys	102
Elliptic curve cryptography explained	103
Elliptic curve arithmetic operations	107
Generating a public key	108
Elliptic curve libraries.....	110
Cryptographic hash functions	111
Ethereum's cryptographic hash function - Keccak-256	112
Which hash function am I using?	113
Ethereum addresses	114
Ethereum address formats	115
Inter Exchange Client Address Protocol (ICAP)	115
Hex encoding with checksum in capitalization (EIP-55)	117
Detecting an error in an EIP-55 encoded address	119
Conclusions.....	120
Wallets	121
Wallet Technology Overview.....	121
Nondeterministic (Random) Wallets	122
Deterministic (Seeded) Wallets	125
HD Wallets (BIP-32/BIP-44)	125
Seeds and Mnemonic Codes (BIP-39)	127
Wallet Best Practices	127

Mnemonic Code Words (BIP-39).....	128
Generating mnemonic words	129
From mnemonic to seed.....	131
Optional passphrase in BIP-39	133
Working with mnemonic codes.....	134
Creating an HD Wallet from the Seed	135
Hierarchical Deterministic Wallets (BIP-32) and paths (BIP-43/44)	136
Extended public and private keys	138
Hardened child key derivation	139
Index numbers for normal and hardened derivation.....	140
HD wallet key identifier (path)	140
Navigating the HD wallet tree structure	141
Conclusions.....	142
Transactions.....	143
The Structure of a Transaction	143
The transaction nonce	144
Keeping track of nonces	146
Gaps in nonces, duplicate nonces, and confirmation	148
Concurrency, transaction origination, and nonces	149
Transaction gas	150
Transaction recipient	152
Transaction value and data.....	153
Transaction with value (payment), and no data payload	153
Transaction with value (payment), and a data payload	154
Transaction with 0 value, only a data payload	154
Transaction with neither value (payment), nor data payload	155
Transmitting value to EOAs and contracts	155
Transmitting a data payload to an EOA or contract	156
Special transaction: Contract creation.....	158
Digital signatures.....	162
Elliptic Curve Digital Signature Algorithm (ECDSA)	162
How Digital Signatures Work.....	163
Creating a digital signature	163
Verifying the Signature	164
ECDSA Math.....	164
Transaction signing in practice	166
Raw transaction creation and signing.....	167
Raw transaction creation with EIP-155	169

The signature prefix value (v) and public key recovery	170
Separating signing and transmission (offline signing)	171
Transaction propagation	173
Recording on the blockchain	174
Multiple signatures (multisig) transactions	174
Conclusions.....	175
Smart contracts and Solidity	177
What is a smart contract?	177
Lifecycle of a smart contract.....	178
Introduction to Ethereum high-level languages.....	179
Building a smart contract with Solidity	181
Selecting a version of Solidity.....	181
Download and Install	182
Development environment.....	183
Writing a simple Solidity program	183
Compiling with the Solidity compiler (<code>solc</code>).....	184
Ethereum contract Application Binary Interface (ABI)	185
Selecting Solidity compiler and language version	186
Programming with Solidity	187
Data types	188
Predefined global variables and functions	190
Transaction/message call context	190
Transaction context.....	191
Block context	191
Address object	192
Built-in functions	192
Contract definition	193
Functions.....	193
Contract constructor and selfdestruct	195
Adding a constructor and selfdestruct to our Faucet example	197
Function modifiers	198
Contract inheritance	200
Error handling (<code>assert</code> , <code>require</code> , <code>revert</code>)	202
Events.....	204
Catching Events	206
Calling other contracts (<code>send</code> , <code>call</code> , <code>callcode</code> , <code>delegatecall</code>)	208
Creating a new instance	208
Addressing an existing instance	210

Raw call, delegatecall	211
Gas considerations	217
Avoid dynamically-sized arrays	217
Avoid calls to other contracts	217
Estimating gas cost	217
Conclusions.....	220
Smart contracts and Vyper	221
Vulnerabilities and Vyper.....	221
Comparison to Solidity.....	221
Modifiers	222
Class inheritance	224
Inline assembly.....	224
Function overloading	224
Variable typecasting	225
Pre-conditions and post-conditions	227
Decorators.....	228
Function and variable ordering	228
Online code editor and compiler	230
Compiling using the command line	230
Protecting against overflow errors at the compiler level	231
Reading and writing data.....	231
ERC20 token interface implementation	232
Conclusions.....	232
Smart contract security	233
Security best practices	233
Security risks and anti-patterns	234
Re-Entrancy	234
Real-World Example: The DAO	240
Arithmetic Over/Underflows	241
Real-World Examples: PoWHC and Batch Transfer Overflow (CVE-2018-10299)	246
Unexpected Ether	246
Further Examples.....	251
Delegatecall	251
Real-World Example: Parity Multisig Wallet (Second Hack)	257
Default Visibilities	260
Real-World Example: Parity MultiSig Wallet (First Hack)	261
Entropy Illusion	263
Real-World Example: PRNG Contracts	264

External Contract Referencing	264
Real-World Example: Re-Entrancy Honey Pot	269
Short Address/Parameter Attack	271
Unchecked CALL Return Values	273
Real-World Example: Etherpot and King of the Ether	275
Race Conditions / Front Running	277
Real-World Examples: ERC20 and Bancor	279
Denial Of Service (DoS)	280
Real-World Examples: GovernMental	283
Block Timestamp Manipulation	283
Real-World Example: GovernMental	285
Constructors with Care	285
Real-World Example: Rubixi	287
Uninitialised Storage Pointers	287
Real-World Examples: Honey Pots: OpenAddressLottery and CryptoRoulette	289
Floating Point and Precision	290
Real-World Example: Ethstick	292
Tx.Origin Authentication	292
Contract libraries	295
Conclusions	296
Tokens	297
What are tokens?	297
How are tokens used?	297
Tokens and fungibility	299
Counterparty risk	299
Tokens and intrinsicality	300
Using tokens: utility or equity	300
It's a duck!	301
Utility tokens: who needs them?	301
Tokens on Ethereum	303
ERC20 Token Standard	303
ERC20 required functions & events	304
ERC20 optional functions	305
The ERC20 interface defined in Solidity	305
ERC20 data structures	306
ERC20 workflows: "transfer" and "approve & transferFrom"	307
ERC20 Implementations	308
Launching our own ERC20 token	309

Interacting with METoken using the truffle console	314
Sending ERC20 tokens to contract addresses	317
Demonstrating the approve & transferFrom workflow	320
Issues with ERC20 tokens.....	324
ERC223 - a proposed token contract interface standard	325
ERC777 - a proposed token contract interface standard	326
ERC777 Hooks.....	328
ERC721 - non-fungible token (deed) standard	329
Token standards	332
What are token standards? What is their purpose?	332
Should you use these standards?.....	333
Security by maturity	333
Extensions to token interface standards	334
Tokens and ICOs	335
Oracles.....	337
Why are oracles needed	337
Oracle use cases and examples	338
Oracle design patterns	339
Data authentication	342
Computation oracles	343
Decentralized oracles	345
Oracle client interfaces in Solidity	346
Conclusions.....	351
Decentralized Applications (DApps)	353
What is a DApp?	354
Smart contracts "back end"	355
Front end (Web User Interface).....	355
Data storage	356
Inter-Planetary File System (IPFS)	356
Swarm.....	356
Decentralized message communications protocols	356
A basic DApp example: Auction DApp	357
Auction DApp: Back-end smart Contracts	359
DApp governance.....	362
Auction DApp: Front-end user interface	363
Further Decentralizing the Auction DApp	365
Storing the Auction DApp on Swarm.....	366
Preparing Swarm	366

Uploading files to Swarm	368
Ethereum Naming System (ENS)	371
History of Ethereum name services	372
The ENS specification	372
Bottom layer: Name Owners and resolvers	373
Namehash algorithm	373
How to choose a valid name	374
Root node ownership	375
Resolvers	375
Middle layer: the ".eth" nodes	375
Vickrey Auctions	376
Top layer of the ENS: the Deeds	377
Registering a name	377
Managing your ENS name	382
Creating an ENS subdomain	383
ENS Resolvers	385
Resolving a name to a Swarm hash (content)	386
From App to DApp	388
Conclusions	389
The Ethereum Virtual Machine	391
What is it?	391
Comparison with Existing Technology	392
The EVM Instruction Set (Bytecode Operations)	393
Ethereum State	398
Compiling Solidity to EVM bytecode	399
Contract Deployment Code	403
Disassembling the Bytecode	404
Turing completeness and Gas	411
Gas	412
Gas Accounting During Execution	412
Gas accounting considerations	413
Gas cost vs. gas price	414
Negative gas cost	415
Block gas limit	415
Who decides what the block gas limit is?	415
Conclusions	416
Consensus	417
Consensus via proof of work (PoW)	418

Consensus via proof of stake (PoS)	418
Ethash: Ethereum's proof of work	419
Casper: Ethereum's proof of stake	420
Principles of consensus	421
Consensus controversy and competition	421
Appendix A: Ethereum Fork History	423
Ethereum Classic (ETC)	423
The Decentralized Autonomous Organization (The DAO)	423
The Re-Entrancy Bug	424
Re-Entrancy Technicals	424
Re-Entrancy Attack Flow	424
The DAO Hard Fork	425
Timeline of The DAO Hard Fork	426
Ethereum and Ethereum Classic	427
Technical Differences	428
The EVM	428
Core Network Development	428
References	430
Appendix B: Ethereum Standards	433
Ethereum Improvement Proposals (EIPs)	433
Table of Most Important EIPs and ERCs	434
Appendix C: Ethereum EVM Opcodes and gas consumption	449
Appendix D: Development Tools, Frameworks and Libraries	461
Frameworks	461
Truffle	461
Installing the truffle framework	461
Integrating a pre-built Truffle project (Truffle Box)	462
Creating a truffle project directory	462
Configuring truffle	465
Using truffle to deploy a contract	466
Truffle migrations - understanding deployment scripts	466
Using the truffle console	469
Embark	472
OpenZeppelin	473
zeppelin_os	477
Utilities	478
EthereumJS helpeth: A command line utility	478
dapp.tools	479

Dapp	479
Seth	479
Hevm.....	479
Evmdis	480
SputnikVM	480
Libraries.....	480
web3.js	480
web3.py	481
EthereumJS.....	481
web3j	481
Etherjar.....	481
Nethereum	482
ethers.js	482
Emerald Platform.....	482
Testing smart contracts	482
On-Blockchain Testing	484
Ganache: A local test blockchain	485
Appendix E: web3.js tutorial.....	487
Description	487
web3.js contract basic interaction in a non-blocked (async) fashion	487
Node.js script execution.....	488
Reviewing the demo script	488
Contract interaction	489
Asynchronous operation with await	492
Index.....	493

Preface

This book is a collaboration between Andreas M. Antonopoulos and Gavin Wood. A series of fortunate coincidences brought these two authors together in an effort that galvanized hundreds of contributors to produce this book, in the best spirit of open source and the creative commons culture.

Gavin had been wishing to write a book that expanded on the Yellow Paper (his technical description of the Ethereum protocol) for some time, primarily to open it up to a wider audience than the original greek-letter-infused document could possibly allow.

Plans were underway---publishers had been found---when Gavin got talking to Andreas. Gavin knew Andreas, from the very beginning of his tenure with Ethereum, as a notable personality in the space who was interested in learning more about Ethereum.

Meanwhile, Andreas had just published "Mastering Bitcoin," which quickly became the authoritative technical guide to Bitcoin and cryptocurrencies. Almost as soon as the book was published, his readers started asking him "When will you write 'Mastering Ethereum'?" Andreas was already considering his next project and found Ethereum to be a compelling technical subject.

Finally, in May 2016, Gavin and Andreas were both coincidentally in the same city at the same time. They met up for a coffee to chat about working on "Mastering Ethereum" together. With both Andreas and Gavin being devotees of the open-source paradigm they both committed to making this a collaborative effort, released under a creative commons license. Thankfully the publishers, O'Reilly Media, were happy to agree and the "Mastering Ethereum" project was officially launched.

Intended audience

This book is mostly intended for coders. If you can use a programming language, this book will teach you how smart contract blockchains work, how to use them, and how to develop smart contracts and decentralized applications with them. The first few chapters are also suitable as an in-depth introduction to Ethereum for noncoders.

The bees on the book's cover

The Western honey bee (*Apis mellifera*) is a species that exhibits highly complex behavior that, ultimately, benefits its hive. Each individual bee operates freely under a set of simple rules and communicate findings of importance by pheromones and waggle dance. This dance carries valuable

information like the position of the sun and relative geographical coordinates from the hive to the target in question. By interpreting this dance, the bees can relay on this information or act on it, thus, carrying out the decentralized will of swarm intelligence.

Although bees form a caste-based society and have a queen for producing offspring, there is no central authority or leader in a beehive. The highly intelligent and sophisticated behavior exhibited by a multi-thousand-member colony is an emergent property that arises from the interaction of the individuals in a social network.

Nature demonstrates that decentralized systems can be resilient and can produce emergent complexity and incredible sophistication without the need for a central authority, hierarchy, or complex parts.

Conventions used in this book

The following typographical conventions are used in this book:

Italic

Indicates new terms, URLs, email addresses, filenames, and file extensions.

Constant width

Used for program listings, as well as within paragraphs to refer to program elements such as variable or function names, databases, data types, environment variables, statements, and keywords.

Constant width bold

Shows commands or other text that should be typed literally by the user.

Constant width italic

Shows text that should be replaced with user-supplied values or values determined by context.



This icon signifies a tip or suggestion.



This icon signifies a general note.



This icon indicates a warning or caution.

Code examples

The examples are illustrated in Solidity, Vyper, and JavaScript, and using the command line of a Unix-like operating system. All code snippets are available in the GitHub repository under the code subdirectory. Fork the book code, try the code examples, or submit corrections via GitHub:

<https://github.com/ethereumbook/ethereumbook>

All the code snippets can be replicated on most operating systems with a minimal installation of compilers, interpreters and libraries for the corresponding languages. Where necessary, we provide basic installation instructions and step-by-step examples of the output of those instructions.

Some of the code snippets and code output have been reformatted for print. In all such cases, the lines have been split by a backslash (\) character, followed by a newline character. When transcribing the examples, remove those two characters and join the lines again and you should see identical results to those shown in the example.

All the code snippets use real values and calculations where possible, so that you can build from example to example and see the same results in any code you write to calculate the same values. For example, the private keys and corresponding public keys and addresses are all real. The sample transactions, contracts, blocks, and blockchain references have all been introduced to the actual Ethereum blockchain and are part of the public ledger, so you can review them.

Using code examples

This book is here to help you get your job done. In general, if example code is offered with this book, you may use it in your programs and documentation. You do not need to contact us for permission unless you're reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O'Reilly books does require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a significant amount of example code from this book into your product's documentation does require permission.

We appreciate, but do not require, attribution. An attribution usually includes the title, author, publisher, ISBN, and copyright. For example: "*Mastering Ethereum* by Andreas M. Antonopoulos and Gavin Wood (O'Reilly), 978-1-491-97194-9. Copyright 2018."

Some editions of this book are offered under an open source license, such as [CC-BY-NC](#)

[<https://creativecommons.org/licenses/by-nc/4.0/>], in which case the terms of that license apply.

If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at permissions@oreilly.com.

References to companies and products

All references to companies and products are intended for educational, demonstration, and reference purposes. The authors do not endorse any of the companies or products mentioned. We have not tested the operation or security of any of the products, projects or code segments shown in this book. Use them at your own risk!

Ethereum addresses and transactions in this book

The Ethereum addresses, transactions, keys, QR codes, and blockchain data used in this book are, for the most part, real. That means you can browse the blockchain, look at the transactions offered as examples, retrieve them with your own scripts or programs, etc.

However, note that the private keys used to construct the addresses printed in this book have been "burned". This means that if you send money to any of these addresses, the money will either be lost forever or will likely be taken since anyone who reads the book can take it using the private keys printed herein.



DO NOT SEND MONEY TO ANY OF THE ADDRESSES IN THIS BOOK. Your money will be taken by another reader, or lost forever.

O'Reilly Safari



Safari (formerly Safari Books Online) is a membership-based training and reference platform for enterprise, government, educators, and individuals.

Members have access to thousands of books, training videos, Learning Paths, interactive tutorials, and curated playlists from over 250 publishers, including O'Reilly Media, Harvard Business Review, Prentice Hall Professional, Addison-Wesley Professional, Microsoft Press, Sams, Que, Peachpit Press, Adobe, Focal Press, Cisco Press, John Wiley & Sons, Syngress, Morgan Kaufmann, IBM Redbooks, Packt, Adobe Press, FT Press, Apress, Manning, New Riders, McGraw-Hill, Jones & Bartlett, and Course Technology,

among others.

For more information, please visit <http://oreilly.com/safari>.

How to contact us

Please address comments and questions concerning this book to the publisher:

Send comments or technical questions about this book to bookquestions@oreilly.com.

For more information about our books, courses, conferences, and news, see our website at <https://www.oreilly.com>.

Find us on Facebook: <https://facebook.com/oreilly>

Follow us on Twitter: <https://twitter.com/oreillymedia>

Watch us on YouTube: <https://www.youtube.com/oreillymedia>

Contacting the authors

Information about *Mastering Ethereum* as well as the Open Edition and translations are available on: <https://ethereumbook.info/>

Contacting Andreas

You can contact Andreas M. Antonopoulos on his personal site: <https://antonopoulos.com/>

Subscribe to Andreas's channel on YouTube: <https://www.youtube.com/aantonop>

Like Andreas's page on Facebook: <https://www.facebook.com/AndreasMAntonopoulos>

Follow Andreas on Twitter: <https://twitter.com/aantonop>

Connect with Andreas on LinkedIn: <https://linkedin.com/company/aantonop>

Andreas would also like to thank all of the patrons who support his work through monthly donations. You can support Andreas on Patreon at: <https://patreon.com/aantonop>

Contacting Gavin

You can contact Dr. Gavin Wood on his personal site: <http://gavwood.com/>

Follow Gavin on Twitter: <https://twitter.com/gavofyork>

Gavin generally hangs out in the Polkadot Watercooler on Riot.im:
<https://riot.im/app/#/room/#polkadot-watercooler:matrix.org>

Acknowledgments by Andreas

I owe my love of words and books to my mother, Theresa, who raised me in a house with books lining every wall. My mother also bought me my first computer in 1982, despite being a self-described technophobe. My father, Menelaos, a civil engineer who published his first book at 80 years old, was the one who taught me logical and analytical thinking and a love of science and engineering.

Thank you all for supporting me throughout this journey.

Acknowledgments by Gavin

My mother secured my first computer for me at the age of 9 years from a neighbor without which my technical progress would no doubt have been lessened. I also owe her my childhood fear of electricity and must acknowledge Trevor and my grandparents, who performed the grave duty of "watching me plug it in" time after time, and without whom said computer would have been useless. I must also acknowledge the various educators I have been lucky to have through my life, from said neighbor Sean (who taught me my first computer program), to Mr. Quinn my primary school teacher who fixed it for me to do more programming and less history through to secondary-school teachers like Richard Furlong-Brown, who fixed it for me to do more programming and less rugby.

I must thank the mother of my children, Jutta, for continued support and the many people in my life, friends new and old, that keep me, roughly-speaking, sane. Finally, a huge dollop of thanks must go to Aeron Buchanan without whom the last five years of my life could never possibly have unfolded in the way they did and without whose time, support and guidance this book would not be in as good a shape as it is.

Contributions

Many contributors offered comments, corrections, and additions to the early-release draft on GitHub.

Contributions on GitHub were facilitated by two GitHub editors who volunteered to project manage, review, edit, merge and approve pull requests and issues:

- Lead Github Editor: Francisco Javier Rojas Garcia (fjrojasgarcia)
- Assisting Github Editor: William Binns (wbnns)

Major contributions were provided in the chapters on DApps, ENS, Fork History, Gas, EVM, Oracles, Smart Contract Security and Vyper. Additional contributions, which were not included in the first edition due to time and space constraints can be found in the contrib folder on the GitHub repository. Thousands of smaller contributions were provided throughout the book, improving the quality, legibility and accuracy of the book. Sincere thanks to all those who contributed!

Following is an alphabetically sorted list of all GitHub contributors, including their GitHub ID in parentheses:

- Abhishek Shandilya (abhishehandy)
- Adam Zaremba (zaremba)
- Adrian Li (adrianmcli)
- Adrian Manning (agemannning)
- Alejandro Santander (ajsantander)
- Alejo Salles (fiiiu)
- Alex Manuskin (amanusk)
- Alex Van de Sande (alexvandesande)
- Anthony Lusardi (pyskell)
- Assaf Yossifoff (assafy)
- Ben Kaufman (ben-kaufman)
- Bok Khoo (bokkypoobah)

- Brian Ethier (dbe)
- Bryant Eisenbach (fubulobu)
- Chanan Sack (chanan-sack)
- Christopher Gondek (christophergondek)
- Chris Remus (chris-remus)
- Cornell Blockchain (CornellBlockchain)
 - Alex Frolov (sashafrolov)
 - Brian Guo (BrianGuo)
 - Brian Leffew (bleffew99)
 - Giancarlo Pacenza (GPacenza)
 - Lucas Switzer (LucasSwitz)
 - Ohad Koronyo (ohadh123)
 - Richard Sun (richardsfc)
- Cory Solovewicz (CorySolovewicz)
- Dan Shields (NukeManDan)
- Daniel Jiang (WizardOfAus)
- Daniel McClure (danielmcclure)
- Daniel Peterson (danrpts)
- Denis Milicevic (D-Nice)
- Dennis Zasnicoff (zasnicoff)
- Diego H. Gurpegui (diegogurpegui)
- Dimitris Tsapakidis (dimitris-t)
- Enrico Cambiaso (auino)
- Ersin Bayraktar (ersinbyrktr)
- Flash Sheridan (FlashSheridan)

- Franco Daniel Berdun (fMercury)
- Harry Moreno (morenoh149)
- Hon Lau (masterlook)
- Hudson Jameson (Souptacular)
- Iuri Matias (iurimatias)
- Ivan Molto (ivanmolto)
- Jacques Dafflon (jacquesd)
- Jason Hill (denifednu)
- Javier Rojas (fjrojasgarcia)
- Joel Gugger (guggerjoel)
- Jonathan Velando (rigzba21)
- Jon Ramvi (ramvi)
- Jules Lainé (fakje)
- Kevin Carter (kcar1)
- Krzysztof Nowak (krzysztof)
- Lane Rettig (lrettig)
- Leo Arias (elopio)
- Luke Schoen (ltfschoen)
- Liang Ma (liangma)
- Marcelo Creimer (mcreimer)
- Martin Berger (drmartinberger)
- Masi Dawoud (mazewoods)
- Matthew Sedaghatfar (sedaghatfar)
- Michael Freeman (stefek99)
- Miguel Baizan (mbaiigl)

- Mike Pumphrey (bmmpxf)
- Mobin Hosseini (iNDicatOr)
- Nagesh Subrahmanyam (chainhead)
- Nichanan Kesonpat (nichanank)
- Nick Johnson (arachnid)
- Omar Boukli-Hacene (oboukli)
- Paulo Trezentos (paulotrezentos)
- Pet3rpan (pet3r-pan)
- Pierre-Jean Subervie (pjsub)
- Pong Cheecharern (Pongch)
- Qiao Wang (qiaowang26)
- Raul Andres Garcia (manilabay)
- Roger Häusermann (haurog)
- Solomon Victorino (bitsol)
- Steve Klise (sklise)
- Sylvain Tissier (SylTi)
- Taylor Masterson (tjmasterson)
- Tim Nugent (timnugent)
- Timothy McCallum (tpmccallum)
- Tomoya Ishizaki (zaq1tomo)
- Vignesh Karthikeyan (meshugah)
- Will Binns (wbnns)
- Xavier Lavayssière (xalava)
- Yash Bhutwala (yashbhutwala)
- Yeramin Santana (ysfdev)

- Zhen Wang (zmxv)
- ztz (zt2)

Without the help offered by everyone listed above, this book would not have been possible. Your contributions demonstrate the power of open source and open culture, and we are eternally grateful for your help. Thank you.

Sources

Some of the content of this book references or sources various public and open-licensed sources:

<https://github.com/ethereum/vyper/blob/master/README.md>

License: The MIT License (MIT)

{nbspc}

<https://vyper.readthedocs.io/en/latest/>

License: The MIT License (MIT)

{nbspc}

<https://solidity.readthedocs.io/en/v0.4.21/common-patterns.html>

License: The MIT License (MIT)

{nbspc}

<https://arxiv.org/pdf/1802.06038.pdf>

License: Arxiv Non-Exclusive-Distribution

{nbspc}

<https://github.com/ethereum/solidity/blob/release/docs/contracts.rst#inheritance>

License: The MIT License (MIT)

{nbspc}

<https://github.com/trailofbits/evm-opcodes>

License: Apache 2.0

{nbspc}

<https://github.com/ethereum/EIPs/>

License: Creative Commons CC0

{nbspc}

<https://blog.sigmaprime.io/solidity-security.html>

Licence: Creative Commons CC BY 4.0

Quick Glossary

This quick glossary contains many of the terms used in relation to Ethereum. These terms are used throughout the book, so bookmark this for quick reference.

Account

An object containing an address, balance, nonce, and optional storage and code. An account can be a contract account or an EOA (externally owned account).

Address

Most generally, this represents an EOA or contract that can receive (destination address) or send (source address) transactions on the blockchain. More specifically, it is the right-most 160 bits of a Keccak hash of an ECDSA public key.

Assert

In Solidity, assert(false) compiles to **0xfe**, an invalid opcode, which uses up all remaining gas and reverts all changes. When an assert() statement fails, something very wrong and unexpected should be happening, and you will need to fix your code. You should use assert to avoid conditions which should never, ever occur.

Big-endian

A positional number representation where the most significant digit is first. The opposite of little-endian, where the least significant digit is first.

BIP

Bitcoin Improvement Proposals. A set of proposals that members of the Bitcoin community have submitted to improve Bitcoin. For example, BIP-21 is a proposal to improve the Bitcoin uniform resource identifier (URI) scheme.

Block

A block is a collection of required information (a block header) about the comprised transactions, and a set of other block headers known as ommers. It is added to the Ethereum network by miners.

Blockchain

In Ethereum, a sequence of blocks validated by the proof-of-work system, each linking to its predecessor all the way to the genesis block. This varies from the Bitcoin protocol in that it does not

have a block size limit; it instead uses varying gas limits.

Bytecode

Abstract instruction set designed for efficient execution by a software interpreter or a virtual machine. Unlike human readable source code, bytecode is expressed in numeric format.

Byzantium fork

Byzantium is the first of two hard forks for the Metropolis development stage. It included EIP-649: Metropolis Difficulty Bomb Delay and Block Reward Reduction, where the Ice Age (see below) was delayed by 1 year, and the block reward was reduced from 5 to 3 ether.

Compiling

Converting code written in a high-level programming language (e.g. Solidity) into a lower level language (e.g. EVM bytecode).

Consensus

When numerous nodes, usually most nodes on the network, all have the same blocks in their locally validated best block chain. Not to be confused with "consensus rules".

Consensus rules

The block validation rules that full nodes follow to stay in consensus with other nodes. Not to be confused with "consensus".

Constantinople

The second part of the Metropolis stage, planned for mid-2018. Expected to include a switch to hybrid Proof-of-Work/Proof-of-Stake consensus algorithm, among other changes.

Contract account

An account containing code that executes whenever it receives a transaction from another account (EOA or contract).

Contract creation transaction

A special transaction, with the "zero address" as the recipient, that is used to register a contract and record it on the Ethereum blockchain (see "zero address").

DAO

Decentralized Autonomous Organization. Companies and other organizations which operate

without hierarchical management. Also may refer to a contract named "The DAO" launched on 30th April 2016, which was then hacked in June 2016 and ultimately motivated a hard fork (codenamed DAO) at block #1,192,000 which reversed the hacked DAO contract, and caused Ethereum and Ethereum Classic to split into two competing systems.

DApp

Decentralized Application. At a minimum, it is a smart contract and a web user-interface. More broadly, a DApp is a web application that is built on top of open, decentralized, peer-to-peer infrastructure services. In addition, many DApps include decentralized storage and/or message protocol and platform.

Deed

Non-fungible token (NFT) standard introduced by the ERC721 proposal. Unlike ERC20 tokens, deeds prove ownership and are not interchangeable, though they are not recognized as legal documents in any jurisdiction, at least not currently (see also "NFT").

Difficulty

A network-wide setting that controls how much computation is required to produce a proof of work.

Digital signature

A digital signing algorithm is a process by which a user can produce a short string of data called a "signature" of a document using a private key such that anyone with the corresponding public key, the signature, and the document can verify that (1) the document was "signed" by the owner of that particular private key, and (2) the document was not changed after it was signed.

ECDSA

Elliptic Curve Digital Signature Algorithm, or ECDSA, is a cryptographic algorithm used by Ethereum to ensure that funds can only be spent by their owners.

EIP

Ethereum Improvement Proposals describe proposed standards for the Ethereum platform. An EIP is a design document providing information to the Ethereum community, describing a new feature or its processes or environment. For more information, see <https://github.com/ethereum/EIPs> (see also "ERC").

Entropy

In the context of cryptography, lack of predictability, or level of randomness. When generating

secret information, such as private keys, algorithms usually rely on a source of high entropy to ensure the output is unpredictable.

ENS

Ethereum Name Service. For more information, see <https://github.com/ethereum/ens/>.

EOA

Externally Owned Account. Accounts created by or for human users of the Ethereum network.

ERC

Ethereum Request for Comments, a label given to some EIPs which attempt to define a specific standard of Ethereum usage.

Ethash

A Proof-of-Work algorithm for Ethereum 1.0. For more information, see <https://github.com/ethereum/wiki/wiki/Ethash>.

Ether

Ether is the native cryptocurrency used by the Ethereum ecosystem, which covers gas costs when executing Smart Contracts. Its symbol is Ξ , the Greek uppercase Xi character.

Event

An event allows the use of EVM logging facilities. DApps can listen for events and use them to trigger JavaScript callbacks in the user interface. For more information, see <http://solidity.readthedocs.io/en/develop/contracts.html#events>.

EVM

Ethereum Virtual Machine, a stack-based virtual machine which executes bytecode. In Ethereum, the execution model specifies how the system state is altered given a series of bytecode instructions and a small tuple of environmental data. This is specified through a formal model of a virtual state machine.

EVM assembly language

A human-readable form of EVM bytecode.

Fallback function

A default function called in the absence of data or a declared function name.

Faucet

A service that dispenses funds in the form of free test ether that can be used on a testnet.

Finney

A denomination of ether. 10^{15} finney = 1 ether.

Fork

This term assumes two main meanings: a change in protocol causing the creation of an alternative chain, or a temporal divergence in two potential block paths during mining.

Frontier

The initial test development stage of Ethereum, which lasted from July 2015 to March 2016.

Ganache

Personal Ethereum blockchain which you can use to run tests, execute commands, and inspect state while controlling how the chain operates.

Gas

A virtual fuel used in Ethereum to execute smart contracts. The Ethereum Virtual Machine uses an accounting mechanism to measure the consumption of gas and limit the consumption of computing resources (see "Turing complete").

Gas limit

The maximum amount of gas a transaction or block may consume.

Gavin Wood

Gavin Wood is a British programmer who is the co-founder and former CTO of Ethereum. In August 2014 he proposed Solidity, a contract-oriented programming language for writing smart contracts.

Genesis block

The first block in a blockchain, used to initialize a particular network and its cryptocurrency.

Geth

Go Ethereum. One of the most prominent implementations of the Ethereum protocol, written in Go.

Hard fork

A hard fork, also known as a Hard-Forking Change, is a permanent divergence in the blockchain; one commonly occurs when non-upgraded nodes can't validate blocks created by upgraded nodes that follow newer consensus rules. Not to be confused with fork, soft fork, software fork or Git fork.

Hash

A fixed-length fingerprint of variable-size input, produced by a hash function.

HD wallet

A wallet using the Hierarchical Deterministic (HD Protocol) key creation and transfer protocol (BIP32).

HD wallet seed

An HD wallet seed, or seed, is a value used to generate the master private key and master chain code for an HD wallet. The wallet seed can be represented by mnemonic words, making it easier for humans to copy, backup and restore private keys.

Homestead

The second development stage of Ethereum, launched in March 2016 at block #1,150,000.

Ice Age

A hard fork of Ethereum at block #200,000 to introduce an exponential difficulty increase (aka Difficulty Bomb), motivating a transition to Proof-of-Stake.

IDE (Integrated Development Environment)

An integrated user interface that typically combines a code editor, compiler, runtime, and debugger.

Immutable Deployed Code Problem

Once a contract's (or library's) code is deployed it becomes immutable. Standard software development practices rely on being able to fix possible bugs and add new features, so this represents a challenge for smart contract development.

Inter-exchange Client Address Protocol (ICAP)

An Ethereum Address encoding that is partly compatible with the International Bank Account Number (IBAN) encoding, offering a versatile, checksummed and interoperable encoding for Ethereum Addresses. ICAP addresses use a new IBAN pseudo-country code: XE, standing for

"eXtended Ethereum", as used in non-jurisdictional currencies (e.g. XBT, XRP, XCP).

Internal transaction (also "message")

A transaction sent from a contract account to another contract account or an EOA.

IPFS

The Inter Planetary File System is a protocol, a network and an open-source project designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system.

Keccak256

Cryptographic hash function used in Ethereum. Keccak256 was standardized as SHA-3.

Key Derivation Function (KDF)

Also known as a "password stretching algorithm", it is used by keystore formats to protect against brute-force, dictionary, and rainbow table attacks on passphrase encryption, by repeatedly hashing the passphrase.

Keystore File

A JSON-encoded file that contains a single (randomly generated) private key, encrypted by a passphrase for extra security.

LevelDB

LevelDB is an open source on-disk key-value store, implemented as a light-weight, single-purpose library, with bindings to many platforms.

Library

A library in Ethereum is a special type of contract that has no payable functions, no fallback function, and no data storage. Therefore, it cannot receive or hold ether, or store data. A library serves as previously deployed code that other contracts can call for read-only computation.

Lightweight client

A lightweight client is an Ethereum client that does not store a local copy of the blockchain, or validate blocks and transactions. It offers the functions of a wallet and can create and broadcast transactions.

Merkle Patricia Tree

A data structure used in Ethereum to efficiently store key-value pairs.

Message

An internal transaction that is never serialized and only sent within the EVM.

Message Call

The act of passing a message from one Account to another. If the destination account is associated with EVM Code, then the VM will be started with the state of said Object and the Message acted upon.

Metropolis Stage

Metropolis is the third development stage of Ethereum, launched in October 2017.

METoken

Mastering Ethereum Token. An ERC20 token used for demonstration in this book.

Miner

A network node that finds valid proof of work for new blocks, by repeated hashing.

Mist

The first Ethereum-enabled browser, built by the Ethereum Foundation. It contains a browser based wallet that was the first implementation of the ERC20 token standard (Fabian Vogelsteller, author of ERC20, was also the main developer of Mist). Mist was also the first wallet to introduce the camelCase checksum (EIP-55, see [\[eip55\]](#)). Mist runs a full node, and offers a full DApp browser with support for Swarm-based storage and ENS addresses.

Network

Referring to the Ethereum network, a peer-to-peer network that propagates transactions and blocks to every Ethereum node (network participant).

NFT

A non-fungible token (also known as a "deed"). This is a token standard introduced by the ERC721 proposal. NFTs can be tracked and traded, but each token is unique and distinct; they are not interchangeable like ERC20 tokens. NFTs can represent ownership of digital or physical assets.

Node

A software client that participates in the network.

Nonce

In cryptography, a value that can only be used once. There are two types of nonce used in Ethereum. (1) An account nonce: A transaction counter in each account, which is used to prevent replay attacks. (2) Proof of work nonce: The random value in a block that was used to satisfy the proof of work.

Ommer

A child block of an ancestor that is not itself an ancestor. When a miner finds a valid block, another miner may have published a competing block which is added to the tip of the blockchain. Unlike Bitcoin, orphaned blocks in Ethereum can be included by newer blocks as ommers and receive a partial block reward. The term "ommer" is the preferred gender-neutral term for the sibling of a parent node, but is also sometimes referred to as an "uncle".

Parity

One of the most prominent interoperable implementations of the Ethereum client software.

Private key

See "Secret Key".

Proof-of-Stake (PoS)

Proof-of-Stake is a method by which a cryptocurrency blockchain protocol aims to achieve distributed consensus. Proof-of-Stake asks users to prove ownership of a certain amount of cryptocurrency (their "stake" in the network) in order to be able to participate in the validation of transactions.

Proof-of-Work (PoW)

A piece of data (the proof) that requires significant computation to find. In Ethereum, miners must find a numeric solution to the Ehash algorithm that meets a network-wide difficulty target.

Public key

A number, derived via a one-way function from a private key, which can be shared publicly and used by anyone to verify a digital signature made with the corresponding private key.

Receipt

Data returned by an Ethereum client to represent the result of a particular transaction, including a hash of the transaction, its block number, the amount of gas used and, in case of deployment of a Smart Contract, the address of the Contract.

Re-entrancy attack

An attack that consists of an Attacker contract calling a Victim contract function in such a way that during execution the Victim calls the Attacker contract again, recursively. This can result, for example, in the theft of funds by skipping parts of the Victim contract that update balances or count withdrawal amounts.

Reward

An amount of ether included in each new block as a reward by the network to the miner who found the Proof-of-Work solution.

Recursive Length Prefix (RLP)

An encoding standard designed by the Ethereum developers to encode and serialize objects (data structures) of arbitrary complexity and length.

Satoshi Nakamoto

The name used by the person or people who designed Bitcoin, created its original reference implementation, and were the first to solve the double-spend problem for digital currency. Their real identity remains unknown.

Singleton

A computer programming term that describes an object of which only a single instance can exist.

Secret key (aka private key)

The secret number that allows Ethereum users to prove ownership of an account or contracts, by producing a digital signature (see public key, address, ECDSA).

SHA

The Secure Hash Algorithm (SHA) is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST).

Serenity

The fourth and final development stage of Ethereum. Serenity does not yet have a planned release date.

Serpent

A procedural (imperative) smart contract programming language with syntax similar to Python.

Smart contract

A program which executes on the Ethereum computing infrastructure.

Solidity

A procedural (imperative) programming language with syntax that is similar to JavaScript, C++ or Java. The most popular and most frequently used language for Ethereum smart contracts. Created by Gavin Wood (co-author of this book).

Solidity inline assembly

EVM assembly language in a Solidity program. Solidity's support for inline assembly makes it easier to write certain operations.

Spurious Dragon

A hard fork of the Ethereum blockchain, which occurred at block #2,675,000 to address more denial of service attack vectors, and another state clearing; see "Tangerine Whistle". Also, a replay attack protection mechanism.

Swarm

A decentralized (P2P) storage network, used along with Web3 and Whisper to build DApps.

Szabo

A denomination of ether. 10^{12} szabo = 1 ether.

Tangerine Whistle

A hard fork of the Ethereum blockchain, which occurred at block #2,463,000 to change the gas calculation for certain I/O-intensive operations and to clear the accumulated state from a denial of service attack, which exploited the low gas cost of those operations.

Testnet

Short for "test network", a network used to simulate the behavior of the main Ethereum network.

Transaction

Data committed to the Ethereum Blockchain signed by an originating account, targeting a specific address. The transaction contains metadata such as the gas limit for the transaction.

Truffle

One of the most commonly used Ethereum Development Frameworks.

Turing complete

A system of data-manipulation rules (such as a computer's instruction set, a programming language, or a cellular automaton) is said to be "Turing complete" or "computationally universal" if it can be used to simulate any Turing machine. The concept is named after English mathematician and computer scientist Alan Turing.

Vitalik Buterin

Vitalik Buterin is a Russian–Canadian programmer and writer primarily known as the co-founder of Ethereum and as the co-founder of Bitcoin Magazine.

Vyper

A high-level programming language, similar to Serpent, with Python-like syntax. Intended to get closer to a pure-functional language. Created by Vitalik Buterin.

Wallet

Software that holds secret keys. Used to access and control Ethereum accounts and interact with Smart Contracts. Keys need not be stored in a wallet, and can instead be retrieved from an offline storage (e.g. a memory card or paper) for improved security. Despite the name, wallets never store the actual coins or tokens.

Web3

The third version of the web. First proposed by Gavin Wood, Web3 represents a new vision and focus for web applications: from centrally owned and managed applications, to applications built on decentralized protocols.

Wei

The smallest denomination of ether. 10^{18} wei = 1 ether.

Whisper

A decentralized (P2P) messaging service. It is used along with Web3 and Swarm to build DApps.

Zero address

A special Ethereum address, composed entirely of zeros, that is specified as the destination address of a contract creation transaction.

What is Ethereum?

Ethereum is often described as "the World Computer". But what does that mean? Let's start with a computer science–focused description, and then try to decipher that with a more practical analysis of Ethereum's capabilities and characteristics, while comparing it to Bitcoin and other decentralized information exchange platforms (or "blockchains" for short).

From a computer science perspective, Ethereum is a deterministic but practically unbounded state machine, consisting of a globally-accessible singleton state and a virtual machine that applies changes to that state.

From a more practical perspective, Ethereum is an open source, globally decentralized computing infrastructure that executes programs called *smart contracts*. It uses a blockchain to synchronize and store the system's *state* changes, along with a cryptocurrency called *ether* to meter and constrain execution resource costs.

The Ethereum platform enables developers to build powerful decentralized applications with built-in economic functions. While providing high availability, auditability, transparency and neutrality, it also reduces or eliminates censorship, and reduces certain counterparty risks.

Compared to Bitcoin

Many people will come to Ethereum with some prior experience of cryptocurrencies, specifically Bitcoin. Ethereum shares many common elements with other open blockchains: a peer-to-peer network connecting participants, a Byzantine fault-tolerant consensus algorithm for synchronization of state updates (a proof-of-work blockchain), the use of cryptographic primitives such as digital signatures and hashes, and a digital currency (ether).

Components of a blockchain

The components of an open, public, blockchain are (usually):

- A peer-to-peer network connecting participants and propagating transactions and blocks of verified transactions, based on a standardized "gossip" protocol.
- Messages, in the form of transactions, representing state transitions.
- A set of consensus rules, governing what constitutes a transaction and what makes for a valid state

transition.

- A state machine that processes transactions according to the consensus rules.
- A chain of cryptographically secured blocks that acts as a journal of all the verified and accepted state transitions.
- A consensus algorithm that decentralizes control over the blockchain, by forcing participants to cooperate in the enforcement of the consensus rules.
- A game-theoretically sound incentivization scheme (e.g. proof-of-work costs plus block rewards) to economically secure the state machine in an open environment.
- One or more open source software implementations of the above ("clients").

All or most of these components are usually combined in a single software client. For example, in Bitcoin, the reference implementation is developed by the *Bitcoin Core* open source project, and implemented as the bitcoind client. In Ethereum, rather than a reference implementation, there is a *reference specification*, a mathematical description of the system in the Yellow Paper (see [Further references](#)). There are a number of clients, which are built according to the reference specification.

In the past, we used the term "blockchain" to represent all of the components above, as a short-hand reference to the combination of technologies that encompass all of the characteristics described. Today, however, there is a huge variety of blockchains with different properties. We need qualifiers to help us understand the characteristics of the blockchain in question, such as *open, public, global, decentralized, neutral, and censorship-resistant*, to identify the important emergent characteristics of a "blockchain" system that these components allow.

Not all blockchains are created equal. When you are told that something is a blockchain, you have not received an answer; rather, you need to start asking a lot of questions to clarify what they mean when they use the word "blockchain". Start by asking for a description of the components above, then ask about whether this "blockchain" exhibits the characteristics of being *open, public, etc..*

Development of Ethereum

In many ways, both the purpose and construction of Ethereum are strikingly different from the open blockchains that preceded it, including Bitcoin.

Ethereum's purpose is not primarily to be a digital currency payment network. While the digital currency *ether* is both integral to and necessary for the operation of Ethereum, ether is intended as a

utility currency to pay for use of the Ethereum platform as the "World Computer".

Unlike Bitcoin, which has a very limited scripting language, Ethereum is designed to be a general-purpose programmable blockchain that runs a *virtual machine* capable of executing code of arbitrary and unbounded complexity. Where Bitcoin's Script language is, intentionally, constrained to simple true/false evaluation of spending conditions, Ethereum's language is *Turing complete*, meaning that Ethereum can straightforwardly function as a general-purpose computer.

The Birth of Ethereum

All great innovations solve real problems, and Ethereum is no exception. Ethereum was conceived at a time when people recognized the power of the Bitcoin model, and were trying to move beyond cryptocurrency applications. But developers faced a conundrum: they either needed to build on top of Bitcoin or start a new blockchain. Building upon Bitcoin meant living within the intentional constraints of the network and trying to find workarounds. The limited set of transaction types, data types and sizes of data storage seemed to limit the sorts of applications that could run directly on Bitcoin; anything else needed additional off-chain layers, and that immediately negated many of the advantages of using a public blockchain. For projects that needed more freedom and flexibility while staying on-chain, a new blockchain was the only option. But that meant a lot of work: bootstrapping all the infrastructure elements, exhaustive testing, etc.

Towards the end of 2013, Vitalik Buterin, a young programmer and Bitcoin enthusiast, started thinking about further extending the capabilities of Bitcoin and Mastercoin (an overlay protocol that extended Bitcoin to offer rudimentary smart contracts). In October of 2013, Vitalik proposed a more generalized approach to the Mastercoin team, one that allowed flexible and scriptable (but not Turing complete) contracts to replace the specialized contract language of Mastercoin. While the Mastercoin team was impressed, this proposal was too radical a change to fit into their development roadmap.

In December 2013, Vitalik started sharing a white paper which outlined the idea behind Ethereum: a Turing-complete, general-purpose blockchain. A few dozen people saw this early draft and offered feedback, helping Vitalik evolve the proposal.

Both of the authors of this book received an early draft of the white paper and commented on it. Andreas M. Antonopoulos was intrigued by the idea and asked Vitalik many questions about the use of a separate blockchain to enforce consensus rules on smart contract execution and the implications of a Turing-complete language. Andreas continued to follow Ethereum's progress with great interest but was in the early stages of writing his book *Mastering Bitcoin*, and did not participate directly in Ethereum until much later. Gavin Wood, however, was one of the first people to reach out to Vitalik and

offer to help with his C++ programming skills. Gavin became Ethereum's co-founder, co-designer and CTO.

As Vitalik recounts in his "[Ethereum Prehistory](https://vitalik.ca/general/2017/09/14/prehistory.html)" [<https://vitalik.ca/general/2017/09/14/prehistory.html>] post:

This was the time when the Ethereum protocol was entirely my own creation. From here on, however, new participants started to join the fold. By far the most prominent on the protocol side was Gavin Wood...

Gavin can also be largely credited for the subtle change in vision from viewing Ethereum as a platform for building programmable money, with blockchain-based contracts that can hold digital assets and transfer them according to pre-set rules, to a general-purpose computing platform. This started with subtle changes in emphasis and terminology, and later this influence became stronger with the increasing emphasis on the "Web 3" ensemble, which saw Ethereum as being one piece of a suite of decentralized technologies, the other two being Whisper and Swarm.

Starting in December 2013, Vitalik and Gavin refined and evolved the idea, together building the protocol layer that became Ethereum.

Ethereum's founders were thinking about a blockchain without a specific purpose, that could support a broad variety of applications by being *programmed*. The idea was that by using a general-purpose blockchain like Ethereum, a developer could program their particular application without having to implement the underlying mechanisms of peer-to-peer networks, blockchains, consensus algorithms, etc. The Ethereum platform was designed to abstract these details and provide a deterministic and secure programming environment for decentralized blockchain applications.

Much like Satoshi, Vitalik and Gavin didn't just invent a new technology, they combined new inventions with existing technologies in a novel way and delivered the prototype code to prove their ideas to the world.

The founders worked for years, building and refining the vision. And on July 30th 2015, the first Ethereum block was mined. The world's computer started serving the world...

Vitalik Buterin's article "A Prehistory of Ethereum" was published in September 2017 and provides a fascinating first-person view of Ethereum's earliest moments.

You can read it at <https://vitalik.ca/general/2017/09/14/prehistory.html>

Ethereum's four stages of development

The birth of Ethereum was the launch of the first stage, named "Frontier". Ethereum's development is planned over four distinct stages, with major changes occurring at each stage. A stage may include sub-releases, known as "hard forks", that change functionality in a way that is not backwards compatible.

The four main development stages are codenamed Frontier, Homestead, Metropolis and Serenity. The intermediate hard forks that have occurred to date are codenamed "Ice Age", "DAO", "Tangerine Whistle", "Spurious Dragon", "Byzantium", and "Constantinople". Both the development stages and the intermediate hard forks are shown on the following timeline, which is "dated" by block number:

Past transitions

Block #0

"Frontier" - The initial stage of Ethereum, lasted from July 30th 2015 to March 2016.

Block #200,000

"Ice Age" - A hard fork to introduce an exponential difficulty increase, to motivate a transition to Proof-of-Stake when ready.

Block #1,150,000

"Homestead" - The second stage of Ethereum, launched in March 2016.

Block #1,192,000

"DAO" - The hard fork that reimbursed victims of the hacked DAO contract and caused Ethereum and Ethereum Classic to split into two competing systems.

Block #2,463,000

"Tangerine Whistle" - A hard fork to change the gas calculation for certain I/O-heavy operations and to clear the accumulated state from a denial of service attack, which exploited the low gas cost of

those operations.

Block #2,675,000

"Spurious Dragon" - A hard fork to address more denial of service attack vectors, and another state clearing. Also, a replay attack protection mechanism.

Current state

We are currently in the *Metropolis* stage, which was planned as two sub-release hard forks (see [Future plans](#)) codenamed *Byzantium* and *Constantinople*. *Byzantium* went into effect in October 2017 and *Constantinople* is anticipated in 2019.

Block #4,370,000

"Metropolis Byzantium" - Metropolis is the third stage of Ethereum, current at the time of writing this book, launched in October 2017. *Byzantium* is the first of two hard forks for Metropolis.

Future plans

After Metropolis' *Byzantium* hard fork, there is one more hard fork planned for Metropolis. Metropolis will be followed by the final stage of Ethereum's deployment, codenamed *Serenity*.

Constantinople

The second part of the Metropolis stage, planned for mid-2018 but since delayed with no set release date.

Serenity

The fourth and final stage of Ethereum. Serenity does not yet have a planned release date.

Ethereum: A general-purpose blockchain

The original blockchain, namely Bitcoin's blockchain, tracks the state of units of bitcoin and their ownership. You can think of Bitcoin as a distributed consensus *state machine*, where transactions cause a global *state transition*, altering the ownership of coins. The state transitions are constrained by the rules of consensus, allowing all participants to (eventually) converge on a common (consensus) state of the system, after several blocks are mined.

Ethereum is also a distributed state machine. But instead of tracking only the state of currency

ownership, Ethereum tracks the state transitions of a general-purpose data store. By "general-purpose data store" we mean a store that can hold any data expressible as a *key-value tuple*. A key-value data store holds arbitrary values, each referenced by some key; for example, the value "Mastering Ethereum" referenced by the key "Book Title". In some ways, this serves the same purpose as the data storage model of *Random Access Memory (RAM)* used by most general-purpose computers. Ethereum has *memory* that stores both code and data and it uses the Ethereum blockchain to track how this memory changes over time. Like a general-purpose stored-program computer, Ethereum can load code into its state machine and *run* that code, storing the resulting state changes in its blockchain. Two of the critical differences from most general-purpose computers are that Ethereum state changes are governed by the rules of consensus and the state is distributed globally. Ethereum answers the question: "What if we could track any arbitrary state and program the state machine to create a world-wide computer operating under consensus?"

Ethereum's components

In Ethereum, the components of a blockchain system described in [Components of a blockchain](#) are, more specifically:

P2P Network

Ethereum runs on the *Ethereum Main Network*, which is addressable on TCP port 30303, and runs a protocol called *Devp2p*.

Consensus rules

Ethereum's consensus rules are defined in the reference specification, the Yellow Paper (see <>references>).

Transactions

Ethereum transactions are network messages that include (among other things) a sender, recipient, value and data payload.

State Machine

Ethereum state transitions are processed by the *Ethereum Virtual Machine (EVM)*, a stack-based virtual machine that executes *bytecode* (machine-language instructions). EVM programs, called "smart contracts", are written in high-level languages (e.g. Solidity) and compiled to bytecode for execution on the EVM.

Data Structures

Ethereum's state is stored locally on each node as a *database* (usually Google's LevelDB), which contains the transactions and system state in a serialized hashed data structure called a *Merkle Patricia Tree*.

Consensus Algorithm

Ethereum uses Nakamoto Consensus, i.e. Bitcoin's consensus model, which uses sequential single-signature blocks, weighted in importance by Proof-of-Work to determine the longest chain and therefore the current state. However, there are plans to move to a Proof-of-Stake weighted voting system, codenamed *Casper*, in the near future.

Economic Security

Ethereum currently uses a Proof-of-Work algorithm called *Ethash*, but this will eventually be dropped with the move to Proof-of-Stake at some point in the future.

Clients

Ethereum has several interoperable implementations of the client software, the most prominent of which are *Go-Ethereum (Geth)* and *Parity*.

Further references

The Ethereum Yellow Paper: <https://ethereum.github.io/yellowpaper/paper.pdf>

The "Beige Paper": a rewrite of the "Yellow Paper" for a broader audience in less formal language:
<https://github.com/chronaeon/beigepaper>

ÐΞVp2p network protocol: <https://github.com/ethereum/wiki/wiki/%C3%90%CE%9EVp2p-Wire-Protocol>

Ethereum Virtual Machine - a list of resources: [https://github.com/ethereum/wiki/wiki/Ethereum-Virtual-Machine-\(EVM\)-Awesome-List](https://github.com/ethereum/wiki/wiki/Ethereum-Virtual-Machine-(EVM)-Awesome-List)

LevelDB Database (used most often to store the local copy of the blockchain): <http://leveldb.org>

Merkle Patricia Trees: <https://github.com/ethereum/wiki/wiki/Patricia-Tree>

Ethash Proof-of-Work: <https://github.com/ethereum/wiki/wiki/Ethash>

Casper Proof-of-Stake v1 Implementation Guide: <https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide>

Go-Ethereum (Geth) Client: <https://geth.ethereum.org/>

Parity Ethereum Client: <https://parity.io/>

Ethereum and Turing completeness

As soon as you start reading about Ethereum, you will immediately hear the term "Turing complete". Ethereum, they say, unlike Bitcoin, is "Turing complete". What exactly does that mean?

The term refers to English mathematician Alan Turing, who is considered the father of computer science. In 1936 he created a mathematical model of a computer consisting of a state machine that manipulates symbols by reading and writing them on sequential memory (resembling an infinite-length paper tape). With this construct, Turing went on to provide a mathematical foundation to answer (in the negative) questions about *universal computability*, meaning whether all problems are solvable. He proved that there are classes of problems that are uncomputable. Specifically, he proved that the *Halting Problem* (whether it is possible, given an arbitrary program and its input, to determine whether the program will eventually stop running) is not solvable.

Alan Turing further defined a system to be *Turing complete* if it can be used to simulate any Turing Machine. Such a system is called a *Universal Turing Machine (UTM)*.

Ethereum's ability to execute a stored program, in a state machine called the Ethereum Virtual Machine, while reading and writing data to memory makes it a Turing-complete system and therefore a Universal Turing Machine. Ethereum can compute any algorithm that can be computed by any Turing Machine, given the limitations of finite memory.

Ethereum's groundbreaking innovation is to combine the general-purpose computing architecture of a stored-program computer with a decentralized blockchain, thereby creating a distributed single-state (singleton) world computer. Ethereum programs run "everywhere", yet produce a common state that is secured by the rules of consensus.

Turing completeness as a "feature"

Hearing that Ethereum is Turing complete, you might arrive at the conclusion that this is a *feature* that is somehow lacking in a system that is Turing Incomplete. Rather, it is the opposite. Turing completeness is very easy to achieve; in fact, the simplest Turing complete state machine known

(Rogozhin, 1996) has 4 states and uses 6 symbols, with a state definition that is only 22 instructions long. Indeed, sometimes systems are found to be "Accidentally Turing complete". A fun reference of such systems can be found here: http://beza1e1.tuxen.de/articles/accidentally_turing_complete.html

However, Turing completeness is very dangerous, particularly in open access systems, like public blockchains, because of the Halting Problem we touched on earlier. For example, modern printers are Turing complete and can be given files to print that send them into a frozen state. The fact that Ethereum is Turing complete means that any program of any complexity can be computed in Ethereum. But that flexibility brings some thorny security and resource management problems. An unresponsive printer can be turned off and turned back on again. That is not possible with a public blockchain.

Implications of Turing completeness

Turing proved that you cannot predict whether a program will terminate by simulating it on a computer. In simple terms, we cannot predict the path of a program without running it. Turing complete systems can run in "infinite loops", a term used (in oversimplification) to describe a program that does not terminate. It is trivial to create a program that runs a loop that never ends. But unintended never-ending loops can arise without warning, due to complex interactions between the starting conditions and the code. In Ethereum, this poses a challenge: every participating node (client), must validate every transaction, running any smart contracts it calls. But as Turing proved, Ethereum can't predict if a smart contract will terminate, or how long it will run, without actually running it (possibly running forever). Whether by accident, or on purpose, a smart contract can be created such that it runs forever when a node attempts to validate it. This is effectively a denial of service attack. Of course, between a program that takes a millisecond to validate and one that runs forever there is an infinite range of nasty, resource hogging, memory-bloating, CPU-overheating programs that simply waste resources. In a world computer, a program that abuses resources gets to abuse the world's resources. How does Ethereum constrain the resources used by a smart contract if it cannot predict resource use in advance?

To answer this challenge, Ethereum introduces a metering mechanism called *gas*. As the EVM executes a smart contract, it carefully accounts for every instruction (computation, data access, etc.). Each instruction has a pre-determined cost in units of gas. When a transaction triggers the execution of a smart contract, it must include an amount of gas that sets the upper limit of computation that can be consumed running the smart contract. The EVM will terminate execution if the amount of gas consumed by computation exceeds the gas available in the transaction. Gas is the mechanism Ethereum uses to allow Turing-complete computation while limiting the resources that any program can consume.

The next question is, 'how does one get gas to pay for computation on the Ethereum world computer?' You won't find gas on any exchanges. It can only be purchased as part of a transaction, and can only be bought with Ether. Ether needs to be sent along with a transaction and it needs to be explicitly earmarked for the purchase of gas, along with an acceptable gas price. Just like at the pump, the price of gas is not fixed. Gas is purchased for the transaction, the computation is executed, and any unused gas is refunded back to the sender of transaction.

From general-purpose blockchains to Decentralized Applications (DApps)

Ethereum started as a way to make a general-purpose blockchain that could be programmed for a variety of uses. But very quickly, Ethereum's vision expanded to become a platform for programming *Decentralized Applications (DApps)*. DApps represent a broader perspective than "smart contracts". A DApp is, at the very least, a smart contract and a web user-interface. More broadly, a DApp is a web application that is built on top of open, decentralized, peer-to-peer infrastructure services.

A DApp is composed of at least:

- Smart contracts on a blockchain.
- A web front-end user-interface.

In addition, many DApps include other decentralized components, such as:

- A decentralized (P2P) storage protocol and platform.
- A decentralized (P2P) messaging protocol and platform.



You may see DApps spelled as ÐApps. The Ð character is the Latin character called "ETH", alluding to Ethereum. To display this character, use the Unicode codepoint 0xD0, or if necessary the HTML character entity eth (or decimal entity #208).

The Third Age of the Internet

In 2004, the term "Web 2.0" came to prominence, describing an evolution of the web towards user-generated content, responsive interfaces and interactivity. Web 2.0 is not a technical specification, but rather a term describing the new focus of web applications.

The concept of DApps is meant to take the World Wide Web to its next natural evolutionary stage, introducing decentralization with peer-to-peer protocols into every aspect of a web application. The term used to describe this evolution is *Web3*, meaning the third "version" of the web. First proposed by Gavin Wood, *web3* represents a new vision and focus for web applications: from centrally owned and managed applications, to applications built on decentralized protocols.

In later chapters we'll explore the Ethereum web3.js JavaScript library, which bridges JavaScript applications that run in your browser with the Ethereum blockchain. The web3.js library also includes an interface to a P2P storage network called *Swarm* and a P2P messaging service called *Whisper*. We can see how these services might work together in [Web3: A suite of decentralized application components for the next evolution of the web](#). With these three components included in a JavaScript library running in your web browser, developers have a full application development suite that allows them to build web3 DApps:

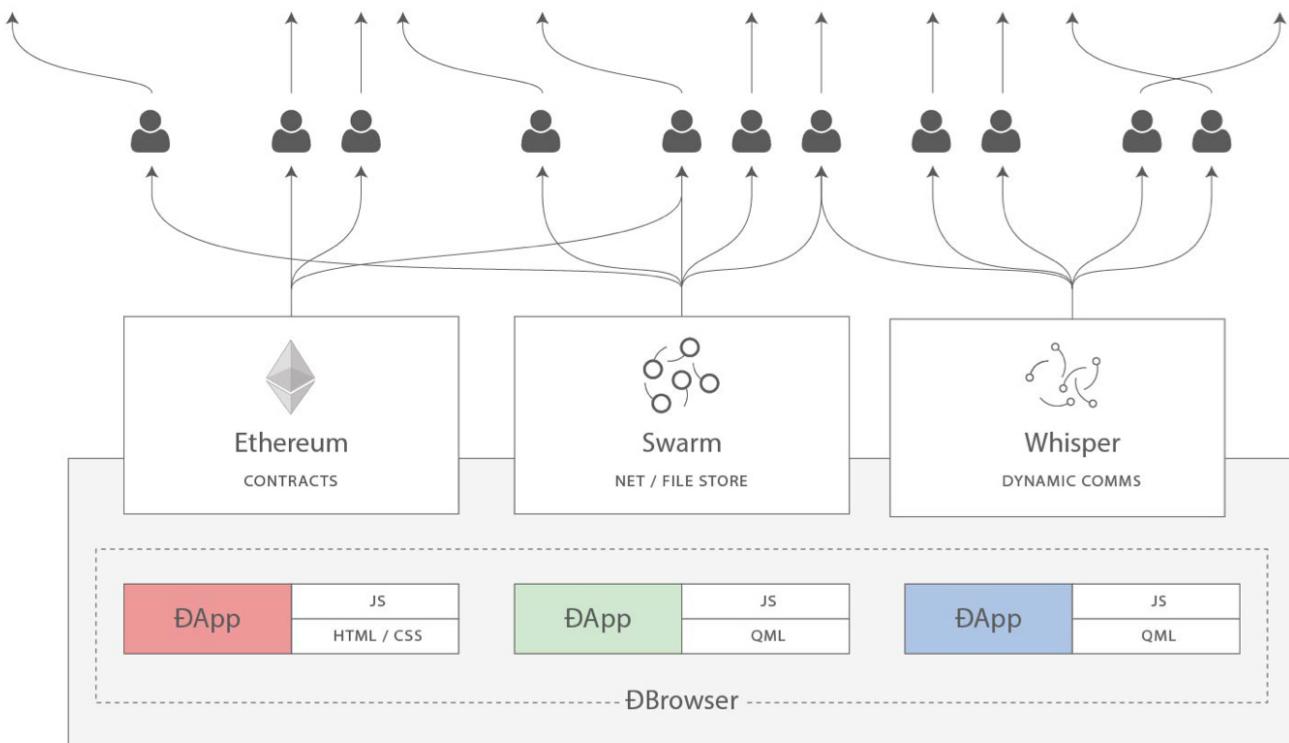


Figure 1. *Web3: A suite of decentralized application components for the next evolution of the web*

Ethereum's development culture

So far we've talked about how Ethereum's goals and technology differ from other blockchains that preceded it, like Bitcoin. Ethereum also has a very different development culture.

In Bitcoin, development is guided by very conservative principles: all changes are carefully studied to ensure that none of the existing systems are disrupted. For the most part, changes are only implemented if they are backwards compatible. Existing clients are allowed to "opt-in", but will continue to operate if they decide not to upgrade.

In Ethereum, by comparison, the community's development culture is focused on the future rather than the past. The (not entirely serious) mantra is "move fast and break things". If a change is needed, it is implemented, even if that means invalidating prior assumptions, breaking compatibility, or forcing clients to update. Ethereum's development culture is characterized by rapid innovation, rapid evolution and a willingness to deploy forward-looking improvements, even if this is at the expense of some backwards compatibility.

What this means to you as a developer, is that you must remain flexible and be prepared to rebuild your infrastructure as some of the underlying assumptions change. One of the big challenges facing developers in Ethereum is the inherent contradiction between deploying code to an immutable system and a development platform that is still evolving. You can't simply "upgrade" your smart contracts. You must be prepared to deploy new ones, migrate users, apps and funds, and start over.

Ironically, this also means that the goal of building systems with more autonomy and less centralized control is still not fully realized. Autonomy and decentralization requires a bit more stability in the platform than you're likely to get in Ethereum in the next few years. In order to "evolve" the platform, you have to be ready to scrap and restart your smart contracts, which means you have to retain a certain degree of control over them.

But, on the positive side, Ethereum is moving forward very fast. There's very little opportunity for "bike-shedding", an expression that means holding up development by arguing over minor details such as how to build the bicycle shed at the back of a nuclear power station. If you start bike-shedding, you might suddenly discover the rest of the development team changed the plan, and ditched bicycles in favor of autonomous hovercraft.

Eventually, the development of the Ethereum platform will slow down and its interfaces will become fixed. But in the meantime, innovation is the driving principle. You'd better keep up, because no one will slow down for you.

Why learn Ethereum?

Blockchains have a very steep learning curve, as they combine multiple disciplines into one domain: programming, information security, cryptography, economics, distributed systems, peer-to-peer networks etc. Ethereum makes this learning curve a lot less steep, so you can get started very quickly. But just below the surface of a deceptively simple environment lies a lot more. As you learn and start looking deeper, there's always another layer of complexity and wonder.

Ethereum is a great platform for learning about blockchains and it's building a massive community of developers, faster than any other blockchain platform. More than any other blockchain, Ethereum is a *developer's blockchain*, built by developers for developers. A developer familiar with JavaScript applications can drop into Ethereum and start producing working code very quickly. For the first few years of Ethereum, it was common to see T-shirts announcing that you can create a token in just five lines of code. Of course, this is a double-edged sword. It's easy to write code, but it's very hard to write *good and secure* code.

What this book will teach you?

This book dives into Ethereum and examines every component. You will start with a simple transaction, dissect how it works, build a simple contract, make it better and follow its journey through the Ethereum system.

You will learn how to use Ethereum, how it works, but also why it is designed the way it is. You will be able to understand how each of the pieces works, and how they fit together and why.

Ethereum Basics

Ether currency units

Ethereum's currency unit is called *ether*, identified also as "ETH" or with the symbols Ξ (from the Greek letter "Xi" that looks like a stylized capital E) or, less often, \blacklozenge , for example, 1 ether, or 1 ETH, or $\Xi 1$, or $\blacklozenge 1$.



Use Unicode character U+039E for Ξ and U+2666 for \blacklozenge .

Ether is subdivided into smaller units, down to the smallest unit possible, which is named *wei*. One *ether* is 1 quintillion *wei* (1×10^{18} or 1,000,000,000,000,000,000). You may hear people refer to the currency "Ethereum" too, but this is a common beginner's mistake. Ethereum is the system, ether is the currency.

The value of ether is always represented internally in Ethereum as an unsigned integer value denominated in *wei*. When you transact 1 ether, the transaction encodes 1000000000000000000000000 wei as the value.

Ether's various denominations have both a *scientific name* using the International System of units (SI), and a colloquial name that pays homage to many of the great minds of computing and cryptography.

[Ether Denominations and Unit Names](#) shows the various units, their colloquial (common) name, and their SI name. In keeping with the internal representation of value, the table shows all denominations in *wei* (first row), with ether shown as 10^{18} *wei* in the 7th row:

Table 1. Ether Denominations and Unit Names

Value (in wei)	Exponent	Common Name	SI Name
1	1	wei	wei
1,000	10^3	babbage	kilowei or femtoether
1,000,000	10^6	lovelace	megawei or picoether
1,000,000,000	10^9	shannon	gigawei or nanoether
1,000,000,000,000	10^{12}	szabo	microether or micro
1,000,000,000,000,000	10^{15}	finney	milliether or milli

Value (in wei)	Exponent	Common Name	SI Name
1,000,000,000,000,000,00	10^{18}	ether	ether
1,000,000,000,000,000,00,000	10^{21}	grand	kiloether
1,000,000,000,000,000,00,000,00	10^{24}		megaether

Choosing an Ethereum wallet

The term "wallet" has come to mean many things, although they are all related and on a day-to-day basis they are pretty much the same thing. We will use the term "wallet" to mean a software application that helps you manage your Ethereum account. In short, an Ethereum wallet is your gateway to the Ethereum system. It holds your keys and can create and broadcast transactions on your behalf.

Choosing an Ethereum wallet can be difficult because there are many different options with different features and designs. Some are more suitable for beginners and some are more suitable for experts. Even if you choose one that you like now, you might decide to switch to a different wallet later on. The Ethereum platform itself is still being improved and the "best" wallets are often the ones that adapt to the changes that come with the platform upgrades.

But don't worry! If you choose a wallet and don't like how it works, you can change wallets quite easily. All you have to do is make a transaction that sends your funds from the old wallet to the new wallet, or move the keys by exporting and importing your private keys.

To get started, we will choose three different types of wallets to use as examples throughout the book: a mobile wallet, a desktop wallet, and a web-based wallet. We've chosen these three wallets because they represent a broad range of complexity and features. However, the selection of these wallets is not an endorsement of their quality or security. They are simply a good starting place for demonstrations and testing.

Remember that for a wallet application to work, it must have access to your private keys, so it is vital that you only download and use wallet applications from sources you trust. Fortunately, in general, the more popular a wallet application is, the more trustworthy it is likely to be. Nevertheless, it is good practice to avoid "putting all your eggs in one basket" and have your Ethereum accounts spread across a couple of wallets.

Starter wallets:

MetaMask

MetaMask is a browser extension wallet that runs in your browser (Chrome, Firefox, Opera or Brave Browser). It is easy to use and convenient for testing, as it is able to connect to a variety of Ethereum nodes and test blockchains. MetaMask is a web-based wallet.

Jaxx

Jaxx is a multi-platform and multi-currency wallet that runs on a variety of operating systems including Android, iOS, Windows, Mac, and Linux. It is often a good choice for new users as it is designed for simplicity and ease of use. Jaxx is either a mobile or desktop wallet, depending on where you install it.

MyEtherWallet (MEW)

MyEtherWallet is a web-based wallet that runs in any browser. It has multiple sophisticated features we will explore in many of our examples. MyEtherWallet is a web-based wallet.

Emerald Wallet

Emerald Wallet is designed to work with Ethereum Classic blockchain, but compatible with other Ethereum-based blockchains. It's an open source desktop application, and works under Windows, Mac and Linux. Emerald wallet can run a full node or connect to a public remote node, working in a "light" mode. It also has a companion tool to do all operations from command line.

We'll start by installing MetaMask on our desktop but first, we'll briefly discuss controlling and managing keys.

Control and responsibility

Open blockchains like Ethereum are important because they operate as a *decentralized* system. That means lots of things, but one crucial aspect is that each user of Ethereum can control their own private keys, which are the things that control access to funds and smart contracts. We sometimes call the combination of access to funds and smart contracts an "account" or "wallet". These terms can get quite complex in their functionality, so we will go into this in more detail later. As a fundamental principle, however, it is as easy as one private key equals one "account". Some users choose to give up control over their private keys by using a third party custodian, such as an online exchange. In this book, we will teach you how to take control and manage your own private keys.

With control comes a big responsibility. If you lose your private keys, you lose access to funds and

contracts. No one can help you regain access; your funds will be locked forever. Here are a few tips to help you manage this responsibility:

- Do not improvise security. Use tried-and-tested standard approaches.
- The more important the account (e.g. the higher the value of the funds controlled, or the more significant the smart contracts accessible), the higher security measures should be taken.
- The highest security is gained from an air-gapped device, but this level is not required for every account.
- Never store your private key in plain form, especially digitally. Fortunately, most user interfaces today won't even let you see the raw private key.
- Private keys can be stored in an encrypted form, as a digital "keystore" file. Being encrypted, they need a password to unlock. When you are prompted to choose a password, make it strong (i.e. long and random), back it up and don't share it. If you don't have a password manager, write it down and store it in a safe and secret place. To access your account, you need both the "keystore" file and the password.
- Do not store any passwords in digital documents, digital photos, screenshots, online drives, encrypted PDFs, etc. Again, do not improvise security. Use a password manager or pen and paper.
- When you are prompted to back up a key as a mnemonic word sequence, use pen and paper to make a physical backup. Do not leave that task for "later"; you will forget. These can be used to rebuild your private key in case you lose all data saved on your system, or if you forget or lose your password. However, they can also be used by attackers to get your private keys, so never store them digitally, and keep the physical copy stored securely in a locked drawer or safe.
- Before transferring any large amounts (especially to new addresses), first do a small test transaction (e.g. less than \$1 value) and wait for confirmation of receipt.
- When you create a new account, start by sending only a small test transaction to the new address. Once you receive the test transaction, try sending back again from that account. There are lots of reasons account creation can go wrong, and if it has gone wrong, it is better to find out with a small loss. If the tests work, all is well.
- Public block explorers are an easy way to independently see whether a transaction has been accepted by the network. However, this convenience has a negative impact on your privacy, because you reveal your addresses to block explorers, which can track you.
- Do not send money to any of the addresses shown in this book. The private keys are listed in the book and someone will immediately take that money.

Now that we've covered some basic best practices for key management and security, let's get to work using MetaMask!

Installing MetaMask

Open the Google Chrome browser and navigate to:

<https://chrome.google.com/webstore/category/extensions>

Search for "MetaMask" and click on the logo of a fox. [The detail page of the MetaMask Chrome Extension](#) should look like this:



Figure 2. The detail page of the MetaMask Chrome Extension

It's important to verify that you are downloading the real MetaMask extension, as sometimes people are able to sneak malicious extensions past Google's filters. The real one:

- Shows the ID nkbihfbeogaeaoehlefnkodbefgpgknn in the address bar
- Is offered by <https://metamask.io>
- Has more than 800 reviews
- Has more than 1,000,000 users

Once you confirm you are looking at the correct extension, click "Add to Chrome" to install it.

Using MetaMask for the first time

Once MetaMask is installed you should see a new icon (head of a fox) in your browser's toolbar. Click on it to get started. You will be asked to accept the terms and conditions and then to create your new Ethereum wallet by entering a password, see [The password page of the MetaMask Chrome Extension](#):

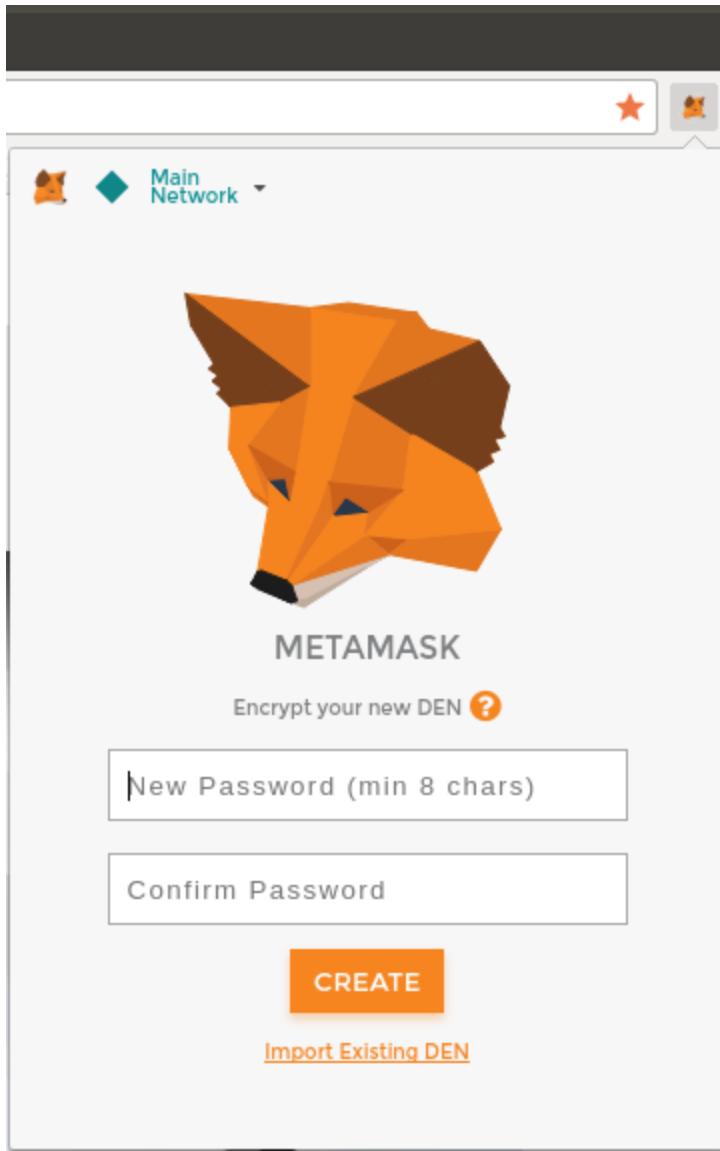


Figure 3. The password page of the MetaMask Chrome Extension



The password controls access to MetaMask, so that it can't be used by anyone with access to your browser.

Once you've set a password, MetaMask will generate a wallet for you and show you a *mnemonic backup* consisting of 12 English words. These words can be used in any compatible wallet to recover access to your funds should something happen to MetaMask or your computer. You do not need the password for

this recovery. The 12 words are sufficient. See [The mnemonic backup of your wallet, created by MetaMask](#):

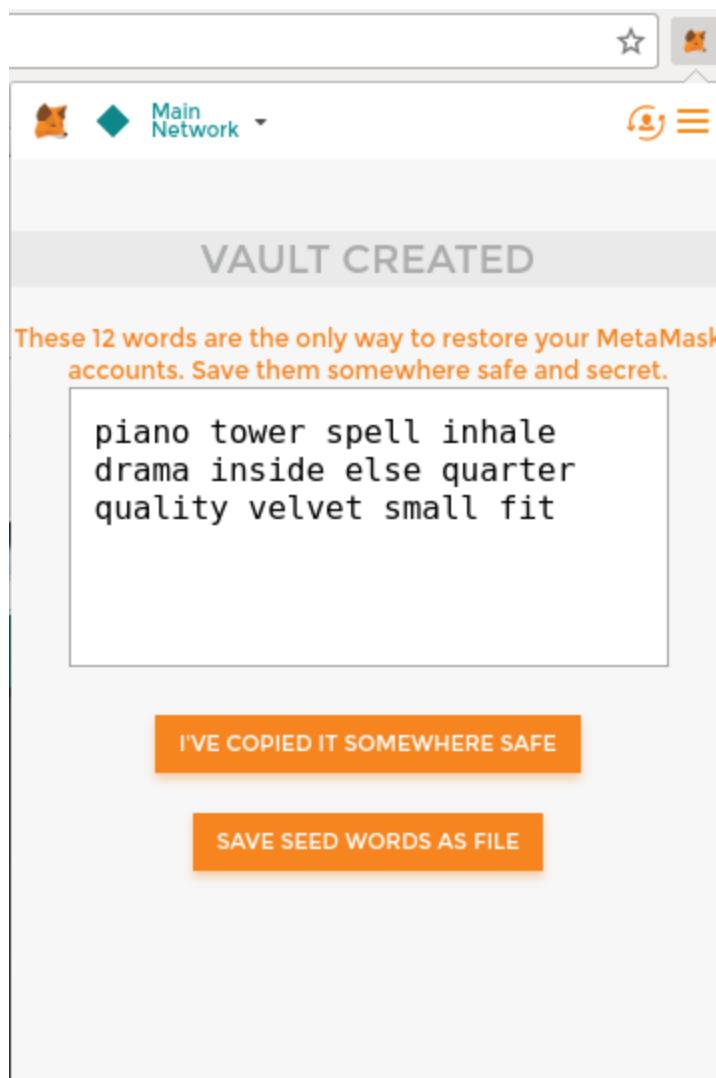


Figure 4. The mnemonic backup of your wallet, created by MetaMask



Backup your mnemonic (12 words) on paper, twice. Store the two paper backups in two separate secure locations, such as a fire resistant safe, a locked drawer or a safe deposit box. Treat the paper backups like cash of equivalent value to what you store in your Ethereum wallet. Anyone with access to these words can gain access and steal your money.

Once you have confirmed that you have stored the mnemonic securely, you'll be able to see the details of your Ethereum account as shown in [Your Ethereum account in MetaMask](#):

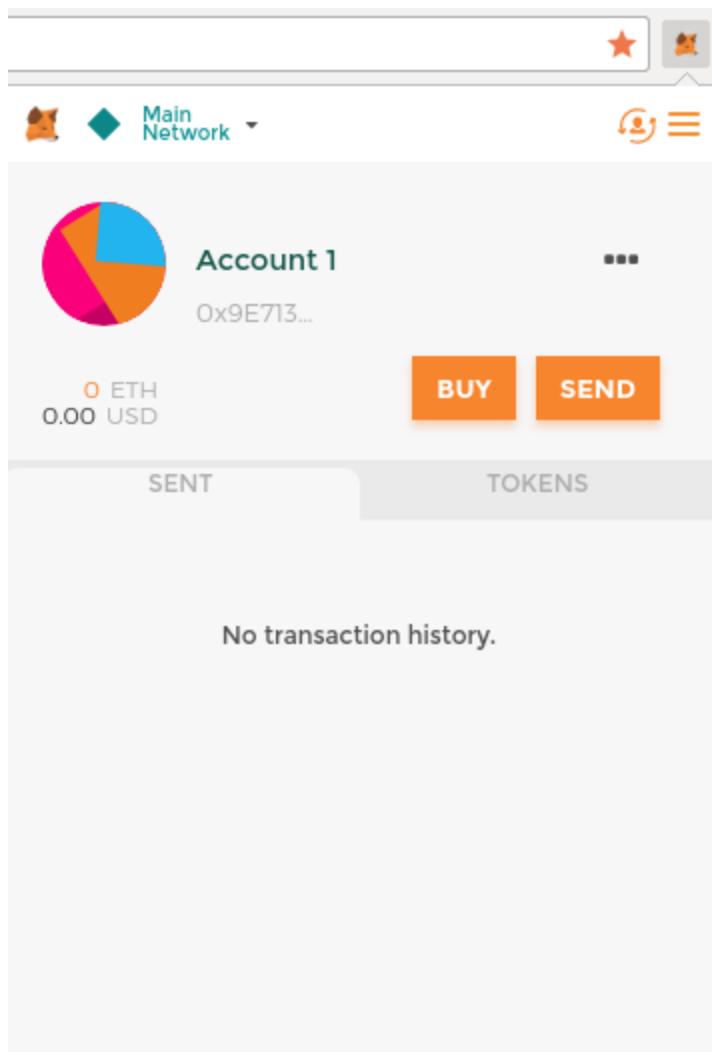


Figure 5. Your Ethereum account in MetaMask

Your account page shows the name of your account ("Account 1" by default), an Ethereum address (0x9E713… in the example) and a colorful icon to help you visually distinguish this account from other accounts. At the top of the account page, you can see which Ethereum network you are currently working on ("Main Network" in the example).

Congratulations! You have set up your first Ethereum wallet.

Switching networks

As you can see on the MetaMask account page, you can choose between multiple Ethereum networks. By default, MetaMask will try to connect to the "Main Network". The other choices are public testnets, any Ethereum node of your choice, or nodes running private blockchains on your own computer (localhost):

Main Ethereum Network

The main public Ethereum blockchain. Real ETH, real value and real consequences.

Ropsten Test Network

Ethereum public test blockchain and network. ETH on this network has no value.

Kovan Test Network

Ethereum public test blockchain and network, using the "Aura" consensus protocol with "Proof-of-Authority" (federated signing). ETH on this network has no value. This test network is supported by "Parity" only. Other Ethereum clients use the "Clique" consensus protocol, which was proposed later, for Proof-of-Authority based verification.

Rinkeby Test Network

Ethereum public test blockchain and network, using the "Clique" consensus protocol with Proof-of-Authority (federated signing). ETH on this network has no value.

Localhost 8545

Connect to a node running on the same computer as the browser. The node can be part of any public blockchain (main or testnet), or a private testnet.

Custom RPC

Allows you to connect MetaMask to any node with a Geth-compatible Remote Procedure Call (RPC) interface. The node can be part of any public or private blockchain.



Your MetaMask wallet uses the same private key and Ethereum address on all the networks it connects to. However, your Ethereum address balance on each Ethereum network will be different. Your keys may control ether and contracts on Ropsten, for example, but not on the Main Network.

Getting some test ether

Our first task is to get our wallet funded. We won't be doing that on the Main Network because real ether costs money and handling it requires a bit more experience. For now, we will load our wallet with some testnet ether.

Switch MetaMask to the *Ropsten Test Network*. Then click "Buy", and click "Ropsten Test Faucet". MetaMask will open a new web page, see [MetaMask Ropsten Test Faucet](https://faucet.metamask.io):

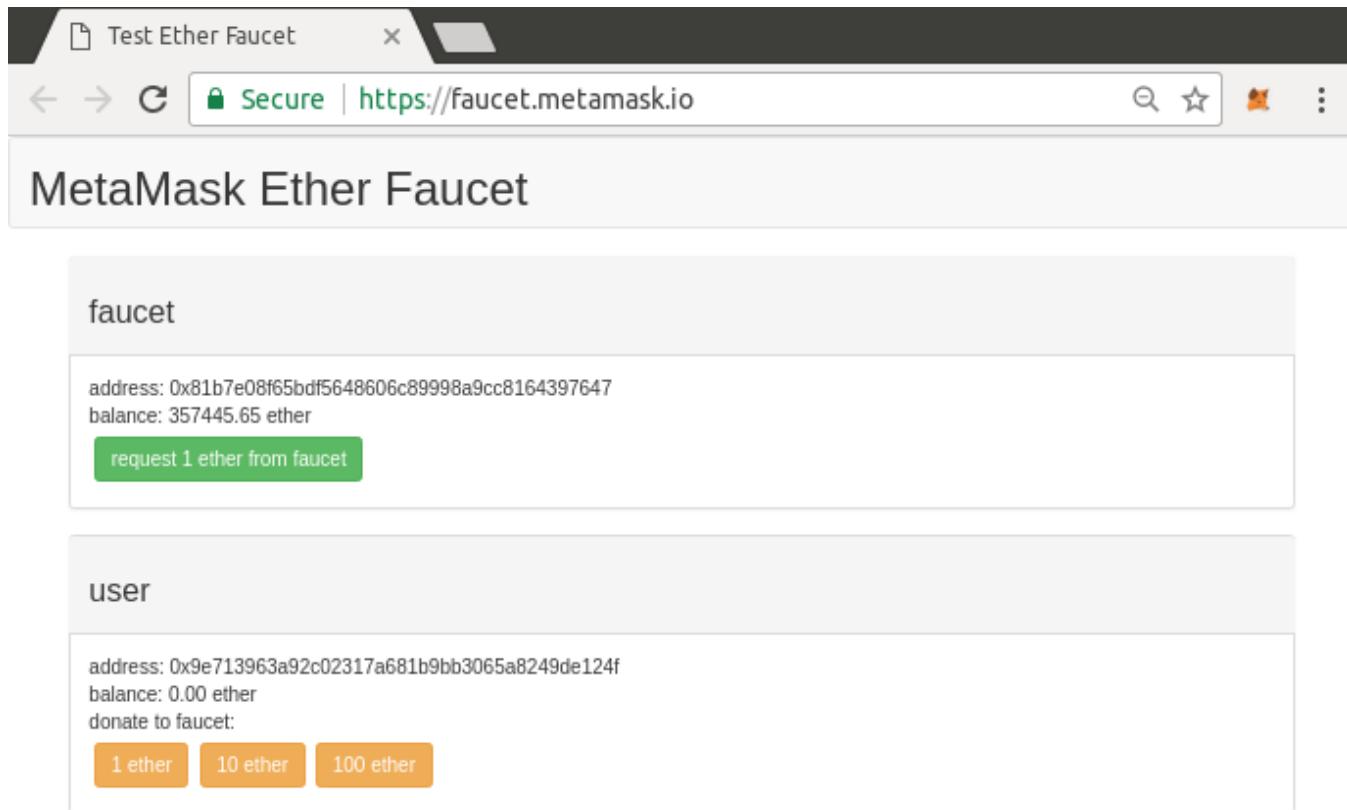


Figure 6. MetaMask Ropsten Test Faucet

You may notice that the web page already contains your MetaMask wallet's Ethereum address. MetaMask integrates Ethereum enabled web pages with your MetaMask wallet. MetaMask can "see" Ethereum addresses on the web page, allowing you, for example, to send a payment to an online shop displaying an Ethereum address. MetaMask can also populate the web page with your own wallet's address as a recipient address if the web page requests it. In this page, the faucet application is asking MetaMask for a wallet address to send test ether to.

Press the green "request 1 ether from faucet" button. You will see a transaction ID appear in the lower part of the page. The faucet app has created a transaction - a payment to you. The transaction ID looks like this:

0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fbc6f9590109e099568090c57

In a few seconds, the new transaction will be mined by the Ropsten miners and your MetaMask wallet will show a balance of 1 ETH. Click on the transaction ID and your browser will take you to a *block explorer*, which is a website that allows you to visualize and explore blocks, addresses, and transactions. MetaMask uses the etherscan.io block explorer, one of the more popular Ethereum block explorers. The transaction containing our payment from the Ropsten Test Faucet is shown in [Etherscan Ropsten Block Explorer](#):

The screenshot shows a web browser window with two tabs: "Test Ether Faucet" and "Ethereum Transaction". The "Ethereum Transaction" tab is active, displaying a secure connection to <https://ropsten.etherscan.io/tx/0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fbc6f9590109e099568090c57>. The page header includes the Etherscan logo, "ROPSTEN (Revival) TESTNET", and navigation links for HOME, BLOCKCHAIN, ACCOUNT, TOKEN, CHART, and MISC. The main content area shows a "Transaction" section with the TxHash: 0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fbc6f9590109e099568090c57. Below it, the TxReceipt Status: is listed as Success. Other transaction details include Block Height: 2546420, TimeStamp: 1 min ago (Jan-29-2018 05:19:35 PM +UTC), From: 0x81b7e08f65bdf5648606c89998a9cc8164397647, To: 0x9e713963a92c02317a681b9bb3065a8249de124f, and Value: 1 Ether (\$0.00). A "Tools & Utilities" dropdown menu is visible on the right.

Figure 7. Etherscan Ropsten Block Explorer

The transaction has been recorded on the Ropsten blockchain and can be viewed at any time by anyone, simply by searching for the transaction ID, or visiting the link:

<https://ropsten.etherscan.io/tx/>

[0x7c7ad5aaea6474adccf6f5c5d6abed11b70a350fbc6f9590109e099568090c57](#)

Try visiting that link, or entering the transaction hash into the [ropsten.etherscan.io](#) website, to see it for yourself.

Sending ether from MetaMask

Once we've received our first test ether from the Ropsten Test Faucet, we will experiment with sending ether, by trying to send some back to the faucet. As you can see on the Ropsten Test Faucet page, there is an option to "donate" 1 ETH to the faucet. This option is available so that once you're done testing, you can return the remainder of your test ether, so that someone else can use it next. Even though test ether has no value, some people hoard it, making it difficult for everyone else to use the test networks. Hoarding test ether is frowned upon!

Fortunately, we are not test ether hoarders.

Click on the orange "1 ether" button to tell MetaMask to create a transaction paying the faucet 1 ether. MetaMask will prepare a transaction and pop-up a window with the confirmation as shown in [Sending 1 ether to the faucet](#):

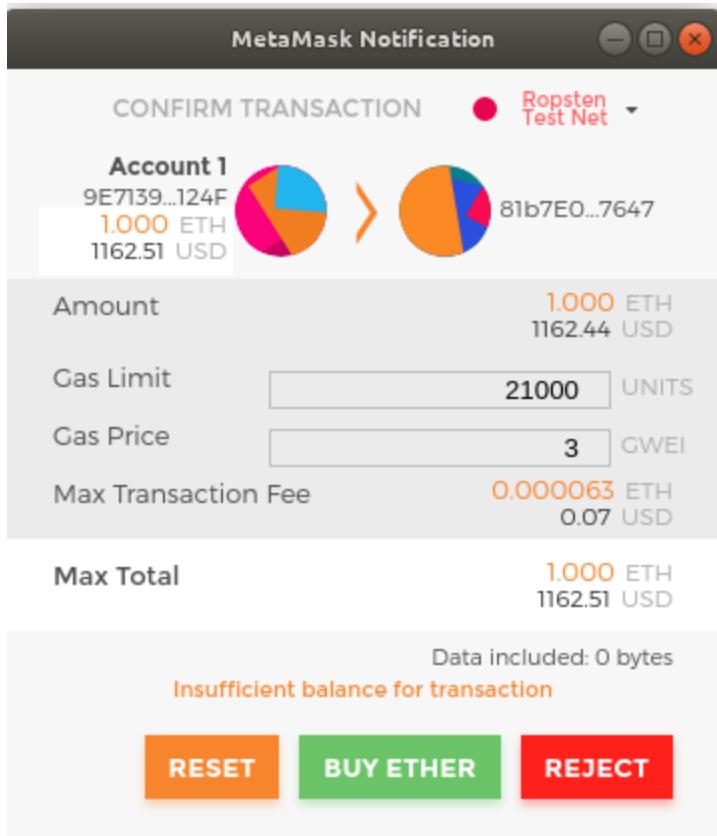


Figure 8. Sending 1 ether to the faucet

Oops! You probably noticed you can't complete the transaction. MetaMask says "Insufficient balance for transaction". At first glance this may seem confusing: we have 1 ETH, we want to send 1 ETH, why is MetaMask saying we have insufficient funds?

The answer is because of the cost of *gas*. Every Ethereum transaction requires payment of a fee, which is collected by the miners to validate the transaction. The fees in Ethereum are charged in a virtual currency called *gas*. You pay for the gas with ether, as part of the transaction.



Fees are required on the test networks too. Without fees, a test network would behave differently from the main network, making it an inadequate testing platform. Fees also protect the test networks from denial of service attacks and poorly constructed contracts (e.g. infinite loops), much like they protect the main network.

When you sent the transaction, MetaMask calculated the average gas price of recent successful

transactions at 3 Gwei, which stands for 3 gigawei. Wei is the smallest subdivision of the ether currency, as we discussed in [Ether currency units](#). The gas cost of sending a basic transaction is 21000 gas units. Therefore, the maximum amount of ETH you spend is $3 * 21000 \text{ Gwei} = 63000 \text{ Gwei} = 0.000063 \text{ ETH}$. Be advised that average gas prices can fluctuate as they are predominantly determined by miners. We will see in a later chapter how you can increase/decrease your gas limit to ensure your transaction takes precedence if need be.

All this to say: to make a 1 ETH transaction costs 1.000063 ETH. MetaMask confusingly rounds that *down* to 1 ETH when showing the total, but the actual amount you need is 1.000063 ETH and you only have 1 ETH. Click "Reject" to cancel this transaction.

Let's get some more test ether! Click on the green "request 1 ether from the faucet" button again and wait a few seconds. Don't worry, the faucet should have plenty of ether and will give you more if you ask.

Once you have a balance of 2 ETH, you can try again. This time, when you click on the orange "1 ether" donation button, you have sufficient balance to complete the transaction. Click "Submit" when MetaMask pops-up the payment window. After all of this, you should see a balance of 0.999937 ETH because you sent 1 ETH to the faucet with 0.000063 ETH in gas.

Exploring the transaction history of an address

By now you have become an expert in using MetaMask to send and receive test ether. Your wallet has received at least two payments and sent at least one. Let's see all these transactions, using the [ropsten.etherscan.io](#) block explorer. You can either copy your wallet address and paste it into the block explorer's search box, or you can have MetaMask open the page for you. Next to your account icon in MetaMask, you will see a button showing three dots. Click on it to show a menu of account-related options, see [MetaMask Account Context Menu](#):

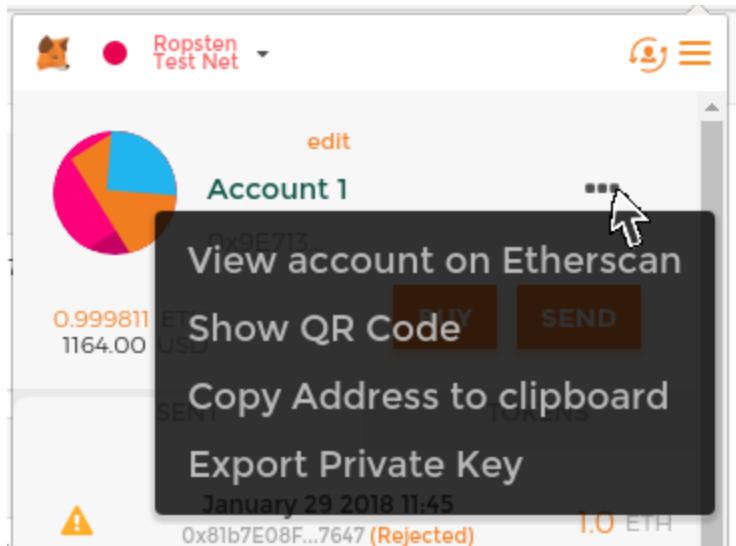


Figure 9. MetaMask Account Context Menu

Select "View Account on Etherscan", to open a web page in the block explorer, showing your account's transaction history as shown in [Address Transaction History on Etherscan](#):

The screenshot shows the Etherscan interface for the Ropsten (Revival) TESTNET. The address 0x9e713963a92c02317A681b9bB3065a8249DE124F is selected. The transaction history section shows the following data:

TxHash	Block	Age	From	To	Value	TxFee	
0x75cd8cea2ec1...	2546517	46 mins ago	0x9e713963a...	OUT	0x81b7e08f65bdf...	1 Ether	0.000063
0x456eb2b66d34...	2546517	46 mins ago	0x9e713963a...	OUT	0x81b7e08f65bdf...	1 Ether	0.000063
0xfc64cb77479f2...	2546487	54 mins ago	0x9e713963a...	OUT	0x81b7e08f65bdf...	1 Ether	0.000063
0xb4c3e7d81130...	2546485	55 mins ago	0x81b7e08f65bdf...	IN	0x9e713963a...	1 Ether	0.00042
0x9597055fe0ad...	2546485	55 mins ago	0x81b7e08f65bdf...	IN	0x9e713963a...	1 Ether	0.00042
0xe21934fb1834...	2546484	55 mins ago	0x81b7e08f65bdf...	IN	0x9e713963a...	1 Ether	0.00042
0x7c7ad5aaea64...	2546420	1 hr 10 mins ago	0x81b7e08f65bdf...	IN	0x9e713963a...	1 Ether	0.00042

Figure 10. Address Transaction History on Etherscan

Here you can see the entire transaction history of your Ethereum address. It shows all the transactions recorded on the Ropsten blockchain where your address is the sender or recipient. Click on a few of these transactions to see more details.

You can explore the transaction history of any address. See if you can explore the transaction history of the Ropsten Test Faucet address (Hint: it is the "sender" address listed in the oldest payment to your address). You can see all the test ether sent from the faucet to you and to other addresses. Every transaction you see can lead you to more addresses and more transactions. Before long you will be lost in the maze of interconnected data. Public blockchains contain an enormous wealth of information, all

of which can be explored programmatically, as we will see in future examples.

Introducing the world computer

We've created a wallet and we've sent and received ether. So far, we've treated Ethereum as a cryptocurrency. But Ethereum is much, much more. In fact, the cryptocurrency function is subservient to Ethereum's function as a world computer, a decentralized smart contract platform. Ether is meant to be used to pay for running *smart contracts*, which are computer programs that run on an emulated computer called the *Ethereum Virtual Machine (EVM)*.

The EVM is a global singleton, meaning that it operates as if it was a global, single-instance computer, running everywhere. Each node on the Ethereum network runs a local copy of the EVM to validate contract execution, while the Ethereum blockchain records the changing *state* of this world computer as it processes transactions and smart contracts. We'll discuss this in much greater detail in [The Ethereum Virtual Machine](#).

Externally Owned Accounts (EOAs) and contracts

The type of account we created in the MetaMask wallet is called an *Externally Owned Account (EOA)*. Externally owned accounts are those that have a private key; having the private key means control over access to funds or contracts. Now, you're probably guessing there is another type of account. The other type of account is a *contract* account. A contract account has smart contract code, which a simple EOA can't have. Furthermore, a contract account does not have a private key. Instead, it is owned (and controlled) by the logic of its smart contract code: the software program recorded on the Ethereum blockchain at the contract account's creation and executed by the EVM.

Contracts have an address, just like EOAs. Contracts can send and receive ether, just like EOAs. However, when a transaction destination is a contract address, it causes that contract to *run* in the EVM, using the transaction, and the transaction's data, as its input. In addition to ether, transactions can contain *data* indicating which specific function in the contract to run and what parameters to pass to that function. In this way, transactions can *call* functions within contracts.

Note that because a contract account does not have a private key, it can not *initiate* a transaction. Only EOAs can initiate transactions, but contracts can react to transactions by calling other contracts, building complex execution paths. One typical use of this is an EOA sending a request transaction to a multi-signature smart contract wallet to send some ETH on to another address. A typical DApp programming pattern is to have Contract A calling Contract B in order to maintain a shared state across users of Contract A.

In the next few sections, we will write our first contract. We will then create, fund, and use that contract with our MetaMask wallet and test ether on the Ropsten test network.

A simple contract: a test ether faucet

Ethereum has many different high-level languages, all of which can be used to write a contract and produce EVM bytecode. You can read about many of the most prominent and interesting ones in [Introduction to Ethereum high-level languages](#). One high-level language is by far the dominant language for smart contract programming: Solidity. Solidity was created by Gavin Wood, the co-author of this book, and has become the most widely used language in Ethereum and beyond. We'll use Solidity to write our first contract.

For our first example, we will write a contract that controls a *faucet*. We've already used a faucet to get test ether on the Ropsten test network. A faucet is a relatively simple thing: it gives out ether to any address that asks, and can be refilled periodically. You can implement a faucet as a wallet controlled by a human or a web server. Today, we will write [Faucet.sol : A Solidity contract implementing a faucet](#):

Faucet.sol : A Solidity contract implementing a faucet

```
// Our first contract is a faucet!
contract Faucet {

    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {

        // Limit withdrawal amount
        require(withdraw_amount <= 1000000000000000);

        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }

    // Accept any incoming amount
    function () public payable {}

}
```

Download Faucet.sol from the book's repository: <https://github.com/ethereumbook/ethereumbook/>

You will find all the code samples for this book in the code subdirectory. Specifically, our Faucet.sol contract is in:

```
code/Solidity/Faucet.sol
```

This is a very simple contract, about as simple as we can make it. It is also a *flawed* contract, demonstrating a number of bad practices and security vulnerabilities. We will learn by examining all of its flaws in later sections. But for now, let's look at what this contract does and how it works, line by line. You will quickly notice that many elements of Solidity are similar to existing programming languages, such as JavaScript, Java or C++.

The first line is a comment:

```
// Our first contract is a faucet!
```

Comments are for humans to read and are not included in the executable EVM bytecode. We usually put them on the line before the code we are trying to explain, or sometimes on the same line. Comments start with two forward slashes //. Everything from the first slash until the end of that line is treated the same as a blank line and ignored.

The next line is where our *actual* contract starts:

```
contract Faucet {
```

This line declares a contract object, similar to a class declaration in other object-oriented languages. The contract definition includes all the lines between the curly braces {} which define a *scope*, much like how curly braces are used in many other programming languages.

Next, we declare the first function of the Faucet contract:

```
function withdraw(uint withdraw_amount) public {
```

The function is named withdraw, which takes one unsigned integer (uint) argument named withdraw_amount. It is declared as a public function, meaning it can be called by other contracts. The

function definition follows between curly braces:

```
require(withdraw_amount <= 1000000000000000000000000);
```

The first part of the withdraw function sets a limit on withdrawals. It uses the built-in Solidity function require to test a precondition, that the withdraw_amount is less than or equal to 1000000000000000000000000 wei, which is the base unit of ether (see [Ether Denominations and Unit Names](#)) and equivalent to 0.1 ether. If the withdraw function is called with a withdraw_amount greater than that amount, the require function here will cause contract execution to stop and fail with an *exception*. Note that statements need to be terminated with a semi-colon in Solidity.

This part of the contract is the main logic of our faucet. It controls the flow of funds out of the contract by placing a limit on withdrawals. It's a very simple control but can give you a glimpse of the power of a programmable blockchain: decentralized software controlling money.

Next comes the actual withdrawal:

```
msg.sender.transfer(withdraw_amount);
```

A couple of interesting things are happening here. The msg object is one of the inputs that all contracts can access. It represents the transaction that triggered the execution of this contract. The attribute sender is the sender address of the transaction. The function transfer is a built-in function that transfers ether from the current contract to the address of the sender. Reading it backward, this means transfer to the sender of the msg that triggered this contract execution. The transfer function takes an amount as its only argument. We pass the withdraw_amount value that was the parameter to the withdraw function declared a few lines above.

The very next line is the closing curly brace, indicating the end of the definition of our withdraw function.

Below we declare one more function:

```
function () public payable {}
```

This function is a so-called "*fallback*" or *default* function, which is called if the transaction that

triggered the contract didn't name any of the declared functions in the contract, or any function at all, or didn't contain data. Contracts can have one such default function (without a name) and it is usually the one that receives ether. That's why it is defined as a public and payable function, which means it can accept ether into the contract. It doesn't do anything, other than accept the ether, as indicated by the empty definition in the curly brackets {}. If we make a transaction that sends ether to the contract address, as if it were a wallet, this function will handle it.

Right below our default function is the final closing curly bracket, which closes the definition of the contract Faucet. That's it!

Compiling the faucet contract

Now that we have our first example contract, we need to use a Solidity compiler to convert the Solidity code into EVM bytecode, so it can be executed by the EVM on the blockchain itself.

The Solidity compiler comes as a) a standalone executable, b) as part of various frameworks, and c) bundled in *Integrated Development Environments (IDEs)*. To keep things simple, we will use one of the more popular IDEs, called Remix.

Use your Chrome browser (with the MetaMask wallet we installed earlier) to navigate to the Remix IDE at:

<https://remix.ethereum.org/>

When you first load Remix, it will start with a sample contract called ballot.sol. We don't need that, so let's close it, clicking on the x on the corner of the tab, as seen in [Close the default example tab](#):

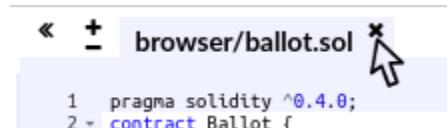


Figure 11. Close the default example tab

Now, add a new tab by clicking on the circular-plus-sign in the left toolbar, naming the new file Faucet.sol, as seen in [Click the plus sign to open a new tab](#)



Figure 12. Click the plus sign to open a new tab

Once you have a new tab open, copy and paste the code from our example Faucet.sol, as seen in [Copy the Faucet example code into the new tab](#):

```
// Version of Solidity compiler this program was written for
pragma solidity ^0.4.19;
// Our first contract is a faucet!
contract Faucet {
    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {
```

Figure 13. Copy the Faucet example code into the new tab

Now we have loaded the Faucet.sol contract into the Remix IDE, the IDE will automatically compile the code. If all goes well, you will see a green box with "Faucet" in it appear on the right, under the Compile tab, confirming the successful compilation, as you'll see in [Remix successfully compiles the Faucet.sol contract](#)

Compile Run Settings Analysis Debugger Support

Start to compile Auto compile ⚠

Faucet ▾ Details Publish on Swarm

Faucet ✕

Figure 14. Remix successfully compiles the Faucet.sol contract

If something goes wrong, the most likely problem is that Remix IDE is using a version of the Solidity compiler that is different from 0.4.19. In that case, our pragma directive will prevent Faucet.sol from

compiling. To change the compiler version, go to the "Settings" tab, set the compiler version to 0.4.19, and try again.

The Solidity compiler has now compiled our Faucet.sol into EVM bytecode. If you are curious, the bytecode looks like this:

```
PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE ISZERO PUSH2 0xF JUMPI PUSH1 0x0
DUP1 REVERT JUMPDEST PUSH1 0xE5 DUP1 PUSH2 0x1D PUSH1 0x0 CODECOPY PUSH1
0x0 RETURN STOP PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT
PUSH1 0x3F JUMPI PUSH1 0x0 CALLDATALOAD PUSH29
0x1000000000000000000000000000000000000000000000000000000000000000 SWAP1 DIV
PUSH4 0xFFFFFFFF AND DUP1 PUSH4 0x2E1A7D4D EQ PUSH1 0x41 JUMPI JUMPDEST
STOP JUMPDEST CALLVALUE ISZERO PUSH1 0x4B JUMPI PUSH1 0x0 DUP1 REVERT
JUMPDEST PUSH1 0x5F PUSH1 0x4 DUP1 DUP1 CALLDATALOAD SWAP1 PUSH1 0x20 ADD
SWAP1 SWAP2 SWAP1 POP POP PUSH1 0x61 JUMP JUMPDEST STOP JUMPDEST PUSH8
0x16345785D8A0000 DUP2 GT ISZERO ISZERO PUSH1 0x77 JUMPI PUSH1 0x0
DUP1 REVERT JUMPDEST CALLER PUSH20
0xFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH2 0x8FC DUP3 SWAP1
DUP2 ISZERO MUL SWAP1 PUSH1 0x40 MLOAD PUSH1 0x0 PUSH1 0x40 MLOAD DUP1
DUP4 SUB DUP2 DUP6 DUP9 DUP9 CALL SWAP4 POP POP POP POP ISZERO ISZERO
PUSH1 0xB6 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP JUMP STOP LOG1 PUSH6
0x627A7A723058 KECCAK256 PUSH9 0x13D1EA839A4438EF75 GASLIMIT CALLVALUE
LOG4 0x5f PUSH24 0x7541F409787592C988A079407FB28B4AD0002900000000000
```

Aren't you glad you are using a high-level language like Solidity instead of programming directly in EVM bytecode? Me too!

Creating the contract on the blockchain

So we have a contract. We've compiled it into bytecode. Now, we need to "register" the contract on the Ethereum blockchain. We will be using the Ropsten testnet to test our contract, so that's the blockchain we want to submit it to.

Registering a contract on the blockchain involves creating a special transaction whose destination is the address 0x00000000000000000000000000000000, also known as the *zero address*. The zero address is a special address that tells the Ethereum blockchain that you want to register a contract. Fortunately, Remix IDE will handle all of that for you and send the transaction to MetaMask.

First, switch to the "Run" tab and select "Injected Web3" in the "Environment" drop-down selection box. This connects Remix IDE to the MetaMask wallet, and through MetaMask to the Ropsten Test Network. Once you do that, you can see "Ropsten" under Environment. Also, in the Account selection box it shows the address of your wallet, see [Remix IDE "Run" tab, with "Injected Web3" environment selected](#)

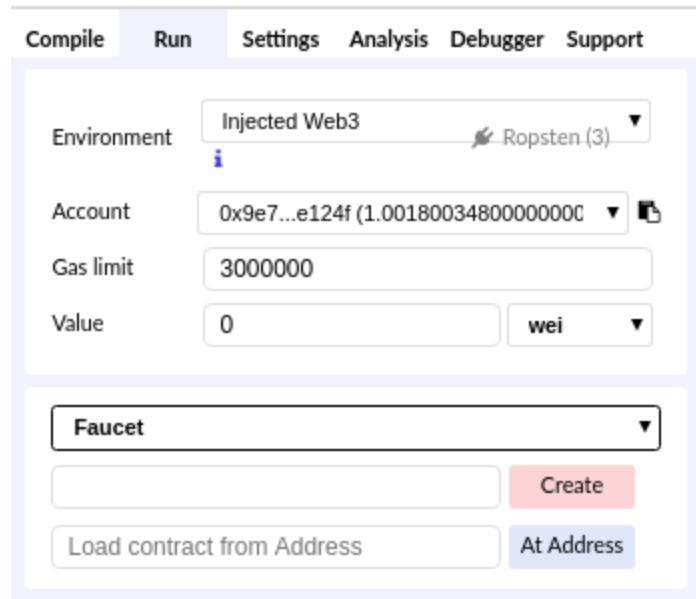


Figure 15. Remix IDE "Run" tab, with "Injected Web3" environment selected

Right below the "Run" settings we just confirmed, is the Faucet contract, ready to be created. Click on the "Deploy" button shown in [Click the Deploy button in the Run tab](#):

Environment

Injected Web3

Ropsten (3)



Account

0x2fd...18cc9 (0.999979 ether)



Gas limit

3000000

Value

0

wei



Faucet

Deploy

Load contract from Address

At Address

Figure 16. Click the Deploy button in the Run tab

Remix will construct the special "creation" transaction and MetaMask will ask you to approve it. As shown in [MetaMask showing the contract creation transaction](#). You'll notice the contract creation transaction has no ether in it, but it has 258 bytes (the compiled contract) and will consume 10 Gwei in gas. Click "Submit" to approve it:

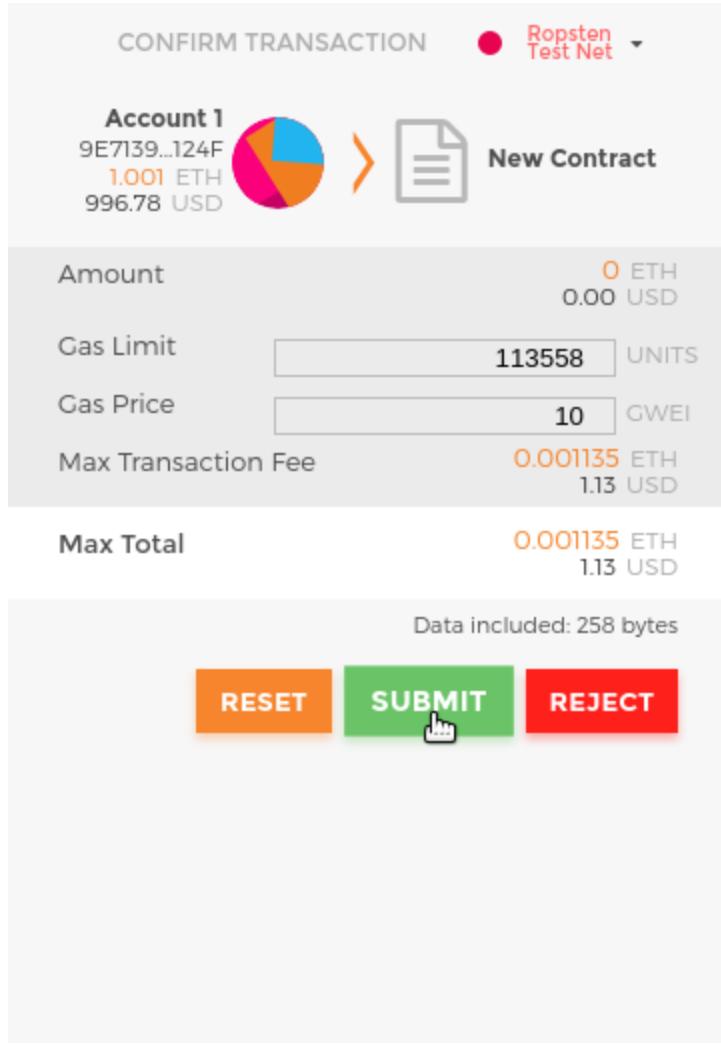


Figure 17. MetaMask showing the contract creation transaction

Now you have to wait. It will take about 15 to 30 seconds for the contract to be mined on Ropsten. Remix won't appear to be doing much, but be patient.

Once the contract is created, it appears at the bottom of the Run tab:



Figure 18. The Faucet contract is ALIVE!

Notice that the Faucet contract, as shown in [The Faucet contract is ALIVE!](#), now has an address of its own: Remix shows it as Faucet at 0x72e....c7829 (although your address, the random letters and numbers, will be different). The small clipboard symbol to the right allows you to copy the contract address into your clipboard. We will use that in the next section.

Interacting with the contract

Let's recap what we've learned so far: Ethereum contracts are programs that control money, which run inside a virtual machine called the EVM. They are created by a special transaction that submits their bytecode to be recorded on the blockchain. Once they are created on the blockchain, they have an Ethereum address, just like wallets. Anytime someone sends a transaction to a contract address it causes the contract to run in the EVM, with the transaction as its input. Transactions sent to contract addresses may have ether or data or both. If they contain ether, it is "deposited" to the contract balance. If they contain data, the data can specify a named function in the contract and call it, passing arguments to the function.

Viewing the contract address in a block explorer

Now, we have a contract recorded on the blockchain and we can see it has an Ethereum address. Let's check it out on the [ropsten.etherscan.io](#) block explorer and see what a contract looks like. Copy the address of the contract by clicking on the clipboard icon next to its name (see [Copy the contract address from Remix](#)):



Figure 19. Copy the contract address from Remix

Keep Remix open; we'll come back to it again later. Now, navigate your browser to ropsten.etherscan.io and paste the address into the search box, as shown in [View the Faucet contract address in the etherscan block explorer](#). You should see the contract's Ethereum address history:

A screenshot of the Etherscan block explorer interface. At the top, there's a logo for "ROPSTEN Etherscan" and a search bar with the placeholder "Search by Address / Txhash / BlockNo" and a "GO" button. Below the search bar are navigation tabs: HOME, BLOCKCHAIN, ACCOUNT (which is selected), TOKEN, CHART, and MISC. The main content area shows the "Contract Address" as 0x72E9D27f206fD62eaC5B81129aa3e774015c7829. Below this, there are two sections: "Contract Overview" and "Misc". The "Contract Overview" section shows "ETH Balance: 0 Ether" and "No Of Transactions: 1 txn". The "Misc" section shows "Contract Creator: 0x9e713963a92c..." and a link to "0x90333f7ecc9d...". Below these sections are tabs for "Transactions" (which is selected) and "Contract Code". The "Transactions" tab shows a table with one row: "Latest 1 txn". The table columns are TxHash, Block, Age, From, To, Value, and [TxFee]. The data row shows "0x90333f7ecc9d...", "2567995", "16 hrs 48 mins ago", "0x9e713963a92c...", "IN", "Contract Creation", "0 Ether", and "0.00113558". At the bottom right of the page is a link "[Download CSV Export]".

Figure 20. View the Faucet contract address in the etherscan block explorer

Funding the contract

For now, the contract only has one transaction in its history: the contract creation transaction. As you can see, the contract also has no ether (zero balance). That's because we didn't send any ether to the contract in the creation transaction, even though we could have.

Our faucet needs funds! Our first project will be to use MetaMask to send ether to the contract. You should still have the address of the contract in your clipboard (if not, copy it again from Remix). Open MetaMask, and send 1 ether to it, exactly as you would any other Ethereum address (see [Send 1 ether to the contract address](#)):

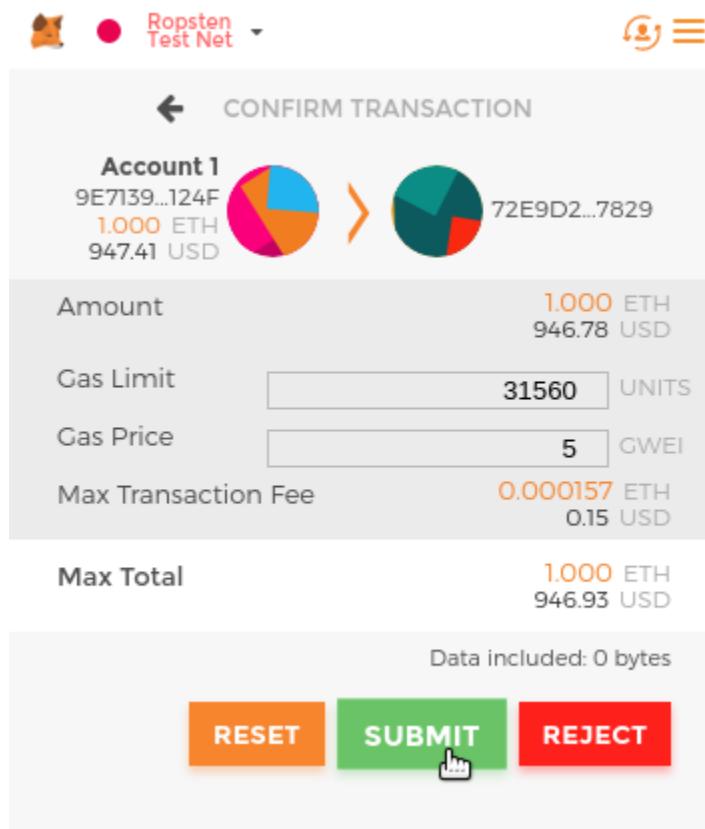


Figure 21. Send 1 ether to the contract address

In a minute, if you reload the etherscan block explorer, it will show another transaction to the contract address and an updated balance of 1 ether.

Remember the unnamed default public payable function in our Faucet.sol code? It looked like this:

```
function () public payable {}
```

When you sent a transaction to the contract address, with no data specifying which function to call, it called this default function. Because we declared it as a payable, it accepted and deposited the 1 ether into the contract account balance. Your transaction caused the contract to run in the EVM, updating its balance. We have funded our faucet!

Withdrawing from our contract

Next, let's withdraw some funds from the faucet. To withdraw, we have to construct a transaction that calls the withdraw function and passes a withdraw_amount argument to it. To keep things simple for now, Remix will construct that transaction for us and MetaMask will present it for our approval.

Return to the Remix tab and look at the contract under the "Run" tab. You should see a red box labeled withdraw with a field entry labeled uint256 withdraw_amount (see [The withdraw function of Faucet.sol, in Remix](#)):



Figure 22. The withdraw function of *Faucet.sol*, in Remix

This is the Remix interface to the contract. It allows us to construct transactions that call the functions defined in the contract. We will enter a withdraw_amount and click the withdraw button to generate the transaction.

First, let's figure out the withdraw_amount. We want to try and withdraw 0.1 ether, which is the maximum amount allowed by our contract. Remember that all currency values in Ethereum are denominated in wei internally, and our withdraw function expects the withdraw_amount to be denominated in wei too. The amount we want is 0.1 ether, which is 1000000000000000000 wei (1 followed by 17 zeros).



Due to a limitation in JavaScript, a number as large as 10^{17} cannot be processed by Remix. Instead, we enclose it in double quotes, to allow Remix to receive it as a string and manipulate it as a BigNumber. If we don't enclose it in quotes, the Remix IDE will fail to process it and display "Error encoding arguments: Error: Assertion failed"

Type "100000000000000000000" (with the quotes) into the withdraw_amount box and click on the withdraw button (see [Click "withdraw" in Remix to create a withdrawal transaction](#)):

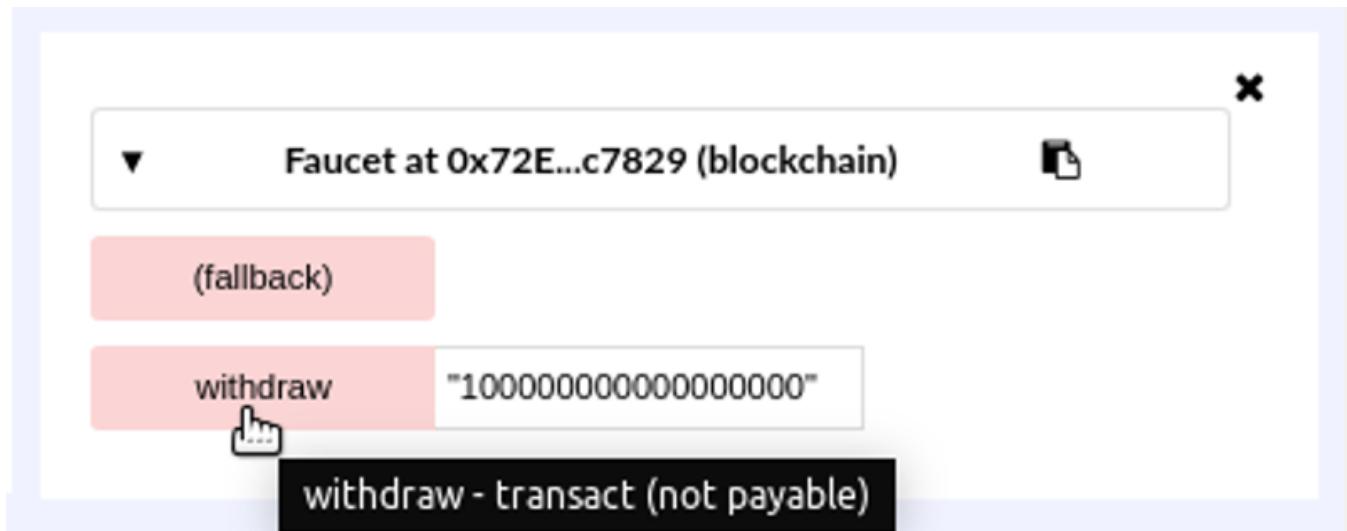


Figure 23. Click "withdraw" in Remix to create a withdrawal transaction

MetaMask will pop-up a transaction window for you to approve. Click "Submit" to send your withdrawal call to the contract (see [MetaMask transaction to call the withdraw function](#)):

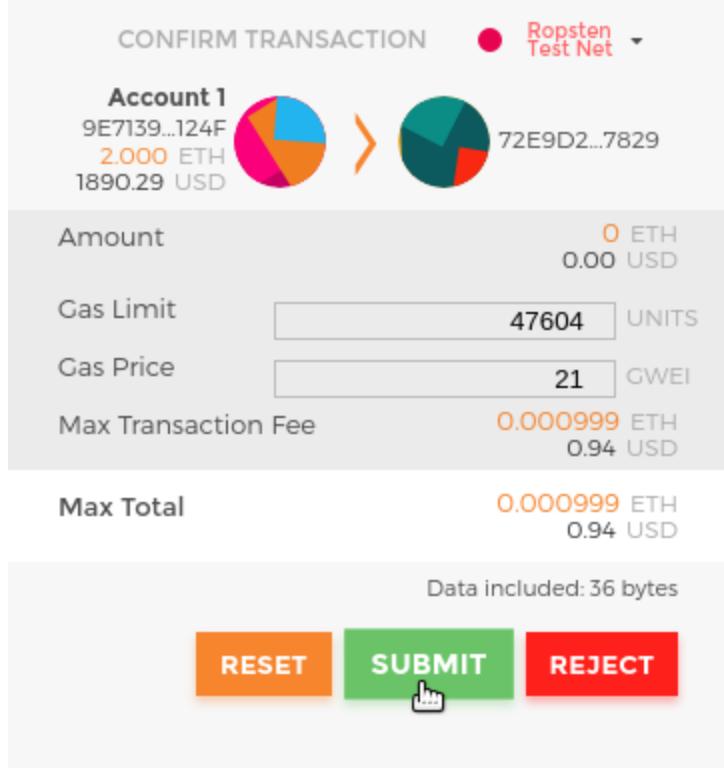


Figure 24. MetaMask transaction to call the withdraw function

Wait a minute and then reload the etherscan block explorer to see the transaction reflected in the Faucet contract address history (see [Etherscan shows the transaction calling the withdraw function](#)):

[Contract Address] [0x72e9d27f206fD62eaC5B81129aa3e774015c7829](#)
[Home](#) / [Contract Accounts](#) / [Address](#)
Contract Overview

Misc

[More Options](#) ▾

ETH Balance: 0.9 Ether

Contract Creator: [0x9e713963a92c...](#) at tx [0x90333f7ecc9d...](#)
No Of Transactions: 3 txns

[Transactions](#)
[Internal Transactions](#)
[Contract Code](#)

Latest 3 txns

TxHash	Block	Age	From	To	Value	[TxFee]
0x3641e33d64dc...	2574307	2 mins ago	0x9e713963a92c...	0x72e9d27f20...	0 Ether	0.000619038
0xebdc3c2ac500...	2574232	18 mins ago	0x9e713963a92c...	0x72e9d27f20...	1 Ether	0.0003156
0x90333f7ecc9d...	2567995	17 hrs 58 mins ago	0x9e713963a92c...	Contract Creation	0 Ether	0.00113558

[\[Download CSV Export\]](#)

Figure 25. Etherscan shows the transaction calling the withdraw function

We now see a new transaction with the contract address as the destination and zero ether. The contract balance has changed and is now 0.9 ether because it sent us 0.1 ether as requested. But we don't see an "OUT" transaction in the contract address history.

Where's the outgoing withdrawal? A new tab has appeared in the contract's address history page, named "Internal Transactions". Because the 0.1 ether transfer originated from the contract code, it is an internal transaction (also called a *message*). Click on the "Internal Transactions" tab shown in [Etherscan shows the internal transaction transferring ether out from the contract](#) to see it:

[Contract Address] 0x72e9d27f206fD62eaC5B81129aa3e774015c7829
[Home](#) / [Contract Accounts](#) / [Address](#)

Contract Overview

ETH Balance:	0.9 Ether
No Of Transactions:	3 txns

Misc

Contract Creator 0x9e713963a92c... at txn 0x90333f7ecc9d...
 More Options ▾

[Transactions](#) | [Internal Transactions](#) | [Contract Code](#)

Internal Transactions as a result of Contract Execution

 Latest 1 Internal Transaction

ParentTxHash	Block	Age	From	To	Value
0x3641e33d64dc...	2574307	2 mins ago	0x72e9d27f20...	→ 0x9e713963a92c...	0.1 Ether

[\[Download CSV Export \]](#)

Figure 26. Etherscan shows the internal transaction transferring ether out from the contract

This "internal transaction" was sent by the contract in this line of code (from the withdraw function in Faucet.sol):

```
msg.sender.transfer(withdraw_amount);
```

To recap: We sent a transaction from our MetaMask wallet that contained data instructions to call the withdraw function with a withdraw_amount argument of 0.1 ether. That transaction caused the contract to run inside the EVM. As the EVM ran the Faucet contract's withdraw function, first it called the require function and validated that our amount was less than or equal to the maximum allowed withdrawal of 0.1 ether. Then it called the transfer function to send us the ether. Running the transfer function generated an internal transaction that deposited 0.1 ether into our wallet address, from the contract's balance. That's the one shown in the "Internal Transactions" tab in etherscan.

Conclusions

In this chapter, we've set up a wallet using MetaMask and we've funded it using a faucet on the Ropsten Test Network. We received ether into our wallet's Ethereum address. Then we sent ether to the faucet's Ethereum address.

Next, we wrote a faucet contract in Solidity. We used the Remix IDE to compile the contract into EVM bytecode. We used Remix to form a transaction and created the faucet contract on the Ropsten blockchain. Once created, the faucet contract had an Ethereum address and we sent it some ether. Finally, we constructed a transaction to call the withdraw function and successfully asked for 0.1 ether. The contract checked our request and sent us 0.1 ether with an internal transaction.

It may not seem like much, but we've just successfully interacted with software that controls money on a decentralized world computer.

We will do a lot more smart contract programming in [Smart contracts and Solidity](#) and learn about best practices and security considerations in [Smart contract security](#).

Ethereum Clients

An Ethereum client is a software application that implements the Ethereum specification and communicates over the peer-to-peer network with other Ethereum clients. Different Ethereum clients *interoperate* if they comply with the reference specification and the standardized communications protocols. While these different clients are implemented by different teams and in different programming languages, they all "speak" the same protocol and follow the same rules. As such, they can all be used to operate and interact with the same Ethereum network.

Ethereum is an *open source* project and the source code for all the major clients are available under open source licenses (e.g. LGPL v3.0), so they are free to download and use for any purpose. Open source means more than simply free to use. It also means that Ethereum is developed by an open community of volunteers and can be modified by anyone. More eyes means more trustworthy code.

Ethereum is defined by a formal specification called the "Yellow Paper" (see [Further references](#)).

This is in contrast to, for example, Bitcoin, which is not defined in any formal way. Where Bitcoin's "specification" is the reference implementation Bitcoin Core, Ethereum's specification is documented in a paper that combines an English and a mathematical (formal) specification. This formal specification, in addition to various Ethereum Improvement Proposals, defines the standard behavior of an Ethereum client. The Yellow Paper is periodically updated as major changes are made to Ethereum.

As a result of Ethereum's clear formal specification, there are a number of independently developed, yet interoperable, software implementations of an Ethereum client. Ethereum has a greater diversity of implementations running on the network than any other blockchain, which is generally regarded as a good thing. Indeed, it has, for example, proven itself to be an excellent way of defending against attacks on the network, because exploitation of a particular client's implementation strategy simply hassles the developers while they patch the exploit, while other clients keep the network running almost unaffected.

Ethereum Networks

There exist a variety of Ethereum-based networks which largely conform to the formal specification defined in the Ethereum "Yellow Paper," but which may or may not interoperate with each other.

Among these Ethereum-based networks are: Ethereum, Ethereum Classic, Ella, Expanse, Ubiq,

Musicoin, and many others. While mostly compatible at the protocol level, these networks often have features or attributes that require maintainers of Ethereum client software to make small changes in order to support each network. Because of this, not every version of Ethereum client software runs every Ethereum-based blockchain.

Currently, there are six main implementations of the Ethereum protocol, written in six different languages:

- Parity, written in Rust
- Geth, written in Go
- cpp-ethereum, written in C++
- pyethereum, written in Python
- Mantis, written in Scala,
- and Harmony, written in Java.

In this section, we will look at the two most common clients, Parity and Geth. We'll learn how to set up a node using each client, and explore some of their command-line and application programming interfaces (APIs).

Should I run a full node?

The health, resilience, and censorship resistance of blockchains depend on having many independently operated and geographically dispersed full nodes. Each full node can help other new nodes obtain the block data to bootstrap their operation, as well as offer the operator an authoritative and independent verification of all transactions and contracts.

However, running a full node will incur a cost in hardware resources and bandwidth. A full node must download more than 80GB of data (as of April 2018; depending on client) and store it on a local hard drive. This data burden increases quite rapidly every day as new transactions and blocks are added. We discuss this topic in greater detail in [Hardware Requirements for a Full Node](#).

A full node running on a live *mainnet* network is not necessary for Ethereum development. You can do almost everything you need to do with a *testnet* node (which connects you to one of the smaller public test blockchains), with a local private blockchain like Ganache, or with a cloud-based Ethereum client offered by a service provider like Infura.

You also have the option of running a remote client, which does not store a local copy of the blockchain or validate blocks and transactions. These clients offer the functionality of a wallet and can create and broadcast transactions. Remote clients can be used to connect to existing networks, such as your own full node, a public blockchain, a public or permissioned (Proof-of-Authority) testnet, or a private local blockchain. In practice, you will likely use a remote client such as MetaMask, Emerald Wallet, MyEtherWallet or MyCrypto as a convenient way to switch between all of the different node options.

The terms "remote client" and "wallet" are used interchangeably, though there are some differences. Usually, a remote client offers an API (such as the web3.js API) in addition to the transaction functionality of a wallet.

Do not confuse the concept of a remote wallet in Ethereum with that of a *light client* (which is analogous to a Simplified Payment Verification client in Bitcoin). Light clients validate block headers and use Merkle proofs to validate the inclusion of transactions in the blockchain and determine their effects, giving them a similar level of security to a full node. Conversely, Ethereum remote clients do not validate block headers or transactions. They entirely trust a full client to give them access to the blockchain, and hence lose significant security and anonymity guarantees. You can mitigate these problems by using a full client you run yourself.

Full Node Advantages and Disadvantages

Choosing to run a full node helps with the operation of the networks you connect it to, but also incurs some mild to moderate costs for you. Let's look at some of the advantages and disadvantages.

Advantages:

- Supports the resilience and censorship resistance of Ethereum-based networks.
- Authoritatively validates all transactions.
- Can interact with any contract on the public blockchain without an intermediary.
- Can directly deploy contracts into the public blockchain without an intermediary.
- Can query (read-only) the blockchain status (accounts, contracts, etc.) offline.
- Can query the blockchain without letting a third party know the information you're reading.

Disadvantages:

- Requires significant and growing hardware and bandwidth resources.

- May require several days to fully sync when first started.
- Must be maintained, upgraded and kept online to remain synced.

Public Testnet Advantages and Disadvantages

Whether or not you choose to run a full node, you will probably want to run a public testnet node. Let's look at some of the advantages and disadvantages of using a public testnet.

Advantages:

- A testnet node needs to sync and store much less data, ~10GB depending on the network (as of April 2018).
- A testnet node can sync fully in a few hours.
- Deploying contracts or making transactions requires test ether, which has no value and can be acquired for free from several "faucets".
- Testnets are public blockchains with many other users and contracts, running "live".

Disadvantages:

- You can't use "real" money on a testnet; it runs on test ether. Consequently, you can't test security against real adversaries, as there is nothing at stake.
- There are some aspects of a public blockchain that you cannot test realistically on testnet. For example, transaction fees, although necessary to send transactions, are not a consideration on testnet, since gas is free. Further, the testnets do not experience network congestion like the public mainnet sometimes does.

Local Blockchain Simulation Advantages and Disadvantages

For many testing purposes, the best option is to launch a single-instance private blockchain. Ganache (formerly named testrpc) is one of the most popular local blockchain simulations that you can interact with, without any other participants. It shares many of the advantages and disadvantages of the public testnet, but also has some differences.

Advantages:

- No syncing and almost no data on disk. You mine the first block yourself.

- No need to obtain test ether: you "award" yourself mining rewards that you can use for testing.
- No other users, just you.
- No other contracts, just the ones you deploy after you launch it.

Disadvantages:

- Having no other users means that it doesn't behave the same as a public blockchain. There's no competition for transaction space or sequencing of transactions.
- No miners other than you means that mining is more predictable, therefore you can't test some scenarios that occur on a public blockchain.
- Having no other contracts means you have to deploy everything that you want to test, including dependencies and contract libraries.
- You can't recreate some of the public contracts and their addresses to test some scenarios (e.g. the DAO contract).

Running an Ethereum client

If you have the time and resources, you should attempt to run a full node, even if only to learn more about the process. In the next few sections we will download, compile, and run the Ethereum clients Parity and Geth. This requires some familiarity with using the command-line interface on your operating system. It's worth installing these clients, whether you choose to run them as full nodes, as testnet nodes, or as clients to a local private blockchain.

Hardware Requirements for a Full Node

Before we get started, you should ensure you have a computer with sufficient resources to run an Ethereum full node. You will need at least 80GB of disk space to store a full copy of the Ethereum blockchain. If you also want to run a full node on the Ethereum testnet, you will need at least an additional 15GB. Downloading 80GB of blockchain data can take a long time, so it's recommended that you work on a fast Internet connection.

Syncing the Ethereum blockchain is very input-output (I/O) intensive. It is best to have a Solid-State Drive (SSD). If you have a mechanical hard disk drive (HDD), you will need at least 8GB of RAM to use as cache. Otherwise, you may discover that your system is too slow to keep up and sync fully.

Minimum Requirements:

- CPU with 2+ cores.
- At least 80GB free storage space.
- 4GB RAM minimum with a SSD, 8GB+ if you have an HDD.
- 8 MBit/sec download Internet service.

These are the minimum requirements to sync a full (but pruned) copy of an Ethereum-based blockchain.

At the time of writing (April 2018) the Parity codebase is lighter on resources, so if you're running with limited hardware you'll likely see better results using Parity.

If you want to sync in a reasonable amount of time and store all the development tools, libraries, clients, and blockchains we discuss in this book, you will want a more capable computer.

Recommended Specifications:

- Fast CPU with 4+ cores.
- 16GB+ RAM.
- Fast SSD with at least 500GB free space.
- 25+ MBit/sec download Internet service.

It's difficult to predict how fast a blockchain's size will increase and when more disk space will be required, so it's recommended to check the blockchain's latest size before you start syncing.



The disk size requirements above assume you will be running a node with default settings, where the blockchain is "pruned" of old state data. If you instead run a full "archival" node, where all state is kept on disk, it will likely require more than 1TB of disk space.

Ethereum: <https://bitinfocharts.com/ethereum/>

Ethereum Classic: <https://bitinfocharts.com/ethereum%20classic/>

Software Requirements for Building and Running a Client (Node)

This section covers Parity and Geth client software. It also assumes you are using a Unix-like command-line environment. The examples show the commands and output as they appear on an Ubuntu GNU/Linux operating system running the Bash shell (command-line execution environment).

Typically every blockchain will have their own version of Geth, while Parity provides support for multiple Ethereum-based blockchains (Ethereum, Ethereum Classic, Ellaism, Expanse, Musicoin) with the same client download.



In many of the examples in this chapter, we will be using the operating system's command-line interface (also known as a "shell"), accessed via a "terminal" application. The shell will display a prompt; you type a command, and the shell responds with some text and a new prompt for your next command. The prompt may look different on your system, but in the following examples, it is denoted by a \$ symbol. In the examples, when you see text after a \$ symbol, don't type the \$ symbol but type the command immediately following it, then press Enter to execute the command. In the examples, the lines below each command are the operating system's responses to that command. When you see the next \$ prefix, you'll know it's a new command and you should repeat the process.

Before we get started, you need to check some software is installed. If you've never done any software development on the computer you are currently using, you will probably need to install some basic tools. For the examples that follow, you will need to install git, the source-code management system; golang, the Go programming language and standard libraries; and Rust, a systems programming language.

Git can be installed by following the instructions here: <https://git-scm.com/>

Go can be installed by following the instructions here: <https://golang.org/>



Geth requirements vary, but if you stick with Go version 1.10 or greater you should be able to compile any version of Geth you want. Of course, you should always refer to the documentation for your chosen flavor of Geth.

The version of golang that is installed on your operating system or is available from your system's package manager may be significantly older than 1.10. If so, remove it and install the latest version from golang.org.

Rust can be installed by following the instructions here: <https://www.rustup.rs/>



Parity requires Rust version 1.27 or greater.

Parity also requires some software libraries, such as OpenSSL and libudev. To install these on a Ubuntu or Debian GNU/Linux compatible system:

```
$ sudo apt-get install openssl libssl-dev libudev-dev cmake
```

For other operating systems, use the package manager of your OS or follow the Wiki instructions (<https://github.com/paritytech/parity/wiki/Setup>) to install the required libraries.

Now you have git, golang, rust, and necessary libraries installed, let's get to work!

Parity

Parity is an implementation of a full node Ethereum client and DApp browser. Parity was written from the "ground up" in Rust, a systems programming language, with the aim of building a modular, secure, and scalable Ethereum client. Parity is developed by Parity Tech, a UK company, and is released under the GPLv3 free software license.



Disclosure: One of the authors of this book, Gavin Wood, is the founder of Parity Tech and wrote much of the Parity client. Parity represents about 25% of the installed Ethereum client base.

To install Parity, you can use the Rust package manager cargo or download the source code from GitHub. The package manager also downloads the source code, so there's not much difference between the two options. In the next section, we will show you how to download and compile Parity yourself.

Installing Parity

The Parity Wiki offers instructions for building Parity in different environments and containers:

<https://github.com/paritytech/parity/wiki/Setup>

We'll build Parity from source. This assumes you have already installed Rust using rustup (See [Software Requirements for Building and Running a Client \(Node\)](#)).

First, let's get the source code from GitHub:

```
$ git clone https://github.com/paritytech/parity
```

Now, let's change to the parity directory and use cargo to build the executable:

```
$ cd parity
$ cargo install
```

If all goes well, you should see something like:

```
$ cargo install
  Updating git repository `https://github.com/paritytech/js-
precompiled.git`
  Downloading log v0.3.7
  Downloading isatty v0.1.1
  Downloading regex v0.2.1

  [...]

  Compiling parity-ipfs-api v1.7.0
  Compiling parity-rpc v1.7.0
  Compiling parity-rpc-client v1.4.0
  Compiling rpc-cli v1.4.0 (file:///home/aantonop/Dev/parity/rpc_cli)
  Finished dev [unoptimized + debuginfo] target(s) in 479.12 secs
$
```

Let's try and run parity to see if it is installed, by invoking the --version option:

```
$ parity --version
Parity
  version Parity/v1.7.0-unstable-02edc95-20170623/x86_64-linux-
gnu/rustc1.18.0
Copyright 2015, 2016, 2017 Parity Technologies (UK) Ltd
License GPLv3+: GNU GPL version 3 or later
<http://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

By Wood/Paronyan/Kotewicz/Drwięga/Volf
  Habermeier/Czaban/Greeff/Gotchac/Redmann
$
```

Great! Now that Parity is installed, we can sync the blockchain and get started with some basic command-line options.

Go-Ethereum (Geth)

Geth is the Go language implementation, which is actively developed by the Ethereum Foundation, so is considered the "official" implementation of the Ethereum client. Typically, every Ethereum-based blockchain will have its own Geth implementation. If you're running Geth, then you'll want to make sure you grab the correct version for your blockchain using one of the repository links below.

Repository Links

Ethereum: <https://github.com/ethereum/go-ethereum> (or <https://geth.ethereum.org/>)

Ethereum Classic: <https://github.com/ethereumproject/go-ethereum>

Ellaism: <https://github.com/ellaism/go-ellaism>

Expanse: <https://github.com/expanse-org/go-expanse>

Musicoind: <https://github.com/Musicoind/go-musicoind>

Ubiq: <https://github.com/ubiq/go-ubiq>



You can also skip these instructions and install a precompiled binary for your platform of choice. The precompiled releases are much easier to install and can be found at the "release" section of the repositories above. However, you may learn more by downloading and compiling the software yourself.

Cloning the repository

Our first step is to clone the git repository, to get a copy of the source code.

To make a local clone of this repository, use the git command as follows, in your home directory or under any directory you use for development:

```
$ git clone <Repository Link>
```

You should see a progress report as the repository is copied to your local system:

```
Cloning into 'go-ethereum'...
remote: Counting objects: 62587, done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 62587 (delta 10), reused 13 (delta 4), pack-reused 62557
Receiving objects: 100% (62587/62587), 84.51 MiB | 1.40 MiB/s, done.
Resolving deltas: 100% (41554/41554), done.
Checking connectivity... done.
```

Great! Now that we have a local copy of Geth, we can compile an executable for our platform.

Building Geth from Source Code

To build Geth, change to the directory where the source code was downloaded and use the make command:

```
$ cd go-ethereum
$ make geth
```

If all goes well, you will see the Go compiler building each component until it produces the geth

executable:

```
build/env.sh go run build/ci.go install ./cmd/geth  
>>> /usr/local/go/bin/go install -ldflags -X  
main.gitCommit=58a1e13e6dd7f52a1d5e67bee47d23fd6cfdee5c -v ./cmd/geth  
github.com/ethereum/go-ethereum/common/hexutil  
github.com/ethereum/go-ethereum/common/math  
github.com/ethereum/go-ethereum/crypto/sha3  
github.com/ethereum/go-ethereum/rlp  
github.com/ethereum/go-ethereum/crypto/secp256k1  
github.com/ethereum/go-ethereum/common  
[...]  
github.com/ethereum/go-ethereum/cmd/utils  
github.com/ethereum/go-ethereum/cmd/geth  
Done building.  
Run "build/bin/geth" to launch geth.  
$
```

Let's make sure geth works without actually starting it running:

```
$ ./build/bin/geth version  
  
Geth  
Version: 1.6.6-unstable  
Git Commit: 58a1e13e6dd7f52a1d5e67bee47d23fd6cfdee5c  
Architecture: amd64  
Protocol Versions: [63 62]  
Network Id: 1  
Go Version: go1.8.3  
Operating System: linux  
[...]
```

Your geth version command may show slightly different information, but you should see a version report much like the one above.

Don't start running geth yet, because it will start synchronizing the blockchain "the slow way" and that will take far too long (weeks). [The First Synchronization of Ethereum-based Blockchains](#) explains the

challenge with the initial synchronization of Ethereum's blockchain.

The First Synchronization of Ethereum-based Blockchains

Normally, when syncing an Ethereum blockchain, your client will download and validate every block and every transaction since the very start, i.e. from the genesis block.

While it is possible to fully sync the blockchain this way, the sync will take a very long time and has high resource requirements (it will need much more RAM, and will take a very long time indeed if you don't have fast storage).

Many Ethereum-based blockchains were the victim of a Denial of Service (DoS) attack at the end of 2016. Blockchains affected by this attack will tend to sync slowly when doing a full sync.

For example, on Ethereum, a new client will make rapid progress until it reaches block 2,283,397. This block was mined on 2016/09/18 and marks the beginning of the DoS attacks. From this block to block 2,700,031 (2016/11/26), the validation of transactions becomes extremely slow, memory intensive, and I/O intensive. This results in validation times exceeding 1 minute per block. Ethereum implemented a series of upgrades, using hard forks, to address the underlying vulnerabilities that were exploited in the denial of service attacks. These upgrades also cleaned up the blockchain by removing some 20 million empty accounts created by spam transactions.

If you are syncing with full validation, your client will slow down and may take several days, or perhaps even longer, to validate the blocks affected by this DoS attack.

Fortunately, most Ethereum clients include an option to perform a "fast" synchronization that skips the full validation of transactions until it has synced to the tip of the blockchain, then resumes full validation.

For Geth, the option to enable fast synchronization is typically called `--fast`. You may need to refer to the specific instructions for your chosen Ethereum chain.

Parity does fast synchronization by default.



Geth can only operate fast synchronization when starting with an empty block database. If you have already started syncing without "fast" mode, Geth cannot switch. It is faster to delete the blockchain data directory and start "fast" syncing from the beginning than to continue syncing with full validation. Be careful to not delete any wallets when deleting the blockchain data!

Running geth or parity

Now that you've understood the challenges of the "first sync", we're ready to start an Ethereum client and sync the blockchain. For both geth and parity, you can use the --help option to see all the configuration parameters. Other than using --fast for geth as outlined in [The First Synchronization of Ethereum-based Blockchains](#), the default settings are usually sensible and appropriate for most uses. Choose how to configure any optional parameters to suit your needs, then start geth or parity to sync the chain. Then wait...



Syncing the Ethereum blockchain will take anywhere from half a day on a very fast system with lots of RAM, to several days on a slower system.

JSON-RPC Interface

Ethereum clients offer an Application Programming Interface (API) and a set of Remote Procedure Call (RPC) commands, which are encoded as JavaScript Object Notation (JSON). You will see this referred to as the *JSON-RPC API*. Essentially, the JSON-RPC API is an interface that allows us to write programs that use an Ethereum client as a *gateway* to an Ethereum network and blockchain.

Usually, the RPC interface is offered over as an HTTP service on port 8545. For security reasons it is restricted, by default, to only accept connections from localhost (the IP address of your own computer which is 127.0.0.1).

To access the JSON-RPC API, you can use a specialized library, written in the programming language of your choice, which provides "stub" function calls corresponding to each available RPC command. Or, you can manually construct HTTP requests and send/receive JSON encoded requests. You can even use a generic command-line HTTP client, like curl, to call the RPC interface. Let's try that. First, ensure that you have Geth configured and running, then switch to a new terminal window (e.g. with **<Ctrl>+<Shift>+N** or **<Ctrl>+<Shift>+T** in an existing terminal window) as shown in [Using curl to call the web3_clientVersion function over JSON-RPC](#):

Using curl to call the web3_clientVersion function over JSON-RPC

```
$ curl -X POST -H "Content-Type: application/json" --data \
'{"jsonrpc":"2.0", "method": "web3_clientVersion", "params":[], "id":1}' \
http://localhost:8545

{"jsonrpc": "2.0", "id": 1,
"result": "Geth/v1.8.0-unstable-02aeb3d7/linux-amd64/go1.8.3"}
```

In this example, we use curl to make an HTTP connection to address http://localhost:8545. We are already running geth, which offers the JSON-RPC API as an HTTP service on port 8545. We instruct curl to use the HTTP POST command and to identify the content as Content-Type: application/json. Finally, we pass a JSON-encoded request as the data component of our HTTP request. Most of our command line is just setting up curl to make the HTTP connection correctly. The interesting part is the actual JSON-RPC command we issue:

```
{"jsonrpc": "2.0", "method": "web3_clientVersion", "params":[], "id":4192}
```

The JSON-RPC request is formatted according to the JSON-RPC 2.0 specification, which you can see here: <https://www.jsonrpc.org/specification>

Each request contains 4 elements:

jsonrpc

Version of the JSON-RPC protocol. This MUST be exactly "2.0".

method

The name of the method to be invoked.

params

A structured value that holds the parameter values to be used during the invocation of the method. This member MAY be omitted.

id

An identifier established by the Client that MUST contain a String, Number, or NULL value if included. The Server MUST reply with the same value in the Response object if included. This

member is used to correlate the context between the two objects.



The id parameter is used primarily when you are making multiple requests in a single JSON-RPC call, a practice called *batching*. Batching is used to avoid the overhead of a new HTTP and TCP connection for every request. In the Ethereum context for example, we would use batching if we wanted to retrieve thousands of transactions in one HTTP connection. When batching, you set a different id for each request and then match it to the id in each response from the JSON-RPC server. The easiest way to implement this is to maintain a counter and increment the value for each request.

The response we receive is:

```
{"jsonrpc":"2.0", "id":4192,  
"result":"Geth/v1.8.0-unstable-02aeb3d7/linux-amd64/go1.8.3"}
```

This tells us that the JSON-RPC API is being served by Geth client version 1.8.0.

Let's try something a bit more interesting. In the next example, we ask the JSON-RPC API for the current price of gas in wei:

```
$ curl -X POST -H "Content-Type: application/json" --data \  
'{"jsonrpc":"2.0", "method":"eth_gasPrice", "params":[], "id":4213}' \  
http://localhost:8545  
  
{"jsonrpc":"2.0", "id":4213, "result":"0x430e23400"}
```

The response, 0x430e23400, tells us that the current gas price is 1.8 Gwei (gigawei or billion wei). If, like me, you don't think in hexadecimal, you can convert it to decimal on the command line with a little bash-fu:

```
$ echo $((0x430e23400))  
18000000000
```

The full JSON-RPC API can be investigated on the Ethereum wiki:

<https://github.com/ethereum/wiki/wiki/JSON-RPC>

Parity's Geth Compatibility Mode

Parity has a special "Geth Compatibility Mode", where it offers a JSON-RPC API that is identical to that offered by geth. To run Parity in Geth Compatibility Mode, use the --geth switch:

```
$ parity --geth
```

Remote Ethereum Clients

Remote clients offer a subset of the functionality of a full client. They do not store the full Ethereum blockchain, so they are faster to set up and require far less data storage.

A remote client offers one or more of the following functions:

- Manage private keys and Ethereum addresses in a wallet.
- Create, sign, and broadcast transactions.
- Interact with smart contracts, using the data payload.
- Browse and interact with DApps.
- Offer links to external services such as block explorers.
- Convert ether units and retrieve exchange rates from external sources.
- Inject a web3 instance into the web browser as a JavaScript object.
- Use a web3 instance provided/injected into the browser by another client.
- Access RPC services on a local or remote Ethereum node.

Some remote clients, for example mobile (smartphone) wallets, offer only basic wallet functionality. Other remote clients are full-blown DApp browsers. Remote clients commonly offer some of the functions of a full node Ethereum client without synchronizing a local copy of the Ethereum blockchain by connecting to a full node being run elsewhere, e.g. by you locally on your machine or on a web server, or by a third party on their servers.

Let's look at some of the most popular remote clients and the functions they offer.

Mobile (Smartphone) Wallets

All mobile wallets are remote clients, because smartphones do not have adequate resources to run a full Ethereum client. Light clients are in development and not in general use for Ethereum. In the case of Parity, it is marked "experimental" and can be used by running parity with the --light option.

Popular mobile wallets include Jaxx, Status, and Trust Wallet. We list these as examples of popular mobile wallets (this is not an endorsement or an indication of the security or functionality of these wallets).

Jaxx

A multi-currency mobile wallet based on BIP39 mnemonic seeds, with support for Bitcoin, Litecoin, Ethereum, Ethereum Classic, ZCash, a variety of ERC20 tokens, and many other currencies. Jaxx is available on Android, iOS, as a browser plugin wallet, and as a desktop wallet for a variety of operating systems. Find it at <https://jaxx.io>

Status

A mobile wallet and DApp browser, with support for a variety of tokens and popular DApps. Available for iOS and Android. Find it at <https://status.im>

Trust Wallet

A mobile Ethereum and Ethereum Classic wallet that supports ERC20 and ERC223 tokens. Trust Wallet is available for iOS and Android. Find it at <https://trustwalletapp.com/>

Cipher Browser

A full-featured Ethereum-enabled mobile DApp browser and wallet. Allows integration with Ethereum apps and tokens. Available for iOS and Android. Find it at <https://www.cipherbrowser.com>

Browser wallets

A variety of wallets and DApp browsers are available as plugins or extensions of web browsers such as Chrome and Firefox. These are remote clients that run inside your browser.

Some of the more popular ones are MetaMask, Jaxx, and MyEtherWallet/MyCrypto.

MetaMask

MetaMask was introduced in [Ethereum Basics](#), and is a versatile browser-based wallet, RPC client, and basic contract explorer. It is available on Chrome, Firefox, Opera, and Brave Browser. Find MetaMask at <https://metamask.io>

At first glance, MetaMask is a browser-based wallet. But, unlike other browser wallets, MetaMask injects a web3 instance into the browser, acting as an RPC client that connects to a variety of Ethereum blockchains (mainnet, Ropsten testnet, Kovan testnet, local RPC node, etc.). The ability to inject a web3 instance and act as a gateway to external RPC services makes MetaMask a very powerful tool for developers and users alike. It can be combined, for example, with MyEtherWallet or MyCrypto, acting as an web3 provider and RPC gateway for those tools.

Jaxx

Jaxx, which was introduced as a mobile wallet in [Mobile \(Smartphone\) Wallets](#), is also available as a Chrome and Firefox extension, and as a desktop wallet. Find it at <https://jaxx.io>

MyEtherWallet (MEW)

MyEtherWallet is a browser-based JavaScript remote client that offers:

- A software wallet running in JavaScript.
- A bridge to popular hardware wallets such as the Trezor and Ledger.
- A web3 interface that can connect to a web3 instance injected by another client (e.g. MetaMask).
- An RPC client that can connect to an Ethereum full client.
- A basic interface that can interact with smart contracts, given a contract's address and Application Binary Interface (ABI).

MyEtherWallet is very useful for testing and as an interface to hardware wallets. It should not be used as a primary software wallet, as it is exposed to threats via the browser environment and is not a secure key storage system.

You must be very careful when accessing MyEtherWallet and other browser-based JavaScript wallets, as they are frequent targets for phishing. Always use a bookmark and not a search engine or link to access the correct web URL. MyEtherWallet can be found at <https://myetherwallet.com>

MyCrypto

Just prior to publication of the first edition of this book, the MyEtherWallet project split into two competing implementations, guided by two independent development teams: a "fork", as it is called in open source development. The two projects are called MyEtherWallet (the original branding) and MyCrypto. At the time of the split, MyCrypto offered identical functionality as MyEtherWallet. It is likely that the two projects will diverge as the two development teams adopt different goals and priorities.

As with MyEtherWallet, you must be very careful when accessing MyCrypto in your browser. Always use a bookmark, or type the URL very carefully (then bookmark it for future use).

MyCrypto can be found at <https://mycrypto.com>

Mist

Mist was the first Ethereum-enabled browser, built by the Ethereum Foundation. It also contains a browser-based wallet that was the first implementation of the ERC20 token standard (Fabian Vogelsteller, author of ERC20 was also the main developer of Mist). Mist was also the first wallet to introduce the camelCase checksum (EIP-155). Mist runs a full node, and offers a full DApp browser with support for Swarm based storage and ENS addresses. Find it at <https://github.com/ethereum/mist>

Keys, Addresses

One of Ethereum's foundational technologies is *cryptography*, which is a branch of mathematics used extensively in computer security. Cryptography means "secret writing" in Greek, but the study of cryptography encompasses more than just secret writing, which is referred to as encryption. Cryptography can, for example, also be used to prove knowledge of a secret without revealing that secret (e.g. with a digital signature), or to prove the authenticity of data (e.g. with digital fingerprints, also known as "hashes"). These types of cryptographic proofs are mathematical tools critical to the operation of the Ethereum platform (and, indeed, all blockchain systems), and are also extensively used in Ethereum applications. Note that, at the time of publication, no part of the Ethereum protocol involves encryption; that is to say all communication with the Ethereum platform and between nodes (including transaction data) are unencrypted and can (necessarily) be read by anyone. This is so everyone can verify the correctness of state updates and consensus can be reached. In the future, advanced cryptographic tools, such as zero knowledge proofs and homomorphic encryption, will be available that will allow for some encrypted calculations to be recorded on the blockchain while still enabling consensus, but, while provision has been made for them, they have yet to be deployed. In this chapter we will introduce some of the cryptography used in Ethereum, namely public key cryptography (PKC), which is used to control ownership of funds, in the form of private keys and addresses.

Introduction

As we saw earlier in the book, Ethereum has two different types of accounts: *Externally Owned Accounts* (EOA) and *Contracts*. In this section we will examine the use of cryptography to establish ownership of ether by externally owned accounts, i.e. private keys. Private keys enable many of the interesting properties of Ethereum, including decentralized trust and control, and ownership attestation.

Ownership of ether by EOAs is established through digital *private keys*, *Ethereum addresses*, and *digital signatures*. The private keys are at the heart of all user interaction with Ethereum. In fact, account addresses are derived directly from private keys: a private key uniquely determines a single Ethereum address, also known as an *account*.

Private keys are not used directly in the Ethereum system in any way, they are never transmitted or stored on Ethereum. That is to say that private keys should remain private and never appear in messages passed to the network, nor should they be stored on-chain; only account addresses and digital signatures are ever transmitted and stored on the Ethereum system. For more information on how to keep private keys safe and secure, see [Control and responsibility](#) and [Wallets](#).

Access and control of funds is achieved with digital signatures, which are also created using the private key. Ethereum transactions require a valid digital signature to be included in the blockchain. Anyone with a copy of a private key has control of the corresponding account and any ether it holds. Assuming a user keeps their private key safe, the digital signatures in Ethereum transactions prove the true owner of the funds, because they prove ownership of the private key.

In public key cryptography based systems, such as that used by Ethereum, keys come in pairs consisting of a private (secret) key and a public key. Think of the public key as similar to a bank account number, and the private key as similar to the secret PIN; it is the latter that provides control over the account, and the former that identifies it to others. The private keys themselves are very rarely seen by Ethereum users; for the most part, they are stored (in encrypted form) in special files and managed by Ethereum wallet software.

In the payment portion of an Ethereum transaction, the intended recipient is represented by an *Ethereum address*, which is used in the same way as the beneficiary account details of a bank transfer. As we will see in more detail below, an Ethereum address for an EOA is generated from the public key portion of a key pair. However, not all Ethereum addresses represent public-private key pairs; they can also represent contracts, which, as we will see in [Smart contracts and Solidity](#), are not backed by private keys.

In the rest of this chapter, we will first explore basic cryptography in a bit more detail and explain the mathematics used in Ethereum. Next, we will look at how keys are generated, stored, and managed. Finally, we will review the various encoding formats used to represent private keys, public keys, and addresses.

Public key cryptography and cryptocurrency

Public key cryptography (also called "asymmetric cryptography") is a core part of modern day information security. First published in the 1970s by Martin Hellman, Whitfield Diffie and Ralph Merkle, it was a monumental breakthrough which incited the first big wave of public interest in the field of cryptography. Before the 70s, strong cryptographic knowledge was kept secret by governments.

Public key cryptography uses unique keys to secure information. These keys are based on mathematical functions that have a special property: it is easy to calculate them, but hard to calculate their inverse. Based on these functions, cryptography enables the creation of digital secrets and unforgeable digital signatures which are secured by the laws of mathematics.

For example, multiplying two large prime numbers together is trivial. But given the product of two large

primes, it is very difficult to find the prime factors (a problem called *prime factorization*). Let's say I present the number 8018009 and tell you it is the product of two primes. Finding those two primes is much harder than it was for me to multiply them to produce 8018009.

Some of these mathematical functions can be inverted easily if you know some secret information. In our example above, if I tell you that one of the prime factors is 2003, you can trivially find the other one with a simple division: $8018009 \div 2003 = 4003$. Such functions are often called *trapdoor functions* because they are very difficult to invert unless you are given a piece of secret information that can be used as a shortcut to reverse the function.

A more advanced category of mathematical functions that is useful in cryptography is based on arithmetic operations on an elliptic curve. In elliptic curve arithmetic, multiplication modulo a prime is simple but division (the inverse) is practically impossible. This is called the *discrete logarithm problem* and there are currently no known trapdoors. *Elliptic curve cryptography* is used extensively in modern computer systems and is the basis of Ethereum's (and other cryptocurrencies') use of private keys and digital signatures.

Read more about cryptography and the mathematical functions that are used in modern cryptography:

Cryptography: <https://en.wikipedia.org/wiki/Cryptography>

Trapdoor Function: https://en.wikipedia.org/wiki/Trapdoor_function



Prime Factorization: https://en.wikipedia.org/wiki/Integer_factorization

Discrete Logarithm: https://en.wikipedia.org/wiki/Discrete_logarithm

Elliptic Curve Cryptography: https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

In Ethereum, we use public key cryptography (also known as asymmetric cryptography) to create the public-private key pair we have been talking about in this chapter. They are considered a "pair" because the public key is derived from the private key. Together, they represent an Ethereum account by providing, respectively, a publicly accessible account handle (the address) and private control over access to any ether in the account and over any authentication the account needs when using smart contracts. The private key controls access by being the unique piece of information needed to create *digital signatures*, which are required to sign transactions to spend any funds in the account. Digital signatures are also used to authenticate owners or users of contracts, as we will see in [Smart contracts](#)

and Solidity.

A digital signature can be created to sign any message. For Ethereum transactions, the details of the transaction itself are used as "the message". The mathematics of cryptography, in this case, elliptic curve cryptography, provides a way for the message (i.e. the transaction details) to be combined with the private key to create a code that can only be produced with knowledge of the private key. That code is called the digital signature. Note that an Ethereum transaction is basically a request to access a particular account with a particular Ethereum address. When a transaction is sent to the Ethereum network in order to move funds or interact with smart contracts, it needs to be sent with a digital signature created with the private key corresponding to the Ethereum address in question. Elliptic curve mathematics means that *anyone* can verify that a transaction is valid, by checking that the digital signature matches the transaction details *and* the Ethereum address to which access is being requested. The verification doesn't involve the private key at all - that remains private. However, the verification process determines beyond doubt that the transaction could have only come from someone with the private key that corresponds to the public key behind the Ethereum address. This is the "magic" of public key cryptography.



In most wallet implementations, the private and public keys are stored together as a *key pair* for convenience. However, the public key can be trivially calculated from the private key, so storing only the private key is also possible.



There is no encryption as part of the Ethereum protocol, i.e. all messages that are sent as part of the operation of the Ethereum network can (necessarily) be read by everyone. As such, private keys are only used to create digital signatures for transaction authentication.

Private keys

A private key is simply a number, picked at random. Ownership and control of the private key is the root of user control over all funds associated with the corresponding Ethereum address, as well as access to contracts that authorize that address. The private key is used to create signatures required to spend ether by proving ownership of funds used in a transaction. The private key must remain secret at all times, because revealing it to third parties is equivalent to giving them control over the ether and contracts secured by that private key. The private key must also be backed up and protected from accidental loss. If it's lost, it cannot be recovered and the funds secured by it are lost forever too.



The Ethereum private key is just a number. One way to pick your private keys randomly is to simply use a coin, pencil, and paper: toss a coin 256 times and you have the binary digits of a random private key you can use in an Ethereum wallet (probably - see below). The public key and address can then be generated from the private key.

Generating a private key from a random number

The first and most important step in generating keys is to find a secure source of entropy, or randomness. Creating an Ethereum private key is essentially the picking a number between 1 and 2^{256} . The exact method you use to pick that number does not matter as long as it is not predictable or deterministic. Ethereum software uses the underlying operating system's random number generator to produce 256 random bits. Usually, the OS random number generator is initialized by a human source of randomness, which is why you may be asked to wiggle your mouse around for a few seconds, or press random keys on your keyboard. An alternative could be cosmic radiation noise on the computer's microphone channel.

More precisely, private keys can be any non-zero number up to a very large number slightly less than 2^{256} - a huge 78-digit number, roughly 1.158×10^{77} . The exact number shares the first 38 digits with 2^{256} and is defined as the order of the elliptic curve used in Ethereum (see [Elliptic curve cryptography explained](#)). To create a private key, we randomly pick a 256-bit number and check that it is within the valid range. In programming terms, this is usually achieved by feeding an even larger string of random bits (collected from a cryptographically secure source of randomness) into a 256-bit hash algorithm such as Keccak-256 or SHA256, both of which will conveniently produce a 256-bit number. If the result is within the valid range, we have a suitable private key. Otherwise, we simply try again with another random number.

Note that the private key generation process is an off-line one; it does not require any communication with the Ethereum network, or indeed any communication with anyone at all. As such, in order to pick a number that no-one else will ever pick, it needs to be truly random. If you choose the number yourself, the chance someone else will try it (and then run off with your ether) is too high. Using a bad random number generator (like the pseudo-random `rand()` function in most programming languages) is even worse, because it is even more obvious and even easier to replicate. Just like with passwords for online accounts, it needs to be unguessable. Fortunately, you never need to remember your private key, so you can take the best possible approach for picking your private key, namely true randomness.



The size of Ethereum's private key space, (roughly 2^{256}) is an unfathomably large number. It is approximately 10^{77} in decimal - that is a number with 77 digits. For comparison, the visible universe is estimated to contain 10^{80} atoms, i.e. there are almost enough private keys to give every atom in the universe an Ethereum account. If you pick a private key randomly, there is no conceivable way anyone will ever guess it or pick it themselves.



Do not write your own code to create a random number or use a "simple" random number generator offered by your programming language. It is vital that you use a cryptographically secure pseudo-random number generator (such as CSPRNG) with a seed from a source of sufficient entropy. Study the documentation of the random number generator library you choose to make sure it is cryptographically secure. Correct implementation of the CSPRNG library is critical to the security of the keys.

The following is a randomly generated private key shown in hexadecimal format (256 bits shown as 64 hexadecimal digits, each 4 bits):

```
f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315
```

Public keys

An Ethereum public key is a *point* on an elliptic curve, meaning it is a set of x and y coordinates that satisfy the elliptic curve equation.

In simpler terms, an Ethereum public key is two numbers, joined together. These numbers are produced from the private key by a calculation that can *only go one way*. That means that it is trivial to calculate a public key if you have the private key, but you cannot calculate the private key from the public key.



MATH is about to happen! Don't panic. If you start to get lost at any point in the following paragraphs, you can skip the next few sections. There are many tools and libraries that will do the math for you.

The public key is calculated from the private key using elliptic curve multiplication, which is practically irreversible: $K = k * G$, where k is the private key, G is a constant point called the *generator point*, K is the

resulting public key and " $*$ " is the special elliptic curve "multiplication" operator. Note the elliptic curve multiplication is not like normal multiplication. It shares functional attributes with normal multiplication, but that is about it. For example, the reverse operation (which would be division for normal numbers), known as "finding the discrete logarithm" - i.e. calculating k if you know K - is as difficult as trying all possible values of k , i.e. a brute-force search that will likely take more time than this universe will allow for.

In simpler terms: arithmetic on the elliptic curve is different from "regular" integer arithmetic. A point (G) can be multiplied by an integer (k) to produce another point (K). But there is no such thing as *division*, so it is not possible to simply "divide" the public key K by the point G to calculate the private key k . This is the one-way mathematical function described in [Public key cryptography and cryptocurrency](#).



Elliptic curve multiplication is a type of function that cryptographers call a "one-way" function: it is easy to do in one direction (multiplication) and impossible to do in the reverse direction (division). The owner of the private key can easily create the public key and then share it with the world knowing that no one can reverse the function and calculate the private key from the public key. This mathematical trick becomes the basis for unforgeable and secure digital signatures that prove ownership of Ethereum funds and control of contracts.

Before we demonstrate how to generate a public key from a private key, let's look at elliptic curve cryptography in a bit more detail.

Elliptic curve cryptography explained

Elliptic curve cryptography is a type of asymmetric or public key cryptography based on the discrete logarithm problem as expressed by addition and multiplication on the points of an elliptic curve.

[A visualization of an elliptic curve](#) is an example of an elliptic curve, similar to that used by Ethereum.



Ethereum uses the exact same elliptic curve, called secp256k1, as Bitcoin. That makes it possible to reuse many of the elliptic curve libraries and tools from Bitcoin.

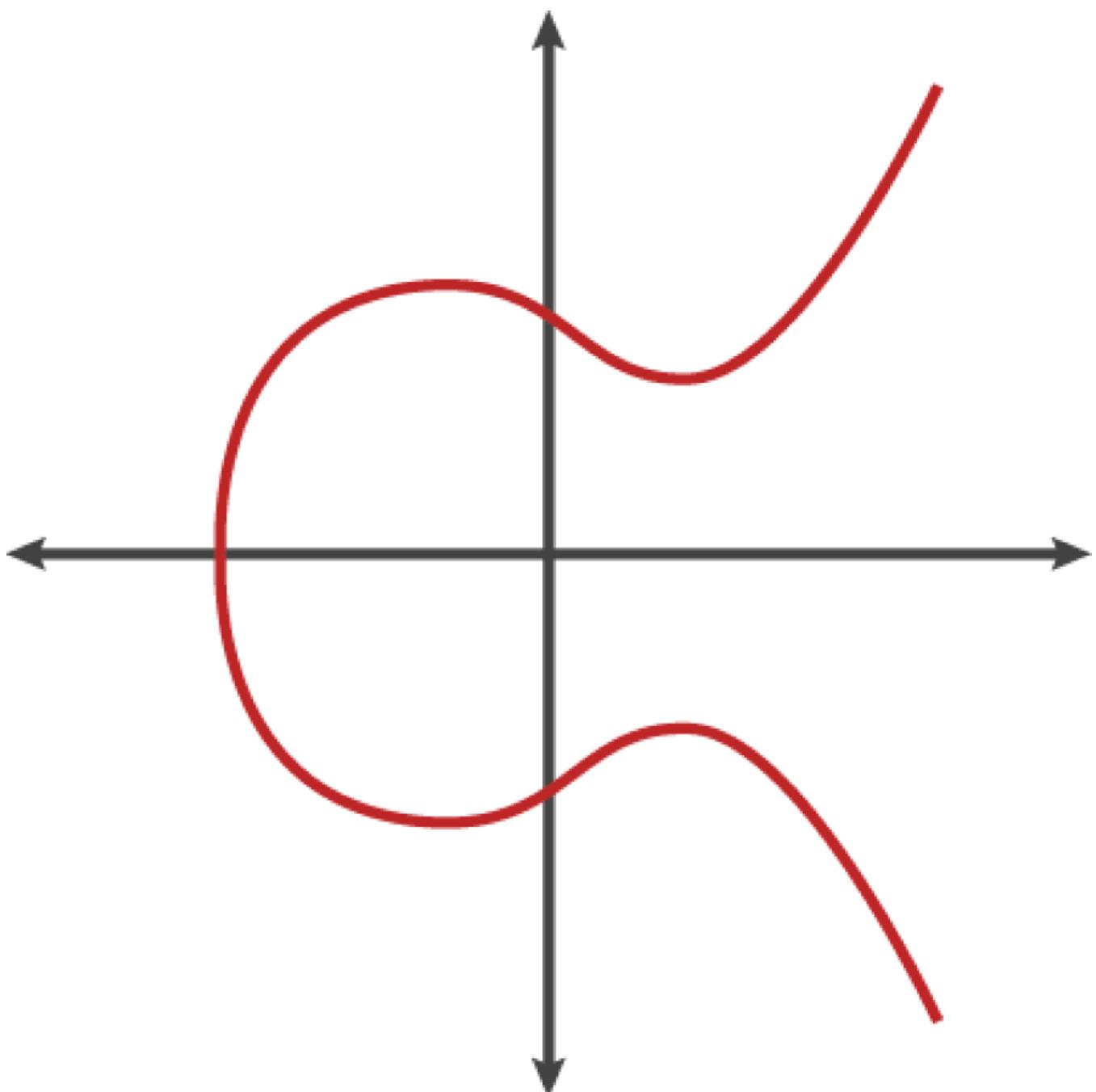


Figure 27. A visualization of an elliptic curve

Ethereum uses a specific elliptic curve and set of mathematical constants, as defined in a standard

called secp256k1, established by the US National Institute of Standards and Technology (NIST). The secp256k1 curve is defined by the following function, which produces an elliptic curve:

or

The *mod p* (modulo prime number p) indicates that this curve is over a finite field of prime order p, also written as (\mathbb{F}_p) , where $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$, which is a very large prime number.

Because this curve is defined over a finite field of prime order instead of over the real numbers, it looks like a pattern of dots scattered in two dimensions, which makes it difficult to visualize. However, the math is identical to that of an elliptic curve over real numbers. As an example, [Elliptic curve cryptography: visualizing an elliptic curve over F\(p\), with p=17](#) shows the same elliptic curve over a much smaller finite field of prime order 17, showing a pattern of dots on a grid. The secp256k1 Ethereum elliptic curve can be thought of as a much more complex pattern of dots on an unfathomably large grid.

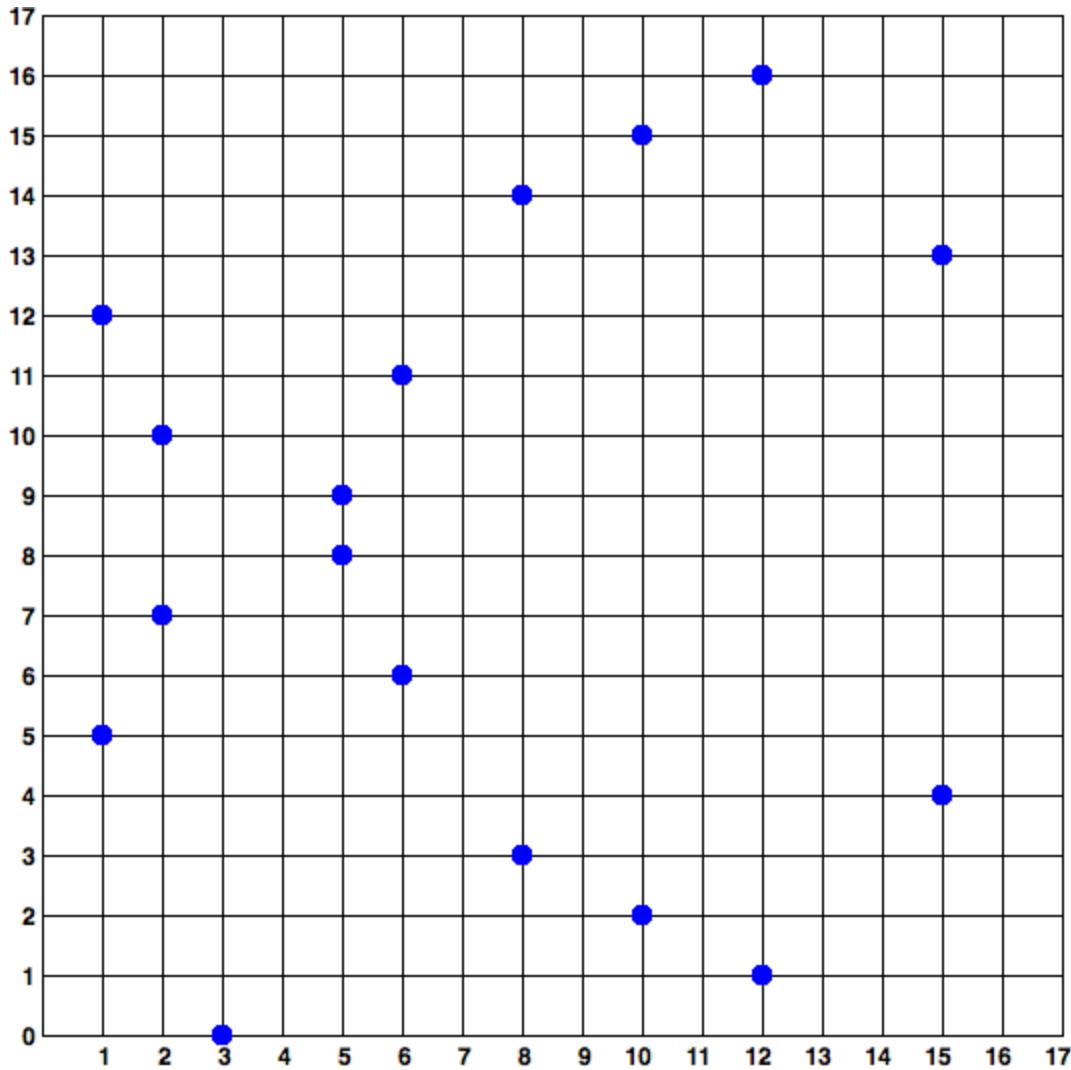


Figure 28. Elliptic curve cryptography: visualizing an elliptic curve over $F(p)$, with $p=17$

So, for example, the following is a point Q with coordinates (x,y) that is a point on the secp256k1 curve:

```

Q =
(497903908252493844860331443559168646076160835201016386814039737492559245
39515,
5957413216189990004586208649392101578003217529175580739928400772105034129
7360)

```

[Using Python to confirm that this point is on the elliptic curve](#) shows how you can check this yourself using Python. The variables x and y are the coordinates of the point Q as above. The variable p is the prime order of the elliptic curve (the prime that is used for all the modulo operations). The last line of Python is the elliptic curve equation (the % operator in Python is the modulo operator). If x and y are indeed the coordinates of a point on the elliptic curve, then they satisfy the equation and the result is zero (0L is a long integer with value zero). Try it yourself, by typing python on a command line and copying each line (after the prompt >>>) from the listing:

Example 1. Using Python to confirm that this point is on the elliptic curve

```
Python 3.4.0 (default, Mar 30 2014, 19:23:13)
[GCC 4.2.1 Compatible Apple LLVM 5.1 (clang-503.0.38)] on darwin
Type "help", "copyright", "credits" or "license" for more
information.

>>> p =
115792089237316195423570985008687907853269984665640564039457584007908
834671663
>>> x =
497903908252493844860331443559168646076160835201016386814039737492559
24539515
>>> y =
595741321618999000458620864939210157800321752917558073992840077210503
41297360
>>> (x ** 3 + 7 - y**2) % p
0L
```

Elliptic curve arithmetic operations

A lot of elliptic curve math looks and works very much like the integer arithmetic we learned at school. Specifically, we can define an addition operator, which instead of jumping along the number line is jumping to other points on the curve. Once we have the addition operator, we can also define multiplication of a point and a whole number, which is equivalent to repeated addition.

Elliptic curve addition is defined such that given two points P_1 and P_2 on the elliptic curve, there is a third point $P_3 = P_1 + P_2$, also on the elliptic curve.

Geometrically, this third point P_3 is calculated by drawing a line between P_1 and P_2 . This line will intersect the elliptic curve in exactly one additional place (amazingly). Call this point $P_3' = (x, y)$. Then reflect in the x-axis to get $P_3 = (x, -y)$.

If P_1 and P_2 are the same point, the line "between" P_1 and P_2 should extend to be the tangent to the curve at this point P_1 . This tangent will intersect the curve at exactly one new point. You can use techniques from calculus to determine the slope of the tangent line. Curiously, these techniques work, even though we are restricting our interest to points on the curve with two integer coordinates!

In elliptic curve math, there is also a point called the "point at infinity," which roughly corresponds to the role of the number zero in addition. On computers, it's sometimes represented by $x = y = 0$ (which doesn't satisfy the elliptic curve equation, but it's an easy separate case that can be checked). There are a couple of special cases that explain the need for the "point at infinity".

In some cases (e.g. if P_1 and P_2 have the same x values but different y values), the line will be exactly vertical, in which case $P_3 = \text{"point at infinity"}$.

If P_1 is the "point at infinity," then $P_1 + P_2 = P_2$. Similarly, if P_2 is the point at infinity, then $P_1 + P_2 = P_1$. This shows how the point at infinity plays the role that zero plays in "normal" arithmetic.

It turns out that $+$ is associative, which means that $(A + B) + C = A + (B + C)$. That means we can write $A + B + C$ (without parentheses) without ambiguity.

Now that we have defined addition, we can define multiplication in the standard way that extends addition. For a point P on the elliptic curve, if k is a whole number, then $k * P = P + P + P + \dots + P$ (k times). Note that k is sometimes (perhaps confusingly) called an "exponent" in this case.

Generating a public key

Starting with a private key in the form of a randomly-generated number k , we multiply it by a predetermined point on the curve called the *generator point* G to produce another point somewhere else on the curve, which is the corresponding public key K . The generator point is specified as part of the secp256k1 standard, is the same for all implementations of secp256k1, and all keys derived from that curve use the same point G :

where k is the private key, G is the generator point, and K is the resulting public key, a point on the curve. Because the generator point is always the same for all Ethereum users, a private key k multiplied with G will always result in the same public key K . The relationship between k and K is fixed, but can only be calculated in one direction, from k to K . That's why an Ethereum address (derived from K) can

be shared with anyone and does not reveal the user's private key (k).

As we described in [Elliptic curve arithmetic operations](#), the multiplication of $k * G$ is equivalent to repeated addition, so $G + G + G + \dots + G$, repeated k times. In summary, to produce a public key K , from a private key k , we add the generator point G to itself, k times.



A private key can be converted into a public key, but a public key cannot be converted back into a private key, because the math only works one way.

Let's apply this calculation to find the public key for the specific private key we showed you in [Private keys](#):

Example private key to public key calculation

```
K = f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315 * G
```

A cryptographic library can help us calculate K , using elliptic curve multiplication. The resulting public key K is defined as a point $K = (x,y)$:

Example public key calculated from the example private key

```
K = (x, y)
```

where

```
x = 6e145cce1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b  
y = 83b5c38e5e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32cccd0
```

In Ethereum you may see public keys represented as a serialization of 130 hexadecimal characters (65 bytes). This is adopted from a standard serialization format proposed by the industry consortium Standards for Efficient Cryptography Group (SECG), documented in [Standards for Efficient Cryptography \(SEC1\)](#) [<http://www.secg.org/sec1-v2.pdf>]. The standard defines four possible prefixes that can be used to identify points on an elliptic curve:

Prefix	Meaning	Length (bytes counting prefix)
--------	---------	--------------------------------

0x00	Point at Infinity	1
0x04	Uncompressed Point	65
0x02	Compressed Point with even Y	33
0x03	Compressed Point with odd Y	33

Ethereum only uses uncompressed public keys, therefore the only prefix that is relevant is (hex) 04. The serialization concatenates the X and Y coordinates of the public key:

```
04 + X-coordinate (32 bytes/64 hex) + Y-coordinate (32 bytes/64 hex)
```

Therefore, the public key we calculated in [Example public key calculated from the example private key](#) is serialized as:

```
046e145ccef1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b83b5c38  
e5e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32ccd0
```

Elliptic curve libraries

There are a couple of implementations of the secp256k1 elliptic curve that are used in cryptocurrency related projects:

OpenSSL

The OpenSSL library offers a comprehensive set of cryptographic primitives, including a full implementation of the secp256k1. For example, to derive the public key, the function EC_POINT_mul() can be used. Find it at <https://www.openssl.org/>

libsecp256k1

Bitcoin Core's libsecp256k1, is a C-language implementation of the secp256k1 elliptic curve and other cryptographic primitives. The libsecp256 of elliptic curve cryptography was written from scratch to replace OpenSSL in Bitcoin Core software, and is considered superior in both performance and security. Find it at: <https://github.com/bitcoin-core/secp256k1>

Cryptographic hash functions

Cryptographic hash functions are used throughout Ethereum. In fact, hash functions are used extensively in almost all cryptographic systems, a fact captured by cryptographer Bruce Schneier who said, "Much more than encryption algorithms, one-way hash functions are the workhorses of modern cryptography".

In this section we will discuss hash functions, explore their basic properties, and see how those properties make them so useful in so many areas of modern cryptography. We address hash functions here, because they are part of the transformation of Ethereum public keys into addresses. They can also be used to create *digital fingerprints*, which aid in the verification of data.

In simple terms, "a hash function is any function that can be used to map data of arbitrary size to data of fixed size". The input to a hash function is called a *pre-image*, the *message* or simply the *input data*. The output is called the *hash*. A special sub-category of hash functions is *cryptographic hash functions*, which have specific properties that are useful to secure platforms, such as Ethereum.

A cryptographic hash function is a *one-way* hash function that maps data of arbitrary size to a fixed-size string of bits. The "one-way" nature means that it is computationally infeasible to recreate the input data if one only knows the output hash. The only way to determine a possible input is to conduct a brute-force search, checking each candidate for a matching output; given that the search space is virtually infinite, it is easy to understand the practical impossibility of the task. Even if you find some input data that creates a matching hash, it may not be the original input data: hash functions are "many to one" functions. Finding two sets of input data that hash to the same output is called finding a "hash collision". Roughly speaking, the better the hash function, the rarer hash collisions are. For Ethereum, they are effectively impossible.

Cryptographic hash functions have five main properties ([Source: Wikipedia/Cryptographic Hash Function](#) [https://en.wikipedia.org/wiki/Cryptographic_hash_function]):

Determinism

A given input message always produces the same hash output.

Verifiability

Computing the hash of a message is efficient (linear complexity).

Uncorrelated

A small change to the message (e.g. one bit change) should change the hash output so extensively

that it cannot be correlated to the hash of the original message.

Irreversibility

Computing the message from its hash is infeasible, equivalent to a brute force search through all possible messages.

Collision Protection

It should be infeasible to calculate two different messages that produce the same hash output.

Resistance to hash collisions is particularly important for avoiding digital signature forgery in Ethereum.

The combination of these properties make cryptographic hash functions useful for a broad range of security applications including:

- Data fingerprinting
- Message integrity (error detection)
- Proof-of-Work
- Authentication (password hashing and key stretching)
- Pseudo-random number generators
- Message commitment (commit–reveal mechanisms)
- Unique identifiers

We will find many of these in Ethereum as we progress through the various layers of the system.

Ethereum's cryptographic hash function - Keccak-256

Ethereum uses the Keccak-256 cryptographic hash function in many places. Keccak-256 was designed as a candidate for the SHA-3 Cryptographic Hash Function Competition held in 2007 by the National Institute of Science and Technology. Keccak was the winning algorithm, which became standardized as Federal Information Processing Standard (FIPS) 202 in 2015.

However, during the period when Ethereum was developed, the NIST standardization was not yet finalized. NIST adjusted some of the parameters of Keccak after the completion of the standards process, allegedly to improve its efficiency. This was occurring at the same time as heroic whistleblower Edward Snowden revealed documents that imply that NIST may have been improperly influenced by

the National Security Agency to intentionally weaken the Dual_EC_DRBG random-number generator standard, effectively placing a backdoor in the standard random number generator. The result of this controversy was a backlash against the proposed changes and a significant delay in the standardization of SHA-3. At the time, the Ethereum Foundation decided to implement the original Keccak algorithm, as proposed by its inventors, rather than the SHA-3 standard as modified by NIST.



While you may see "SHA-3" mentioned throughout Ethereum documents and code, many if not all of those instances actually refer to Keccak-256, not the finalized FIPS-202 SHA-3 standard. The implementation differences are slight, having to do with padding parameters, but they are significant in that Keccak-256 produces different hash outputs from FIPS-202 SHA-3 for the same input.

Due to the confusion created by the difference between the hash function used in Ethereum (Keccak-256) and the finalized standard (FIP-202 SHA-3), there is an effort underway to rename all instances of sha3 in all code, opcodes and libraries to keccak256. See [ERC-59](#) [<https://github.com/ethereum/EIPs/issues/59>] for details.

Which hash function am I using?

How can you tell if the software library you are using is FIPS-202 SHA-3 or Keccak-256, if both might be called "SHA-3"?

An easy way to tell is to use a *test vector*, an expected output for a given input. The test most commonly used for a hash function is the *empty input*. If you run the hash function with an empty string as input you should see the following results (as shown in [Testing whether the SHA-3 library you are using is Keccak-256 or FIPS-202 SHA-3](#)):

Testing whether the SHA-3 library you are using is Keccak-256 or FIPS-202 SHA-3

```
Keccak256("") =  
c5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470  
  
SHA3("") =  
a7ffc6f8bf1ed76651c14756a061d662f580ff4de43b49fa82d80a4b80f8434a
```

Regardless of what the function is called, you can test it to see whether it is the original Keccak-256, or the final NIST standard FIPS-202 SHA-3, by running the simple test above. Remember, Ethereum uses

Keccak-256, even though it is often called SHA-3 in the code.

Next, let's examine the first application of Keccak-256 in Ethereum, which is to produce Ethereum addresses from public keys.

Ethereum addresses

Ethereum addresses are *unique identifiers* that are derived from public keys or contracts using the Keccak-256 one-way hash function.

In our previous examples, we started with a private key and used elliptic curve multiplication to derive a public key:

Private Key k :

```
k = f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315
```

Public Key K (X and Y coordinates concatenated and shown as hex):

```
K =
6e145cce1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b83b5c38e5
e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32ccd0
```



It is worth noting that the public key is not formatted with the prefix (hex) 04 when the address is calculated.

We use Keccak-256 to calculate the *hash* of this public key:

```
Keccak256(K) =
2a5bc342ed616b5ba5732269001d3f1ef827552ae1114027bd3ecf1f086ba0f9
```

Then we keep only the last 20 bytes (least significant bytes), which is our Ethereum address:

```
001d3f1ef827552ae1114027bd3ecf1f086ba0f9
```

Most often you will see Ethereum addresses with the prefix "0x" that indicates it is hexadecimal-encoded, like this:

```
0x001d3f1ef827552ae1114027bd3ecf1f086ba0f9
```

Ethereum address formats

Ethereum addresses are hexadecimal numbers, identifiers derived from the last 20 bytes of the Keccak-256 hash of the public key.

Unlike Bitcoin addresses, which are encoded in the user interface of all clients to include a built-in checksum to protect against mistyped addresses, Ethereum addresses are presented as raw hexadecimal without any checksum.

The rationale behind that decision was that Ethereum addresses would eventually be hidden behind abstractions (such as name services) at higher layers of the system and that checksums should be added at higher layers if necessary.

In reality, these higher layers were developed too slowly and this design choice led to a number of problems in the early days of the ecosystem, including the loss of funds due to mistyped addresses and input validation errors. Furthermore, because Ethereum name services were developed slower than initially expected, alternative encodings such as ICAP were adopted very slowly by wallet developers.

Inter Exchange Client Address Protocol (ICAP)

The *Inter exchange Client Address Protocol (ICAP)* is an Ethereum Address encoding that is partly compatible with the International Bank Account Number (IBAN) encoding, offering a versatile, checksummed and interoperable encoding for Ethereum Addresses. ICAP addresses can encode Ethereum Addresses or common names registered with an Ethereum name registry. You can read more about ICAP on the Ethereum Wiki: <https://github.com/ethereum/wiki/wiki/ICAP:-Inter-exchange-Client-Address-Protocol>

IBAN is an international standard for identifying bank account numbers, mostly used for wire transfers. It is broadly adopted in the European Single Euro Payments Area (SEPA) and beyond. IBAN is a

centralized and heavily regulated service. ICAP is a decentralized but compatible implementation for Ethereum addresses.

An IBAN consists of a string of up to 34 alphanumeric characters (case-insensitive) comprising a country code, checksum, and bank account identifier (which is country-specific).

ICAP uses the same structure by introducing a non-standard country code "XE" that stands for "Ethereum", followed by a two-character checksum and 3 possible variations of an account identifier:

Direct

Up to 30 alphanumeric character big-endian base-36 integer representing the least significant bits of an Ethereum address. Because this encoding fits less than the full 155 bits of a general Ethereum address, it only works for Ethereum addresses that start with one or more zero bytes. The advantage is that it is compatible with IBAN, in terms of the field length and checksum. Example: XE60HAMICDXSV5QXVJA7TJW47Q9CHWKJD (33 characters long)

Basic

Same as the "Direct" encoding except that it is 31 characters long. This allows it to encode any Ethereum address, but makes it incompatible with IBAN field validation. Example: XE18CHDJBPLTBCJ03FE9O2NS0BPOJVQCU2P (35 characters long)

Indirect

Encodes an identifier that resolves to an Ethereum address through a name registry provider. It uses 16 alphanumeric characters, comprising an *asset identifier* (e.g. ETH), a name service (e.g. XREG) and a 9-character name (e.g. KITTYCATS), which is a human-readable name. Example: XE##ETHXREGKITTYCATS (20 characters long), where the "##" should be replaced by the two computed checksum characters.

We can use the helpeth command-line tool to create ICAP addresses. Let's try with our example private key (prefixed with 0x and passed as a parameter to helpeth):

```
$ helpeth keyDetails -p  
0xf8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315  
  
Address: 0x001d3f1ef827552ae1114027bd3ecf1f086ba0f9  
Address (checksum): 0x001d3F1ef827552Ae1114027BD3ECF1f086bA0F9  
ICAP: XE60 HAMI CDXS V5QX VJA7 TJW4 7Q9C HWKJ D  
Public key:  
0x6e145cce1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b83b5c38  
e5e2b0c8529d7fa3f64d46daa1ece2d9ac14cab9477d042c84c32ccd0
```

The `helpeth` command constructs a hexadecimal Ethereum address as well as an ICAP address for us. The ICAP address for our example key is:

```
XE60HAMICDXSV5QXVJA7TJW47Q9CHWKJD
```

Because our example Ethereum address happens to start with a zero byte, it can be encoded using the "Direct" ICAP encoding method that is valid in IBAN format. You can tell because it is 33 characters long.

If our address did not start with a zero, it would be encoded with the "Basic" encoding, which would be 35 characters long and invalid as an IBAN.



The chances of any Ethereum address starting with a zero byte are 1 in 256. To generate one like that, it will take on average 256 attempts with 256 different random private keys before we find one that works as an IBAN-compatible "Direct" encoded ICAP address.

At this time, ICAP is unfortunately only supported by a few wallets.

Hex encoding with checksum in capitalization (EIP-55)

Due to the slow deployment of ICAP and name services, a standard was proposed by Ethereum Improvement Proposal 55 (EIP-55). You can read the details at: <https://github.com/Ethereum/EIPs/blob/master/EIPS/eip-55.md>

EIP-55 offers a backward-compatible checksum for Ethereum addresses by modifying the capitalization of the hexadecimal address. The idea is that Ethereum addresses are case-insensitive and all wallets

are supposed to accept Ethereum addresses expressed in capital or lower-case characters, without any difference in interpretation.

By modifying the capitalization of the alphabetic characters in the address, we can convey a checksum that can be used to protect the integrity of the address against typing or reading mistakes. Wallets that do not support EIP-55 checksums simply ignore the fact that the address contains mixed capitalization. But those that do support it, can validate it and detect errors with a 99.986% accuracy.

The mixed-caps encoding is subtle and you may not notice it at first. Our example address is:

```
0x001d3f1ef827552ae1114027bd3ecf1f086ba0f9
```

with an EIP-55 mixed-capitalization checksum it becomes:

```
0x001d3F1ef827552Ae1114027BD3ECF1f086bA0F9
```

Can you tell the difference? Some of the alphabetic (A-F) characters from the hexadecimal encoding alphabet are now capital, while others are lower case. You might not even have noticed the difference unless you looked carefully.

EIP-55 is quite simple to implement. We take the Keccak-256 hash of the lower-case hexadecimal address. This hash acts as a digital fingerprint of the address, giving us a convenient checksum. Any small change in the input (the address) should cause a big change in the resulting hash (the checksum), allowing us to detect errors effectively. The hash of our address is then encoded in the capitalization of the address itself. Let's break it down, step-by-step:

1. Hash the lower-case address, without the 0x prefix:

```
Keccak256("001d3f1ef827552ae1114027bd3ecf1f086ba0f9")
23a69c1653e4ebbb619b0b2cb8a9bad49892a8b9695d9a19d8f673ca991deae1
```

2. Capitalize each alphabetic address character if the corresponding hex digit of the hash is greater than or equal to 0x8. This is easier to show if we line up the address and the hash:

```
Address : 001d3f1ef827552ae1114027bd3ecf1f086ba0f9  
Hash    : 23a69c1653e4ebbb619b0b2cb8a9bad49892a8b9...
```

Our address contains an alphabetic character d in the fourth position. The fourth character of the hash is 6, which is less than 8. So, we leave the d lower-case. The next alphabetic character in our address is f, in the sixth position. The sixth character of the hexadecimal hash is c, which is greater than 8. Therefore, we capitalize the F in the address, and so on. As you can see, we only use the first 20-bytes (40 hex characters) of the hash as a checksum, since we only have 20-bytes (40 hex characters) in the address to capitalize appropriately.

Check the resulting mixed-captitals address yourself and see if you can tell which characters were capitalized and which characters they correspond to in the address hash:

```
Address : 001d3F1ef827552Ae1114027BD3ECF1f086bA0F9  
Hash    : 23a69c1653e4ebbb619b0b2cb8a9bad49892a8b9...
```

Detecting an error in an EIP-55 encoded address

Now, let's look at how EIP-55 addresses will help us find an error. Let's assume we have printed out an Ethereum address, which is EIP-55 encoded:

```
0x001d3F1ef827552Ae1114027BD3ECF1f086bA0F9
```

Now let's make a basic mistake in reading that address. The character before the last one is a capital "F". For this example let's assume we misread that as a capital "E". We type in the (incorrect address) into our wallet:

```
0x001d3F1ef827552Ae1114027BD3ECF1f086bA0E9
```

Fortunately, our wallet is EIP-55 compliant! It notices the mixed capitalization and attempts to validate the address. It converts it to lower case, and calculates the checksum hash:

```
Keccak256("001d3f1ef827552ae1114027bd3ecf1f086ba0e9")
5429b5d9460122fb4b11af9cb88b7bb76d8928862e0a57d46dd18dd8e08a6927
```

As you can see, even though the address has only changed by one character (in fact, only one bit as "e" and "f" are 1 bit apart), the hash of the address has changed radically. That's the property of hash functions that makes them so useful for checksums!

Now, let's line up the two and check the capitalization:

```
001d3F1ef827552Ae1114027BD3ECF1f086bA0E9
5429b5d9460122fb4b11af9cb88b7bb76d892886...
```

It's all wrong! Several of the alphabetic characters are incorrectly capitalized. Remember that the capitalization is the encoding of the *correct* checksum.

The capitalization of the address we input doesn't match the checksum just calculated, meaning something has changed in the address, and an error has been introduced.

Conclusions

In this chapter we had a brief survey of public key cryptography and focused on the use of public and private keys in Ethereum and the use of cryptographic tools, such as hash functions, in the creation and verification of Ethereum addresses. We also looked at digital signatures and how they can demonstrate ownership of a private key without revealing that private key. In [Wallets](#), we will put these ideas together and look at how wallets can be used to manage collections of keys.

Wallets

The word "wallet" is used to describe a few different things in Ethereum.

At a high level, a wallet is a software application that serves as the primary user interface to Ethereum. The wallet controls access to a user's money, managing keys and addresses, tracking the balance, and creating and signing transactions. In addition, some Ethereum wallets can also interact with contracts, such as ERC20 tokens.

More narrowly, from a programmer's perspective, the word *wallet* refers to the system used to store and manage a user's keys. Every wallet has a key management component. For some wallets, that's all there is. Other wallets are part of a much broader category, that of *browsers*, which are interfaces to Ethereum-based decentralized applications, or *DApps*, which we will examine in more detail in [Decentralized Applications \(DApps\)](#). There are no clear lines of distinction between the various categories that are conflated under the term *wallet*.

In this section we will look at wallets as containers for private keys, and as systems for managing these keys.

Wallet Technology Overview

In this section we summarize the various technologies used to construct user-friendly, secure, and flexible Ethereum wallets.

One key consideration in designing wallets is balancing convenience and privacy. The most convenient Ethereum wallet is one with a single private key and address that you re-use for everything. Unfortunately, such a solution is a privacy nightmare, as anyone can easily track and correlate all your transactions. Using a new key for every transaction is best for privacy, but becomes very difficult to manage. The correct balance is difficult to achieve, but that's why good wallet design is paramount.

A common misconception about Ethereum is that Ethereum wallets contain ether or tokens. In fact, very strictly speaking, the wallet holds only keys. The ether or other tokens are recorded on the Ethereum blockchain. Users control the tokens on the network by signing transactions with the keys in their wallets. In a sense, an Ethereum wallet is a *keychain*. Having said that, given that the keys held by the wallet are the only things that are needed to transfer ether or tokens to others, in practice this distinction is fairly irrelevant. Where the difference does matter is in changing one's mindset from dealing with the centralized system of conventional banking (where only you, and the bank, can see the

money in your account, and you only need convince the bank that you want to move funds to make a transaction) to the decentralized system of blockchain platforms (where everyone can see the ether balance of an account, although they probably don't know the account's owner, and everyone needs to be convinced the owner wants to move funds for a transaction to be enacted). In practice this means that there is an independent way to check an account's balance, without needing its wallet. Moreover, you can move your account handling from your current wallet to a different wallet, if you grow to dislike the wallet app you started out using.



Ethereum wallets contain keys, not ether or tokens. Wallets are like keychains containing pairs of private and public keys. Users sign transactions with the private keys, thereby proving they own the ether. The ether is stored on the blockchain.

There are two primary types of wallets, distinguished by whether the keys they contain are related to each other or not.

The first type is a *nondeterministic wallet*, where each key is independently generated from a different random number. The keys are not related to each other. This type of wallet is also known as a JBOK wallet from the phrase "Just a Bunch Of Keys".

The second type of wallet is a *deterministic wallet*, where all the keys are derived from a single master key, known as the *seed*. All the keys in this type of wallet are related to each other and can be generated again if one has the original seed. There are a number of different *key derivation* methods used in deterministic wallets. The most commonly-used derivation method uses a tree-like structure and is known as a *hierarchical deterministic* or *HD* wallet.

To make deterministic wallets slightly more secure against data-loss accidents, such as having your phone stolen, or dropping it in the toilet, the seeds are often encoded as a list of words (in English or another language) for you to write down and use in the event of an accident. Such a list is known as the wallet's *mnemonic code words*. Of course, if someone gets hold of your mnemonic code words, then they can also recreate your wallet and thus gain access to your ether and smart contracts. As such, be very, very careful with your recovery word list! Never store it electronically, in a file, on your computer or phone. Write it down on paper and store it in a safe and secure place.

The next few sections introduce each of these technologies at a high level.

Nondeterministic (Random) Wallets

In the first Ethereum wallet (produced for the Ethereum pre-sale), each wallet file stored a single

randomly-generated private key. Such wallets are being replaced with deterministic wallets because these "old style" wallets are in many ways inferior. For example, it is considered good practice to avoid Ethereum address reuse as part of maximizing your privacy while using Ethereum, i.e. to use a new address (which needs a new private key) every time you receive funds. You can go further and use a new address for each transaction, although this can get expensive if you deal a lot with tokens. To follow this practice, a nondeterministic wallet will need to regularly increase its list of keys, which means you will need to make regular backups. If you ever lose your data (disk failure, drink accident, phone stolen) before you've managed to back-up your wallet, you lose access to your funds and smart contracts. The "type 0" nondeterministic wallets are the hardest to deal with, because they create a new wallet file for every new address in a "just in time" manner.

Nevertheless, many Ethereum clients (including geth) use a *keystore* file, which is a JSON-encoded file that contains a single (randomly generated) private key, encrypted by a passphrase for extra security. The JSON file contents look like this:

```
{
  "address": "001d3f1ef827552ae1114027bd3ecf1f086ba0f9",
  "crypto": {
    "cipher": "aes-128-ctr",
    "ciphertext": "233a9f4d236ed0c13394b504b6da5df02587c8bf1ad8946f6f2b58f055507ece",
    "cipherparams": {
      "iv": "d10c6ec5bae81b6cb9144de81037fa15"
    },
    "kdf": "scrypt",
    "kdfparams": {
      "dklen": 32,
      "n": 262144,
      "p": 1,
      "r": 8,
      "salt": "99d37a47c7c9429c66976f643f386a61b78b97f3246adca89abe4245d2788407"
    },
    "mac": "594c8df1c8ee0ded8255a50caf07e8c12061fd859f4b7c76ab704b17c957e842"
  },
  "id": "4fcbb2ba4-ccdb-424f-89d5-26cce304bf9c",
  "version": 3
}
```

The keystore format uses a *Key Derivation Function (KDF)*, also known as a password stretching algorithm, which protects against brute-force, dictionary, and rainbow table attacks. In simple terms, the private key is not encrypted by the passphrase directly. Instead, the passphrase is *stretched*, by repeatedly hashing it. The hashing function is repeated for 262,144 rounds, which can be seen in the keystore JSON as the parameter `crypto.kdfparams.n`. An attacker trying to brute-force the passphrase would have to apply 262,144 rounds of hashing for every attempted passphrase, which slows down the attack sufficiently to make it infeasible for passphrases of sufficient complexity and length.

There are a number of software libraries that can read and write the keystore format, such as the JavaScript library `keythereum`:

<https://github.com/ethereumjs/keythereum>



The use of nondeterministic wallets is discouraged for anything other than simple tests. They are too cumbersome to back up and use for anything but the most basic of situations. Instead, use an industry-standard-based HD wallet with a mnemonic seed for backup.

Deterministic (Seeded) Wallets

Deterministic or "seeded" wallets are wallets that contain private keys that are all derived from a single *seed*. The seed is a randomly-generated number that is combined with other data, such as an index number or "chain code" (see [HD Wallets \(BIP-32/BIP-44\)](#)), to derive any number of private keys. In a deterministic wallet, the seed is sufficient to recover all the derived keys, and therefore a single backup, at creation time, is sufficient to secure all the funds and smart contract access of the wallet. The seed is also sufficient for a wallet export or import, allowing for easy migration of all the keys between different wallet implementations. This design also makes the security of the seed of upmost importance, as only the seed is needed to gain access to the entire wallet. On the other hand, being able to focus security efforts on a single piece of data can be seen as an advantage.

HD Wallets (BIP-32/BIP-44)

Deterministic wallets were developed to make it easy to derive many keys from a single seed. Currently, the most advanced form of deterministic wallets is the hierarchical deterministic (HD) wallet defined by Bitcoin's BIP-32 standard. HD wallets contain keys derived in a tree structure, such that a parent key can derive a sequence of child keys, each of which can derive a sequence of grandchild keys, and so on. This tree structure is illustrated in [HD wallet: a tree of keys generated from a single seed](#).

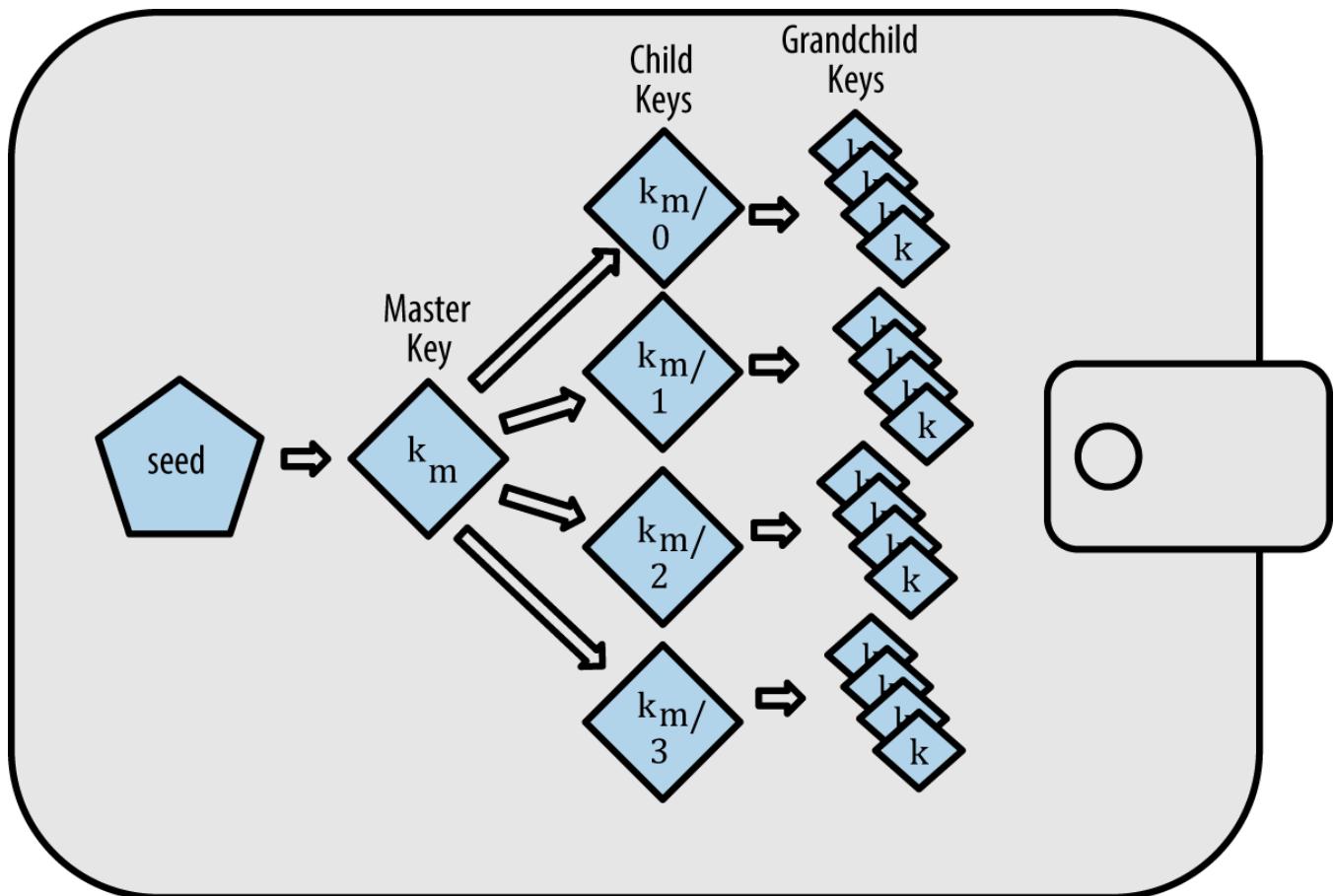


Figure 29. HD wallet: a tree of keys generated from a single seed

HD wallets offer several advantages over simpler deterministic wallets:

First, the tree structure can be used to express additional organizational meaning, such as when a specific branch of subkeys is used to receive incoming payments and a different branch is used to receive change from outgoing payments. Branches of keys can also be used in corporate settings, allocating different branches to departments, subsidiaries, specific functions, or accounting categories.

The second advantage of HD wallets is that users can create a sequence of public keys without having access to the corresponding private keys. This allows HD wallets to be used on an insecure server or in a watch-only or receive-only capacity, where the wallet doesn't have the private keys that can spend the funds.

Seeds and Mnemonic Codes (BIP-39)

There are many ways to encode a private key for secure back-up and retrieval. The currently preferred method is using a sequence of words, which, when taken together in the correct order, can uniquely recreate the private key. This is sometimes known as a *mnemonic*, and the approach has been standardized by BIP-39. Today, many Ethereum wallets (as well as wallets for other cryptocurrencies) use this standard, and can import and export seeds for backup and recovery using interoperable mnemonics.

To see why this approach has become popular, let's have a look at an example:

A seed for a deterministic wallet, in hex

```
FCCF1AB3329FD5DA3DA9577511F8F137
```

A seed for a deterministic wallet, from a 12-word mnemonic

```
wolf juice proud gown wool unfair  
wall cliff insect more detail hub
```

In practical terms, the chance of an error when writing down the hex sequence is unacceptably high. In contrast, the list of known words is quite easy to deal with, mainly because there is a high level of redundancy in the writing of words, especially English words. If "insect" had been recorded by accident, it could quickly be determined, upon the need for wallet recovery, that "insect" is not a valid English word and that "insect" should be used instead. We are talking about writing down a representation of the seed because that is good practice when managing HD wallets: the seed is needed to recover a wallet in the case of data loss (whether through accidents or theft) and so a backup is very prudent. However, the seed must be kept extremely private, and so digital back-ups should be carefully avoided; hence the advice to back up with pen and paper.

In summary, the use of a recovery word list to encode the seed for an HD wallet makes for the easiest way to safely export, transcribe, record on paper, read without error, and import a private key set into another wallet.

Wallet Best Practices

As cryptocurrency wallet technology has matured, certain common industry standards have emerged

that make wallets broadly interoperable, easy to use, secure, and flexible. These standards also allow wallets to derive keys for multiple different cryptocurrencies, all from a single mnemonic. These common standards are:

- Mnemonic code words, based on BIP-39
- HD wallets, based on BIP-32
- Multipurpose HD wallet structure, based on BIP-43
- Multicurrency and multiaccount wallets, based on BIP-44

These standards may change or may be obsoleted by future developments, but for now they form a set of interlocking technologies that have become the *de facto* wallet standard for most blockchain platforms and their cryptocurrencies.

The standards have been adopted by a broad range of software and hardware wallets, making all these wallets interoperable. A user can export a mnemonic generated in one of these wallets and import it to another wallet, recovering all keys and addresses.

Some examples of software wallets supporting these standards include (listed alphabetically) Jaxx, MetaMask, MyCrypto, and MyEtherWallet (MEW). Examples of hardware wallets supporting these standards include (listed alphabetically) Keepkey, Ledger, and Trezor.

The following sections examine each of these technologies in detail.



If you are implementing an Ethereum wallet, it should be built as an HD wallet, with a seed encoded as a mnemonic code for backup, following the BIP-32, BIP-39, BIP-43, and BIP-44 standards, as described in the following sections.

Mnemonic Code Words (BIP-39)

Mnemonic code words are word sequences that encode a random number used as a seed to derive a deterministic wallet. The sequence of words is sufficient to recreate the seed, and from there recreate the wallet and all the derived keys. A wallet application that implements deterministic wallets with mnemonic words will show the user a sequence of 12 to 24 words when first creating a wallet. That sequence of words is the wallet backup, and can be used to recover and recreate all the keys in the same or any compatible wallet application. As we explained above, mnemonic word lists make it easier for users to back up wallets, because they are easy to read and correctly transcribe.



Mnemonic words are often confused with "brainwallets". They are not the same. The primary difference is that a brainwallet consists of words chosen by the user, whereas mnemonic words are created randomly by the wallet and presented to the user. This important difference makes mnemonic words much more secure, because humans are very poor sources of randomness. Perhaps more importantly, using the term "brainwallet" suggests that the words have to be memorized, which is a terrible idea, and a recipe for not having your backup when you need it.

Mnemonic codes are defined in BIP-39. Note that BIP-39 is one implementation of a mnemonic code standard. There is a different standard, *with a different set of words*, used by the Electrum Bitcoin wallet and predating BIP-39. BIP-39 was proposed by the company behind the Trezor hardware wallet and is incompatible with Electrum's implementation. However, BIP-39 has now achieved broad industry support across dozens of interoperable implementations and should be considered the *de facto* industry standard. Furthermore, BIP-39 can be used to produce multicurrency wallets supporting Ethereum, whereas Electrum seeds cannot.

BIP-39 defines the creation of a mnemonic code and seed, which we describe here in nine steps. For clarity, the process is split into two parts: steps 1 through 6 are shown in [Generating mnemonic words](#) and steps 7 through 9 are shown in [From mnemonic to seed](#).

Generating mnemonic words

Mnemonic words are generated automatically by the wallet using the standardized process defined in BIP-39. The wallet starts from a source of entropy, adds a checksum, and then maps the entropy to a word list:

1. Create a cryptographically random sequence S of 128 to 256 bits.
2. Create a checksum of S by taking the first $\text{length-of-S} \div 32$ bits of the SHA256 hash of S.
3. Add the checksum to the end of the random sequence S.
4. Divide the sequence-and-checksum concatenation into sections of 11 bits.
5. Map each 11 bit value to a word from the predefined dictionary of 2048 words.
6. The mnemonic code is the sequence of words, maintaining the order.

[Generating entropy and encoding as mnemonic words](#) shows how entropy is used to generate mnemonic words.

Mnemonic Words 128-bit entropy/12-word example

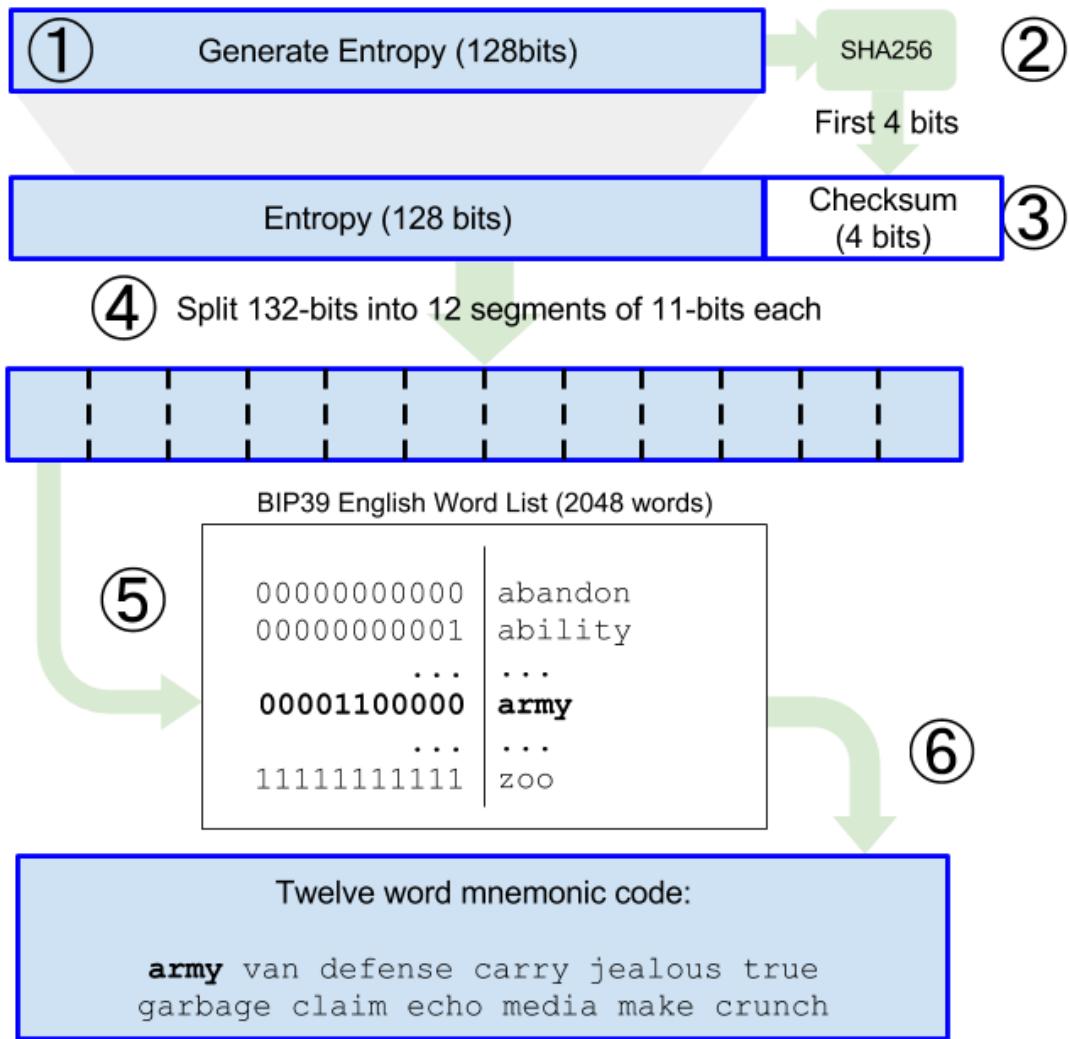


Figure 30. Generating entropy and encoding as mnemonic words

[Mnemonic codes: entropy and word length](#) shows the relationship between the size of the entropy data and the length of mnemonic codes in words.

Table 2. Mnemonic codes: entropy and word length

Entropy (bits)	Checksum (bits)	Entropy + checksum (bits)	Mnemonic length (words)
128	4	132	12
160	5	165	15
192	6	198	18
224	7	231	21
256	8	264	24

From mnemonic to seed

The mnemonic words represent entropy with a length of 128 to 256 bits. The entropy is then used to derive a longer (512-bit) seed through the use of the key-stretching function PBKDF2. The seed produced is then used to build a deterministic wallet and derive its keys.

The key-stretching function takes two parameters: the mnemonic and a *salt*. The purpose of a salt in a key-stretching function is to make it difficult to build a lookup table enabling a brute-force attack. In the BIP-39 standard, the salt has another purpose: it allows the introduction of a passphrase that serves as an additional security factor protecting the seed, as we will describe in more detail in [Optional passphrase in BIP-39](#).

The process described in steps 7 through 9 continues from the process described previously in [Generating mnemonic words](#):

7. The first parameter to the PBKDF2 key-stretching function is the *mnemonic* produced in step 6.
8. The second parameter to the PBKDF2 key-stretching function is a *salt*. The salt is composed of the string constant "mnemonic" concatenated with an optional user-supplied passphrase.
9. PBKDF2 stretches the mnemonic and salt parameters using 2048 rounds of hashing with the HMAC-SHA512 algorithm, producing a 512-bit value as its final output. That 512-bit value is the seed.

[From mnemonic to seed](#) shows how a mnemonic is used to generate a seed.

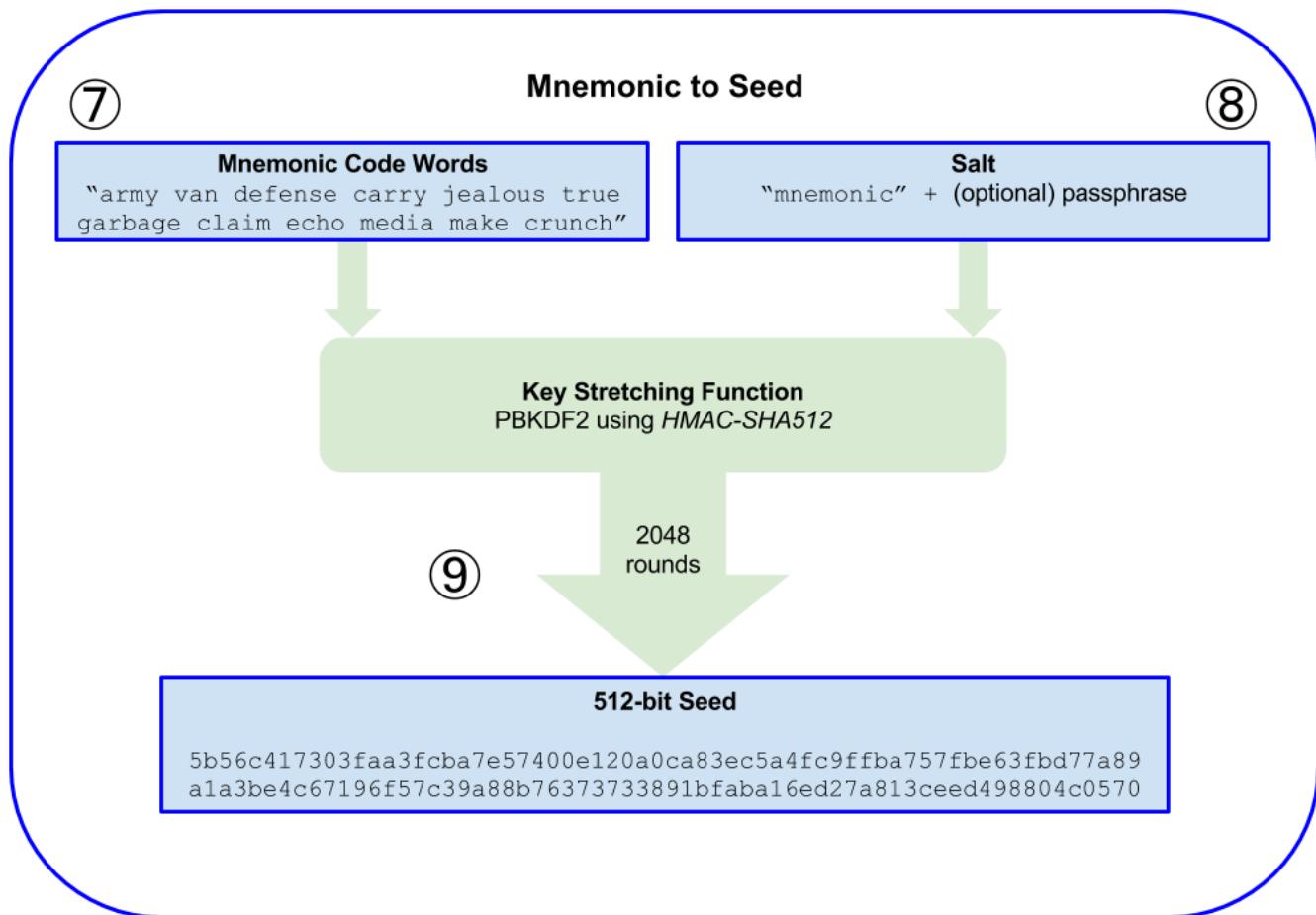


Figure 31. From mnemonic to seed



The key-stretching function, with its 2048 rounds of hashing, is a somewhat effective protection against brute-force attacks against the mnemonic or the passphrase. It makes it costly (in computation) to try more than a few thousand passphrase and mnemonic combinations, while the number of possible derived seeds is vast (2^{512} , or about 10^{154}), far bigger than the number of atoms in the visible universe (about 10^{80}).

Tables [128-bit entropy mnemonic code, no passphrase, resulting seed](#), [128-bit entropy mnemonic code, with passphrase, resulting seed](#), and [256-bit entropy mnemonic code, no passphrase, resulting seed](#) show some examples of mnemonic codes and the seeds they produce.

Table 3. 128-bit entropy mnemonic code, no passphrase, resulting seed

Entropy input (128 bits)	0c1e24e5917779d297e14d45f14e1a1a
Mnemonic (12 words)	army van defense carry jealous true garbage claim echo media make crunch
Passphrase	(none)
Seed (512 bits)	5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fdbd77a89a1a3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0570

Table 4. 128-bit entropy mnemonic code, with passphrase, resulting seed

Entropy input (128 bits)	0c1e24e5917779d297e14d45f14e1a1a
Mnemonic (12 words)	army van defense carry jealous true garbage claim echo media make crunch
Passphrase	SuperDuperSecret
Seed (512 bits)	3b5df16df2157104cfdd22830162a5e170c0161653e3afe6c88defefb0818c793dbb28ab3ab091897d0715861dc8a18358f80b79d49acf64142ae57037d1d54

Table 5. 256-bit entropy mnemonic code, no passphrase, resulting seed

Entropy input (256 bits)	2041546864449caff939d32d574753fe684d3c947c3346713dd8423e74abcf8c
Mnemonic (24 words)	cake apple borrow silk endorse fitness top denial coil riot stay wolf luggage oxygen faint major edit measure invite love trap field dilemma oblige
Passphrase	(none)
Seed (512 bits)	3269bce2674acbd188d4f120072b13b088a0ecf87c6e4cae41657a0bb78f5315b33b3a04356e53d062e55f1e0deaa082df8d487381379df848a6ad7e98798404

Optional passphrase in BIP-39

The BIP-39 standard allows the use of an optional passphrase in the derivation of the seed. If no passphrase is used, the mnemonic is stretched with a salt consisting of the constant string "mnemonic", producing a specific 512-bit seed from any given mnemonic. If a passphrase is used, the stretching function produces a *different* seed from that same mnemonic. In fact, given a single mnemonic, every possible passphrase leads to a different seed. Essentially, there is no "wrong" passphrase. All

passphrases are valid and they all lead to different seeds, forming a vast set of possible uninitialized wallets. The set of possible wallets is so large (2^{512}) that there is no practical possibility of brute-forcing or accidentally guessing one that is in use, as long as the passphrase has sufficient complexity and length.



There are no "wrong" passphrases in BIP-39. Every passphrase leads to some wallet, which unless previously used will be empty.

The optional passphrase creates two important features:

- A second factor (something memorized) that makes a mnemonic useless on its own, protecting mnemonic backups from compromise by a thief.
- A form of plausible deniability or "duress wallet," where a chosen passphrase leads to a wallet with a small amount of funds used to distract an attacker from the "real" wallet that contains the majority of funds.

However, it is important to note that the use of a passphrase also introduces the risk of loss:

- If the wallet owner is incapacitated or dead and no-one else knows the passphrase, the seed is useless and all the funds stored in the wallet are lost forever.
- Conversely, if the owner backs up the passphrase in the same place as the seed, it defeats the purpose of a second factor.

While passphrases are very useful, they should only be used in combination with a carefully planned process for backup and recovery, considering the possibility of surviving the owner and allowing their heirs to recover the cryptocurrency.

Working with mnemonic codes

BIP-39 is implemented as a library in many different programming languages:

[python-mnemonic](https://github.com/trezor/python-mnemonic) [<https://github.com/trezor/python-mnemonic>]

The reference implementation of the standard by the SatoshiLabs team that proposed BIP-39, in Python

[ConsenSys/eth-lightwallet](https://github.com/ConsenSys/eth-lightwallet) [<https://github.com/ConsenSys/eth-lightwallet>]

Lightweight JS Ethereum Wallet for nodes and browser (with BIP-39)

[npm/bip39](https://www.npmjs.com/package/bip39) [https://www.npmjs.com/package/bip39]

JavaScript implementation of Bitcoin BIP-39: Mnemonic code for generating deterministic keys

There is also a BIP-39 generator implemented in a standalone webpage, which is extremely useful for testing and experimentation. [A BIP-39 generator as a standalone web page](https://iancoleman.github.io/bip39/) shows a standalone web page that generates mnemonics, seeds, and extended private keys.

Mnemonic

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect, since the words require a particular structure (the last word is a checksum)

For more info see the [BIP39 spec](#)

Generate

a random

12

word mnemonic, or enter your own below.

BIP39 Mnemonic	army van defense carry jealous true garbage claim echo media make crunch
BIP39 Passphrase (optional)	
BIP39 Seed	5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fb77a89a1a3be4c6719 6f57c39a88b76373733891bfaba16ed27a813ceed498804c0570
Coin	Bitcoin
BIP32 Root Key	xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6 i6ddYjb5PLtUdMZn8LhvuCVhGcQntq5rn7JVMqnie

Figure 32. A BIP-39 generator as a standalone web page

The page (<https://iancoleman.github.io/bip39/>) can be used offline in a browser, or accessed online.

Creating an HD Wallet from the Seed

HD wallets are created from a single *root seed*, which is a 128-, 256-, or 512-bit random number. Most

commonly, this seed is generated from a *mnemonic* as detailed in the previous section.

Every key in the HD wallet is deterministically derived from this root seed, which makes it possible to re-create the entire HD wallet from that seed in any compatible HD wallet. This makes it easy to export, back up, restore, and import HD wallets containing thousands or even millions of keys by transferring just the mnemonic from which the root seed is derived.

Hierarchical Deterministic Wallets (BIP-32) and paths (BIP-43/44)

Most HD wallets follow the BIP-32 standard, which has become a *de facto* industry standard for deterministic key generation. You can read the detailed specification in:

<https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>

We won't be discussing the details of BIP-32 here, only the components necessary to understand how it is used in wallets. The main important aspect is the tree-like hierarchical relationships that it is possible for the derived keys to have, as you can see in [HD wallet: a tree of keys generated from a single seed](#). We will also need to understand the idea of *extended keys* and *hardened keys*, which are explained in the following sections.

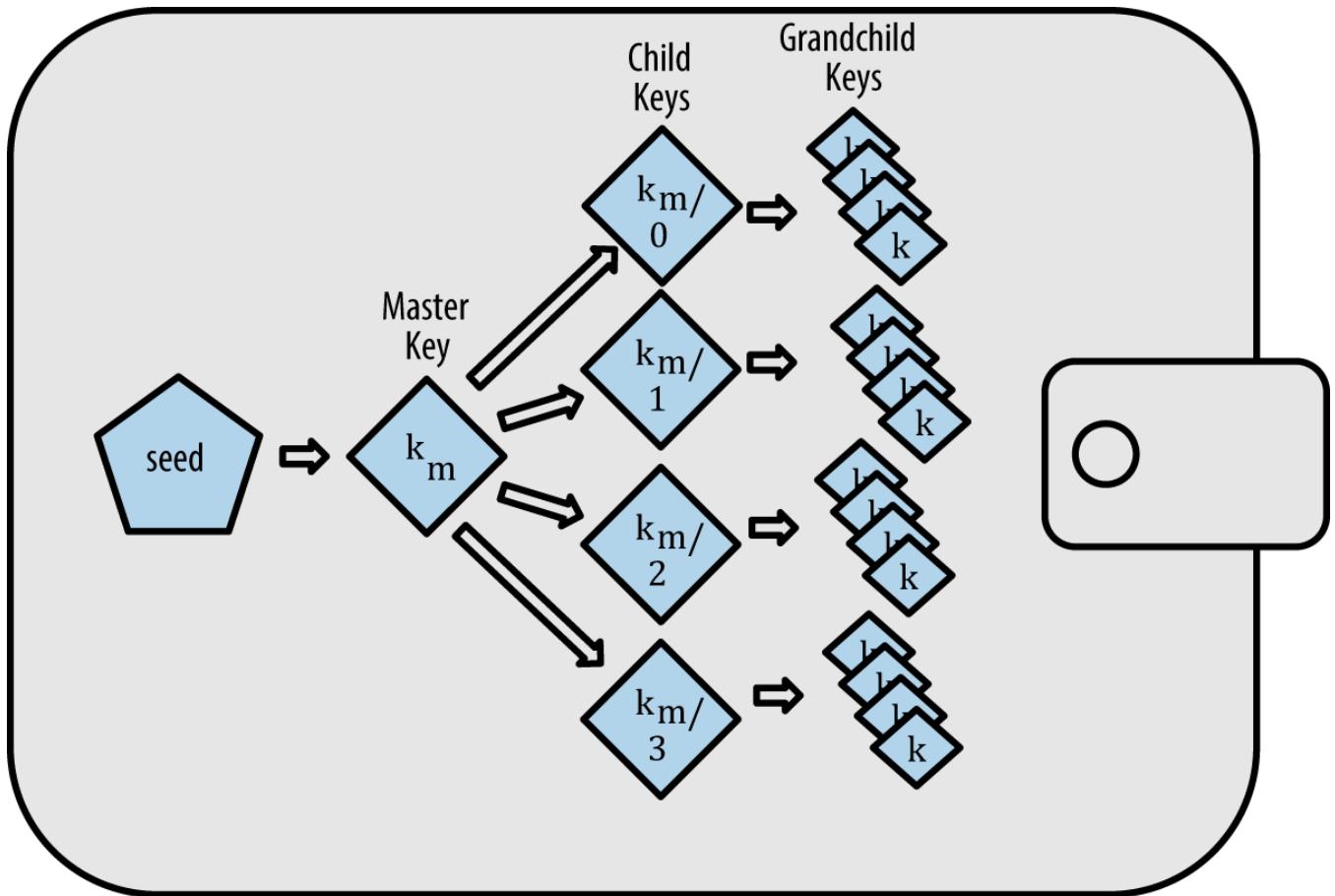


Figure 33. HD wallet: a tree of keys generated from a single seed

There are dozens of interoperable implementations of BIP-32 offered in many software libraries:

[Consensys/eth-lightwallet](https://github.com/ConsenSys/eth-lightwallet) [<https://github.com/ConsenSys/eth-lightwallet>]

Lightweight JS Ethereum Wallet for nodes and browser (with BIP-32)

There is also a BIP-32 standalone web page generator that is very useful for testing and experimentation with BIP-32:

<http://bip32.org/>



The standalone BIP-32 generator is not an HTTPS site. That's to remind you that the use of this tool is not secure. It is only for testing. You should not use the keys produced by this site with real funds.

Extended public and private keys

In BIP-32 terminology, keys can be "extended" so that they can produce "children". In this way, keys become *extended keys*. With the right mathematical operations, extended "parent" keys can be used to derive "child" keys and thus produce the hierarchy of keys and addresses described earlier in this chapter. A parent key doesn't have to be at the top of the tree. They can be picked out from anywhere in the tree hierarchy. Extending a key involves taking the key itself and appending a special *chain code* to it. A chain code is a 256 bit binary string that is mixed with each key to produce child keys.

If the key is a private key, it is an *extended private key* distinguished by the prefix *xprv*:

```
xprv9s21ZrQH143K2JF8RafpqtKiTbsbaxEeUaMnNHsm5o6wCW3z8ySyH4UxFVSfZ8n7ESu7f  
gir8imbZKLYVBxFPND1pniTZ81vKfd45EHKX73
```

An *extended public key* is distinguished by the prefix *xpub*:

```
xpub661MyMwAqRbcEnKbXcCqD2GT1di5zQxVqoHPAgHNe8dv5JP8gWmDroS6kFHJnLZd23tW  
evhdn4urGJ6b264DfTGKr8zjmYDjyDTi9U7iyT
```

A very useful characteristic of HD wallets is the ability to derive child public keys from parent public keys, *without* having the private keys. This gives us two ways to derive a child public key: either directly from the child private key, or from the parent public key.

An extended public key can be used, therefore, to derive all of the *public* keys (and only the public keys) in that branch of the HD wallet structure.

This shortcut can be used to create very secure public key–only deployments, where a server or application has a copy of an extended public key, but no private keys whatsoever. That kind of deployment can produce an infinite number of public keys and Ethereum addresses, but cannot spend any of the money sent to those addresses. Meanwhile, on another, more secure server, the extended private key can derive all the corresponding private keys to sign transactions and spend the money.

One common application of this method is to install an extended public key on a web server that serves an e-commerce application. The web server can use the public key derivation function to create a new Ethereum address for every transaction (e.g., for a customer shopping cart). The web server will not have any private keys that would be vulnerable to theft. Without HD wallets, the only way to do this is to generate thousands of Ethereum addresses on a separate secure server and then preload them on the e-commerce server. That approach is cumbersome and requires constant maintenance to ensure that the e-commerce server doesn't run out of keys. Hence the preference to use extended public keys from HD wallets.

Another common application of this solution is for cold-storage or hardware wallets. In that scenario, the extended private key can be stored in a hardware wallet, while the extended public key can be kept online. The user can create "receive" addresses at will, while the private keys are safely stored offline. To spend the funds, the user can use the extended private key in an offline signing Ethereum client, or sign transactions on the hardware wallet device.

Hardened child key derivation

The ability to derive a branch of public keys from an xpub (extended public key) is very useful, but it comes with a potential risk. Access to an xpub does not give access to child private keys. However, because the xpub contains the chain code (used to derive child public keys from the parent public key), if a child private key is known, or somehow leaked, it can be used with the chain code to derive all the other child private keys. A single leaked child private key, together with a parent chain code, reveals all the private keys of all the children. Worse, the child private key together with a parent chain code can be used to deduce the parent private key.

To counter this risk, HD wallets use an alternative derivation function called *hardened derivation*, which "breaks" the relationship between parent public key and child chain code. The hardened derivation function uses the parent private key to derive the child chain code, instead of the parent public key. This creates a "firewall" in the parent/child sequence, with a chain code that cannot be used to compromise a parent or sibling private key.

In simple terms, if you want to use the convenience of an xpub to derive branches of public keys, without exposing yourself to the risk of a leaked chain code, you should derive it from a hardened parent, rather than a normal parent. Best practice is to have the level-1 children of the master keys always derived by hardened derivation, to prevent compromise of the master keys.

Index numbers for normal and hardened derivation

It is clearly desirable to be able to derive more than one child key from a given parent key. To manage this, an index number is used. Each index number, when combined with a parent key using the special child derivation function, gives a different child key. The index number used in the BIP-32 parent-to-child derivation function is a 32-bit integer. To easily distinguish between keys derived through the normal (unhardened) derivation function versus keys derived through hardened derivation, this index number is split into two ranges. Index numbers between 0 and 2^{31} ;1 (0x0 to 0xFFFFFFFF) are used *only* for normal derivation. Index numbers between 2^{31} and 2^{32} ;1 (0x80000000 to 0xFFFFFFFF) are used *only* for hardened derivation. Therefore, if the index number is less than 2^{31} , the child is normal, whereas if the index number is equal or above 2^{31} , the child is hardened.

To make the index number easier to read and display, the index number for hardened children is displayed starting from zero, but with a prime symbol. The first normal child key is therefore displayed as 0, whereas the first hardened child (index 0x80000000) is displayed as 0';. In sequence then, the second hardened key would have index 0x80000001 and would be displayed as 1';, and so on. When you see an HD wallet index i';, that means $2^{31} + i$.

HD wallet key identifier (path)

Keys in an HD wallet are identified using a "path" naming convention, with each level of the tree separated by a slash (/) character (see [HD wallet path examples](#)). Private keys derived from the master private key start with "m". Public keys derived from the master public key start with "M". Therefore, the first child private key of the master private key is m/0. The first child public key is M/0. The second grandchild of the first child is m/0/1, and so on.

The "ancestry" of a key is read from right to left, until you reach the master key from which it was derived. For example, identifier m/x/y/z describes the key that is the z-th child of key m/x/y, which is the y-th child of key m/x, which is the x-th child of m.

Table 6. HD wallet path examples

HD path	Key described
m/0	The first (0) child private key from the master private key (m)
m/0/0	The first grandchild private key of the first child (m/0)

HD path	Key described
m/0'/0	The first normal grandchild of the first <i>hardened</i> child (m/0')
m/1/0	The first grandchild private key of the second child (m/1)
M/23/17/0/0	The first great-great-grandchild public key of the first great-grandchild of the 18th grandchild of the 24th child

Navigating the HD wallet tree structure

The HD wallet tree structure is tremendously flexible. The flip side of this is that it also allows for unbounded complexity: each parent extended key can have 4 billion children: 2 billion normal children and 2 billion hardened children. Each of those children can have another 4 billion children, and so on. The tree can be as deep as you want, with a potentially infinite number of generations. With all that potential, therefore, it can become quite difficult to navigate these very large trees.

Two BIPs offer a way to manage this potential complexity by creating standards for the structure of HD wallet trees. BIP-43 proposes the use of the first hardened child index as a special identifier that signifies the "purpose" of the tree structure. Based on BIP-43, an HD wallet should use only one level-1 branch of the tree, with the index number defining its purpose of the wallet by identifying the structure and namespace of the rest of the tree. More specifically, an HD wallet using only branch m/i $\cdot\cdot\cdot$ /… is intended to signify a specific purpose and that purpose is identified by index number "i".

Extending that specification, BIP-44 proposes a multi-currency multi-account structure signified by setting the "purpose" number to 44'. All HD wallets following the BIP-44 structure are identified by the fact that they only used one branch of the tree: m/44'/*.

BIP-44 specifies the structure as consisting of five predefined tree levels:

```
m / purpose' / coin_type' / account' / change / address_index
```

The first-level "purpose" is always set to 44'. The second-level "coin_type" specifies the type of cryptocurrency coin, allowing for multicurrency HD wallets where each currency has its own subtree under the second level. There are several currencies defined in a standards document, called SLIP0044:

<https://github.com/satoshilabs/slips/blob/master/slip-0044.md>

A few examples: Ethereum is m/44"/60"/, Ethereum Classic is m/44"/61"/, Bitcoin is m/44"/0"/, and Testnet for all currencies is m/44"/1"/.

The third level of the tree is "account," which allows users to subdivide their wallets into separate logical subaccounts, for accounting or organizational purposes. For example, an HD wallet might contain two Ethereum "accounts": m/44"/60"/0"/ and m/44"/60"/1"/. Each account is the root of its own subtree.

Because BIP-44 was created originally for Bitcoin, it contains a "quirk" that isn't relevant in the Ethereum world. On the fourth level of the path, "change", an HD wallet has two subtrees: one for creating receiving addresses and one for creating change addresses. Only the "receive" path is used in Ethereum, as there is no necessity for a change address like there is in Bitcoin. Note that whereas the previous levels used hardened derivation, this level uses normal derivation. This is to allow the account level of the tree to export extended public keys for use in a non-secured environment. Usable addresses are derived by the HD wallet as children of the fourth level, making the fifth level of the tree the "address_index". For example, the third receiving address for Ethereum payments in the primary account would be M/44"/60"/0"/0/2. [BIP-44 HD wallet structure examples](#) shows a few more examples.

Table 7. BIP-44 HD wallet structure examples

HD path	Key described
M/44"/60"/0"/0/2	The third receiving public key for the primary Ethereum account
M/44"/0"/3"/1/14	The fifteenth change-address public key for the fourth Bitcoin account
m/44"/2"/0"/0/1	The second private key in the Litecoin main account, for signing transactions

Conclusions

Wallets are the foundation of any user-facing blockchain application. They allow users to manage collections of keys and addresses. Wallets also allow users to demonstrate their ownership of ether, and authorize transactions, by applying digital signatures as we will see in [Transactions](#), next.

Transactions

Transactions are signed messages originated by an externally owned account, transmitted by the Ethereum network, and recorded on the Ethereum blockchain. This basic definition conceals a lot of surprising and fascinating details. Another way to look at transactions is that they are the only thing that can trigger a change of state, or cause a contract to execute in the EVM. Ethereum is a global singleton state machine, and transactions are the only thing that can make that state machine "tick", changing its state. Contracts don't run on their own. Ethereum doesn't run autonomously. Everything starts with a transaction.

In this chapter, we will dissect transactions, show how they work, and understand the details. Note that much of this chapter is addressed to those who are interested in managing their own transactions at a low level, e.g. because they are writing a wallet app; you don't have to worry about this if you are happy using existing wallet applications, although you may find the details interesting!

The Structure of a Transaction

First let's take a look at the basic structure of a transaction, as it is serialized and transmitted on the Ethereum network. Each client and application that receives a serialized transaction will store it in-memory using its own internal data structure, perhaps embellished with metadata that doesn't exist in the network serialized transaction itself. The network serialization is the only standard form of a transaction.

A transaction is a serialized binary message that contains the following data:

nonce

A sequence number, issued by the originating EOA, used to prevent message replay.

gas price

The price of gas (in wei) the originator is willing to pay.

gas limit

The maximum amount of gas the originator is willing to buy for this transaction.

to

Destination Ethereum address.

value

Amount of ether to send to the destination.

data

Variable length binary data payload.

v,r,s

The three components of an ECDSA digital signature of the originating EOA.

The transaction message's structure is serialized using the Recursive Length Prefix (RLP) encoding scheme, which was created specifically for simple, byte-perfect data serialization in Ethereum. All numbers in Ethereum are encoded as big-endian integers, of lengths that are multiples of 8 bits.

Note that the field labels ("to", "gas limit", etc.) are shown here for clarity, but are not part of the transaction serialized data, which contains the field values RLP-encoded. In general, RLP does not contain any field delimiters or labels. RLP's length prefix is used to identify the length of each field. Anything beyond the defined length, therefore, belongs to the next field in the structure.

While this is the actual transaction structure transmitted, most internal representations and user interface visualizations embellish this with additional information, derived from the transaction or from the blockchain.

For example, you may notice there is no "from" data in the address identifying the originator EOA. That is because the EOA's public key can be derived from the v,r,s components of the ECDSA signature. The address can, in turn, be derived from the public key. When you see a transaction showing a "from" field, that was added by the software used to visualize the transaction. Other metadata frequently added to the transaction by client software include the block number (once it is mined and included in the blockchain) and a transaction ID (calculated hash). Again, this data is derived from the transaction, and does not form part of the transaction message itself.

The transaction nonce

The nonce is one of the most important and least understood components of a transaction. The definition in the Yellow Paper (see [Further references](#)) reads:

nonce: A scalar value equal to the number of transactions sent from this address or, in the case of accounts with associated code, the number of contract-creations made by this account.

Strictly speaking, the nonce is an attribute of the originating address, i.e. it only has meaning in the context of the sending address. However, the nonce is not stored explicitly as part of an account's state on the blockchain. Instead it is calculated dynamically, by counting the number of confirmed transactions that have originated from an address.

There are two scenarios where the existence of a transaction-counting nonce is important: the usability feature of transactions being included in the order of creation, and the vital feature of transaction duplication protection. Let's look at an example scenario for each of these:

1. Imagine you wish to make two transactions. You have an important payment to make of 6 ether, and also another payment of 8 ether. You sign and broadcast the 6 ether transaction first, because it is the more important one, and then you sign and broadcast the second, 8 ether transaction. Sadly, you have overlooked the fact that your account contains only 10 ether, so the network can't accept both transactions: one of them will fail. Because you sent the more important 6 ether one first, you understandably expect that one to go through and the 8 ether one to be rejected. However, in a decentralized system like Ethereum, nodes may receive the transactions in either order; there is no guarantee that a particular node will have one transaction propagated to it before the other. As such, it will almost certainly be the case that some nodes receive the 6 ether transaction first and others receive the 8 ether transaction first. Without the nonce, it would be random as to which one gets accepted and which rejected. However, with the nonce included, the first transaction you sent will have a nonce of, let's say 3, while the 8 ether transaction has the next nonce value, i.e. 4, and so will be ignored until the transactions with nonces from 0 to 3 have been processed, even if the 8 ether transaction is received first. Phew!
2. Now imagine you have an account with 100 ether. Fantastic! You find someone online who will accept payment in ether for a mcguffin-widget that you really want to buy. You send them 2 ether and they send you the mcguffin-widget. Lovely. To make that 2 ether payment, you signed a transaction sending 2 ether from your account to their account, and then broadcast it to the Ethereum network to be verified and included on the blockchain. Now, without a nonce value in the transaction, a second transaction sending 2 ether to the same address a second time will look exactly the same as the first transaction. This would mean that anyone who saw your transaction on the Ethereum network (which means everyone, including the recipient, or your enemies) can "replay" the transaction again and again and again until all your ether is gone simply by copy-

pasting your original transaction and resending it to the network. However, with the nonce value included in the transaction data, *every single transaction is unique*, even when sending the same amount of ether to the send recipient address multiple times. This means that by having the incrementing nonce as part of the transaction it is simply not possible for anyone to "duplicate" a payment you have made.

In summary, it is important to note that the use of the nonce is actually vital for an *account-based* protocol, in contrast to the "UTXO" mechanism of the Bitcoin protocol.

Keeping track of nonces

In practical terms, the nonce is an up-to-date count of the number of *confirmed* (i.e. on-chain) transactions that have originated from an account. To find out what the nonce is, you can interrogate the blockchain, for example via the web3 interface. Open a Javascript console in a browser with MetaMask running, or use the truffle console command to access the Javascript web3 library, then type:

```
web3.eth.getTransactionCount("0x9e713963a92c02317a681b9bb3065a8249de124f")
)
40
```



The nonce is a zero-based counter, meaning the first transaction has nonce 0. In the example above, we have a transaction count of 40, meaning nonces 0 through 39 have been seen. The next transaction's nonce will need to be 40.

Your wallet will keep track of nonces for each address it manages. It's fairly simple to do that, as long as you are only originating transactions from a single point. Let's say you are writing your own wallet software or some other application that originates transactions. How do you track nonces?

When you create a new transaction, you assign the next nonce in the sequence. But until it is confirmed, it will not count towards the getTransactionCount total.



Be careful when using the getTransactionCount function for counting pending transactions, because you might run into some problems if you send a few transactions in a row.

Let's look at an example:

```

web3.eth.getTransactionCount("0x9e713963a92c02317a681b9bb3065a8249de124f"
, "pending")
40
web3.eth.sendTransaction({from: web3.eth.accounts[0], to:
"0xB0920c523d582040f2BCB1bD7FB1c7C1ECEbdB34", value: web3.toWei(0.01,
"ether")});
web3.eth.getTransactionCount("0x9e713963a92c02317a681b9bb3065a8249de124f"
, "pending")
41
web3.eth.sendTransaction({from: web3.eth.accounts[0], to:
"0xB0920c523d582040f2BCB1bD7FB1c7C1ECEbdB34", value: web3.toWei(0.01,
"ether")});
web3.eth.getTransactionCount("0x9e713963a92c02317a681b9bb3065a8249de124f"
, "pending")
41
web3.eth.sendTransaction({from: web3.eth.accounts[0], to:
"0xB0920c523d582040f2BCB1bD7FB1c7C1ECEbdB34", value: web3.toWei(0.01,
"ether")});
web3.eth.getTransactionCount("0x9e713963a92c02317a681b9bb3065a8249de124f"
, "pending")
41

```

As you can see, the first transaction we sent increased the transaction count to 41, showing the pending transaction. But when we sent 3 more transactions in quick succession, the `getTransactionCount` call didn't count them. It only counted one, even though you might expect there to be 3 pending in the mempool. If we wait a few seconds to allow for network communications to settle down, the `getTransactionCount` call will return the expected number. But in the interim, while there are more than one transactions pending, it might not help us.

When you build an application that constructs transactions, it cannot rely on `getTransactionCount` for pending transactions. Only when pending and confirmed are equal (all outstanding transactions are confirmed) can you trust the output of `getTransactionCount` to start your nonce counter. Thereafter, keep track of the nonce in your application until each transaction confirms.

Parity's JSON RPC interface offers the `parity_nextNonce` function, that returns the next nonce that should be used in a transaction. The `parity_nextNonce` function counts nonces correctly, even if you construct several transactions in rapid succession without confirming them.



Parity has a web console for accessing the JSON RPC interface, but here we are using a command line HTTP client to access it.

```
curl --data
'{"method": "parity_nextNonce", "params": ["0x9e713963a92c02317a681b9bb3065a
8249de124f"], "id": 1, "jsonrpc": "2.0"}' -H "Content-Type: application/json"
-X POST localhost:8545

{"jsonrpc": "2.0", "result": "0x32", "id": 1}
```

Gaps in nonces, duplicate nonces, and confirmation

It is important to keep track of nonces if you are creating transactions programmatically, especially if you are doing so from multiple independent processes simultaneously.

The Ethereum network processes transactions sequentially, based on the nonce. That means that if you transmit a transaction with nonce 0 and then transmit a transaction with nonce 2, the second transaction will not be included in any blocks. It will be stored in the mempool, while the Ethereum network waits for the missing nonce to appear. All nodes will assume that the missing nonce has simply been delayed and that the transaction with nonce 2 was received out of sequence.

If you then transmit a transaction with the missing nonce 1, both transactions (nonces 1 and 2) will be processed and included (if valid, of course). Once you fill the gap, the network can mine the out-of-sequence transaction that it held in the mempool.

What this means is that if you create several transactions in sequence and one of them does not get officially included in any blocks, all the subsequent transactions will be "stuck", waiting for the missing nonce. A transaction can create an inadvertent "gap" in the nonce sequence because it is invalid or has insufficient gas. To get things moving again, you have to transmit a valid transaction with the missing nonce. You should be equally mindful that once a tx with the "missing" nonce is validated by the network, all the broadcast transactions with subsequent nonces will incrementally become valid; it is not possible to "recall" a transaction!

If on the other hand you accidentally duplicate a nonce, for example by transmitting two transactions with the same nonce, but different recipients or values, then one of them will be confirmed and one will be rejected. Which one is confirmed will be determined by the sequence in which they arrive at the first validating node that receives them, i.e. it will be fairly random.

As you can see, keeping track of nonces is necessary and if your application doesn't manage that process correctly, you will run into problems. Unfortunately, things get even more difficult if you are trying to do this concurrently, as we will see in the next section.

Concurrency, transaction origination, and nonces

Concurrency is a complex aspect of computer science, and it crops up unexpectedly sometimes, especially in decentralized and distributed real-time systems like Ethereum.

In simple terms, concurrency is when you have simultaneous computation by multiple independent systems. These can be in the same program (e.g. multi-threading), on the same CPU (e.g. multi-processing), or on different computers (i.e. distributed systems). Ethereum, by definition, is a system that allows concurrency of operations (nodes, clients, DApps), but enforces a singleton state through consensus.

Now, imagine that we have multiple independent wallet applications that are generating transactions from the same address or addresses. One example of such a situation would be an exchange processing withdrawals from the exchange's hot wallet (a wallet whose keys are stored online, in contrast to a cold wallet where the keys are never online). Ideally, you'd want to have more than one computer processing withdrawals, so that it doesn't become a bottleneck or single point of failure. However, this quickly becomes problematic, as having more than one computer producing withdrawals will result in some thorny concurrency problems, not least of which is the selection of nonces. How do multiple computers generating, signing and broadcasting transactions from the same hot wallet account coordinate?

You could use a single computer to assign nonces, on a first-come first-served basis to computers signing transactions. However, this computer is now a single point of failure. Worse, if several nonces are assigned and one of them never gets used (because of a failure in the computer processing the transaction with that nonce), all subsequent transactions get stuck.

Another approach would be to generate the transactions, but not assign a nonce to them (and therefore leave them unsigned - remember that the nonce is an integral part of the transaction data and therefore needs to be included in the digital signature that authenticates the transaction). Then queue them to a single node that signs them and also keeps track of nonces. Again, this would be a choke point in the process: the signing and tracking of nonces is the part of your operation that is likely to become congested under load, whereas the generation of the unsigned transaction is the part you don't really need to parallelize. You would have some concurrency, but it would be lacking in a critical part of the process.

In the end, these concurrency problems, on top of the difficulty of tracking account balances and transaction confirmations in independent processes, force most implementations towards avoiding concurrency and creating bottlenecks such as a single process handling all withdrawal transactions in an exchange, or setting up multiple hot wallets that can work completely independently for withdrawals and only need to be intermittently re-balanced.

Transaction gas

We discuss *gas* in detail in [Gas](#). However, let's cover some basics about the role of the `gasPrice` and `gasLimit` components of a transaction.

Gas is the fuel of Ethereum. Gas is not ether - it's a separate virtual currency with its own exchange rate against ether. Ethereum uses gas to control the amount of resources that a transaction can use, since it will be processed on thousands of computers around the world. The open-ended (Turing complete) computation model requires some form of metering in order to avoid denial of service attacks or inadvertently resource-devouring transactions.

Gas is separate from ether in order to protect the system from the volatility that might arise along with rapid changes in the value of ether, and also as a way to manage the important and sensitive ratios between the costs of the various resources that gas pays for (namely, computation, memory and storage).

The `gasPrice` field in a transaction allows the transaction originator to set the exchange rate of each unit of gas that they are willing to pay. Gas price is measured in wei per gas unit. For example, in a transaction we recently created for an example in this book, our wallet had set the `gasPrice` to 3 Gwei (3 Giga-wei or 3 billion wei).

The popular site ethgasstation.info provides information on the current prices of gas, and other relevant gas metrics for the Ethereum main network:

<https://ethgasstation.info/>

Wallets can adjust the `gasPrice` in transactions they originate, to achieve faster confirmation of transactions. The higher the `gasPrice`, the faster the transaction is likely to confirm. Conversely, lower priority transactions can carry a reduced price, resulting in slower confirmation. The minimum value that `gasPrice` that can be set to is zero, which means a fee-free transaction. During periods of low demand for space in a block, such transactions might very well get mined.



The minimum acceptable gasPrice is zero. That means that wallets can generate completely free transactions. Depending on capacity, these may never be confirmed, but there is nothing in the protocol that prohibits free transactions. You can find several examples of such transactions successfully included on the Ethereum blockchain.

The web3 interface offers a gasPrice suggestion, by calculating a median price across several blocks:

```
truffle(mainnet)> web3.eth.getGasPrice(console.log)
truffle(mainnet)> null BigNumber { s: 1, e: 10, c: [ 1000000000 ] }
```

The second important field related to gas is gasLimit. This is explained in more detail in [Gas](#). In simple terms, gasLimit gives the maximum number of units of gas the transaction originator is willing to buy in order to complete the transaction. For simple payments, meaning transactions that transfer ether from one EOA to another EOA, the gas amount needed is fixed at 21,000 gas units. To calculate how much ether that will cost, you multiply 21,000 by the gasPrice you're willing to pay; for example:

```
truffle(mainnet)> web3.eth.getGasPrice(function(err, res)
{console.log(res*21000)} )
truffle(mainnet)> 2100000000000000
```

If your transaction's destination address is a contract, then the amount of gas needed can be estimated but cannot be determined with accuracy. That's because a contract can evaluate different conditions that lead to different execution paths, with different total gas costs. That means that the contract may execute only a simple computation or a more complex one, depending on conditions that are outside of your control and cannot be predicted. To demonstrate this, let's look at an example: we can write a smart contract that increments a counter each time it is called and executes a particular loop a number of times equal to the call count. Maybe on the 100th call it gives out a special prize, like a lottery, but needs additional computation to calculate the prize. If you call the contract 99 times one thing happens, but on the 100th something very different happens. The amount of gas you would pay for that depends on how many other transactions have called that function before your transaction is included in a block. Perhaps your estimate is based on being the 99th transaction and just before your transaction is confirmed, someone else calls the contract for the 99th time. Now you're the 100th transaction to call and the computation effort (and gas cost) is much higher.

To borrow a common analogy used in Ethereum, you can think of gasLimit as the capacity of the fuel tank in your car (your car is the transaction). You fill the tank with as much gas as you think it will need for the journey (the computation needed to validate your transaction). You can estimate the amount to some degree, but there might be unexpected changes to your journey, such as a diversion (a more complex execution path), which increase fuel consumption.

The analogy to a fuel tank is somewhat misleading, however. It's actually more like a credit account for a gas station company, where you pay after the trip is completed, based on how much gas you actually used. When you transmit your transaction, one of the first validation steps is to check that the account it originated from has enough ether to pay the gasPrice * gas fee. But the amount is not actually deducted from your account until the transaction finishes executing. You are only billed for gas actually consumed by your transaction, but you have to have enough balance for the maximum amount you are willing to pay before you send your transaction.

Transaction recipient

The recipient of a transaction is specified in the to field. This contains a 20-byte Ethereum address. The address can be an EOA or a contract address.

Ethereum does no further validation of this field. Any 20-byte value is considered valid. If the 20-byte value corresponds to an address without a corresponding private key, or without a corresponding contract, the transaction is still valid. Ethereum has no way of knowing whether an address was correctly derived from a public key (and therefore from a private key) in existence.



The Ethereum protocol does not validate recipient addresses in transactions. You can send to an address that has no corresponding private key or contract, thereby "burning" the ether, rendering it forever unspendable. Validation should be done at the user interface level.

Sending a transaction to the wrong address will probably *burn* the ether sent, rendering it forever inaccessible (unspendable), since most addresses do not have a known private key and therefore no signature can be generated to spend it. It is assumed that validation of the address happens at the user interface level (see [\[eip55\]](#)). In fact, there are a number of valid reasons for burning ether, for example as a disincentive to cheating in payment channels and other smart contracts, and, since the amount of ether is finite, burning ether effectively distributes the value burned to all ether holders (in proportion to the amount of ether they hold).

Transaction value and data

The main "payload" of a transaction is contained in two fields: value and data. Transactions can have both value and data, only value, only data, or neither value nor data. All four combinations are valid.

A transaction with only value is a *payment*. A transaction with only data is an *invocation*. A transaction with both value and data is both a payment and an invocation. A transaction with neither value nor data - well that's probably just a waste of gas! But it is still possible.

Let's try all of the above combinations:

First, we set the source and destination addresses from our wallet, just to make the demo easier to read:

```
src = web3.eth.accounts[0];
dst = web3.eth.accounts[1];
```

Transaction with value (payment), and no data payload

```
web3.eth.sendTransaction({from: src, to: dst, value: web3.toWei(0.01, "ether"), data: ""});
```

Our wallet shows a confirmation screen, indicating the value to send, and no data payload, as shown in [Parity wallet showing a transaction with value, but no data](#):

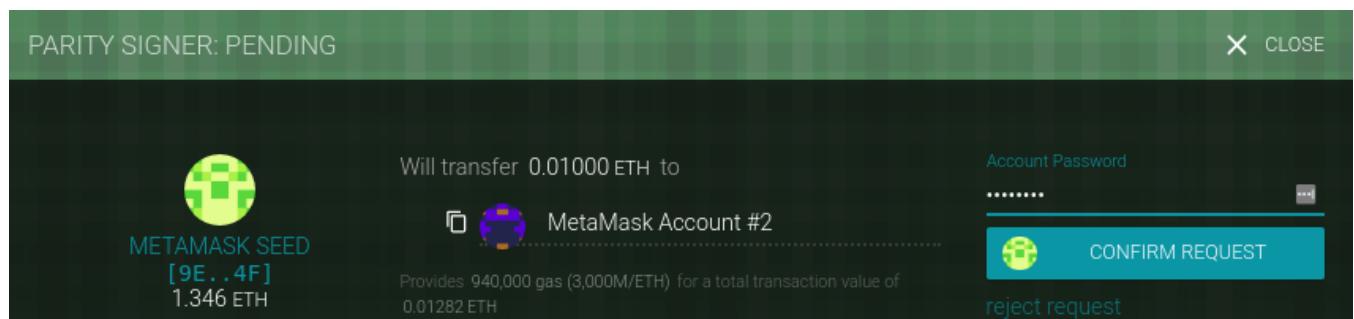


Figure 34. Parity wallet showing a transaction with value, but no data

Transaction with value (payment), and a data payload

```
web3.eth.sendTransaction({from: src, to: dst, value: web3.toWei(0.01, "ether"), data: "0x1234"});
```

Our wallet shows a confirmation screen, indicating the value to send and a data payload, as shown in [Parity wallet showing a transaction with value and data](#):

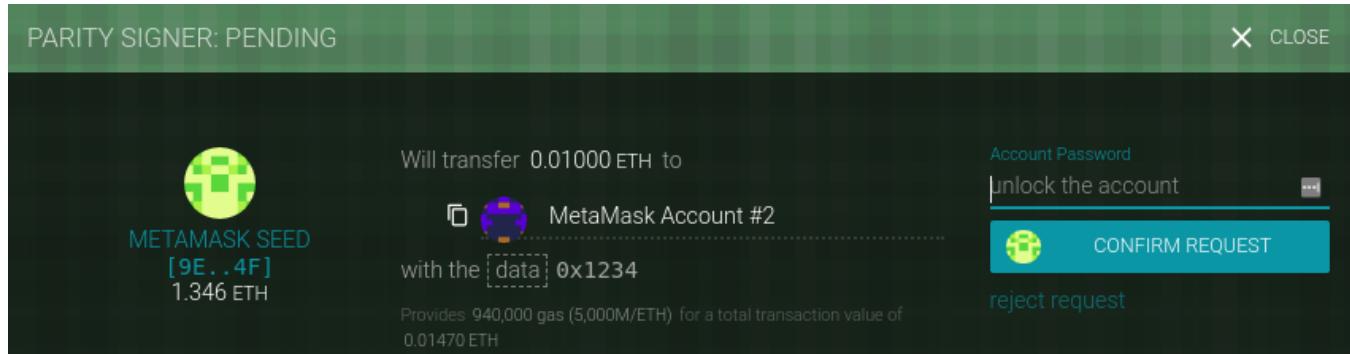


Figure 35. Parity wallet showing a transaction with value and data

Transaction with 0 value, only a data payload

```
web3.eth.sendTransaction({from: src, to: dst, value: 0, data: "0x1234"});
```

Our wallet shows a confirmation screen, indicating the value as 0 and a data payload, as shown in [Parity wallet showing a transaction with no value, only data](#):

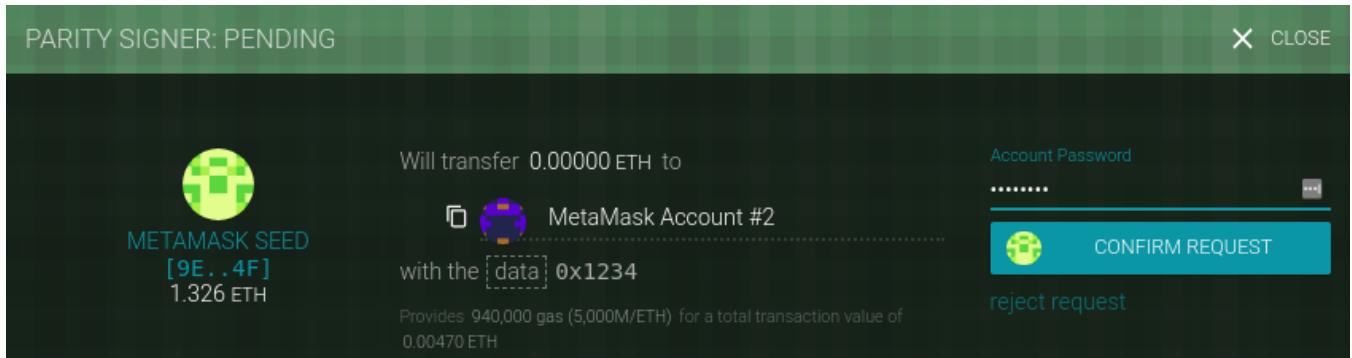


Figure 36. Parity wallet showing a transaction with no value, only data

Transaction with neither value (payment), nor data payload

```
web3.eth.sendTransaction({from: src, to: dst, value: 0, data: ""});
```

Our wallet shows a confirmation screen, indicating 0 value and no data, as shown in [Parity wallet showing a transaction with no value, and no data](#):

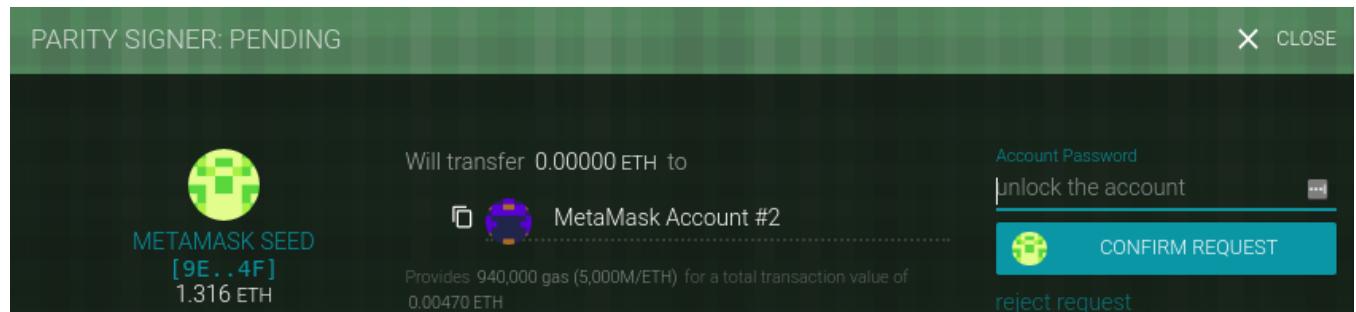


Figure 37. Parity wallet showing a transaction with no value, and no data

Transmitting value to EOAs and contracts

When you construct an Ethereum transaction that contains value, it is the equivalent of a *payment*. Such transactions behave differently depending on whether the destination address is a contract or not.

For EOA addresses, or rather for any address that isn't flagged as a contract on the blockchain, Ethereum will record a state change, adding the value you sent to the balance of the address. If the

address has not been seen before, it will be added to the client's internal representation of the state and its balance initialized to the value of your payment.

If the destination address (to) is a contract, then the EVM will execute the contract and will attempt to call the function named in the data payload of your transaction. If there is no data in your transaction, the EVM will call a *fallback* function and, if that function is payable, will execute it to determine what to do next. If there is no fallback function, then the effect of the transaction will be to increase the balance of the contract, exactly like a payment to a wallet.

A contract can reject incoming payments by throwing an exception immediately when a function is called, or as determined by conditions coded in a function. If the function terminated successfully (without an exception), then the contract's state is updated to reflect an increase in the contract's ether balance.

Transmitting a data payload to an EOA or contract

When your transaction contains data, it is most likely addressed to a contract address. That doesn't mean you cannot send a data payload to an EOA - that is completely valid in the Ethereum protocol. However, in that case, the interpretation of the data is up to the wallet you use to access the EOA. It is ignored by the Ethereum protocol. Most wallets also ignore any data received in a transaction to an EOA they control. In the future, it is possible that standards may emerge that allow wallets to interpret data the way contracts do, thereby allowing transactions to invoke functions running inside user wallets. The critical difference is that any interpretation of the data payload by an EOA is not subject to Ethereum's consensus rules, unlike a contract execution.

For now, let's assume your transaction is delivering data to a contract address. In that case, the data will be interpreted by the EVM as a *contract invocation*. Most contracts use this data more specifically as a *function invocation*, calling the named function and passing any encoded arguments to the function.

The data payload sent to an ABI-compatible contract (which you can assume all contracts are) is a hex-serialized encoding of:

A function selector

The first 4 bytes of the Keccak256 hash of the function's *prototype*. This allows the contract to unambiguously identify which function you wish to invoke.

The function arguments

The function's arguments, encoded according to the rules for the various elementary types defined in the ABI specification.

In [Faucet.sol : A Solidity contract implementing a faucet](#), we defined a function for withdrawals:

```
function withdraw(uint withdraw_amount) public {
```

The *prototype* of the withdraw function is defined as the string containing the name of the function, followed by the data type of each of its arguments enclosed in parentheses and separated by a single comma. The function name is withdraw and it takes a single argument that is a uint (which is an alias for uint256). So the prototype of withdraw would be:

```
withdraw(uint256)
```

Let's calculate the Keccak256 hash of this string (we can use the truffle console or any JavaScript web3 console to do that):

```
web3.sha3("withdraw(uint256)");
'0x2e1a7d4d13322e7b96f9a57413e1525c250fb7a9021cf91d1540d5b69f16a49f'
```

The first 4 bytes of the hash are 0x2e1a7d4d. That's our "function selector" value, which will tell the contract which function we want to call.

Next, let's calculate a value to pass as the argument withdraw_amount. We want to withdraw 0.01 ether. Let's encode that to a hex-serialized big-endian unsigned 256-bit integer, denominated in wei:

```
withdraw_amount = web3.toWei(0.01, "ether");
'1000000000000000'
withdraw_amount_hex = web3.toHex(withdraw_amount);
'0x2386f26fc10000'
```

Now, we add the function selector to the amount (padded to 32 bytes):

That's the data payload for our transaction, invoking the withdraw function and requesting 0.01 ether as the withdraw_amount.

Special transaction: Contract creation

There is one special case of a transaction: contract creation. This is a transaction that *creates* a new contract on the blockchain, deploying it for future use. Contract creation transactions are sent to a special destination address: the zero address; the to field in a contract registration transaction contains the address 0x0. This address represents neither an EOA (there is no corresponding private-public key pair) nor a contract. It can never spend ether or initiate a transaction. It is only used as a destination, with the special meaning "create this contract".

While the zero address is intended only for contract creation, it sometimes receives payments from various addresses. There are two explanations for this: either it is by accident, resulting in the loss of ether, or it is an intentional *ether burn* (deliberately destroying ether by sending it to an address from which it can never be spent). However, if you want to do an intentional ether burn, you should make your intention clear to the network and use the specially designated burn address instead:

0x00dEaD



Any ether sent to the designated burn address 0x0...dEd above will become unspendable and lost forever.

A contract creation transaction need only contain a data payload that contains the compiled bytecode which will create the contract. The only effect of this transaction is to create the contract. You can include an ether amount in the value field if you want to set the new contract up with a starting balance, but that is entirely optional. If you send value (ether) to the contract creation address without a data payload (no contract), then the effect is the same as sending to a burn address - there is no contract to credit so the ether is lost.

As an example, we can create the Faucet.sol contract used in [Ethereum Basics](#), by manually creating a transaction to the zero address and the contract in the data payload. The contract needs to be compiled into a bytecode representation. This can be done with the Solidity compiler.

```
> solc --bin Faucet.sol
```

Binary:

```
6060604052341561000f57600080fd5b60e58061001d6000396000f300606060405260043  
610603f576000357c0100000000000000000000000000000000000000000000000000000000000000  
00900463fffffffffffff1680632e1a7d4d146041575b005b3415604b57600080fd5b605f60048  
080359060200190919050506061565b005b67016345785d8a000081111515156077576000  
80fd5b3373fffffffffffff166108fc829081150290604  
051600060405180830381858888f19350505050151560b657600080fd5b505600a165627a  
7a72305820d276ddd56041f7dc2d2eab69f01dd0a0146446562e25236cf4ba5095d2ee802  
f0029
```

The same information can also be obtained from the Remix online compiler.

Now we can create the transaction.

```
> src = web3.eth.accounts[0];  
> faucet_code =  
"0x6060604052341561000f57600080fd5b60e58061001d6000396000f300606060405260  
043610603f576000357c010000000000000000000000000000000000000000000000000000000000  
00000900463fffffffffffff1680632e1a7d4d146041575b005b3415604b57600080fd5b605f60  
048080359060200190919050506061565b005b67016345785d8a000081111515156077576  
00080fd5b3373fffffffffffff166108fc829081150290  
604051600060405180830381858888f19350505050151560b657600080fd5b505600a1656  
27a7a72305820d276ddd56041f7dc2d2eab69f01dd0a0146446562e25236cf4ba5095d2ee  
802f0029";  
  
> web3.eth.sendTransaction({from: src, to: 0, data: faucet_code, gas:  
113558, gasPrice: 20000000000});  
  
"0xbcc327ae5d369f75b98c0d59037eec41d44dfaef5447fd753d9f2db9439124b"
```

It is good practice to always specify a to parameter, even in the case of the zero address contract creation, because the cost of accidentally sending your ether to 0x0 and losing it forever is too great. You should also specify gasPrice and the gas limit.

Once the contract is mined we can see it on etherscan block explorer, as shown in [Etherscan showing the contract successfully mined](#):

Figure 38. Etherscan showing the contract successfully mined

You can look at the receipt of transaction to get information about the contract.

Here we can see the address of the contract. We can send funds to and receive funds from the contract as shown in [Transmitting a data payload to an EOA or contract](#).

After a while, both transactions are visible on etherscan, as shown in Etherscan showing the transactions for sending and receiving funds:

Transactions	Internal Transactions	Code	Events			
Latest 3 txns						
TxHash	Block	Age	From	To	Value	[TxFee]
0x59836029e7ce43...	3105346	1 min ago	0x2a966a87db5913...	IN	0xb226270965b433...	0 Ether 0.00029414
0x6ebf2e1fe95cc9c...	3105319	6 mins ago	0x2a966a87db5913...	IN	0xb226270965b433...	0.1 Ether 0.00029456
0xbcc327ae5d369f...	3105256	33 mins ago	0x2a966a87db5913...	IN	Contract Creation	0 Ether 0.0227116

Figure 39. Etherscan showing the transactions for sending and receiving funds

Digital signatures

So far, we have not delved into any detail about digital signatures. In this section, we look at how digital signatures work and how they can be used to present proof of ownership of a private key without revealing that private key.

Elliptic Curve Digital Signature Algorithm (ECDSA)

The digital signature algorithm used in Ethereum is the *Elliptic Curve Digital Signature Algorithm*, or

ECDSA. ECDSA is the algorithm used for digital signatures based on elliptic curve private–public key pairs, as described in [Elliptic curve cryptography explained](#).

A digital signature serves three purposes in Ethereum (see [Wikipedia's Definition of a "Digital Signature"](#)). First, the signature proves that the owner of the private key, who is by implication the owner of an Ethereum account, has *authorized* the spending of ether, or execution of a contract. Secondly, the proof of authorization is *undeniable* (non-repudiation). Thirdly, the signature proves that the transaction data have not and *cannot be modified* by anyone after the transaction has been signed.

Wikipedia's Definition of a "Digital Signature"

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Source: https://en.wikipedia.org/wiki/Digital_signature

How Digital Signatures Work

A digital signature is a *mathematical scheme* that consists of two parts. The first part is an algorithm for creating a signature, using a private key (the signing key), from a message (which in our case is the transaction). The second part is an algorithm that allows anyone to verify the signature by only using the message and a public key.

Creating a digital signature

In Ethereum's implementation of ECDSA, the "message" being signed is the transaction, or more accurately, the Keccak256 hash of the RLP-encoded data from the transaction. The signing key is the EOA's private key. The result is the signature:

where:

- k is the signing private key
- m is the RLP-encoded transaction
- $F_{keccak256}$ is the Keccak256 hash function

- F_{sig} is the signing algorithm
- Sig is the resulting signature

More details on the mathematics of ECDSA can be found in [ECDSA Math](#).

The function F_{sig} produces a signature Sig that is composed of two values, commonly referred to as R and S :

$Sig = (R, S)$

Verifying the Signature

To verify the signature, one must have the signature (R and S), the serialized transaction, and the public key that corresponds to the private key used to create the signature. Essentially, verification of a signature means "Only the owner of the private key that generated this public key could have produced this signature on this transaction".

The signature verification algorithm takes the message (i.e. a hash of the transaction for our usage), the signer's public key and the signature (R and S values), and returns true if the signature is valid for this message and public key.

ECDSA Math

As mentioned previously, signatures are created by a mathematical function F_{sig} that produces a signature composed of two values R and S . In this section we look at the function F_{sig} in more detail.

The signature algorithm first generates an *ephemeral* (temporary) private key in a cryptographically secure way. This temporary key is used in the calculation of the R and S values to ensure that the sender's actual private key can't be calculated by attackers watching signed transactions on the Ethereum network.

As we know from [Public keys](#), the ephemeral private key is used to derive the corresponding (ephemeral) public key, so we have:

1. A cryptographically-secure random number q , which is used as the ephemeral private key, and
2. the corresponding ephemeral public key Q , generated from q and the elliptic curve generator point G .

The R value of the digital signature is then the x coordinate of the ephemeral public key Q .

From there, the algorithm calculates the S value of the signature, such that:

$$S \equiv q^{-1} (\text{Keccak256}(m) + R * k) \pmod{p}$$

where:

- q is the ephemeral private key
- R is the x coordinate of the ephemeral public key
- k is the signing (EOA owner's) private key
- m is the transaction data
- p is the prime order of the elliptic curve

Verification is the inverse of the signature generation function, using the R, S values and the sender's public key to calculate a value Q , which is a point on the elliptic curve (the ephemeral public key used in signature creation):

1. Check all inputs are correctly formed
2. Calculate $w = S^{-1} \pmod{p}$
3. Calculate $u_1 = \text{Keccak256}(m) * w \pmod{p}$
4. Calculate $u_2 = R * w \pmod{p}$
5. Finally, calculate the point on the elliptic curve $Q \equiv u_1 * G + u_2 * K \pmod{p}$

where:

- R and S are the signature values
- K is the signer's (EOA owner's) public key
- m is the transaction data that was signed
- G is the elliptic curve generator point
- p is the prime order of the elliptic curve

If the x coordinate of the calculated point Q is equal to R , then the verifier can conclude that the

signature is valid.

Note that in verifying the signature, the private key is neither known nor revealed.



ECDSA is necessarily a fairly complicated piece of math; a full explanation is beyond the scope of this book. A number of great guides online take you through it step by step: search for "ECDSA explained" or try this one: <http://bit.ly/2r0HhGB>

Transaction signing in practice

To produce a valid transaction, the originator must digitally sign the message, using the Elliptic Curve Digital Signature algorithm. When we say "sign the transaction", we actually mean "sign the Keccak256 hash of the RLP serialized transaction data". The signature is applied to the hash of the transaction data, not the transaction itself.

To sign a transaction in Ethereum, the originator must:

1. Create a transaction data structure, containing nine fields: nonce, gasPrice, gasLimit, to, value, data, chainID, 0, 0
2. Produce an RLP-encoded serialized message of the transaction data structure
3. Compute the Keccak256 hash of this serialized message
4. Compute the ECDSA signature, signing the hash with the originating EOA's private key
5. Append the ECDSA signature's computed v, r and s values to the transaction

The special signature variable v indicates two things: the chain ID and the recovery identifier to help the ECDSArecover function check the signature. It is calculated as either one of 27 or 28, or as the chain ID doubled plus 35 or 36. For more information on the chain ID, see [Raw transaction creation with EIP-155](#). The recovery identifier (27 or 28 in the "old style" signatures, or 35 or 36 in the full "Spurious Dragon" style transactions) is used to indicate the parity of the y component of the public key (see [The signature prefix value \(v\) and public key recovery](#) for more details).



At block #2,675,000, Ethereum implemented the "Spurious Dragon" hard fork that, among other changes, introduced a new signing scheme that includes transaction replay protection (preventing transactions meant for one network being replayed on others). This new signing scheme is specified in EIP-155. This change affects the form of the transaction and its signature, so attention must be paid to the first of the three signature variables (i.e. v), which takes one of two forms and indicates the data fields included in the transaction message being hashed.

Raw transaction creation and signing

Let's create a raw transaction and sign it, using the `ethereumjs-tx` library. This demonstrates the functions that would normally be used inside a wallet, or an application that signs transactions on behalf of a user. The source code for this example is in `raw_tx_demo.js` in the GitHub repository. Download it here: https://github.com/ethereumbook/ethereumbook/blob/develop/code/web3js/raw_tx/raw_tx_demo.js

```
// Load requirements first:  
//  
// npm init  
// npm install ethereumjs-tx  
//  
// Run with: $ node raw_tx_demo.js  
const ethTx = require('ethereumjs-tx');  
  
const txData = {  
    nonce: '0x0',  
    gasPrice: '0x09184e72a000',  
    gasLimit: '0x30000',  
    to: '0xb0920c523d582040f2bcb1bd7fb1c7c1ecebdb34',  
    value: '0x00',  
    data: '',  
    v: "0x1c", // Ethereum main net chainID  
    r: 0,  
    s: 0  
};  
  
tx = new ethTx(txData);  
console.log('RLP-Encoded Tx: 0x' + tx.serialize().toString('hex'))  
  
txHash = tx.hash(); // This step encodes into RLP and calculates the hash  
console.log('Tx Hash: 0x' + txHash.toString('hex'))  
  
// Sign transaction  
const privKey =  
Buffer.from('91c8360c4cb4b5fac45513a7213f31d4e4a7bfcb4630e9fbf074f42a203a  
c0b9', 'hex');  
tx.sign(privKey);  
  
serializedTx = tx.serialize();  
rawTx = 'Signed Raw Transaction: 0x' + serializedTx.toString('hex');  
console.log(rawTx)
```

Run the example code:

```
$ node raw_tx_demo.js
RLP-Encoded Tx:
0xe6808609184e72a0008303000094b0920c523d582040f2bcb1bd7fb1c7c1ecebdb34808
0
Tx Hash:
0xaa7f03f9f4e52fcf69f836a6d2bbc7706580adce0a068ff6525ba337218e6992
Signed Raw Transaction:
0xf866808609184e72a0008303000094b0920c523d582040f2bcb1bd7fb1c7c1ecebdb348
0801ca0ae236e42bd8de1be3e62fea2fafac7ec6a0ac3d699c6156ac4f28356a4c034fda0
422e3e6466347ef6e9796df8a3b6b05bed913476dc84bbfca90043e3f65d5224
```

Raw transaction creation with EIP-155

The EIP-155 "Simple Replay Attack Protection" standard specifies a replay-attack-protected transaction encoding, which includes a *chain identifier* inside the transaction data, prior to signing. This ensures that transactions created for one blockchain (e.g. Ethereum main network) are invalid on another blockchain (e.g. Ethereum Classic or Ropsten test network). Therefore, transactions broadcast on one network cannot be *replayed* on another, hence the name of the standard.

EIP-155 adds three fields to the main six fields of the transaction data structure, namely the chain identifier, 0, and 0. These three fields are added to the transaction data *before it is encoded and hashed*. The three additional fields therefore change the transaction's hash, to which the signature is later applied. By including the chain identifier in the data being signed, the transaction signature prevents any changes, as the signature is invalidated if the chain identifier is modified. Therefore, EIP-155 makes it impossible for a transaction to be replayed on another chain, because the signature's validity depends on the chain identifier.

The chain identifier field takes a value according to network the transaction is meant for:

Chain	Chain ID
Ethereum main net	1
Morden (obsolete), Expanse	2
Ropsten	3
Rinkeby	4
Rootstock main net	30

Rootstock test net	31
Kovan	42
Ethereum Classic main net	61
Ethereum Classic test net	62
Geth private testnets	1337

The resulting transaction structure is RLP-encoded, hashed and signed. The signature algorithm is modified slightly to encode the chain identifier in the v prefix too.

For more details, see the EIP-155 specification: <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-155.md>

The signature prefix value (v) and public key recovery

As mentioned in [The Structure of a Transaction](#), the transaction message doesn't include any "from" field. That's because the originator's public key can be computed directly from the ECDSA signature. Once you have the public key, you can compute the address easily. The process of recovering the signer's public key is called *Public Key Recovery*.

Given the values r and s that were computed in [ECDSA Math](#), we can compute two possible public keys.

First, we compute two elliptic curve points R and R', from the x coordinate r value that is in the signature. There are two points, because the elliptic curve is symmetric across the x-axis, so that for any value x there are two possible values that fit the curve, one on each side of the x-axis.

From r, we also calculate r^{-1} , which is the multiplicative inverse of r.

Finally we calculate z, which is the n lowest bits of the message hash, where n is the order of the elliptic curve.

The two possible public keys are then:

$$K_1 = r^{-1} (sR - zG)$$

and

$$K_2 = r^{-1} (sR' - zG)$$

where:

- K_1 and K_2 are the two possibilities for the signer's public key
- r^{-1} is the multiplicative inverse of the signature's r value
- s is the signature's s value
- R and R' are the two possibilities for the ephemeral public key Q
- z are the n -lowest bits of the message hash
- G is the elliptic curve generator point

To make things more efficient, the transaction signature includes a prefix value v , which tells us which of the two possible R values are the ephemeral public key. If v is even, then R is the correct value. If v is odd, then it is R' . That way, we need to calculate only one value for R and only one value for K .

Separating signing and transmission (offline signing)

Once a transaction is signed, it is ready to transmit to the Ethereum network. The three steps of creating, signing, and broadcasting a transaction normally happen as a single operation, for example using `web3.eth.sendTransaction`. However, as we saw in [Raw transaction creation and signing](#), you can create and sign the transaction in two separate steps. Once you have a signed transaction, you can then transmit it using `web3.eth.sendSignedTransaction`, which takes a hex-encoded and signed transaction and transmits it on the Ethereum network.

Why would you want to separate the signing and transmission of transactions? The most common reason is security: the computer that signs a transaction must have unlocked private keys loaded in memory. The computer that does the transmitting must be connected to the internet (and be running an Ethereum client). If these two functions are on one computer, then you have private keys on an online system, which is quite dangerous. Separating the functions of signing and transmitting and performing them on different machines (on an offline and online device, respectively) is called *offline signing* and is a common security practice.

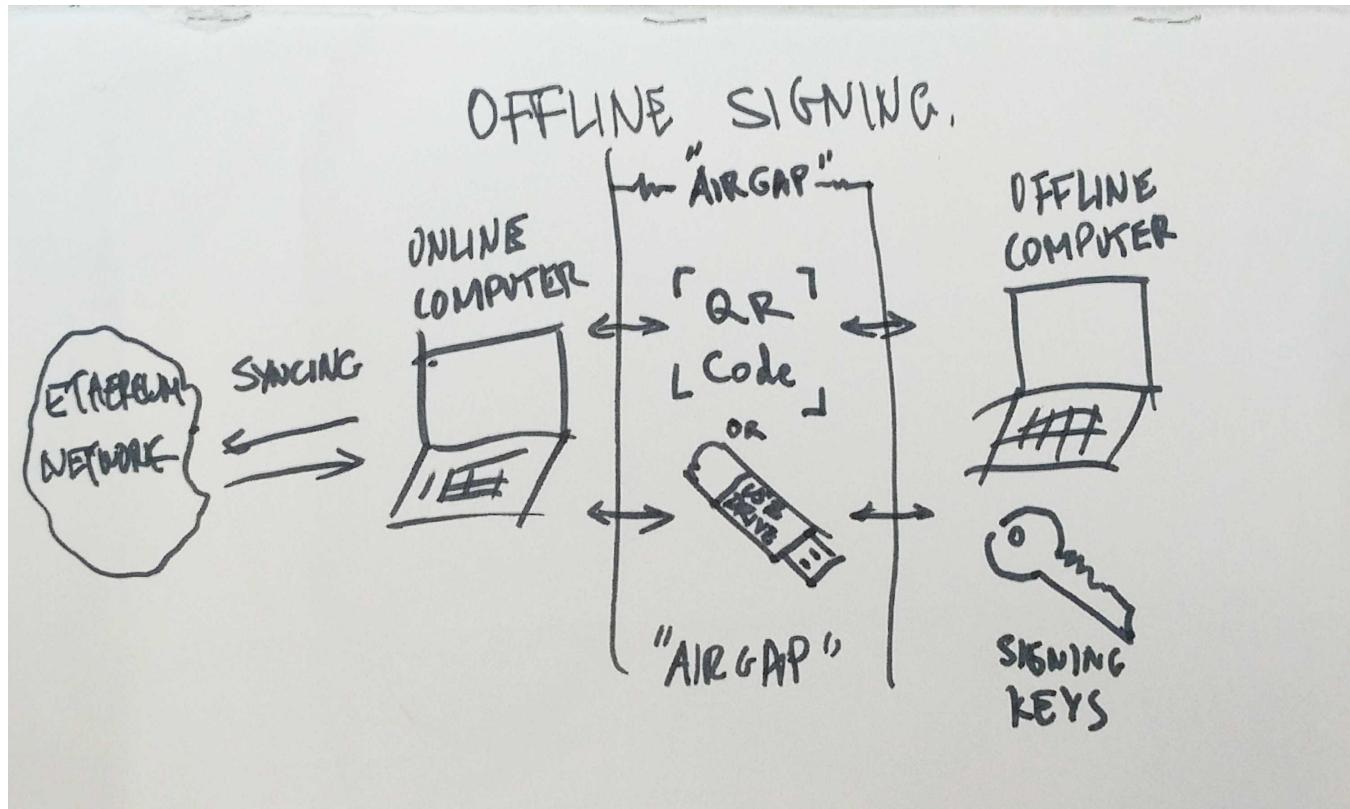


Figure 40. Offline signing of Ethereum transactions

[Offline signing of Ethereum transactions](#) shows the process:

1. Create unsigned transaction: On the online computer where the current state of the account, notably the current nonce and funds available, can be retrieved.
2. Signing: transfer the unsigned transaction to an "air-gapped" offline device for transaction signing, e.g. via a QR code or USB flash drive.
3. Transmission: transfer the signed transaction (back) to an online device for broadcast on the Ethereum blockchain, e.g. via QR code or USB flash drive.

Depending on the level of security you need, your "offline signing" computer can have varying degrees of separation from the online computer, ranging from an isolated and firewalled subnet (online but segregated) to a completely offline system known as an *air-gapped* system. In an air-gapped system there is no network connectivity at all - the computer is separated from the online environment by a gap of "air". To sign transactions you transfer them to and from the air-gapped computer using data

storage media or (better) a webcam and QR code. Of course, this means you must manually transfer every transaction you want signed, and this doesn't scale.

While not many environments can utilize a fully air-gapped system, even a small degree of isolation has significant security benefits. For example, an isolated subnet with a firewall that only allows a message-queue protocol through can offer a much-reduced attack surface and much higher security than signing on the online system. Many companies use a protocol such as ZeroMQ (0MQ) for this purpose. With a setup like that, transactions are serialized and queued for signing. The queuing protocol transmits the serialized message, in a way similar to a TCP socket, to the signing computer. The signing computer reads the serialized transactions from the queue (carefully), applies a signature with the appropriate key, and places them on an outgoing queue. The outgoing queue transmits the signed transactions to a computer with an Ethereum client that de-queues them and transmits them.

Transaction propagation

The Ethereum network uses a "flood routing" protocol. Each Ethereum client acts as a *node* in a *Peer-to-Peer (P2P)* network, which (ideally) forms a *mesh* network. No network node is special: they all act as equal peers. We will use the term "node" to refer to an Ethereum client that is connected to and participates in the P2P network.

Transaction propagation starts with the originating Ethereum node creating (or receiving from offline) a signed transaction. The transaction is validated and then transmitted to all the other Ethereum nodes that are *directly* connected to the originating node. On average, each Ethereum node maintains connections to at least 13 other nodes, called its *neighbors*. Each neighbor node validates the transaction as soon as they receive it. If they agree that it is valid, they store a copy and propagate it to all their neighbors (except the one it came from). As a result, the transaction ripples outwards from the originating node, *flooding* across the network, until all nodes in the network have a copy of the transaction. Nodes can filter the messages they propagate, but the default is to propagate all valid transaction messages they receive.

Within just a few seconds, an Ethereum transaction propagates to all the Ethereum nodes around the globe. From the perspective of each node, it is not possible to discern the origin of the transaction. The neighbor that sent it to our node may be the originator of the transaction or may have received it from one of its neighbors. To be able to track the origin of transactions, or interfere with propagation, an attacker would have to control a significant percentage of all nodes. This is part of the security and privacy design of P2P networks, especially as applied to blockchain networks.

Recording on the blockchain

While all the nodes in Ethereum are equal peers, some of them are operated by *miners* and are feeding transactions and blocks to *mining farms*, which are computers with high-performance Graphical Processing Units (GPUs). The mining computers add transactions to a candidate block and attempt to find a *Proof-of-Work* that makes the candidate block valid. We will discuss this in more detail in [Consensus](#).

Without going into too much detail, valid transactions will eventually be included in a block of transactions and, thus, recorded in the Ethereum blockchain. Once mined into a block, transactions also modify the state of the Ethereum singleton, either by modifying the balance of an account (in the case of a simple payment), or by invoking contracts that change their internal state. These changes are recorded alongside the transaction, in the form of a transaction *receipt*, which may also include *events*. We will examine all this in much more detail in [The Ethereum Virtual Machine](#)

Our transaction has completed its journey from creation to signing by an EOA, propagation, and finally mining. It has changed the state of the singleton and left an indelible mark on the blockchain.

Multiple signatures (multisig) transactions

If you are familiar with Bitcoin's scripting capabilities, you know that it is possible to create a Bitcoin multisig account which can only spend funds when multiple parties sign the transaction (e.g. 2 of 2 or 3 of 4 signatures). Ethereum's basic EOA value transactions have no provisions for multiple signatures; however, arbitrary signing restrictions can be enforced by smart contracts with any conditions you can think of, to handle the transfer of ether and tokens alike.

To take advantage of this capability, ether has to be transferred to a "wallet contract" that is programmed with the spending rules desired, such as multi-signature requirements or spending limits (or combinations of the two). The wallet contract then sends the funds when prompted by an authorized EOA once the spending conditions have been satisfied. For example, to protect your ether under a multisig condition, transfer the ether to a multisig contract. Whenever you want to send funds to another account, all the required users will need to send transactions to the contract using a regular wallet app, effectively authorizing the contract to perform the final transaction.

These contracts can also be designed to require multiple signatures before executing local code or to trigger other contracts. The security of the scheme is ultimately determined by the multisig contract code.

The ability to implement multi-signature transactions as a smart contract demonstrates the flexibility of Ethereum. However, it is a double-edged sword, as the extra flexibility can lead to bugs that undermine the security of multi-signature schemes. There are, in fact, a number of proposals to create a multi-signature command in the EVM that removes the need for smart contracts, at least for the simple M-of-N multi-signature schemes. This would be equivalent to Bitcoin's multi-signature system that is part of the core consensus rules and has proven to be robust and secure.

Conclusions

Transactions are the starting point of every activity in the Ethereum system. Transactions are the "inputs" that cause the Ethereum Virtual Machine to evaluate contracts, update balances, and more generally modify the state of the Ethereum blockchain. Next, we will work with smart contracts in a lot more detail and learn how to program in the Solidity contract-oriented language.

Smart contracts and Solidity

As we discussed in [Ethereum Basics](#), there are two different types of account in Ethereum: Externally Owned Accounts (EOAs) and contract accounts. EOAs are controlled by users, often via software, such as a wallet application, that are external to the Ethereum platform. In contrast to that, contract accounts are controlled by their program code (also commonly referred to as smart contracts) that is executed by the Ethereum Virtual Machine (EVM). In short, EOAs are simple accounts without any associated code or data storage, whereas contract accounts have both associated code and data storage. EOAs are controlled by transactions created and cryptographically signed with a private key in the "real world" external to and independent of the protocol, whereas contract accounts do not have private keys and so "control themselves" in the predetermined way prescribed by their smart contract code. Both types of accounts are identified by an Ethereum address. In this section, we will discuss contract accounts, and the program code that controls them: smart contracts.

What is a smart contract?

The term *smart contract* has been used over the years to describe a wide variety of different things. In the 1990s, cryptographer Nick Szabo coined the term and defined it as “a set of promises, specified in digital form, including protocols within which the parties perform on the other promises”. Since then, the concept of smart contracts has evolved, especially after the introduction of decentralized blockchain platforms with the invention of Bitcoin in 2009. In the context of Ethereum, the term is actually a bit of a misnomer, given that Ethereum smart contracts are neither smart nor legal contracts, but the term has stuck. In this book, we use the term “smart contract” to refer to immutable computer programs that run deterministically in the context of an Ethereum Virtual Machine as part of the Ethereum network protocol, i.e. on the decentralized Ethereum world computer.

Let's unpack that definition:

- Computer programs: Smart contracts are simply computer programs. The word contract has no legal meaning in this context.
- Immutable: Once deployed, the code of a smart contract cannot change. Unlike traditional software, the only way to modify a smart contract is to deploy a new instance.
- Deterministic: The outcome of the execution of a smart contract is the same for everyone who runs it, given the context of the transaction that initiated its execution and the state of the Ethereum blockchain at the moment of execution.

- The EVM context: Smart contracts operate with a very limited execution context. They can access their own state, the context of the transaction that called them and some information about the most recent blocks.
- Decentralized world computer: The EVM runs as a local instance on every Ethereum node, but because all instances of the EVM operate on the same initial state and produce the same final state, the system as a whole operates as a single "world computer".

Lifecycle of a smart contract

Smart contracts are typically written in a high-level language, such as Solidity. But in order to run, they must be compiled to the low-level bytecode that runs in the EVM. Once compiled, they are deployed on the Ethereum platform using a special *contract creation* transaction which is identified as such by being sent to the special contract creation address, namely 0x0. Each contract is identified by an Ethereum address, which is derived from the contract creation transaction as a function of the originating account and nonce. The Ethereum address of a contract can be used in a transaction as the recipient, sending funds to the contract or calling one of the contract's functions. Note that, unlike EOAs, there are no keys associated with an account created for a new smart contract. As the contract creator, you don't get any special privileges at the protocol level (although you can explicitly code them into the smart contract, of course). You certainly don't receive the private key for the contract account - it doesn't exist - we can say that smart contract accounts own themselves.

Importantly, contracts *only run if they are called by a transaction*. All smart contracts in Ethereum are executed, ultimately, because of a transaction initiated from an Externally Owned Account. A contract can call another contract that can call another contract, and so on, but the first contract in such a chain of execution will always have been called by a transaction from an EOA. Contracts never run "on their own", or "run in the background". Contracts effectively lie dormant until a transaction triggers execution, either directly or indirectly as part of a chain of contract calls. It is also worth noting that smart contracts are not executed "in parallel" in any sense - the Ethereum world computer can be considered to be a single-threaded machine.

Transactions are *atomic*, regardless of how many contracts they call or what those contracts do when called. Transactions execute in their entirety, with any changes in the global state (contracts, accounts, etc.) recorded only if all execution terminates successfully. Successful termination means that the program executed without an error and reached the end of execution. If execution fails due to an error, all of its effects (changes in state) are "rolled back" as if the transaction never ran. A failed transaction is still recorded as having been attempted, and the ether spent on gas for the execution is deducted from the originating account, but it otherwise has no other effects on contract or account state.

As mentioned above, it is important to remember that a contract's code cannot be changed. However a contract can be "deleted", removing the code and its internal state (storage) from its address, leaving a blank account. Any transactions sent to that account address after the contract has been deleted do not result in any code execution, because there is no longer any code there to execute. To delete a contract, you execute an EVM opcode called SELFDESTRUCT (previously called SUICIDE). That operation costs "negative gas", a gas refund, thereby incentivizing the release of network client resources from the deletion of stored state. Deleting a contract in this way does not remove the transaction history (past) of the contract, since the blockchain itself is immutable. It is also important to note that the SELFDESTRUCT capability will only be available if the contract author programmed the smart contract to have that functionality. If the contract's code does not have a SELFDESTRUCT opcode, or it is inaccessible, the smart contract can not be deleted.

Introduction to Ethereum high-level languages

The EVM is a virtual machine that runs a special form of *machine code* called *EVM bytecode*, just like your computer's CPU, which runs machine code such as x86_64. We will examine the operation and language of the EVM in much more detail in [The Ethereum Virtual Machine](#). In this section we will look at how smart contracts are written to run on the EVM.

While it is possible to program smart contracts directly in bytecode, EVM bytecode is rather unwieldy and very difficult for programmers to read and understand. Instead, most Ethereum developers use a high-level language to write programs, and a compiler to convert them into bytecode.

While any high-level language could be adapted to write smart contracts, adapting an arbitrary language to be compilable to EVM bytecode is quite a cumbersome exercise and would in general lead to some amount of confusion. Smart contracts operate in a highly constrained and minimalistic execution environment (the EVM). In addition, a special set of EVM-specific system variables and functions need to be available. As such, it is easier to build a smart contract language from scratch than it is to make a general-purpose language suitable for writing smart contracts. As a result, a number of special-purpose languages have emerged for programming smart contracts. Ethereum has several such languages, together with the compilers needed to produce EVM-executable bytecode.

In general, programming languages can be classified into two broad programming paradigms: declarative and imperative, also known as "functional" and "procedural", respectively. In declarative programming, we write functions that express the *logic* of a program, but not its *flow*. Declarative programming is used to create programs where there are no *side effects*, meaning that there are no changes to state outside of a function. Declarative programming languages include Haskell and SQL. Imperative programming, by contrast, is where a programmer writes a set of procedures that combine

the logic and flow of a program. Imperative programming languages include C++ and Java. Some languages are “hybrid”, meaning that they encourage declarative programming but can also be used to express an imperative programming paradigm. Such hybrids include Lisp, JavaScript, and Python. In general, any imperative language can be used to write in a declarative paradigm, but it often results in inelegant code. By comparison, pure declarative languages cannot be used to write in an imperative paradigm. In purely declarative languages, *there are no “variables”*.

While imperative programming is more commonly used by programmers, it can be very difficult to write programs that execute *exactly as expected*. The ability of any part of the program to change the state of any other makes it difficult to reason about a program’s execution and introduces many opportunities for bugs. Declarative programming by comparison makes it easier to understand how a program will behave: since it has no side effects, any part of a program can be understood in isolation.

In smart contracts, bugs literally cost money. As a result, it is critically important to write smart contracts without unintended effects. To do that, you must be able to clearly reason about the expected behavior of the program. So, declarative languages play a much bigger role in smart contracts than they do in general-purpose software. Nevertheless, as you will see below, the most widely-used language for smart contracts (Solidity) is imperative. Programmers, like most humans, resist change!

Currently supported high-level programming languages for smart contracts include (ordered by approximate age):

LLL

A functional (declarative) programming language, with Lisp-like syntax. It was the first high-level language for Ethereum smart contracts but is rarely used today.

Serpent

A procedural (imperative) programming language with a syntax similar to Python. Can also be used to write functional (declarative) code, though it is not entirely free of side effects.

Solidity

A procedural (imperative) programming language with a syntax similar to JavaScript, C++ or Java. The most popular and frequently used language for Ethereum smart contracts.

Vyper

A more recently developed language, similar to Serpent and again with Python-like syntax. Intended to get closer to a pure-functional Python-like language than Serpent, but not to replace Serpent.

Bamboo

A newly developed language, influenced by Erlang, with explicit state transitions and without iterative flows (loops). Intended to reduce side effects and increase auditability. Very new and yet to be widely adopted.

As you can see, there are many languages to choose from. However, of all these Solidity is by far the most popular, to the point of being the *de facto* high-level language of Ethereum and even other EVM-like blockchains. We will spend most of our time using Solidity, but will also explore some of the examples in other high-level languages, to gain an understanding of their different philosophies.

Building a smart contract with Solidity

Solidity was created by Gavin Wood (co-author of this book) as a language explicitly for writing smart contracts with features to directly support execution in the decentralized environment of the Ethereum world computer. The resulting attributes are quite general and so it has ended up being used for coding smart contracts on several other blockchain platforms. It was developed by Christian Reitwessner and then also by Alex Beregszaszi, Liana Husikyan, Yoichi Hirai and several former Ethereum core contributors. Solidity is now developed and maintained as an independent project on GitHub:

<https://github.com/ethereum/solidity>

The main "product" of the Solidity project is the *Solidity Compiler (solc)*, which converts programs written in the Solidity language to EVM bytecode. The project also manages the important Application Binary Interface (ABI) standard for Ethereum smart contracts, which we will explore in detail in this chapter. Each version of the Solidity compiler corresponds to and compiles a specific version of the Solidity language.

To get started, we will download a binary executable of the Solidity compiler. Then we will develop and compile a simple contract, following on from the example we started with in [Ethereum Basics](#).

Selecting a version of Solidity

Solidity follows a versioning model called *semantic versioning* (<https://semver.org/>), which specifies version numbers structured as three numbers separated by dots: MAJOR.MINOR.PATCH. The "major" number is incremented for major and *backwards incompatible* changes, the "minor" number is incremented as backwards compatible features are added in between major releases, and the "patch" number is incremented for backwards compatible bug fixes.

At the time of writing, Solidity is at version 0.4.24. The rules for major version 0, which is for initial development of a project, are different: anything may change at any time. In practice, Solidity increments treats the "minor" number as if it were the major version, and the "patch" number as if it were the minor version. Therefore, in 0.4.24, 4 is considered to be the major version, and 24 the minor version.

The 0.5 major version release of Solidity is anticipated imminently.

As we saw in [Ethereum Basics](#), your Solidity programs can contain a pragma directive that specifies the minimum and maximum version of Solidity that it is compatible with, and can be used to compile your contract.

Since Solidity is rapidly evolving it is best to always use the latest release.

Download and Install

There are a number of methods you can use to download and install Solidity, either as a binary release or by compiling from source code. You can find detailed instruction in the Solidity documentation at:

<https://solidity.readthedocs.io/en/latest/installing-solidity.html>

Here's see how to install the latest binary release of Solidity on an Ubuntu/Debian operating system, using the apt package manager:

```
$ sudo add-apt-repository ppa:ethereum/ethereum  
$ sudo apt update  
$ sudo apt install solc
```

Once you have solc installed, check the version by running:

```
$ solc --version  
solc, the solidity compiler commandline interface  
Version: 0.4.24+commit.e67f0147.Linux.g++
```

There are a number of other ways to install Solidity, depending on your operating system and requirements, including compiling from the source code directly. For more information see:

<https://github.com/ethereum/solidity>

Development environment

To develop in Solidity, you can use any text editor and solc on the command-line. However, you might find that some text editors designed for development, such as Emacs, Vim and Atom, offer additional features such as syntax highlighting and macros that make Solidity development easier.

There are also web-based development environments, such as Remix IDE (<https://remix.ethereum.org/>), and EthFiddle (<https://ethfiddle.com/>).

Use the tools that make you productive. In the end, Solidity programs are just plain text files. While fancy editors and development environments can make things easier, you don't need anything more than a simple text editor, such as nano (Linux/Unix),TextEdit (macOS) or even NotePad (Windows). Simply save your program source code with a .sol extension and it will be recognized by the Solidity compiler as a Solidity program.

Writing a simple Solidity program

In [Ethereum Basics](#) we wrote our first Solidity program, [Faucet.sol : A Solidity contract implementing a faucet](#). When we first built the Faucet, we used the Remix IDE to compile and deploy the contract. In this section, we will revisit, improve, and embellish Faucet.

Our first attempt looked like this:

```
// Our first contract is a faucet!
contract Faucet {

    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {

        // Limit withdrawal amount
        require(withdraw_amount <= 1000000000000000);

        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }

    // Accept any incoming amount
    function () public payable {}

}
```

Compiling with the Solidity compiler (solc)

Now, we will use the Solidity compiler on the command-line to compile our contract directly. The Solidity compiler solc offers a variety of options, which you can see by passing the --help argument.

We use the --bin and --optimize arguments of solc to produce an optimized binary of our example contract [Compiling Faucet.sol with solc](#):

Compiling Faucet.sol with solc

The result that solc produces is a hex serialized binary that can be submitted to the Ethereum blockchain.

Ethereum contract Application Binary Interface (ABI)

In computer software, an Application Binary Interface (ABI) is an interface between two program modules; often, between the operating system and user programs. An ABI defines how data structures and functions are accessed in **machine code**; this is not to be confused with an API, which defines this access in high-level, often human-readable formats as **source code**. The ABI is thus the primary way of encoding and decoding data into and out of machine code.

In Ethereum, the ABI is used to encode contract calls for the EVM and to read data out of transactions. The purpose of an ABI is to define the functions in the contract that can be invoked and describe how each function will accept arguments and return its result.

A contract's ABI is specified as a JSON array of function descriptions (see [Functions](#)) and events (see [Events](#)). A function description is a JSON object with fields for `type`, `name`, `inputs`, `outputs`, `constant`, and `payable`. An event description object has fields for `type`, `name`, `inputs`, and `anonymous`.

We use the `solc` command-line Solidity compiler to produce the ABI for our `Faucet.sol` example contract:

```
$ solc --abi Faucet.sol
===== Faucet.sol:Faucet =====
Contract JSON ABI
[{"constant":false,"inputs":[{"name":"withdraw_amount","type":"uint256"}]
,"name":"withdraw","outputs":[],"payable":false,"stateMutability":"nonpayable","type":"function"}, {"payable":true,"stateMutability":"payable","type":"fallback"}]
```

As you can see, the compiler produces a JSON array describing the two functions that are defined by Faucet.sol. This JSON can be used by any application that wants to access the Faucet contract once it is deployed. Using the ABI, an application such as a wallet or DApp browser can construct transactions that call the functions in Faucet with the correct arguments and argument types. For example, a wallet would know that to call the function withdraw it would have to provide a uint256 argument named withdraw_amount. The wallet could prompt the user to provide that value, then create a transaction that encodes it and executes the withdraw function.

All that is needed for an application to interact with a contract is an ABI and the address where the contract has been deployed.

Selecting Solidity compiler and language version

As we saw in [Compiling Faucet.sol with solc](#), our Faucet contract compiles successfully with Solidity version 0.4.21. But what if we had used a different version of the Solidity compiler? The language is still in constant flux and things may change in unexpected ways. Our contract is fairly simple, but what if our program used a feature that was only added in Solidity version 0.4.19 and we tried to compile it with 0.4.18?

To resolve such issues, Solidity offers a *compiler directive* known as a *version pragma* that instructs the compiler that the program expects a specific compiler (and language) version. Let's look at an example:

```
pragma solidity ^0.4.19;
```

The Solidity compiler reads the version pragma and will produce an error if the compiler version is incompatible with the version pragma. In this case, our version pragma says that this program can be compiled by a Solidity compiler with a minimum version of 0.4.19. The symbol `^` states, however, that we allow compilation with any *minor revision* above 0.4.19, e.g. 0.4.20, but not 0.5.0 (which is a major

revision, not a minor revision). Pragma directives are not compiled into EVM bytecode. They are only used by the compiler to check compatibility.

Let's add a pragma directive to our Faucet contract. We will name the new file Faucet2.sol, to keep track of our changes as we proceed through these examples starting in [Faucet2.sol : Adding the version pragma to Faucet](#):

Faucet2.sol : Adding the version pragma to Faucet

```
// Version of Solidity compiler this program was written for
pragma solidity ^0.4.19;

// Our first contract is a faucet!
contract Faucet {

    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {

        // Limit withdrawal amount
        require(withdraw_amount <= 10000000000000000);

        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }

    // Accept any incoming amount
    function () public payable {}

}
```

Adding a version pragma is best practice, as it avoids problems with mismatched compiler and language versions. We will explore best practice and continue to improve the Faucet contract throughout this chapter.

Programming with Solidity

In this section, we will look at some of the capabilities of the Solidity language. As we mentioned in [Ethereum Basics](#), our first contract example was very simple and also flawed in various ways. We'll

gradually improve it, while learning how to use Solidity. This won't be a comprehensive Solidity tutorial however, as Solidity is quite complex and rapidly evolving. We'll cover the basics and give you enough of a foundation to be able to explore the rest on your own. The documentation for Solidity can be found at <https://solidity.readthedocs.io/en/latest/>

Data types

First, let's look at some of the basic data types offered in Solidity:

boolean (bool)

Boolean value, true or false, with logical operators ! (not), && (and), || (or), == (equal), != (not equal).

integer (int, uint)

Signed (int) and unsigned (uint) integers, declared in increments of 8 bits from int8 to uint256.

Without a size suffix, 256-bit quantities are used, to match the word size of the EVM.

fixed point (fixed, ufixed)

Fixed point numbers, declared with (u)fixedMxN where M is the size in bits (increments of 8 up to 256) and N is the number of decimals after the point (up to 18), e.g. ufixed32x2

address

A 20-byte Ethereum address. The address object has many helpful member functions, the main ones being balance (returns the account balance) and transfer (transfer ether to the account).

byte array (fixed)

Fixed-size arrays of bytes, declared with bytes1 up to bytes32.

byte array (dynamic)

Variable-sized arrays of bytes, declared with bytes or string.

enum

User-defined type for enumerating discrete values: enum NAME {LABEL1, LABEL 2, ...}.

arrays

An array of any type, either fixed or dynamic: uint32[][5] is a fixed-size array of five dynamic arrays of unsigned integers

struct

User-defined data containers for grouping variables: struct NAME {TYPE1 VARIABLE1; TYPE2 VARIABLE2; ...}.

mapping

Hash lookup tables for key => value pairs: mapping(KEY_TYPE => VALUE_TYPE) NAME.

In addition to the data types above, Solidity also offers a variety of value literals that can be used to calculate different units:

time units

The units seconds, minutes, hours, and days can be used as a suffix, converting to multiples of the base unit seconds.

ether units

The units wei, finney, szabo, and ether can be used as a suffix, converting to multiples of the base unit wei.

So far, in our Faucet contract example, we used uint (which is an alias for uint256), for the withdraw_amount variable. We also indirectly used an address variable, which we set with msg.sender. We will use more of these data types in our examples in the rest of this chapter.

Let's use one of the unit multipliers, to improve the readability of our example contract Faucet. In the withdraw function we limit the maximum withdrawal, expressing the amount limit as wei, the base unit of ether:

```
require(withdraw_amount <= 1000000000000000000);
```

That's not very easy to read, so we can improve our code by using the unit multiplier ether, to express the value in ether instead of wei:

```
require(withdraw_amount <= 0.1 ether);
```

Predefined global variables and functions

When a contract is executed in the EVM, it has access to a small set of global objects. These include the `block`, `msg` and `tx` objects. In addition, Solidity exposes a number of EVM opcodes as predefined Solidity functions. In this section we will examine the variables and functions you can access from within a smart contract in Solidity.

Transaction/message call context

The `msg` object is the transaction call (EOA originated) or message call (contract originated) that launched this contract execution. It contains a number of useful attributes:

msg.sender

We've already used this one. It represents the address that initiated this contract call, not necessarily the originating EOA that sent the transaction. If our contract was called directly by an EOA transaction, then this is the address that signed the transaction, but otherwise it will be a contract address.

msg.value

The value of ether sent with this call (in wei).

msg.gas

The amount of gas left in the gas supply of this execution environment. It was deprecated in Solidity v0.4.21, and replaced by the `gasleft()` function.

msg.data

The data payload of this call into our contract.

msg.sig

The first four bytes of the data payload, which is the function selector.



Whenever a contract calls another contract, the values of all the attributes of `msg` change, to reflect the new caller's information. The only exception to this is the `delegatecall` function, which runs the code of another contract/library within the original `msg` context.

Transaction context

The tx object provides a means of accessing transaction related information:

tx.gasprice

The gas price in the calling transaction

tx.origin

The address of the originating EOA for this transaction. WARNING: unsafe!

Block context

The block object contains information about the current block:

block.blockhash(blockNumber)

The block hash of the specified block number, up to 256 blocks in the past. Deprecated and replaced with the blockhash() function in Solidity v0.4.22.

block.coinbase

The address of the recipient of the current block's fees and block reward.

block.difficulty

The difficulty (Proof-of-Work) of the current block.

block.gaslimit

The maximum amount of gas that can be spent across all transactions included in the current block.

block.number

The current block number (blockchain height).

block.timestamp

The timestamp placed in the current block by the miner, the number of seconds since the Unix epoch.

Address object

Any address, either passed as an input, or cast from a contract object, has a number of attributes and methods:

address.balance

The balance of the address, in wei. For example, the current contract balance is `address(this).balance`.

address.transfer(amount)

Transfer the amount (wei) to this address, throwing an exception on any error. We used this function in our Faucet example as a method on the `msg.sender` address, as `msg.sender.transfer()`.

address.send(amount)

Similar to `transfer` above, only instead of throwing an exception, it returns false on error. **WARNING:** always check the return value of `send()`.

address.call(payload)

Low-level CALL function - can construct an arbitrary message call with a data payload. Returns false on error. **WARNING:** unsafe - recipient can (accidentally or maliciously) use up all your gas causing your contract to halt with an OOG exception; always check the return value of `call()`.

address.callcode(payload)

Low-level CALLCODE function - like `address(this).call(...)` but with this contract's code replaced with that of `address`. Returns false on error. **WARNING:** advanced use only!

address.delegatecall()

Low-level DELEGATECALL function - like `callcode(...)` but with the full msg context seen by the current contract. Returns false on error. **WARNING:** advanced use only!

Built-in functions

Other functions worth noting are:

addmod, mulmod

Modulo addition and multiplication. For example, `addmod(x,y,k)` calculates $(x + y) \% k$.

`keccak256, sha256, sha3, ripemd160`

Functions to calculate hashes with various standard hash algorithms.

`ecrecover`

Recover the address used to sign a message from the signature.

`selfdestruct(recipient_address)`

delete the current contract, sending any remaining ether in the account to recipient_address.

`this`

the address of the currently executing contract account.

Contract definition

Solidity's principal data type is contract; our Faucet example simply defines a contract object. Similar to any object in an object-oriented language, the contract is a container that includes data and methods.

Solidity offers two other object types that are similar to a contract:

`interface`

An interface definition is structured exactly like a contract, except none of the functions are defined, they are only declared. This type of declaration is often called a *stub*; it tells you the functions' arguments and return types without any implementation. An interface specifies the "shape" of a contract; when inherited, each of the functions declared by the interface must be defined by the child.

`library`

A library contract is one that is meant to be deployed only once and used by other contracts, using the `delegatecall` method (see [Address object](#)).

Functions

Within a contract, we define functions that can be called by an EOA transaction or another contract. In our Faucet example, we have two functions: `withdraw` and the (unnamed) *fallback* function.

[Solicity function declaration syntax](#) shows the syntax we use to declare a function in Solidity:

```
function FunctionName([parameters]) {public|private|internal|external  
[pure|constant|view|payable] [modifiers] [returns (return types)]}
```

Figure 41. Solicity function declaration syntax

Let's look at each of these components:

FunctionName

The name of the function, which is used to call the function in a transaction (from an EOA), from another contract, or even from within the same contract. One function in each contract may be defined without a name, in which case it is the *fallback* function, which is called when no other function is named. The fallback function cannot have any arguments or return anything.

parameters

Following the name, we specify the arguments that must be passed to the function, with their names and types. In our Faucet example we defined uint withdraw_amount as the only argument to the withdraw function.

The next set of keywords (public, private, internal, external) specify the function's *visibility*:

public

Public is the default; such functions can be called by other contracts, EOA transactions, or from within the contract. In our Faucet example, both functions are defined as public.

external

External functions are like public, except they cannot be called from within the contract, unless explicitly prefixed with the keyword this.

internal

Internal functions are only accessible from within the contract - they cannot be called by another contract or EOA transaction. They can be called by derived contracts (those that inherit this one).

private

Private functions are like internal functions but cannot be called by derived contracts.

Keep in mind, the terms internal and private are somewhat misleading. Any function or data inside a

contract is always *visible* on the public blockchain, meaning that anyone can see the code or data. The keywords above only affect how and when a function can be *called*.

The next set of keywords (pure, constant, view, payable) affect the behavior of the function:

constant or view

A function marked as a *view* promises not to modify any state. The term *constant* is an alias for *view* that will be deprecated. At this time, the compiler does not enforce the *view* modifier, only producing a warning, but this is expected to become an enforced keyword in v0.5 of Solidity.

pure

A pure function is one that neither reads nor writes any variables in storage. It can only operate on arguments and return data, without reference to any stored data. Pure functions are intended to encourage declarative-style programming without side-effects or state.

payable

A payable function is one that can accept incoming payments. Functions without payable will reject incoming payments. There are two exceptions, due to design decisions in the EVM: coinbase payments and SELFDESTRUCT inheritance will be paid, even if the fallback function is not attributed as payable, but this makes sense because code execution is not part of those payments anyway.

As you can see in our Faucet example, we have one payable function (the fallback function), which is the only function that can receive incoming payments.

Contract constructor and selfdestruct

There is a special function that is only used once. When a contract is created, it also runs the *constructor function* if one exists, to initialize the state of the contract. The constructor is run in the same transaction as the contract creation. The constructor function is optional, as you'll notice our Faucet example has no constructor function.

Constructors can be specified in two ways. Up to and including Solidity v0.4.21, the constructor is a function whose name matches the name of the contract, as you'll see in the example [Constructor function prior to Solidity v0.4.22](#):

Constructor function prior to Solidity v0.4.22

```
contract MEContract {  
    function MEContract() {  
        // This is the constructor  
    }  
}
```

The difficulty with this format is that if the contract name is changed and the constructor function name is not changed, it is no longer a constructor. Likewise, if there is an accidental typo in the naming of the contract and/or constructor, the function is again no longer a constructor. This can cause some pretty nasty, unexpected and difficult-to-find bugs. Imagine for example if the constructor is setting the owner of the contract for purposes of control. If the function is not actually the constructor because of a naming error, not only will the owner be left unset at the time of contract creation, but the function may also be deployed as a permanent and "callable" part of the contract, like a normal function, allowing any third party to hijack the contract and become the "owner" after contract creation.

To address the potential problems with constructor functions being based on having an identical name as the contract, Solidity v0.4.22 introduces a constructor keyword that operates like a constructor function but does not have a name. Renaming the contract does not affect the constructor at all. Also, it is easier to identify which function is the constructor. It looks like this:

```
pragma ^0.4.22  
contract MEContract {  
    constructor () {  
        // This is the constructor  
    }  
}
```

To summarize, a contract's lifecycle starts with a creation transaction from an EOA or contract account. If there is a constructor, it is executed as part of contract creation, to initialize the state of the contract as it is being created, and is then discarded.

The other end of the contract's lifecycle is *contract destruction*. Contracts are destroyed by a special EVM opcode called SELFDESTRUCT. It used to be called SUICIDE, but that name was deprecated due to the negative associations of the word. In Solidity, this opcode is exposed as a high level built-in function

called `selfdestruct`, which takes one argument: the address to receive any ether balance remaining in the contract account. It looks like this:

```
selfdestruct(address recipient);
```

Note that you must explicitly add this command to your contract if you want it to be deletable - this is the only way a contract can be deleted, and it is not present by default. In this way, users of a contract who might rely on a contract being there forever, can be certain that a contract can't be deleted if it doesn't contain a `SELFDESTRUCT` opcode.

Adding a constructor and `selfdestruct` to our Faucet example

The Faucet example contract we introduced in [Ethereum Basics](#) does not have any constructor or `selfdestruct` functions. It is an eternal contract that cannot be deleted. Let's change that, by adding a constructor and `selfdestruct` function. We probably want the `selfdestruct` to be callable *only* by the EOA that originally created the contract. By convention, this is usually stored in an address variable called `owner`. Our constructor sets the `owner` variable, and the `selfdestruct` function will first check that the `owner` called it directly.

First our constructor:

```
// Version of Solidity compiler this program was written for
pragma solidity ^0.4.22;

// Our first contract is a faucet!
contract Faucet {

    address owner;

    // Initialize Faucet contract: set owner
    constructor() {
        owner = msg.sender;
    }

    [...]
```

We've changed the pragma directive to specify v0.4.22 as the minimum version for this example, as we are using the new constructor keyword introduced in v0.4.22 of Solidity. Our contract now has an address type variable named owner. The name "owner" is not special in any way. We could call this address variable "potato" and still use it the same way. The name owner simply makes its purpose clear.

Then, our constructor, which runs as part of the contract creation transaction, assigns the address from msg.sender to the owner variable. We used msg.sender in the withdraw function to identify the initiator of the withdrawal request. In the constructor however, the msg.sender is the EOA or contract address that initiated contract creation. We know this is the case *because* this is a constructor function: it only runs once, during contract creation.

Now we can add a function to destroy the contract. We need to make sure that only the owner can run this function, so we will use a require statement to control access. Here's how it will look:

```
// Contract destructor
function destroy() public {
    require(msg.sender == owner);
    selfdestruct(owner);
}
```

If anyone other calls this destroy function from an address other than owner, it will fail. But if the same address stored in owner by the constructor calls it, the contract will self-destruct and send any remaining balance to the owner address. Note that we did not use the unsafe tx.origin to determine whether the owner wished to destroy the contract - using tx.origin would allow malign contracts to destroy your contract without your permission.

Function modifiers

Solidity offers a special type of function which is called a *function modifier*. You apply modifiers to functions by adding the modifier name in the function declaration. Modifier functions are most often used to create conditions that apply to many functions within a contract. We have an access control statement already, in our destroy function. Let's create a function modifier that expresses that condition:

onlyOwner function modifier

```
modifier onlyOwner {
    require(msg.sender == owner);
}
```

In [onlyOwner function modifier](#) we see the declaration of a function modifier, named `onlyOwner`. This function modifier sets a condition on any function that it modifies, requiring that the address stored as the owner of the contract is the same as the address of the transaction's `msg.sender`. This is the basic design pattern for access control, allowing only the owner of a contract to execute any function that has the `onlyOwner` modifier.

You may have noticed that our function modifier has a peculiar syntactic "placeholder" in it, an underscore followed by a semicolon (`_;`). This placeholder is replaced by the code of the function that is being modified. Essentially, the modifier is "wrapped around" the modified function, placing its code in the location identified by the underscore character.

To apply a modifier, you add its name to the function declaration. More than one modifier can be applied to a function, as a comma-separated list, applied in the sequence they are declared.

Let's rewrite our `destroy` function to use the `onlyOwner` modifier:

```
function destroy() public onlyOwner {
    selfdestruct(owner);
}
```

The function modifier's name (`onlyOwner`) is after the keyword `public` and tells us that the `destroy` function is modified by the `onlyOwner` modifier. Essentially you can read this as "Only the owner can destroy this contract". In practice, the resulting code is equivalent to "wrapping" the code from `onlyOwner` around `destroy`.

Function modifiers are an extremely useful tool because they allow us to write preconditions for functions and apply them consistently, making the code easier to read and, as a result, easier to audit for security. They are most often used for access control, however, they are quite versatile and can be used for a variety of other purposes.

Inside a modifier, you can access all the values (variables and arguments) visible to the modified function. In this case, we can access the owner variable, which is declared within the contract. However, the inverse is not true: you cannot access any of the modifier's variables inside the modified function.

Contract inheritance

Solidity's contract object supports *inheritance*, which is a mechanism for extending a base contract with additional functionality. To use inheritance, specify a parent contract with the keyword is:

```
contract Child is Parent {  
    ...  
}
```

With this construct, the Child contract inherits all the methods, functionality, and variables of Parent. Solidity also supports multiple inheritance, which can be specified by comma-separated contract names after the keyword is:

```
contract Child is Parent1, Parent2 {  
    ...  
}
```

Contract inheritance allows us to write our contracts in such a way as to achieve modularity, extensibility and reuse. We start with contracts that are simple and implement the most generic capabilities, then extend them by inheriting those capabilities in more specialized contracts.

In our Faucet contract, we introduced the constructor and destructor, together with access control for an owner, assigned on construction. Those capabilities are quite generic: many contracts will have them. We can define them as generic contracts, then use inheritance to extend them to the Faucet contract.

We start by defining a base contract owned, which has an owner variable, setting it in the contract's constructor:

```
contract owned {
    address owner;

    // Contract constructor: set owner
    constructor() {
        owner = msg.sender;
    }

    // Access control modifier
    modifier onlyOwner {
        require(msg.sender == owner);
        -
    }
}
```

Next, we define a base contract mortal, which inherits owned:

```
contract mortal is owned {
    // Contract destructor
    function destroy() public onlyOwner {
        selfdestruct(owner);
    }
}
```

As you can see, the mortal contract can use the onlyOwner function modifier, defined in owned. It indirectly also uses the owner address variable and the constructor defined in owned. Inheritance makes each contract simpler and focused on its specific functionality, allowing us to manage the details in a modular way.

Now we can further extend the owned contract, inheriting its capabilities in Faucet:

```
contract Faucet is mortal {  
    // Give out ether to anyone who asks  
    function withdraw(uint withdraw_amount) public {  
        // Limit withdrawal amount  
        require(withdraw_amount <= 0.1 ether);  
        // Send the amount to the address that requested it  
        msg.sender.transfer(withdraw_amount);  
    }  
    // Accept any incoming amount  
    function () public payable {}  
}
```

By inheriting `mortal`, which in turn inherits `owned`, the `Faucet` contract now has the `constructor` and `destroy` functions, and a defined owner. The functionality is the same as when those functions were within `Faucet`, but now we can reuse those functions in other contracts without writing them again. Code reuse and modularity make our code cleaner, easier to read, and easier to audit.

Error handling (`assert`, `require`, `revert`)

A contract call can terminate and return an error. Error handling in Solidity is handled by four functions: `assert`, `require`, `revert`, and `throw` (now deprecated).

When a contract terminates with an error, all the state changes (changes to variables, balances, etc.) are reverted, all the way up the chain of contract calls if more than one contract was called. This ensures that transactions are atomic, meaning they either complete successfully or have no effect on state and are reverted entirely.

The `assert` and `require` functions operate in the same way, evaluating a condition and stopping execution with an error if the condition is false. By convention, `assert` is used when the outcome is expected to be true, meaning that we use `assert` to test internal conditions. By comparison, `require` is used when testing inputs (such as function arguments or transaction fields), setting our expectations for those conditions.

We've used `require` in our function modifier `onlyOwner`, to test that the message sender is the owner of the contract:

```
require(msg.sender == owner);
```

The require function acts as a *gate condition*, preventing execution of the rest of the function and producing an error if it is not satisfied.

As of Solidity v0.4.22, require can also include a helpful text message that can be used to show the reason for the error. The error message is recorded in the transaction log. So we can improve our code, by adding an error message in our require function:

```
require(msg.sender == owner, "Only the contract owner can call this function");
```

The revert and throw functions halt the execution of the contract and revert any state changes. The throw function is obsolete and will be removed in future versions of Solidity - you should use revert instead. The revert function can also take an error message as the only argument, which is recorded in the transaction log.

Certain conditions in a contract will generate errors regardless of whether we explicitly check for them. For example, in our Faucet contract, we don't check whether there is enough ether to satisfy a withdrawal request. That's because the transfer function will fail with an error and revert the transaction if there is insufficient balance to make the transfer:

```
msg.sender.transfer(withdraw_amount);
```

However, it might be better to check explicitly and provide a clear error message on failure. We can do that by adding a require statement before the transfer:

```
require(this.balance >= withdraw_amount,  
       "Insufficient balance in faucet for withdrawal request");  
msg.sender.transfer(withdraw_amount);
```

Additional error checking code like this will increase gas consumption slightly, but it offers better error reporting than if omitted. You will need to find the right balance between gas consumption and verbose

error checking based on the expected use of your contract. In the case of a Faucet intended for a testnet, we'd probably err on the side of extra reporting even if it costs more gas. Perhaps for a mainnet contract we'd choose to be frugal with our gas usage instead.

Events

Events are Solidity constructs that facilitate the production of transaction logs. When a transaction completes (successfully or not), it produces a *transaction receipt*, as we will see in [The Ethereum Virtual Machine](#). The transaction receipt contains *log* entries that provide information about the actions that occurred during the execution of the transaction. Events are the Solidity high-level objects that are used to construct these logs.

Events are especially useful for light clients and DApp services, which can "watch" for specific events and report them to the user-interface, or make a change in the state of the application to reflect an event in an underlying contract.

Event objects take arguments that are serialized and recorded in the transaction logs, in the blockchain. You can supply the keyword `indexed` before an argument, to make the value part of an indexed table (hash table) that can be searched or filtered by an application.

We have not added any events in our Faucet example, so far, so let's do that. We will add two events, one to log any withdrawals and one to log any deposits. We will call these events `Withdrawal` and `Deposit` respectively. First, we define the events in the Faucet contract:

```
contract Faucet is mortal {  
    event Withdrawal(address indexed to, uint amount);  
    event Deposit(address indexed from, uint amount);  
  
    [...]  
}
```

We've chosen to make the addresses indexed, to allow searching and filtering in any user interface built to access our Faucet.

Next, we use the `emit` keyword to incorporate the event data in the transaction logs:

```

// Give out ether to anyone who asks
function withdraw(uint withdraw_amount) public {
    [...]
    msg.sender.transfer(withdraw_amount);
    emit Withdrawal(msg.sender, withdraw_amount);
}
// Accept any incoming amount
function () public payable {
    emit Deposit(msg.sender, msg.value);
}

```

The resulting Faucet.sol contract looks like this example: [Faucet8.sol: Revised Faucet contract, with events](#).

Faucet8.sol: Revised Faucet contract, with events

```

// Version of Solidity compiler this program was written for
pragma solidity ^0.4.22;

contract owned {
    address owner;
    // Contract constructor: set owner
    constructor() {
        owner = msg.sender;
    }
    // Access control modifier
    modifier onlyOwner {
        require(msg.sender == owner, "Only the contract owner can call
this function");
        -
    }
}

contract mortal is owned {
    // Contract destructor
    function destroy() public onlyOwner {
        selfdestruct(owner);
    }
}

```

```
}

contract Faucet is mortal {
    event Withdrawal(address indexed to, uint amount);
    event Deposit(address indexed from, uint amount);

    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {
        // Limit withdrawal amount
        require(withdraw_amount <= 0.1 ether);
        require(this.balance >= withdraw_amount,
            "Insufficient balance in faucet for withdrawal request");
        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
        emit Withdrawal(msg.sender, withdraw_amount);
    }
    // Accept any incoming amount
    function () public payable {
        emit Deposit(msg.sender, msg.value);
    }
}
```

Catching Events

OK, so we've set up our contract to emit events. How do we see the results of a transaction and "catch" the events? The web3.js library provides a data structure that contains a transaction's logs. Within those we can see the events generated by the transaction.

Let's use truffle to run a test transaction on the revised Faucet contract. Follow the instructions in [Truffle](#) to set up a project directory and compile the Faucet code. The source code can be found in the book's GitHub repository under code/truffle/FaucetEvents.

```

$ truffle develop
truffle(develop)> compile
truffle(develop)> migrate
Using network 'develop'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
    ...
    ... 0xb77ceae7c3f5afb7fbe3a6c5974d352aa844f53f955ee7d707ef6f3f8e6b4e61
      Migrations: 0x8cdaf0cd259887258bc13a92c0a6da92698644c0
Saving successful migration to network...
  ...
  ... 0xd7bc86d31bee32fa3988f1c1eabce403a1b5d570340a3a9cdba53a472ee8c956
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying Faucet...
  ...
  ... 0xfa850d754314c3fb83f43ca1fa6ee20bc9652d891c00a2f63fd43ab5fb0d781
    Faucet: 0x345ca3e014aaf5dca488057592ee47305d9b3e10
Saving successful migration to network...
  ...
  ... 0xf36163615f41ef7ed8f4a8f192149a0bf633fe1a2398ce001bf44c43dc7bdda0
Saving artifacts...

truffle(develop)> Faucet.deployed().then(i => {FaucetDeployed = i})
truffle(develop)> FaucetDeployed.send(web3.toWei(1, "ether")).then(res =>
{ console.log(res.logs[0].event, res.logs[0].args) })
Deposit { from: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
  amount: BigNumber { s: 1, e: 18, c: [ 10000 ] } }
truffle(develop)> FaucetDeployed.withdraw(web3.toWei(0.1,
"ether")).then(res => { console.log(res.logs[0].event, res.logs[0].args)
})
Withdrawal { to: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
  amount: BigNumber { s: 1, e: 17, c: [ 1000 ] } }

```

After deploying the contract using the `deployed()` function, we execute two transactions. The first transaction is a deposit (using `send`), which emits a `Deposit` event in the transaction logs:

```

Deposit { from: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
  amount: BigNumber { s: 1, e: 18, c: [ 10000 ] } }

```

Next, we use the withdraw function to make a withdrawal. This emits a Withdrawal event:

```
Withdrawal { to: '0x627306090abab3a6e1400e9345bc60c78a8bef57',  
amount: BigNumber { s: 1, e: 17, c: [ 1000 ] } }
```

To get these events, we looked at the logs array returned as a result (res) of the transactions. The first log entry (logs[0]) contains an event name in logs[0].event and the event arguments in logs[0].args. By showing these on the console, we can see the emitted event name and the event arguments.

Events are a very useful mechanism, not only for intra-contract communication, but also for debugging during development.

Calling other contracts (send, call, callcode, delegatecall)

Calling other contracts from within your contract is a very useful but potentially dangerous operation. We'll examine the various ways you can achieve this and evaluate the risks of each method. In short, the risks arise from the fact that you may have no idea about a contract you are calling into or which is calling into your contract. When writing smart contracts, you must keep in mind that, while you may mostly expect to be dealing with EOAs, there is nothing to stop arbitrarily complex and perhaps malign contracts from calling into and being called by your code.

Creating a new instance

The safest way to call another contract is if you create that other contract yourself. That way, you are certain of its interfaces and behavior. To do this, you can simply instantiate it, using the keyword new, as in other object-oriented languages. In Solidity, the keyword new will create the contract on the blockchain and return an object that you can use to reference it. Let's say you want to create and call a Faucet contract from within another contract called Token:

```
contract Token is mortal {  
    Faucet _faucet;  
  
    constructor() {  
        _faucet = new Faucet();  
    }  
}
```

This mechanism for contract construction ensures that you know the exact type of contract and its interface. The contract Faucet must be defined within the scope of Token, which you can do with an import statement if the definition is in another file:

```
import "Faucet.sol";

contract Token is mortal {
    Faucet _faucet;

    constructor() {
        _faucet = new Faucet();
    }
}
```

We can optionally specify the value of ether transfer on creation, and pass arguments to the new contract's constructor:

```
import "Faucet.sol";

contract Token is mortal {
    Faucet _faucet;

    constructor() {
        _faucet = (new Faucet).value(0.5 ether)();
    }
}
```

We can also then call the Faucet functions. In this example, we call the destroy function of Faucet, from within the destroy function of Token:

```
import "Faucet.sol";

contract Token is mortal {
    Faucet _faucet;

    constructor() {
        _faucet = (new Faucet).value(0.5 ether)();
    }

    function destroy() ownerOnly {
        _faucet.destroy();
    }
}
```

Note that, while you are the owner of the Token contract, the Token contract itself owns the new Faucet contract, so only the Token contract can destroy it.

Addressing an existing instance

Another way we can call a contract is to cast the address of an existing instance of the contract. With this method, we apply a known interface to an existing instance. It is therefore critically important that we know, for sure, that the instance we are addressing is in fact of the type we assume. Let's look at an example:

```
import "Faucet.sol";

contract Token is mortal {

    Faucet _faucet;

    constructor(address _f) {
        _faucet = Faucet(_f);
        _faucet.withdraw(0.1 ether)
    }
}
```

Here, we take an address provided as an argument to the constructor, `_f`, and we cast it to a Faucet object. This is much riskier than the previous mechanism, because we don't know for sure whether that address actually is a Faucet object. When we call withdraw, we are assuming that it accepts the same arguments and executes the same code as our Faucet declaration, but we can't be sure. For all we know, the withdraw function at this address could execute something completely different from what we expect, even if it is named the same. Using addresses passed as input and casting them into specific objects is therefore much more dangerous than creating the contract ourselves.

Raw call, delegatecall

Solidity offers some even more "low-level" functions for calling other contracts. These correspond directly to EVM opcodes of the same name and allow us to construct a contract-to-contract call manually. As such, they represent the most flexible *and* the most dangerous mechanisms for calling other contracts.

Here's the same example, using a call method:

```
contract Token is mortal {  
    constructor(address _faucet) {  
        _faucet.call("withdraw", 0.1 ether);  
    }  
}
```

As you can see, this type of call, is a *blind* call into a function, very much like constructing a raw transaction, only from within a contract's context. It can expose our contract to a number of security risks, most importantly *re-entrancy*, which we will discuss in more detail in [Re-Entrancy](#). The call function will return false if there is a problem, so we can evaluate the return value, for error handling:

```
contract Token is mortal {  
    constructor(address _faucet) {  
        if !_faucet.call("withdraw", 0.1 ether)) {  
            revert("Withdrawal from faucet failed");  
        }  
    }  
}
```

Another variant of call is delegatecall, which replaced the more dangerous callcode. The callcode method will be deprecated soon, so it should not be used.

As mentioned in [Address object](#), a delegatecall is different from a call, in that the msg context does not change. For example, whereas a call changes the value of msg.sender to be the calling contract, a delegatecall keeps the same msg.sender as it is in the calling contract. Essentially, delegatecall runs the code of another contract inside the context of the execution of the current contract. It is most often used to invoke code from a library. It also allows you to draw on the pattern of using library functions stored elsewhere, but have that code work with the storage data of your contract.

The delegate call should be used with great caution. It can have some unexpected effects, especially if the contract you call was not designed as a library.

Let's use an example contract to demonstrate the various call semantics used by call and delegatecall for calling libraries and contracts. We use an event to log the details of each call and see how the calling context changes depending on the call type:

CallExamples.sol: An example of different call semantics.

```
pragma solidity ^0.4.22;

contract calledContract {
    event callEvent(address sender, address origin, address from);
    function calledFunction() public {
        emit callEvent(msg.sender, tx.origin, this);
    }
}

library calledLibrary {
    event callEvent(address sender, address origin, address from);
    function calledFunction() public {
        emit callEvent(msg.sender, tx.origin, this);
    }
}

contract caller {
    function make_calls(calledContract _calledContract) public {

        // Calling the calledContract and calledLibrary directly
        _calledContract.calledFunction();
        calledLibrary.calledFunction();

        // Low level calls using the address object for calledContract
        require(address(_calledContract).call(bytes4(keccak256("calledFunction()"))));

        require(address(_calledContract).delegatecall(bytes4(keccak256("calledFunction()"))));
    }
}
```

As you can see in [CallExamples.sol: An example of different call semantics.](#), our main contract is caller, which calls a library calledLibrary and a contract calledContract. Both the called library and contract have identical functions calledFunction, which emit an event calledEvent. The event calledEvent logs three pieces of data: msg.sender, tx.origin, and this. Each time calledFunction is called it may have a different execution context (with different values for the potentially all the context variables), depending on whether it is called directly or through delegatecall.

In caller, we first call the contract and library directly, by invoking the calledFunction in each. Then, we explicitly use the low-level functions call and delegatecall to call the calledContract.calledFunction. This way we can see how the various calling mechanisms behave.

Let's run this in a truffle development environment and capture the events, to see how it looks:

```

truffle(develop)> migrate
Using network 'develop'.
[...]
Saving artifacts...
truffle(develop)> web3.eth.accounts[0]
'0x627306090abab3a6e1400e9345bc60c78a8bef57'
truffle(develop)> caller.address
'0x8f0483125fcb9aaefa9209d8e9d7b9c8b9fb90f'
truffle(develop)> calledContract.address
'0x345ca3e014aaf5dca488057592ee47305d9b3e10'
truffle(develop)> calledLibrary.address
'0xf25186b5081ff5ce73482ad761db0eb0d25abfbf'
truffle(develop)> caller.deployed().then( i => { callerDeployed = i })

truffle(develop)>
callerDeployed.make_calls(calledContract.address).then(res => {
res.logs.forEach( log => { console.log(log.args) }})
{ sender: '0x8f0483125fcb9aaefa9209d8e9d7b9c8b9fb90f',
origin: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
from: '0x345ca3e014aaf5dca488057592ee47305d9b3e10' }
{ sender: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
origin: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
from: '0x8f0483125fcb9aaefa9209d8e9d7b9c8b9fb90f' }
{ sender: '0x8f0483125fcb9aaefa9209d8e9d7b9c8b9fb90f',
origin: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
from: '0x345ca3e014aaf5dca488057592ee47305d9b3e10' }
{ sender: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
origin: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
from: '0x8f0483125fcb9aaefa9209d8e9d7b9c8b9fb90f' }

```

Let's see what happened here. We called the `make_calls` function and passed the address of `calledContract`, then caught the four events emitted by each of the different calls. Look at the `make_calls` function and let's walk through each step.

The first call is:

```
_calledContract.calledFunction();
```

Here, we're calling the calledContract.calledFunction directly, using the high-level ABI for calledFunction. The event emitted is:

```
sender: '0x8f0483125fcb9aaaefa9209d8e9d7b9c8b9fb90f',
origin: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
from: '0x345ca3e014aaaf5dca488057592ee47305d9b3e10'
```

As you can see, msg.sender is the address of the caller contract. The tx.origin is the address of our account web3.eth.accounts[0] that sent the transaction to caller. The event was emitted by calledContract, as we can see from the last argument in the event.

The next call in make_calls, is to the library:

```
calledLibrary.calledFunction();
```

It looks identical to how we called the contract, but behaves **very** differently. Let's look at the second event emitted:

```
sender: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
origin: '0x627306090abab3a6e1400e9345bc60c78a8bef57',
from: '0x8f0483125fcb9aaaefa9209d8e9d7b9c8b9fb90f'
```

This time, the msg.sender is not the address of caller. Instead it is the address of our account, and is the same as the transaction origin. That's because when you call a library, the call is always delegatecall and runs within the context of the caller. So, when calledLibrary code was running, it inherited the execution context of caller, as if its code was running inside caller. The variable this (shown as from in the event emitted) is the address of caller, even though it is accessed from within calledLibrary.

The next two calls, using the low-level call and delegatecall, verify our expectations, emitting events that mirror what we just saw above.

Gas considerations

Gas is described in more detail in [Gas](#), and is an incredibly important consideration in smart contract programming. Gas is a resource constraining the maximum amount of computation that Ethereum will allow a transaction to consume. If the gas limit is exceeded during computation, the following series of events occurs:

- An "out of gas" exception is thrown.
- The state of the contract prior to execution is restored (reverted).
- All ether used to pay for the gas is taken as a transaction fee; it is *not* refunded.

Because gas is paid by the user who initiates the transaction, users are discouraged from calling functions that have a high gas cost. It is thus in the programmer's best interest to minimize the gas cost of a contract's functions. To this end, there are certain practices that are recommended when constructing smart contracts, so as to minimize the gas cost of a function call.

Avoid dynamically-sized arrays

Any loop through a dynamically sized array where a function performs operations on each element or searches for a particular element introduces the risk of using too much gas. Indeed, the contract may run out of gas before finding the desired result, or before acting on every element, thus wasting time and ether without giving any result at all.

Avoid calls to other contracts

Calling other contracts, especially when the gas cost of their functions is not known, introduces the risk of running out of gas. Avoid using libraries that are not well tested and broadly used. The less scrutiny a library has received from other programmers, the greater the risk of using it.

Estimating gas cost

If you need to estimate the gas necessary to execute a certain method of a contract considering its arguments, you could use the following procedure:

```
var contract = web3.eth.contract(abi).at(address);
var gasEstimate = contract.myAwesomeMethod.estimateGas(arg1, arg2, {from: account});
```

gasEstimate will tell us the number of gas units needed for its execution. It is an estimate because of the Turing completeness of the EVM - it is relatively trivial to create a function that will take vastly different amounts of gas to execute different calls. Even production code can change execution paths in subtle ways, resulting in hugely different gas costs from one call to the call. However, most functions are sensible and `estimateGas` will give a good estimate most of the time.

To obtain the **gas price** from the network you can use;

```
var gasPrice = web3.eth.getGasPrice();
```

And from there, estimate the **gas cost**:

```
var gasCostInEther = web3.fromWei((gasEstimate * gasPrice), 'ether');
```

Let's apply our gas estimation functions to estimating the gas cost of our Faucet example, using the code from the book's repository found here:

```
code/truffle/FaucetEvents
```

We start truffle in development mode, and execute a JavaScript file [gas_estimates.js: Using the estimateGas function](#), which contains:

gas_estimates.js: Using the estimateGas function

```
var FaucetContract = artifacts.require("./Faucet.sol");

FaucetContract.web3.eth.getGasPrice(function(error, result) {
    var gasPrice = Number(result);
    console.log("Gas Price is " + gasPrice + " wei"); // "1000000000000000"

    // Get the contract instance
    FaucetContract.deployed().then(function(FaucetContractInstance) {

        // Use the keyword 'estimateGas' after the function name to get
        // the gas estimation for this particular function (aprove)
        FaucetContractInstance.send(web3.toWei(1, "ether"));
        return
    FaucetContractInstance.withdraw.estimateGas(web3.toWei(0.1, "ether"));

}).then(function(result) {
    var gas = Number(result);

    console.log("gas estimation = " + gas + " units");
    console.log("gas cost estimation = " + (gas * gasPrice) + " wei");
    console.log("gas cost estimation = " +
    FaucetContract.web3.fromWei((gas * gasPrice), 'ether') + " ether");
    });
});
```

Here's how that looks in the truffle development console:

```
$ truffle develop

truffle(develop)> exec gas_estimates.js
Using network 'develop'.

Gas Price is 20000000000 wei
gas estimation = 31397 units
gas cost estimation = 6279400000000000 wei
gas cost estimation = 0.00062794 ether
```

It is recommended that you evaluate the gas cost of functions as part of your development workflow, to avoid any surprises when deploying contracts to the mainnet.

Conclusions

In this chapter we started working with smart contracts in detail and explored the Solidity contract programming language. We took a simple example contract Faucet.sol and gradually improved it and made it more complex, using it to explore various aspects of the Solidity language. Next, in [Smart contracts and Vyper](#) we will work with Vyper, another contract oriented programming language. We will compare Vyper to Solidity, showing some of the differences in the design of these two languages and deepening our understanding of smart contract programming.

Smart contracts and Vyper

Vyper is an experimental, contract-oriented programming language for the Ethereum Virtual Machine (EVM) which strives to provide superior auditability, by making it easier for developers to produce intelligible code. In fact, one of the principles of Vyper is to make it virtually impossible for developers to write misleading code.

In this chapter we will look at common problems with smart contracts, introduce the Vyper contract programming language and compare it to Solidity, demonstrating the differences.

Vulnerabilities and Vyper

A recent study [https://arxiv.org/pdf/1802.06038.pdf] analyzed nearly one million deployed, Ethereum, smart contracts and found that many of these smart contracts contained serious vulnerabilities. During their analysis, the researchers outlined three basic categories of trace vulnerabilities. The categories include:

Suicidal contracts

Smart contracts which can be killed by arbitrary addresses

Greedy contracts

Smart contracts which can reach a state in which they cannot release Ether

Prodigal contracts

Smart contracts which can be made to release Ether to arbitrary addresses

Vulnerabilities are introduced into smart contracts via code. It may be strongly argued that these and other vulnerabilities are not intentionally introduced into smart contracts. Nevertheless, undesirable smart contract code evidently results in the unexpected loss of funds for Ethereum users, and this is not ideal. Vyper is designed to make it easier to write secure code, or equally to make it more difficult to accidentally write misleading or vulnerable code.

Comparison to Solidity

One of the ways in which Vyper tries to make unsafe code harder to write is by deliberately *omitting* some of Solidity's features. It is important for those considering developing smart contracts, in Vyper, to understand what features Vyper does *not* have, and why. Therefore, in this next section, we will explore

those features and provide justification for why they have been omitted.

Modifiers

In Solidity, you can write a function using modifiers. For example, the following function called `changeOwner` will run the code in a modifier, called `onlyBy`, as part of its execution.

```
function changeOwner(address _newOwner)
    public
    onlyBy(owner)
{
    owner = _newOwner;
}
```

As we can see below, the modifier called `onlyBy` enforces a rule in relation to ownership. As you can see, this particular modifier acts as a mechanism to perform a pre-check on behalf of the `changeOwner` function.

```
modifier onlyBy(address _account)
{
    require(msg.sender == _account);
    -
}
```

Modifiers are not just there to perform checks, as shown above. In fact, as modifiers, they can significantly change a smart contract's environment, in the context of the calling function. Put simply, modifiers are pervasive.

Let's look at another Solidity style example.

```

enum Stages {
    SafeStage
    DangerStage,
    FinalStage
}

uint public creationTime = now;
Stages public stage = Stages.SafeStage;

function nextStage() internal {
    stage = Stages(uint(stage) + 1);
}

modifier stageTimeConfirmation() {
    if (stage == Stages.SafeStage &&
        now >= creationTime + 10 days)
        nextStage();
    -
}

function a()
public
stageTimeConfirmation
// More code goes here
{
}

```

On one hand, developers should always check any other code, which their own code is calling. However, it is possible that under certain situations (like time constraints or exhaustion, resulting in lack of concentration) a developer may overlook a single line of code. This is especially the case if a developer has to jump around inside a large file whilst mentally keeping track of the function call hierarchy and committing the state of smart contract variables to memory.

Let's look at the above example, in a bit more depth. Imagine that a developer is writing a public function called `a`. The developer is new to this contract and is utilizing a modifier written by someone else. At a glance it appears that the `stageTimeConfirmation` modifier is simply performing some checks in relation to the age of the contract in relation to the calling function. What the developer may

not realize is that the modifier is also calling another function; `nextStage`. In this, simplistic demonstration scenario, the overall result of simply calling the public function `a`, results in the smart contract's `stage` variable moving from `SafeStage` to `DangerStage`.

Vyper's has done away with modifiers altogether. The recommendations from Vyper are as follows. If only performing assertions with modifiers, then simply use in-line checks and asserts as part of the function. If modifying smart contract state and so forth, then again, make these changes explicitly part of the function. Doing this improves audit-ability and readability, as the reader doesn't have to mentally (or manually) "wrap" the modifier code around the function to see what it does.

Class inheritance

Inheritance allows programmers to harness pre-written code by acquiring pre-existing functionality, properties and behaviors from existing software libraries. Inheritance is powerful and promotes the reuse of code. Solidity supports multiple inheritance as well as polymorphism, but while these are key features of object oriented programming, Vyper does not support them. Vyper maintains that the implementation of inheritance requires coders and auditors to jump between multiple files in order to understand what the program is doing. Vyper also takes the view that multiple inheritance can make code too complicated to understand, a view tacitly admitted by the Solidity [documentation](#) [<https://github.com/ethereum/solidity/blob/release/docs/contracts.rst#inheritance>], which gives an example of how multiple inheritance can be problematic.

Inline assembly

Inline assembly gives developers low-level access to the Ethereum Virtual Machine (EVM), allowing Solidity programs to perform operations by directly accessing EVM instructions. For example, the following inline assembly code adds 3 to memory location 0x80:

```
3 0x80 mload add 0x80 mstore
```

Vyper considers the loss of readability to be too high a price to pay for the extra power, and thus does not support inline assembly.

Function overloading

Function overloading allows developers to write multiple functions of the same name. Which function is used on a given occasion depends on the types of the arguments supplied. Take the following two

functions, for example:

```
function f(uint _in) public pure returns (uint out) {
    out = 1;
}

function f(uint _in, bytes32 _key) public pure returns (uint out) {
    out = 2;
}
```

The first function (named f) accepts an input argument of type uint; the second function (also named f) accepts two arguments, one of type uint and one of type bytes32. Having multiple function definitions with the same name taking different arguments can be confusing, so Vyper does not support function overloading.

Variable typecasting

There are two sorts of typecasting.

Implicit typecasting is often performed at compile time. For example if a type conversion is semantically sound and no information is likely to be lost, the compiler can perform an implicit conversion, such as converting a variable of type uint8 to uint16. The earliest versions of Vyper allowed implicit typecasting of variables, but recent versions do not.

Explicit typecasts can be inserted in Solidity. Unfortunately, they can lead to unexpected behavior. For example, casting a uint32 to the smaller type uint16 simply removes the higher-order bits, as demonstrated below.

```
uint32 a = 0x12345678;
uint16 b = uint16(a);
//Variable b is 0x5678 now
```

Vyper instead has a convert() function to perform explicit casts. The convert function (found on line 82 of [convert.py](https://github.com/ethereum/vyper/blob/master/vyper/types/convert.py) [https://github.com/ethereum/vyper/blob/master/vyper/types/convert.py]) is as follows:

```
def convert(expr, context):
    output_type = expr.args[1].s
    if output_type in conversion_table:
        return conversion_table[output_type](expr, context)
    else:
        raise Exception("Conversion to {} is
invalid.".format(output_type))
```

Note the use of conversion_table (found on line 90 of the same file), which looks like this:

```
conversion_table = {
    'int128': to_int128,
    'uint256': to_uint256,
    'decimal': to_decimal,
    'bytes32': to_bytes32,
}
```

When a developer calls convert, it references conversion_table, which ensures that the appropriate conversion is performed. For example, if a developer passes an 'int128' to the convert function, the to_int128 function on line 26 of the same (convert.py) file will be executed. The to_int128 function is as follows:

```

@signature(('int128', 'uint256', 'bytes32', 'bytes'), 'str_literal')
def to_int128(expr, args, kwargs, context):
    in_node = args[0]
    typ, len = get_type(in_node)
    if typ in ('int128', 'uint256', 'bytes32'):
        if in_node.typ.is_literal and not SizeLimits.MINNUM <=
in_node.value <= SizeLimits.MAXNUM:
            raise InvalidLiteralException("Number out of range:
{}".format(in_node.value), expr)
        return LLLnode.from_list(
            ['clamp', ['mload', MemoryPositions.MINNUM], in_node,
['mload', MemoryPositions.MAXNUM]], typ=BaseType('int128'),
pos=getpos(expr)
        )
    else:
        return byte_array_to_num(in_node, expr, 'int128')

```

As you can see, the conversion process ensures that no information can be lost; if it could be, an exception is raised. The conversion code prevents truncation (as seen above) as well as other anomalies which would ordinarily be allowed by implicit typecasting.

Choosing explicit over implicit typecasting means that the developer is responsible for performing all casts. While this approach does produce more verbose code, it also improves the safety and auditability of smart contracts.

Pre-conditions and post-conditions

Vyper handles pre-conditions, post-conditions and state changes explicitly. Whilst this produces redundant code, it also allows for maximal readability and safety. When writing a smart contract in Vyper, a developer should observe the following 3 points. Ideally, each of the 3 points should be carefully considered and then thoroughly documented in the code. Doing so will improve the design of the code, ultimately making code more readable and auditable.

- Condition - What is the current state/condition of the Ethereum state variables?
- Effects - What effects will this smart contract code have on the condition of the state variables upon execution i.e. what *will* be affected, and what *will not* be affected? Are these effects congruent with the smart contract's intentions?

- Interaction - Now that the first two steps have been exhaustively dealt with, it is time to run the code. Before deployment, logically step through the code and consider all of the possible permanent outcomes, consequences and scenarios of executing the code, including interactions with other contracts.

Decorators

Decorators like `@private` `@public` `@constant` and `@payable` may be used at the start of each function.

@private decorator

The `@private` decorator makes the function inaccessible from outside the contract.

@public decorator

The `@public` decorator makes the function both visible and executable publicly. For example, even the Ethereum wallet will display such functions when viewing the contract.

@constant decorator

Functions with the `@constant` decorator are not allowed to change state variables. In fact, the compiler will reject the entire program (with an appropriate error) if the function tries to change a state variable.

@payable decorator

Only functions with the `@payable` decorator are allowed to transfer value.

Vyper implements [the logic of decorators](#) [https://github.com/ethereum/vyper/blob/master/vyper/signatures/function_signature.py#L93] explicitly. For example, the Vyper compilation process will fail if a function has both a `@payable` decorator and a `@constant` decorator. This makes sense because a function that transfers value has by definition updated the state, so cannot be `@constant`. Each Vyper function must be decorated with either `@public` or `@private` (but not both!).

Function and variable ordering

Each individual Vyper smart contract consists of a single Vyper file only. In other words, all of a given Vyper smart contract's code, including all functions, variables and so forth exist in one place. Vyper requires that each smart contract's function and variable declarations are physically written in a

particular order. Solidity does not have this requirement at all. Let's take a quick look at a Solidity example.

```
pragma solidity ^0.4.0;

contract ordering {

    function topFunction()
    external
    returns (bool) {
        initializedBelowTopFunction = this.lowerFunction();
        return initializedBelowTopFunction;
    }

    bool initializedBelowTopFunction;
    bool lowerFunctionVar;

    function lowerFunction()
    external
    returns (bool) {
        lowerFunctionVar = true;
        return lowerFunctionVar;
    }

}
```

In the above Solidity example the function called *topFunction* is calling another function *lowerFunction*. This function called *topFunction* is also assigning a value to a variable called *initializedBelowTopFunction*. As you can see, Solidity does not require these functions and variables to be physically declared before being called upon by the executing code. The above is valid Solidity code which will compile successfully.

Vyper's ordering requirements are not a new thing, in fact these ordering requirements have always been present in Python programming. The ordering, required by Vyper, is straight forward and logical as we will see in this next example.

```
# Declare a variable called theBool
theBool: public(bool)

# Declare a function called topFunction
@public
def topFunction() -> bool:
    # Assign a value to the already declared function called theBool
    self.theBool = True
    return self.theBool

# Declare a function called lowerFunction
@public
def lowerFunction():
    # Call the already declared function called topFunction
    assert self.topFunction()
```

The above Vyper syntax example shows the correct ordering of functions and variables in a Vyper smart contract. Note how the variable *theBool* and the function *topFunction* are declared before they are assigned a value and called respectively. If *theBool* was declared below *topFunction* or if *topFunction* was declared below *lowerFunction* this contract would not compile.

Online code editor and compiler

Vyper has its own [online code editor and compiler](https://vyper.online) [<https://vyper.online>], which allows you to write and then compile your smart contracts into Bytecode, ABI and LLL using only your web browser. The Vyper online compiler has a variety of prewritten smart contracts for your convenience. These include a simple open auction, safe remote purchases, ERC20 token and more.

Compiling using the command line

Each Vyper contract is saved in a single file with the .vy extension. Once installed Vyper can compile and provide bytecode by running the following command:

```
vyper ~/hello_world.vy
```

The human-readable ABI description (in JSON format) can then be obtained by running the following command:

```
vyper -f json ~/hello_world.v.py
```

Protecting against overflow errors at the compiler level

Overflow errors in software can be catastrophic when dealing with real value. This [transaction](#) [<https://etherscan.io/tx/0xad89ff16fd1ebe3a0a7cf4ed282302c06626c1af33221ebe0d3a470aba4a660f>] shows the malicious transfer of over 57,896,044,618,658,100,000,000,000,000,000,000,000,000,000,000,000 BEC tokens. The transaction, which occurred in mid April of 2018, is the result of an integer overflow issue in BeautyChain's ERC20 token contract (BecToken.sol). Solidity developers do have libraries like [SafeMath](#) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/master/contracts/math/SafeMath.sol>] as well as Ethereum smart contract security analysis tools like [Mythril](#) [<https://github.com/ConsenSys/mythril>]. However, unfortunately in cases such as this, developers are not forced to use the safety tools. Put simply, if safety is not enforced by the language, developers can write unsafe code which will successfully compile and later on "successfully" execute.

Vyper has built-in overflow protection, implemented in a two-pronged approach. Firstly, Vyper provides a [SafeMath equivalent](#) [<https://github.com/ethereum/vyper/blob/master/vyper/parser/expr.py#L275>] which includes the necessary exception cases for integer arithmetic. Secondly, Vyper uses clamps whenever a literal constant is loaded, a value is passed to a function, or a variable is assigned. Clamps are implemented via custom functions in the Low-level Lisp-like Language (LLL) compiler, and cannot be disabled. (The Vyper compiler outputs LLL rather than EVM bytecode; this simplifies the development of Vyper itself.)

Reading and writing data

Smart contracts can write data to two places: Ethereum's global state trie and Ethereum's chain data. While it is costly to store, read and modify data, these storage operations are a necessary component of most smart contracts.

Global state

The state variables in a given smart contract are stored in Ethereum's global state trie; a given smart contract can only store, read and modify data specifically in relation to that contract's address (i.e.

smart contracts can not read or write to other smart contracts).

Log

As previously mentioned, a smart contract can also write to Ethereum's chain data through log events. While Vyper initially employed the `_log_` syntax for declaring these events, an update has been made which brings Vyper's event declaration more in line with Solidity's original syntax. For example, Vyper's declaration of an event called `MyLog` was originally `MyLog: __log__({arg1: indexed(bytes[3])})`. Vyper's syntax has now become `MyLog: event({arg1: indexed(bytes[3])})`. It is important to note that the execution of the log event in Vyper was, and still is, as follows: `log.MyLog("123")`.

While smart contracts can write to Ethereum's chain data (through log events), smart contracts are unable to read the on-chain log events which they created. Notwithstanding, one of the advantages of writing to Ethereum's chain data via log events is that logs can be discovered and read, on the public chain, by light clients. For example, the `logsBloom` value in a mined block can indicate whether or not a log event is present. Once the existence of log events has been established, the log data can be obtained from a given transaction receipt.

ERC20 token interface implementation

Vyper implements ERC20 as a precompiled contract, allowing these smart contracts to be easily used out of the box. Contracts in Vyper must be declared as global variables. An example for declaring the `ERC20` variable is as follows.

```
token: address(ERC20)
```

Conclusions

Vyper is a powerful and interesting new contract-oriented programming languages. Its design is biased towards "correctness", at the expense of some flexibility. This may allow programmers to write better smart contracts and avoid certain pitfalls that cause serious vulnerabilities to arise. Next, we will look at smart contract security in more detail. Some of the nuances of Vyper design may become more apparent once you read about all the possible security problems that can arise in smart contracts.

Smart contract security

Security is one of the most important considerations when writing smart contracts. In the field of smart contract programming, mistakes are costly and easily exploited. In this chapter we will look at security best practices and design patterns, as well as "security anti-patterns", which are practices and patterns that can introduce vulnerabilities in our smart contracts.

As with other programs, a smart contract will execute exactly what is written, which is not always what the programmer intended. Furthermore, all smart contracts are public and any user can interact with them simply by creating a transaction. Any vulnerability can be exploited and losses are almost always impossible to recover. It is therefore critical to follow best practices and use well tested design patterns.

Security best practices

Defensive programming is a style of programming that is particularly well suited to programming smart contracts and has the following characteristics:

Minimalism/Simplicity

Complexity is the enemy of security. The simpler the code, and the less it does, the lower the chance of a bug or unforeseen effect. When first engaging in smart contract programming, developers are tempted to try to write a lot of code. Instead, you should look through your smart contract code and try to find ways to do less, with fewer lines of code, with less complexity and with fewer "features". If someone tells you that their project has produced "thousands of lines of code" for their smart contracts, you should question the security of that project. Simpler is more secure.

Code reuse

Try not to reinvent the wheel. If a library or contract already exists that does most of what you need, reuse it. Within your own code, follow the DRY principle: Don't Repeat Yourself. If you see any snippet of code repeat more than once, ask yourself whether it could be written as a function or library and reused. Code that has been extensively used and tested is likely more secure than any new code you write. Beware of any Not Invented Here attitude, where you are tempted to "improve" a feature or component by building it from scratch. The security risk is often greater than the improvement value.

Code quality

Smart-contract code is unforgiving. Every bug can lead to monetary loss. You should not treat smart

contract programming the same way as general-purpose programming. Writing DApps in Solidity is not like creating a web widget in JavaScript. Rather, you should apply rigorous engineering and software development methodologies, akin to aerospace engineering or a similarly unforgiving engineering discipline. Once you "launch" your code, there's little you can do to fix any problems.

Readability/Auditability

Your code should be clear and easy to comprehend. The easier it is to read, the easier it is to audit. Smart contracts are public, as everyone can read the bytecode and anyone can reverse engineer it. Therefore, it is beneficial to develop your work in public, using collaborative and open source methodologies, to draw upon the collective wisdom of the developer community and benefit from the highest common denominator of open source development. You should write code that is well documented and easy to read, following the style and naming conventions that are part of the Ethereum community.

Test coverage

Test everything that you can. Smart contracts run in a public execution environment, where anyone can execute them with whatever input they want. You should never assume that input, such as function arguments, is well formed, properly bounded or has a benign purpose. Test all arguments to make sure they are within expected ranges and properly formatted before allowing execution of your code to continue.

Security risks and anti-patterns

As a smart contract programmer, you should be familiar with the most common security risks, so as to be able to detect and avoid the programming patterns that leave them exposed to these risks. In the next several sections we will look at different security risks, examples of how vulnerabilities can arise and countermeasures or preventative solutions that can be used to address them.

Re-Entrancy

One of the features of Ethereum smart contracts is the ability to call and utilise code of other external contracts. Contracts also typically handle ether, and as such often send ether to various external user addresses. The operation of calling external contracts, or sending ether to an address, requires the contract to submit an external call. These external calls can be hijacked by attackers whereby they force the contract to execute further code (through a fallback function), including calls back into itself. Attacks of this kind were used in the infamous DAO hack.

For further reading on re-entrancy attacks, see https://medium.com/@gus_tavo_guim/reentrancy-attack-on-smart-contracts-how-to-identify-the-exploitable-and-an-example-of-an-attack-4470a2d8dfe4 or https://consensys.github.io/smart-contract-best-practices/known_attacks/#dos-with-unexpected-revert.

The Vulnerability

This attack can occur when a contract sends ether to an unknown address. An attacker can carefully construct a contract at an external address which contains malicious code in the fallback function. Thus, when a contract sends ether to this address, it will invoke the malicious code. Typically the malicious code executes a function on the vulnerable contract, performing operations not expected by the developer. The term "re-entrancy" comes from the fact that the external malicious contract calls a function on the vulnerable contract and the path of code execution "*re-enters*" it.

To clarify this, consider the simple vulnerable contract [EtherStore.sol](#), which acts as an Ethereum vault that allows depositors to withdraw only 1 ether per week.

EtherStore.sol:

```
contract EtherStore {  
  
    uint256 public withdrawalLimit = 1 ether;  
    mapping(address => uint256) public lastWithdrawTime;  
    mapping(address => uint256) public balances;  
  
    function depositFunds() public payable {  
        balances[msg.sender] += msg.value;  
    }  
  
    function withdrawFunds (uint256 _weiToWithdraw) public {  
        require(balances[msg.sender] >= _weiToWithdraw);  
        // limit the withdrawal  
        require(_weiToWithdraw <= withdrawalLimit);  
        // limit the time allowed to withdraw  
        require(now >= lastWithdrawTime[msg.sender] + 1 weeks);  
        require(msg.sender.call.value(_weiToWithdraw)());  
        balances[msg.sender] -= _weiToWithdraw;  
        lastWithdrawTime[msg.sender] = now;  
    }  
}
```

This contract has two public functions, `depositFunds()` and `withdrawFunds()`. The `depositFunds()` function simply increments the sender's balance. The `withdrawFunds()` function allows the sender to specify the amount of wei to withdraw. This function is intended to succeed only if the requested amount to withdraw is less than 1 ether and a withdrawal has not occurred in the last week.

The vulnerability is in line 17, where the contract sends the user their requested amount of ether. Consider an attacker creating the following contract:

Attack.sol:

```
import "EtherStore.sol";

contract Attack {
    EtherStore public etherStore;

    // initialise the etherStore variable with the contract address
    constructor(address _etherStoreAddress) {
        etherStore = EtherStore(_etherStoreAddress);
    }

    function attackEtherStore() public payable {
        // attack to the nearest ether
        require(msg.value >= 1 ether);
        // send eth to the depositFunds() function
        etherStore.depositFunds.value(1 ether)();
        // start the magic
        etherStore.withdrawFunds(1 ether);
    }

    function collectEther() public {
        msg.sender.transfer(this.balance);
    }

    // fallback function - where the magic happens
    function () payable {
        if (etherStore.balance > 1 ether) {
            etherStore.withdrawFunds(1 ether);
        }
    }
}
```

How can the malicious contract [Attack.sol](#): exploit the **EtherStore** contract? First, the attacker would create the above contract (let's say at the address `0x0...123`) with the **EtherStore**'s contract address as the sole constructor parameter. This will initialize and point the public variable **etherStore** to the contract to be attacked.

The attacker would then call the `attackEtherStore()` function, with some amount of ether (greater than or equal to 1), let us assume `1 ether` for the time being. In this example, we will also assume a number of other users have deposited ether into this contract, such that it's current balance is `10 ether`. The following would then occur:

1. **Attack.sol - Line 15** - The `depositFunds()` function of the EtherStore contract will be called with a `msg.value` of `1 ether` (and a lot of gas). The sender (`msg.sender`) will be our malicious contract (`0x0...123`). Thus, `balances[0x0..123] = 1 ether`.
2. **Attack.sol - Line 17** - The malicious contract will then call the `withdrawFunds()` function of the EtherStore contract with a parameter of `1 ether`. This will pass all the requirements (Lines 12–16 of the EtherStore contract) as no previous withdrawals have been made.
3. **EtherStore.sol - Line 17** - The contract will then send `1 ether` back to the malicious contract.
4. **Attack.sol - Line 25** - The payment to the malicious contract will then execute the fallback function.
5. **Attack.sol - Line 26** - The total balance of the EtherStore contract was `10 ether` and is now `9 ether` so this if statement passes.
6. **Attack.sol - Line 27** - The fallback function then calls the EtherStore `withdrawFunds()` function again and 're-enters' the EtherStore contract.
7. **EtherStore.sol - Line 11** - In this second call to `withdrawFunds()`, the attacking contract's balance is still `1 ether` as line 18 has not yet been executed. Thus, we still have `balances[0x0..123] = 1 ether`. This is also the case for the `lastWithdrawTime` variable. Again, we pass all the requirements.
8. **EtherStore.sol - Line 17** - The attacking contract withdraws another `1 ether`.
9. **Steps 4-8 will repeat** - until it is no longer the case that `EtherStore.balance > 1` as dictated by line 26 in `Attack.sol`.
10. **Attack.sol - Line 26** - Once there less 1 (or less) ether left in the EtherStore contract, this if statement will fail. This will then allow lines 18 and 19 of the EtherStore contract to be executed (for each call to the `withdrawFunds()` function).
11. **EtherStore.sol - Lines 18 and 19** - The `balances` and `lastWithdrawTime` mappings will be set and the execution will end.

The final result is that the attacker has withdrawn all but 1 ether from the **EtherStore** contract in a single transaction.

Preventative Techniques

There are a number of common techniques which help avoid potential re-entrancy vulnerabilities in smart contracts. The first is to (whenever possible) use the built-in `transfer()` [https://solidity.readthedocs.io/en/latest/units-and-global-variables.html#address-related] function when sending ether to external contracts. The transfer function only sends **2300 gas** with the external call, which is not enough for the destination address/contract to call another contract (i.e. re-enter the sending contract).

The second technique is to ensure that all logic that changes state variables happen before ether is sent out of the contract (or any external call). In the **EtherStore** example, lines 18 and 19 of **EtherStore.sol** should be put before line 17. It is good practice to place any code that performs external calls to unknown addresses as the last operation in a localised function or piece of code execution. This is known as the `checks-effects-interactions` [https://solidity.readthedocs.io/en/latest/security-considerations.html#use-the-checks-effects-interactions-pattern] pattern.

A third technique is to introduce a mutex. That is, to add a state variable which locks the contract during code execution, preventing re-entrant calls.

Applying all of these techniques (all three are unnecessary, but we do it for demonstrative purposes) to **EtherStore.sol**, gives the re-entrancy-free contract:

```

contract EtherStore {

    // initialise the mutex
    bool reEntrancyMutex = false;
    uint256 public withdrawalLimit = 1 ether;
    mapping(address => uint256) public lastWithdrawTime;
    mapping(address => uint256) public balances;

    function depositFunds() public payable {
        balances[msg.sender] += msg.value;
    }

    function withdrawFunds (uint256 _weiToWithdraw) public {
        require(!reEntrancyMutex);
        require(balances[msg.sender] >= _weiToWithdraw);
        // limit the withdrawal
        require(_weiToWithdraw <= withdrawalLimit);
        // limit the time allowed to withdraw
        require(now >= lastWithdrawTime[msg.sender] + 1 weeks);
        balances[msg.sender] -= _weiToWithdraw;
        lastWithdrawTime[msg.sender] = now;
        // set the reEntrancy mutex before the external call
        reEntrancyMutex = true;
        msg.sender.transfer(_weiToWithdraw);
        // release the mutex after the external call
        reEntrancyMutex = false;
    }
}

```

Real-World Example: The DAO

The DAO [[https://en.wikipedia.org/wiki/The_DAO_\(organization\)](https://en.wikipedia.org/wiki/The_DAO_(organization))] (Decentralized Autonomous Organization) was one of the major hacks that occurred in the early development of Ethereum. At the time, the contract held over \$150 million USD. Re-entrancy played a major role in the attack, which ultimately led to the hard fork that created Ethereum Classic (ETC). For a good analysis of the DAO exploit, see <http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>.

Arithmetic Over/Underflows

The Ethereum Virtual Machine (EVM) specifies fixed-size data types for integers. This means that an integer variable can represent only a certain range of numbers. A `uint8` for example, can only store numbers in the range [0,255]. Trying to store 256 into a `uint8` will result in 0. If care is not taken, variables in Solidity can be exploited if user input is unchecked and calculations are performed which result in numbers that lie outside the range of the data type that stores them.

For further reading on arithmetic over/underflows, see **How to Secure Your Smart Contracts** at <https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-1-c33048d4d17d>, **Ethereum Smart Contract Best Practices** at https://consensys.github.io/smart-contract-best-practices/known_attacks/#integer-overflow-and-underflow and **Ethereum, Solidity and integer overflows: programming blockchains like 1970** at <https://randomoracle.wordpress.com/2018/04/27/ethereum-solidity-and-integer-overflows-programming-blockchains-like-1970/>

The Vulnerability

An over/underflow occurs when an operation is performed that requires a fixed size variable to store a number (or piece of data) that is outside the range of the variable's data type.

For example, subtracting 1 from a `uint8` (unsigned integer of 8 bits, i.e. non-negative) variable whose value is 0 will result in the number 255. This is an underflow. We have assigned a number below the range of the `uint8`, the result *wraps around* and gives the largest number a `uint8` can store. Similarly, adding $2^8=256$ to a `uint8` will leave the variable unchanged as we have wrapped around the entire length of the `uint`. Two simple analogies of this behaviour are speedometers in cars which measure distance travelled (they restart to 0, after the largest number, i.e. 999999 is surpassed) and periodic mathematical functions (adding 2π to the argument of `sin()` leaves the value unchanged).

Adding numbers larger than the data type's range is called an overflow. For clarity, adding 257 to a `uint8` that currently has a value of 0 will result in the number 1. It is sometimes instructive to think of fixed-size variables being cyclic, where we start again from zero if we add numbers above the largest possible stored number, and start counting down from the largest number if we subtract from 0. In the case of signed `int` types, which *can* represent negative numbers, we start again once we reach the largest negative value; for example, if we try to subtract 1 from a `uint8` whose value is -128, we will get 127.

These kinds of numerical gotchas allow attackers to misuse code and create unexpected logic flows. For

example, consider the time locking contract [TimeLock.sol](#):

TimeLock.sol:

```
contract TimeLock {  
  
    mapping(address => uint) public balances;  
    mapping(address => uint) public lockTime;  
  
    function deposit() public payable {  
        balances[msg.sender] += msg.value;  
        lockTime[msg.sender] = now + 1 weeks;  
    }  
  
    function increaseLockTime(uint _secondsToIncrease) public {  
        lockTime[msg.sender] += _secondsToIncrease;  
    }  
  
    function withdraw() public {  
        require(balances[msg.sender] > 0);  
        require(now > lockTime[msg.sender]);  
        balances[msg.sender] = 0;  
        msg.sender.transfer(balances[msg.sender]);  
    }  
}
```

This contract is designed to act like a time vault, where users can deposit ether into the contract and it will be locked there for at least a week. The user may extend the wait time to longer than 1 week if they choose, but once deposited, the user can be sure their ether is locked in safely for at least a week, or so this contract intends.

In the event a user is forced to hand over their private key a contract such as this may be handy to ensure ether is unobtainable in short periods of time. If a user had locked in **100 ether** in this contract and handed their keys over to an attacker, an attacker could use an overflow to receive the ether, regardless of the **lockTime**.

The attacker could determine the current **lockTime** for the address they now hold the key for (its a public variable). Let's call this **userLockTime**. They could then call the **increaseLockTime** function

and pass as an argument the number `2^256 - userLockTime`. This number would be added to the current `userLockTime` and cause an overflow, resetting `lockTime[msg.sender]` to `0`. The attacker could then simply call the `withdraw` function to obtain their reward.

Let's look at another example, this one from the Ethernaut challenges. See <https://github.com/OpenZeppelin/ethernaut>.

SPOILER ALERT: If you have not yet done the Ethernaut challenges, this gives a solution to one of the levels.

```
pragma solidity ^0.4.18;

contract Token {

    mapping(address => uint) balances;
    uint public totalSupply;

    function Token(uint _initialSupply) {
        balances[msg.sender] = totalSupply = _initialSupply;
    }

    function transfer(address _to, uint _value) public returns (bool) {
        require(balances[msg.sender] - _value >= 0);
        balances[msg.sender] -= _value;
        balances[_to] += _value;
        return true;
    }

    function balanceOf(address _owner) public constant returns (uint
balance) {
        return balances[_owner];
    }
}
```

This is a simple token contract which employs a `transfer()` function, allowing participants to move their tokens around. Can you see the error in this contract?

The flaw comes in the `transfer()` function. The require statement on line 13 can be bypassed using

an underflow. Consider a user with a zero balance. They could call the `transfer()` function with any non-zero `_value` and pass the require statement on line 13. This is because `balances[msg.sender]` is zero (and a `uint256`) so subtracting any positive amount (excluding `2^256`) will result in a positive number due to the underflow we described above. This is also true for line 14, where our balance will be credited with a positive number. Thus, in this example, we have achieved free tokens due to an underflow vulnerability.

Preventative Techniques

The current conventional technique to guard against under/overflow vulnerabilities is to use or build mathematical libraries which replace the standard math operators addition, subtraction and multiplication (division is excluded as it does not cause over/underflows and the EVM reverts on division by 0).

[OpenZepplin](https://github.com/OpenZeppelin/zeppelin-solidity) [<https://github.com/OpenZeppelin/zeppelin-solidity>] have done a great job in building and auditing secure libraries for the Ethereum community. In particular, their Safe Math Library, at <https://github.com/OpenZeppelin/zeppelin-solidity/blob/master/contracts/math/SafeMath.sol>, can be used to avoid under/overflow vulnerabilities.

To demonstrate how these libraries are used in Solidity, let us correct the `TimeLock` contract, using Open Zepplin's `SafeMath` library. The overflow-free version of the contract is:

```
library SafeMath {  
  
    function mul(uint256 a, uint256 b) internal pure returns (uint256) {  
        if (a == 0) {  
            return 0;  
        }  
        uint256 c = a * b;  
        assert(c / a == b);  
        return c;  
    }  
  
    function div(uint256 a, uint256 b) internal pure returns (uint256) {  
        // assert(b > 0); // Solidity automatically throws when dividing by 0  
        uint256 c = a / b;  
        // assert(a == b * c + a % b); // There is no case in which this  
        doesn't hold  
    }  
}
```

```

        return c;
    }

function sub(uint256 a, uint256 b) internal pure returns (uint256) {
    assert(b <= a);
    return a - b;
}

function add(uint256 a, uint256 b) internal pure returns (uint256) {
    uint256 c = a + b;
    assert(c >= a);
    return c;
}

contract TimeLock {
    using SafeMath for uint; // use the library for uint type
    mapping(address => uint256) public balances;
    mapping(address => uint256) public lockTime;

    function deposit() public payable {
        balances[msg.sender] = balances[msg.sender].add(msg.value);
        lockTime[msg.sender] = now.add(1 weeks);
    }

    function increaseLockTime(uint256 _secondsToIncrease) public {
        lockTime[msg.sender] =
lockTime[msg.sender].add(_secondsToIncrease);
    }

    function withdraw() public {
        require(balances[msg.sender] > 0);
        require(now > lockTime[msg.sender]);
        balances[msg.sender] = 0;
        msg.sender.transfer(balances[msg.sender]);
    }
}

```

Notice that all standard math operations have been replaced by the those defined in the **SafeMath**

library. The **TimeLock** contract no longer performs any operation which is capable of under/overflow.

Real-World Examples: PoWHC and Batch Transfer Overflow (CVE-2018-10299)

Proof of Weak Hands Coin (PoWHC), originally devised as a joke of sorts, was a Ponzi scheme written by an internet collective. Unfortunately it seems that the author(s) of the contract had not seen over/underflows before and consequently, 866 ether was liberated from its contract. A good overview of how the underflow occurs (which is not too dissimilar to the Ethernaut challenge above) is given in <https://blog.goodaudience.com/how-800k-evaporated-from-the-powh-coin-ponzi-scheme-overnight-1b025c33b530>.

Another example comes from the implementation of a **batchTransfer()** function into a group of ERC20 token contracts. See <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>. The implementation contained an overflow. Learn more details about the overflow at <https://medium.com/@peckshield/alert-new-batchoverflow-bug-in-multiple-erc20-smart-contracts-cve-2018-10299-511067db6536>.

Unexpected Ether

Typically, when ether is sent to a contract it must execute either the fallback function or another function defined in the contract. There are two exceptions to this, where ether can exist in a contract without having executed any code. Contracts which rely on code execution for every ether sent to the contract can be vulnerable to attacks where ether is forcibly sent to a contract.

For further reading on this, see How to Secure Your Smart Contracts: 6 at <https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-2-730db0aa4834> and Solidity security patterns - forcing ether to a contract at <http://danielszego.blogspot.com.au/2018/03/solidity-security-patterns-forcing.html>.

The Vulnerability

A common defensive programming technique that is useful in enforcing correct state transitions or validating operations is *invariant checking*. This technique involves defining a set of invariants (metrics or parameters that should not change) and checking these invariants remain unchanged after a single (or many) operation(s). This is typically good design, provided the invariants being checked are in fact invariants. One example of an invariant is the **totalSupply** of a fixed issuance **ERC20** [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>] token. As no function should modify this invariant, one could add a check to the **transfer()** function that ensures the **totalSupply** remains unmodified, to ensure

the function is working as expected.

In particular, there is one apparent *invariant*, that it may be tempting to use but can in fact be manipulated by external users (regardless of the rules put in place in the smart contract). This is the current ether stored in the contract. Often when developers first learn Solidity they have the misconception that a contract can only accept or obtain ether via payable functions. This misconception can lead to contracts that have false assumptions about the ether balance within them which can lead to a range of vulnerabilities. The smoking gun for this vulnerability is the (incorrect) use of `this.balance`. As we will see, incorrect uses of `this.balance` can lead to serious vulnerabilities of this type.

There are two ways in which ether can (forcibly) be sent to a contract without using a `payable` function or executing any code on the contract. These are listed below.

Self-Destruct / Suicide

Any contract is able to implement the `selfdestruct(address)` [http://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html#self-destruct] function, which removes all bytecode from the contract address and sends all ether stored there to the parameter-specified address. If this specified address is also a contract, no functions (including the fallback) get called. Therefore, the `selfdestruct()` function can be used to forcibly send ether to any contract regardless of any code that may exist in the contract, even contracts with no payable functions. This means any attacker can create a contract with a `selfdestruct()` function, send ether to it, call `selfdestruct(target)` and force ether to be sent to a `target` contract. Martin Swende has an excellent blog post at http://martin.swende.se/blog/Ethereum_quirks_and_vulns.html describing some quirks of the self-destruct opcode (Quirk #2) along with a description of how client nodes were checking incorrect invariants which could have led to a rather catastrophic crash of the Ethereum network.

Pre-sent Ether

The second way a contract can obtain ether without using a `selfdestruct()` function or calling any payable functions is to pre-load the contract address with ether. Contract addresses are deterministic, in fact the address is calculated from the Keccak256 (commonly synonymous with SHA-3) hash of the address creating the contract and the transaction nonce which creates the contract. Specifically, it is of the form: `address = sha3(rlp.encode([account_address, transaction_nonce]))` (see [Keyless Ether](https://blog.sigmaprime.io/solidity-security.html#keyless-eth) [https://blog.sigmaprime.io/solidity-security.html#keyless-eth] for some fun use cases of this). This means anyone can calculate what a contract's address will be before it is created and thus send ether to that address. When the contract is created it will have a non-zero ether balance.

Let's explore some pitfalls that can arise given the above knowledge.

Consider the overly-simple contract [EtherGame.sol](#):

EtherGame.sol:

```
contract EtherGame {  
  
    uint public payoutMileStone1 = 3 ether;  
    uint public mileStone1Reward = 2 ether;  
    uint public payoutMileStone2 = 5 ether;  
    uint public mileStone2Reward = 3 ether;  
    uint public finalMileStone = 10 ether;  
    uint public finalReward = 5 ether;  
  
    mapping(address => uint) redeemableEther;  
    // users pay 0.5 ether. At specific milestones, credit their accounts  
    function play() public payable {  
        require(msg.value == 0.5 ether); // each play is 0.5 ether  
        uint currentBalance = this.balance + msg.value;  
        // ensure no players after the game as finished  
        require(currentBalance <= finalMileStone);  
        // if at a milestone credit the players account  
        if (currentBalance == payoutMileStone1) {  
            redeemableEther[msg.sender] += mileStone1Reward;  
        }  
        else if (currentBalance == payoutMileStone2) {  
            redeemableEther[msg.sender] += mileStone2Reward;  
        }  
        else if (currentBalance == finalMileStone ) {  
            redeemableEther[msg.sender] += finalReward;  
        }  
        return;  
    }  
  
    function claimReward() public {  
        // ensure the game is complete  
        require(this.balance == finalMileStone);  
        // ensure there is a reward to give  
    }  
}
```

```
        require(redeemableEther[msg.sender] > 0);
        redeemableEther[msg.sender] = 0;
        msg.sender.transfer(redeemableEther[msg.sender]);
    }
}
```

This contract represents a simple game (which would naturally involve race-conditions) whereby players send `0.5 ether` to the contract in hope to be the player that reaches one of three milestones first. Milestones are denominated in ether. The first to reach the milestone may claim a portion of the ether when the game has ended. The game ends when the final milestone (`10 ether`) is reached; users can then claim their rewards.

The issues with the `EtherGame` contract come from the poor use of `this.balance` in both lines 14 (and by association 16) and 32. A mischievous attacker could forcibly send a small amount of ether, let's say `0.1 ether` via the `selfdestruct()` function (discussed above) to prevent any future players from reaching a milestone. As all legitimate players can only send `0.5 ether` increments, `this.balance` would no longer be multiples of `0.5 ether`, as it would also have the `0.1 ether` contribution. This prevents all the if conditions on lines 18, 21 and 24 from being true.

Even worse, a vengeful attacker who missed a milestone could forcibly send `10 ether` (or an equivalent amount of ether that pushes the contract's balance above the `finalMileStone`), which would lock all rewards in the contract forever. This is because the `claimReward()` function will always revert, due to the require on line 32 (i.e. `this.balance` is greater than `finalMileStone`).

Preventative Techniques

This sort of vulnerability typically arises from the misuse of `this.balance`. Contract logic, when possible, should avoid being dependent on exact values of the balance of the contract, because it can be artificially manipulated. If applying logic based on `this.balance`, you have to cope with unexpected balances.

If exact values of deposited ether are required, a self-defined variable should be used that is incremented in payable functions, to safely track the deposited ether. This variable will not be influenced by the forced ether sent via a `selfdestruct()` call.

With this in mind, a corrected version of the `EtherGame` contract could look like:

```
contract EtherGame {  
  
    uint public payoutMileStone1 = 3 ether;  
    uint public mileStone1Reward = 2 ether;  
    uint public payoutMileStone2 = 5 ether;  
    uint public mileStone2Reward = 3 ether;  
    uint public finalMileStone = 10 ether;  
    uint public finalReward = 5 ether;  
    uint public depositedWei;  
  
    mapping (address => uint) redeemableEther;  
  
    function play() public payable {  
        require(msg.value == 0.5 ether);  
        uint currentBalance = depositedWei + msg.value;  
        // ensure no players after the game has finished  
        require(currentBalance <= finalMileStone);  
        if (currentBalance == payoutMileStone1) {  
            redeemableEther[msg.sender] += mileStone1Reward;  
        }  
        else if (currentBalance == payoutMileStone2) {  
            redeemableEther[msg.sender] += mileStone2Reward;  
        }  
        else if (currentBalance == finalMileStone ) {  
            redeemableEther[msg.sender] += finalReward;  
        }  
        depositedWei += msg.value;  
        return;  
    }  
  
    function claimReward() public {  
        // ensure the game is complete  
        require(depositedWei == finalMileStone);  
        // ensure there is a reward to give  
        require(redeemableEther[msg.sender] > 0);  
        redeemableEther[msg.sender] = 0;  
        msg.sender.transfer(redeemableEther[msg.sender]);  
    }  
}
```

Here, we have just created a new variable, `depositedEther`, which keeps track of the known ether deposited, and it is this variable which we use for our tests. Note that we no longer have any reference to `this.balance`.

Further Examples

A few examples of exploitable contracts were given in the [Underhanded Solidity Contest](#) [<https://github.com/Arachnid/uscc/tree/master/submissions-2017/>], which also provides extended examples of a number of the pitfalls raised in this section.

Delegatecall

The `CALL` and `DELEGATECALL` opcodes are useful in allowing Ethereum developers to modularise their code. Standard external message calls to contracts are handled by the `CALL` opcode, whereby code is run in the context of the external contract/function. The `DELEGATECALL` opcode is almost identical, except that the code executed at the targeted address is run in the context of the calling contract, and `msg.sender` and `msg.value` remain unchanged. This feature enables the implementation of *libraries*, allowing developers to deploy reusable code once and call it from future contracts.

Although the differences between these two opcodes are simple and intuitive, the use of `DELEGATECALL` can lead to unexpected code execution.

For further reading, see [Ethereum Stack Exchange Question](#) [<https://ethereum.stackexchange.com/questions/3667/difference-between-call-callcode-and-delegatecall>] and [Solidity Docs](#) [<https://solidity.readthedocs.io/en/latest/introduction-to-smart-contracts.html#delegatecall-callcode-and-libraries>].

The Vulnerability

As a result of the context-preserving nature of `DELEGATECALL`, building vulnerability-free custom libraries is not as easy as one might think. The code in libraries themselves can be secure and vulnerability-free; however, when run in the context of another application new vulnerabilities can arise. Let's see a fairly complex example of this, using Fibonacci numbers.

Consider the following library, [`FibonacciLib.sol`](#), which can generate the Fibonacci sequence and sequences of similar form. Note, this code was modified from <https://github.com/web3j/web3j/blob/master/codegen/src/test/resources/solidity/fibonacci/Fibonacci.sol>.

FibonacciLib.sol

```
// library contract - calculates fibonacci-like numbers;
contract FibonacciLib {
    // initializing the standard fibonacci sequence;
    uint public start;
    uint public calculatedFibNumber;

    // modify the zeroth number in the sequence
    function setStart(uint _start) public {
        start = _start;
    }

    function setFibonacci(uint n) public {
        calculatedFibNumber = fibonacci(n);
    }

    function fibonacci(uint n) internal returns (uint) {
        if (n == 0) return start;
        else if (n == 1) return start + 1;
        else return fibonacci(n - 1) + fibonacci(n - 2);
    }
}
```

This library provides a function which can generate the n -th Fibonacci number in the sequence. It allows users to change the starting number of the sequence (**start**) and calculate the n -th Fibonacci-like numbers in this new sequence.

Let us now consider a contract, [FibonacciBalance.sol](#): that utilises this library.

FibonacciBalance.sol:

```
contract FibonacciBalance {  
  
    address public fibonacciLibrary;  
    // the current fibonacci number to withdraw  
    uint public calculatedFibNumber;  
    // the starting fibonacci sequence number  
    uint public start = 3;  
    uint public withdrawalCounter;  
    // the fibonancci function selector  
    bytes4 constant fibSig = bytes4(sha3("setFibonacci(uint256)"));  
  
    // constructor - loads the contract with ether  
    constructor(address _fibonacciLibrary) public payable {  
        fibonacciLibrary = _fibonacciLibrary;  
    }  
  
    function withdraw() {  
        withdrawalCounter += 1;  
        // calculate the fibonacci number for the current withdrawal user  
        // this sets calculatedFibNumber  
        require(fibonacciLibrary.delegatecall(fibSig,  
withdrawalCounter));  
        msg.sender.transfer(calculatedFibNumber * 1 ether);  
    }  
  
    // allow users to call fibonacci library functions  
    function() public {  
        require(fibonacciLibrary.delegatecall(msg.data));  
    }  
}
```

This contract allows a participant to withdraw ether from the contract, with the amount of ether being equal to the Fibonacci number corresponding to the participants' withdrawal order; i.e., the first participant gets 1 ether, the second also gets 1, the third gets 2, the forth gets 3, the fifth 5 and so on (until the balance of the contract is less than the Fibonacci number being withdrawn).

There are a number of elements in this contract that may require some explanation. Firstly, there is an interesting-looking variable, `fibSig`. This holds the first 4 bytes of the Keccak (SHA-3) hash of the string '`setFibonacci(uint256)`'. This is known as the [function selector](#) [<https://solidity.readthedocs.io/en/latest/abi-spec.html#function-selector>] and is put into `calldata` to specify which function of a smart contract will be called. It is used in the `delegatecall` function on line 21 to specify that we wish to run the `fibonacci(uint256)` function. The second argument in `delegatecall` is the parameter we are passing to the function. Secondly, we assume that the address for the `FibonacciLib` library is correctly referenced in the constructor (section [External Contract Referencing](#) discusses some potential vulnerabilities relating to this kind of contract reference initialisation).

Can you spot any errors in this contract? If one were to deploy this contract, fill it with ether and call `withdraw()`, it will likely revert.

You may have noticed that the state variable `start` is used in both the library and the main calling contract. In the library contract, `start` is used to specify the beginning of the Fibonacci sequence and is set to `0`, whereas it is set to `3` in the `FibonacciBalance` contract. You may also have noticed that the fallback function in the `FibonacciBalance` contract allows all calls to be passed to the library contract, which allows for the `setStart()` function of the library contract to be called also. Recalling that we preserve the state of the contract, it may seem that this function would allow you to change the state of the `start` variable in the local `FibonacciBalance` contract. If so, this would allow one to withdraw more ether, as the resulting `calculatedFibNumber` is dependent on the `start` variable (as seen in the library contract). In actual fact, the `setStart()` function does not (and cannot) modify the `start` variable in the `FibonacciBalance` contract. The underlying vulnerability in this contract is significantly worse than just modifying the `start` variable.

Before discussing the actual issue, we take a quick detour to understanding how state variables (`storage` variables) actually get stored in contracts. State or `storage` variables (variables that persist over individual transactions) are placed into `slots` sequentially as they are introduced in the contract. (There are some complexities here, and the reader is encouraged to read <http://solidity.readthedocs.io/en/latest/miscellaneous.html#layout-of-state-variables-in-storage> for a more thorough understanding).

As an example, let's look at the library contract. It has two state variables, `start` and `calculatedFibNumber`. The first variable is `start`; being first, it is stored in the contract's storage at `slot[0]` (i.e. the first slot). The second variable, `calculatedFibNumber`, is placed in the next available storage slot, `slot[1]`. If we look at the function `setStart()`, it takes an input and sets `start` to whatever the input was. This function is therefore setting `slot[0]` to whatever input we provide in the `setStart()` function. Similarly, the `setFibonacci()` function sets

`calculatedFibNumber` to the result of `fibonacci(n)`. Again, this is simply setting storage `slot[1]` to the value of `fibonacci(n)`.

Now let's look at the `FibonacciBalance` contract. Storage `slot[0]` now corresponds to `fibonacciLibrary` address and `slot[1]` corresponds to `calculatedFibNumber`. It is in this incorrect mapping that the vulnerability occurs. `delegatecall` preserves contract context. This means that code that is executed via `delegatecall` will act on the state (i.e. storage) of the calling contract.

Now notice that in `withdraw()` on line 21 we execute `fibonacciLibrary.delegatecall(fibSig, withdrawalCounter)`. This calls the `setFibonacci()` function, which, as we discussed, modifies storage `slot[1]`, which in our current context is `calculatedFibNumber`. This is as expected (i.e. after execution, `calculatedFibNumber` is modified). However, recall that the `start` variable in the `FibonacciLib` contract is located in storage `slot[0]`, which is the `fibonacciLibrary` address in the current contract. This means that the function `fibonacci()` will give an unexpected result. This is because it references `start(slot[0])`, which in the current calling context is the `fibonacciLibrary` address (which will often be quite large, when interpreted as a `uint`). Thus it is likely that the `withdraw()` function will revert, as it will not contain `uint(fibonacciLibrary)` amount of ether, which is what `calculatedFibNumber` will return.

Even worse, the `FibonacciBalance` contract allows users to call all of the `fibonacciLibrary` functions via the fallback function at line 26. As we discussed earlier, this includes the `setStart()` function. We discussed that this function allows anyone to modify or set storage `slot[0]`. In this case, storage `slot[0]` is the `fibonacciLibrary` address. Therefore, an attacker could create a malicious contract (an example of one is given below), convert the address to a `uint` (this can be done in Python easily using `int('<address>', 16)`), and then call `setStart(<attack_contract_address_as_uint>)`. This will change `fibonacciLibrary` to the address of the attack contract. Then, whenever a user calls `withdraw()` or the fallback function, the malicious contract will run (which can steal the entire balance of the contract) because we've modified the actual address for `fibonacciLibrary`. An example of such an attack contract would be:

```
contract Attack {
    uint storageSlot0; // corresponds to fibonacciLibrary
    uint storageSlot1; // corresponds to calculatedFibNumber

    // fallback - this will run if a specified function is not found
    function() public {
        storageSlot1 = 0; // we set calculatedFibNumber to 0, so that if
withdraw
        // is called we don't send out any ether.
        <attacker_address>.transfer(this.balance); // we take all the
ether
    }
}
```

Notice that this attack contract modifies the `calculatedFibNumber` by changing storage `slot[1]`. In principle, an attacker could modify any other storage slots they choose, to perform all kinds of attacks on this contract. I encourage all readers to put these contracts into Remix at <https://remix.ethereum.org> and experiment with different attack contracts and state changes through these `delegatecall` functions.

It is also important to notice that when we say that `delegatecall` is state-preserving, we are not talking about the variable names of the contract, rather the actual storage slots to which those names point. As you can see from this example, a simple mistake can lead to an attacker hijacking the entire contract and its ether.

Preventative Techniques

Solidity provides the `library` keyword for implementing library contracts (see the Solidity Docs at <https://solidity.readthedocs.io/en/latest/contracts.html?highlight=library#libraries> for further details). This ensures the library contract is stateless and non-self-destructable. Forcing libraries to be stateless mitigates the complexities of storage context demonstrated in this section. Stateless libraries also prevent attacks whereby attackers modify the state of the library directly in order to affect the contracts that depend on the library's code. As a general rule of thumb, when using `DELEGATECALL` pay careful attention to the possible calling context of both the library contract and the calling contract, and whenever possible build state-less libraries.

Real-World Example: Parity Multisig Wallet (Second Hack)

The Second Parity Multisig Wallet hack is an example of how the context of well-written library code can be exploited if run outside its intended context. There are a number of good explanations of this hack, such as this overview: Parity Multisig Hacked. Again. at <https://medium.com/chain-cloud-company-blog/parity-multisig-hack-again-b46771eaa838> by Anthony Akentiev, and An In-Depth Look at the Parity Multisig Bug at <http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/>.

To add to these references, let's explore the contracts that were exploited. The library and wallet contract can be found on the parity GitHub <https://github.com/paritytech/parity/blob/b640df8fbb964da7538eef268dffc125b081a82f/js/src/contracts/snippets/enhanced-wallet.sol>.

There are two contracts of interest here, the library contract and the wallet contract.

The library contract:

```
contract WalletLibrary is WalletEvents {  
  
    ...  
  
    // throw unless the contract is not yet initialized.  
    modifier only_uninitialized { if (m_numOwners > 0) throw; _; }  
  
    // constructor - just pass on the owner array to the multiowned and  
    // the limit to daylimit  
    function initWallet(address[] _owners, uint _required, uint _daylimit)  
only_uninitialized {  
    initDaylimit(_daylimit);  
    initMultiowned(_owners, _required);  
}  
  
    // kills the contract sending everything to `_to`.  
    function kill(address _to) onlymanyowners(sha3(msg.data)) external {  
        suicide(_to);  
    }  
  
    ...  
}
```

and the wallet contract:

```

contract Wallet is WalletEvents {

    ...

    // METHODS

    // gets called when no other function matches
    function() payable {
        // just being sent some cash?
        if (msg.value > 0)
            Deposit(msg.sender, msg.value);
        else if (msg.data.length > 0)
            _walletLibrary.delegatecall(msg.data);
    }

    ...

    // FIELDS
    address constant _walletLibrary =
0xcafecafecafecafecafecafecafecafecafe;
}

```

Notice that the `Wallet` contract essentially passes all calls to the `WalletLibrary` contract via a delegate call. The constant `_walletLibrary` address in this code snippet acts as a placeholder for the actually deployed `WalletLibrary` contract (which was at `0x863DF6BFa4469f3ead0bE8f9F2AAE51c91A907b4`).

The intended operation of these contracts was to have a simple low-cost deployable `Wallet` contract whose code base and main functionality was in the `WalletLibrary` contract. Unfortunately, the `WalletLibrary` contract is itself a contract and maintains its own state. Can you see why this might be an issue?

It is possible to send calls to the `WalletLibrary` contract itself. Specifically, the `WalletLibrary` contract could be initialised, and become owned. A user did this, by calling `initWallet()` function on the `WalletLibrary` contract, becoming an owner of the library contract. The same user, subsequently called the `kill()` function. Because the user was an owner of the Library contract, the modifier passed and the library contract self-destructed. As all `Wallet` contracts in existence refer to this library

contract and contain no method to change this reference, all of their functionality, including the ability to withdraw ether, was lost along with the **WalletLibrary** contract. As a result, all ether in all parity multi-sig wallets of this type instantly became lost or permanently unrecoverable.

Default Visibilities

Functions in Solidity have visibility specifiers which dictate how they can be called. The visibility determines whether a function can be called externally by users, by other derived contracts, only internally or only externally. There are four visibility specifiers, which are described in detail in the Solidity Docs at <http://solidity.readthedocs.io/en/latest/contracts.html?highlight=library#visibility-and-getters>. Functions default to **public**, allowing users to call them externally. We shall now see how incorrect use of visibility specifiers can lead to some devastating vulnerabilities in smart contracts.

The Vulnerability

The default visibility for functions is **public**, so functions that do not specify their visibility will be callable by external users. The issue arises when developers mistakenly omit visibility specifiers on functions which should be private (or only callable within the contract itself).

Let's quickly explore a trivial example.

```
contract HashForEther {  
  
    function withdrawWinnings() {  
        // Winner if the last 8 hex characters of the address are 0.  
        require(uint32(msg.sender) == 0);  
        _sendWinnings();  
    }  
  
    function _sendWinnings() {  
        msg.sender.transfer(this.balance);  
    }  
}
```

This simple contract is designed to act as an address guessing bounty game. To win the balance of the contract, a user must generate an Ethereum address whose last 8 hex characters are 0. Once obtained, they can call the **withdrawWinnings()** function to obtain their bounty.

Unfortunately, the visibility of the functions have not been specified. In particular, the `_sendWinnings()` function is `public` and thus any address can call this function to steal the bounty.

Preventative Techniques

It is good practice to always specify the visibility of all functions in a contract, even if they are intentionally `public`. Recent versions of solc show a warning for functions that have no explicit visibility set, to encourage this practice.

Real-World Example: Parity MultiSig Wallet (First Hack)

In the first Parity multi-sig hack, about \$31M worth of Ether was stolen, mostly from three wallets. A good recap of exactly how this was done is given by Haseeb Qureshi in <https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce>.

Essentially, the multi-sig wallet is constructed from a base `Wallet` contract, which calls a library contract containing the core functionality (as described in the [Real-World Example: Parity Multisig Wallet \(Second Hack\)](#) section). The library contract contains the code to initialise the wallet, as can be seen from the following snippet:

```

contract WalletLibrary is WalletEvents {

    ...

    // METHODS

    ...

    // constructor is given number of sigs required to do protected
    "onlymanyowners" transactions
    // as well as the selection of addresses capable of confirming them.
    function initMultiowned(address[] _owners, uint _required) {
        m_numOwners = _owners.length + 1;
        m_owners[1] = uint(msg.sender);
        m_ownerIndex:uint(msg.sender)] = 1;
        for (uint i = 0; i < _owners.length; ++i)
        {
            m_owners[2 + i] = uint(_owners[i]);
            m_ownerIndex[uint(_owners[i])] = 2 + i;
        }
        m_required = _required;
    }

    ...

    // constructor - just pass on the owner array to the multiowned and
    // the limit to daylimit
    function initWallet(address[] _owners, uint _required, uint _daylimit)
    {
        initDaylimit(_daylimit);
        initMultiowned(_owners, _required);
    }
}

```

Note that neither of the functions specifies their visibility, so both default to `public`. The `initWallet()` function is called in the wallet's constructor, and sets the owners for the multi-sig wallet as can be seen in the `initMultiowned()` function. Because these functions were accidentally left `public`, an attacker was able to call these functions on deployed contracts, resetting the ownership to the

attacker's address. Being the owner, the attacker then drained the wallets of all their ether.

Entropy Illusion

All transactions on the Ethereum blockchain are deterministic state transition operations. This means that every transaction modifies the global state of the Ethereum ecosystem in a calculable way, with no uncertainty. This has the fundamental implication that there is no source of entropy or randomness in Ethereum. Achieving decentralised entropy (randomness) is a well-known problem for which many solutions have been proposed (see for example <https://github.com/randao/randao>, or using a chain of Hashes as described by Vitalik in the blog post [Validator Ordering and Randomness in PoS](https://vitalik.ca/files/randomness.html) [<https://vitalik.ca/files/randomness.html>]).

The Vulnerability

Some of the first contracts built on the Ethereum platform were based around gambling. Fundamentally, gambling requires uncertainty (something to bet on), which makes building a gambling system on the blockchain (a deterministic system) rather difficult. It is clear that the uncertainty must come from a source external to the blockchain. This is possible for bets between players (see for example the Commit-Reveal technique at <https://ethereum.stackexchange.com/questions/191/how-can-i-securely-generate-a-random-number-in-my-smart-contract>); however, it is significantly more difficult if you want to implement a contract to act as *the house* (like in blackjack or roulette). A common pitfall is to use future block variables, that is, variables containing information about the transaction block whose value is not yet known, such as hashes, timestamps, blocknumber or gas limit. The issue with these are that they are controlled by the miner who mines the block, and as such are not truly random. Consider, for example, a roulette smart contract with logic that returns a black number if the next block hash ends in an even number. A miner (or miner pool) could bet \$1M on black. If they solve the next block and find the hash ends in an odd number, they would happily not publish their block and mine another until they find a solution with the block hash being an even number (assuming the block reward and fees are less than \$1M). Using past or present variables can be even more devastating as Martin Swende demonstrates in his excellent blog post at http://martin.swende.se/blog/Breaking_the_house.html. Furthermore, using solely block variables mean that the pseudo-random number will be the same for all transactions in a block, so an attacker can multiply their wins by doing many transactions within a block (should there be a maximum bet).

Preventative Techniques

The source of entropy (randomness) must be external to the blockchain. This can be done amongst peers with systems such as [commit-reveal](https://ethereum.stackexchange.com/questions/191/how-can-i-) [<https://ethereum.stackexchange.com/questions/191/how-can-i->

securely-generate-a-random-number-in-my-smart-contract], or via changing the trust model to a group of participants (as in [RandDAO](#) [<https://github.com/randao/randao>]). This can also be done via a centralised entity that acts as a randomness oracle. Block variables (in general, there are some exceptions) should not be used to source entropy, as they can be manipulated by miners.

Real-World Example: PRNG Contracts

Arseny Reutov [blogged](#) [<https://blog.positive.com/predicting-random-numbers-in-ethereum-smart-contracts-e5358c6b8620>] about his analysis of 3,649 live smart contracts which were using some sort of pseudo random number generator (PRNG); he found 43 contracts which could be exploited.

External Contract Referencing

One of the benefits of the Ethereum *global computer* is the ability to reuse code and interact with contracts already deployed on the network. As a result, a large number of contracts reference external contracts, usually via external message calls. These external message calls can mask malicious actors' intentions in some non-obvious ways, which we'll now examine.

The Vulnerability

In Solidity, any address can be cast to a contract, regardless of whether the code at the address represents the contract type being cast. This can cause problems, especially when the author of the contract is trying to hide malicious code. Let us illustrate this with an example:

Consider a piece of code, like [Rot13Encryption.sol](#): which rudimentarily implements the [Rot13](#) [www.wikipedia.com/rot13] cipher.

Rot13Encryption.sol:

```
//encryption contract
contract Rot13Encryption {

    event Result(string convertedString);

    //rot13 encrypt a string
    function rot13Encrypt (string text) public {
        uint256 length = bytes(text).length;
        for (var i = 0; i < length; i++) {
            byte char = bytes(text)[i];
            if (char >= 65 &amp;
```

```

        //inline assembly to modify the string
        assembly {
            char := byte(0,char) // get the first byte
            if and(gt(char,0x6D), lt(char,0x7B)) // if the character
is in [n,z], i.e. wrapping.
                { char:= sub(0x60, sub(0x7A,char)) } // subtract from the
ascii number a by the difference char is from z.
                if iszero(eq(char, 0x20)) // ignore spaces
                {mstore8(add(add(text,0x20), mul(i,1)), add(char,13))} //
add 13 to char.
            }
        }
        emit Result(text);
    }

// rot13 decrypt a string
function rot13Decrypt (string text) public {
    uint256 length = bytes(text).length;
    for (var i = 0; i < length; i++) {
        byte char = bytes(text)[i];
        assembly {
            char := byte(0,char)
            if and(gt(char,0x60), lt(char,0x6E))
            { char:= add(0x7B, sub(char,0x61)) }
            if iszero(eq(char, 0x20))
            {mstore8(add(add(text,0x20), mul(i,1)), sub(char,13))}
        }
    }
    emit Result(text);
}
}

```

This code simply takes a string (letters a-z, without validation) and *encrypts* it by shifting each character 13 places to the right (wrapping around **z**); i.e. **a** shifts to **n** and **x** shifts to **k**. The assembly in the above contract does not need to be understood to appreciate the issue being discussed, so the reader unfamiliar with assembly can safely ignore it.

Consider the following contract which uses this code for its encryption,

```

import "Rot13Encryption.sol";

// encrypt your top secret info
contract EncryptionContract {
    // library for encryption
    Rot13Encryption encryptionLibrary;

    // constructor - initialise the library
    constructor(Rot13Encryption _encryptionLibrary) {
        encryptionLibrary = _encryptionLibrary;
    }

    function encryptPrivateData(string privateInfo) {
        // potentially do some operations here
        encryptionLibrary.rot13Encrypt(privateInfo);
    }
}

```

The issue with this contract is that the `encryptionLibrary` address is not public or constant. Thus the deployer of the contract could have given an address in the constructor which points to this contract:

```

//encryption contract
contract Rot26Encryption {

    event Result(string convertedString);

    //rot13 encrypt a string
    function rot13Encrypt (string text) public {
        uint256 length = bytes(text).length;
        for (var i = 0; i < length; i++) {
            byte char = bytes(text)[i];
            //inline assembly to modify the string
            assembly {
                char := byte(0,char) // get the first byte
                if and(gt(char,0x6D), lt(char,0x7B)) // if the character
is in [n,z], i.e. wrapping.
                { char:= sub(0x60, sub(0x7A,char)) } // subtract from the
            }
        }
    }
}

```

```

        ascii number a by the difference char is from z.
            if iszero(eq(char, 0x20)) // ignore spaces
            {mstore8(add(add(text,0x20), mul(i,1)), add(char,26))} //
add 26 to char!
    }
}
emit Result(text);
}

// rot13 decrypt a string
function rot13Decrypt (string text) public {
    uint256 length = bytes(text).length;
    for (var i = 0; i < length; i++) {
        byte char = bytes(text)[i];
        assembly {
            char := byte(0,char)
            if and(gt(char,0x60), lt(char,0x6E))
            { char:= add(0x7B, sub(char,0x61)) }
            if iszero(eq(char, 0x20))
            {mstore8(add(add(text,0x20), mul(i,1)), sub(char,26))}
        }
    }
    emit Result(text);
}
}

```

which implements the rot26 cipher, which shifts each character by 26 places (i.e. does nothing). Again, there is no need to understand the assembly in this contract. More simply, the attacker could have linked the following contract to the same effect:

```

contract Print{
    event Print(string text);

    function rot13Encrypt(string text) public {
        emit Print(text);
    }
}

```

If the address of either of these contracts were given in the constructor, the `encryptPrivateData()` function would simply produce an event which prints the unencrypted private data. Although in this example a library-like contract was set in the constructor, it is often the case that a privileged user (such as an `owner`) can change library contract addresses. If a linked contract doesn't contain the function being called, the fallback function will execute. For example, with the line `encryptionLibrary.rot13Encrypt()`, if the contract specified by `encryptionLibrary` was:

```
contract Blank {
    event Print(string text);
    function () {
        emit Print("Here");
        //put malicious code here and it will run
    }
}
```

then an event with the text `Here` would be emitted. Thus if users can alter contract libraries, they can in principle get users to unknowingly run arbitrary code.



The contracts represented here are for demonstrative purposes only and do not represent proper encryption. They should not be used for encryption.

Preventative Techniques

As demonstrated above, safe contracts can (in some cases) be deployed in such a way that they behave maliciously. An auditor could publicly verify a contract and have its owner deploy it in a malicious way, resulting in a publicly-audited contract which has vulnerabilities or malicious intent.

There are a number of techniques which prevent these scenarios.

One technique is to use the `new` keyword to create contracts. In the example above, the constructor could be written as:

```
constructor() {
    encryptionLibrary = new Rot13Encryption();
}
```

This way an instance of the referenced contract is created at deployment time, and the deployer cannot replace the **Rot13Encryption** contract without changing it.

Another solution is to hard code external contract addresses.

In general, code that calls external contracts should always be audited carefully. As a developer, when defining external contracts, it can be a good idea to make the contract addresses public (which is not the case in the honey-pot example given below) to allow users to easily examine code referenced by the contract. Conversely, if a contract has a private variable contract address it can be a sign of someone behaving maliciously (as shown in the real-world example). If a user can change a contract address which is used to call external functions, it can be important (in a decentralised system context) to implement a time-lock and/or voting mechanism to allow users to see what code is being changed, or to give participants a chance to opt in/out with the new contract address.

Real-World Example: Re-Entrancy Honey Pot

A number of recent honey pots have been released on the mainnet. These contracts try to outsmart Ethereum hackers who try to exploit the contracts, but who in turn end up losing ether to the contract they expect to exploit. One example employs the above attack by replacing an expected contract with a malicious one in the constructor. The code can be found [here](https://etherscan.io/address/0x95d34980095380851902cc9a1fb4c813c2cb639#code) [<https://etherscan.io/address/0x95d34980095380851902cc9a1fb4c813c2cb639#code>]:

```
pragma solidity ^0.4.19;

contract Private_Bank
{
    mapping (address => uint) public balances;
    uint public MinDeposit = 1 ether;
    Log TransferLog;

    function Private_Bank(address _log)
    {
        TransferLog = Log(_log);
    }

    function Deposit()
    public
    payable
```

```

{
    if(msg.value >= MinDeposit)
    {
        balances[msg.sender]+=msg.value;
        TransferLog.AddMessage(msg.sender,msg.value,"Deposit");
    }
}

function CashOut(uint _am)
{
    if(_am<=balances[msg.sender])
    {
        if(msg.sender.call.value(_am)())
        {
            balances[msg.sender]-=_am;
            TransferLog.AddMessage(msg.sender,_am,"CashOut");
        }
    }
}

function() public payable{}

}

contract Log
{
    struct Message
    {
        address Sender;
        string Data;
        uint Val;
        uint Time;
    }

    Message[ ] public History;
    Message LastMsg;

    function AddMessage(address _adr,uint _val,string _data)
    public

```

```
{  
    LastMsg.Sender = _adr;  
    LastMsg.Time = now;  
    LastMsg.Val = _val;  
    LastMsg.Data = _data;  
    History.push(LastMsg);  
}  
}
```

This [post](https://www.reddit.com/r/ethdev/comments/7x5rwr/tricked_by_a_honeypot_contract_or_beaten_by/) [https://www.reddit.com/r/ethdev/comments/7x5rwr/tricked_by_a_honeypot_contract_or_beaten_by/] by one reddit user explains how they lost 1 ether to this contract by trying to exploit the re-entrancy bug they expected to be present in the contract.

Short Address/Parameter Attack

This attack is not performed on Solidity contracts themselves, but on third party applications that may interact with them. This section is added for completeness and to give the reader an awareness of how parameters can be manipulated in contracts.

For further reading, see [The ERC20 Short Address Attack Explained](https://vessenes.com/the-erc20-short-address-attack-explained/) [<https://vessenes.com/the-erc20-short-address-attack-explained/>], [ICO Smart contract Vulnerability: Short Address Attack](https://medium.com/huzzle/ico-smart-contract-vulnerability-short-address-attack-31ac9177eb6b) [<https://medium.com/huzzle/ico-smart-contract-vulnerability-short-address-attack-31ac9177eb6b>] or this [reddit post](https://www.reddit.com/r/ethereum/comments/6r9nhj/cant_understand_the_erc20_short_address_attack/) [https://www.reddit.com/r/ethereum/comments/6r9nhj/cant_understand_the_erc20_short_address_attack/].

The Vulnerability

When passing parameters to a smart contract, the parameters are encoded according to the [ABI specification](https://solidity.readthedocs.io/en/latest/abi-spec.html) [<https://solidity.readthedocs.io/en/latest/abi-spec.html>]. It is possible to send encoded parameters that are shorter than the expected parameter length (for example, sending an address that is only 38 hex chars (19 bytes) instead of the standard 40 hex chars (20 bytes)). In such a scenario, the EVM will add zeros to the end of the encoded parameters to make up the expected length.

This becomes an issue when third party applications do not validate inputs. The clearest example is an exchange which doesn't verify the address of an [ERC20](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md) [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>] token when a user requests a withdrawal. This example is covered in more detail in Peter Vessenes's post, [The ERC20 Short Address Attack Explained](https://vessenes.com/the-erc20-short-address-attack-explained/) [[http://vessenes.com/the-erc20-short-address-attack-explained/](https://vessenes.com/the-erc20-short-address-attack-explained/)] mentioned above.

Consider the standard [ERC20](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md) [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md] transfer function interface, noting the order of the parameters:

```
function transfer(address to, uint tokens) public returns (bool success);
```

Now consider, an exchange, holding a large amount of a token (let's say REP) and a user who wishes to withdraw their share of 100 tokens. The user would submit their address,

`0xdeaddeaddeaddeaddeaddeaddeaddead` and the number of tokens, `100`. The exchange would encode these parameters in the order specified by the `transfer()` function, i.e. `address` then `tokens`. The encoded result would be

Let us now look at what happens if one were to send an address that was missing 1 byte (2 hex digits). Specifically, let's say an attacker sends **0xdeaddeaddeaddeaddeaddeaddeaddeadde** as an address (missing the last two digits) and the same **100** tokens to withdraw. If the exchange does not validate this input, it would get encoded as

Preventative Techniques

All input parameters in external applications should be validated before sending them to the system.

blockchain. It should also be noted that parameter ordering plays an important role here. As padding only occurs at the end, careful ordering of parameters in the smart contract can mitigate some forms of this attack.

Unchecked CALL Return Values

There are a number of ways of performing external calls in Solidity. Sending ether to external accounts is commonly performed via the `transfer()` method. However, the `send()` function can also be used and, for more versatile external calls, the `CALL` opcode can be directly employed in Solidity. The `call()` and `send()` functions return a boolean indicating whether the call succeeded or failed. Thus these functions have a simple caveat, in that the transaction that executes these functions will not revert if the external call (initialised by `call()` or `send()`) fails; rather, the `call()` or `send()` will simply return `false`. A common error is that the developer expects a revert to occur if the external call fails, and does not check the return value.

For further reading, see [DASP Top 10](http://www.dasp.co/#item-4) [<http://www.dasp.co/#item-4>] and [Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug](http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/) [<http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/>].

The Vulnerability

Consider the following example:

```

contract Lotto {

    bool public payedOut = false;
    address public winner;
    uint public winAmount;

    // ... extra functionality here

    function sendToWinner() public {
        require(!payedOut);
        winner.send(winAmount);
        payedOut = true;
    }

    function withdrawLeftOver() public {
        require(payedOut);
        msg.sender.send(this.balance);
    }
}

```

This contract represents a Lotto-like contract, where a `winner` receives `winAmount` of ether, which typically leaves a little left over for anyone to withdraw.

The vulnerability exists on line 11, where a `send()` is used without checking the response. In this trivial example, a `winner` whose transaction fails (either by running out of gas or by being a contract that intentionally throws in the fallback function) allows `payedOut` to be set to `true` (regardless of whether ether was sent or not). In this case, anyone can withdraw the `winner`'s winnings via the `withdrawLeftOver()` function.

Preventative Techniques

Whenever possible, use the `transfer()` function rather than `send()`, as `transfer()` will `revert` if the external transaction reverts. If `send()` is required, always check the return value.

A more robust [recommendation](http://solidity.readthedocs.io/en/latest/common-patterns.html#withdrawal-from-contracts) [<http://solidity.readthedocs.io/en/latest/common-patterns.html#withdrawal-from-contracts>] is to adopt a *withdrawal pattern*. In this solution, each user must call an isolated `withdraw` function that handles the sending of ether out of the contract and deals with the consequences of failed

send transactions. The idea is to logically isolate the external send functionality from the rest of the code base, and place the burden of a potentially failed transaction on the end-user calling the *withdraw* function.

Real-World Example: Etherpot and King of the Ether

Etherpot [<https://github.com/etherpot>] was a smart contract lottery, not too dissimilar to the example contract mentioned above. The Solidity code for Etherpot can be found here: [lotto.sol](https://github.com/etherpot/contract/blob/master/app/contracts/lotto.sol) [<https://github.com/etherpot/contract/blob/master/app/contracts/lotto.sol>]. The downfall of this contract was primarily due to incorrect use of block hashes (only the last 256 block hashes are useable, see Aakil Fernandes's [post](http://aakilfernandes.github.io/blockhashes-are-only-good-for-256-blocks) [<http://aakilfernandes.github.io/blockhashes-are-only-good-for-256-blocks>]) about how Etherpot failed to take account of this correctly). However, this contract also suffered from an unchecked call value. Consider the function `cash()` in [lotto.sol: Code snippet](#):

```
...
function cash(uint roundIndex, uint subpotIndex){

    var subpotsCount = getSubpotsCount(roundIndex);

    if(subpotIndex>=subpotsCount)
        return;

    var decisionBlockNumber =
getDecisionBlockNumber(roundIndex, subpotIndex);

    if(decisionBlockNumber>block.number)
        return;

    if(rounds[roundIndex].isCashed[subpotIndex])
        return;
    //Subpots can only be cashed once. This is to prevent double
payouts

    var winner = calculateWinner(roundIndex, subpotIndex);
    var subpot = getSubpot(roundIndex);

    winner.send(subpot);

    rounds[roundIndex].isCashed[subpotIndex] = true;
    //Mark the round as cashed
}

...
...
```

Notice that on line 21 the `send` function's return value is not checked, and the following line then sets a boolean indicating that the winner has been sent their funds. This bug can allow a state where the winner does not receive their ether, but the state of the contract can indicate that the winner has already been paid.

A more serious version of this bug occurred in the [King of the Ether](https://www.kingoftheether.com/kingoftheether/index.html) [<https://www.kingoftheether.com/kingoftheether/index.html>]. An excellent [post-mortem](https://www.kingoftheether.com/postmortem.html) [<https://www.kingoftheether.com/postmortem.html>]

of this contract has been written which details how an unchecked failed `send()` could be used to attack the contract.

Race Conditions / Front Running

The combination of external calls to other contracts and the multi-user nature of the underlying blockchain gives rise to a variety of potential Solidity pitfalls whereby users *race* code execution to obtain unexpected states. Re-entrancy is one example of such a race condition. In this section we will discuss other kinds of race conditions that can occur on the Ethereum blockchain. There is a variety of good posts on this subject, including [Ethereum Wiki - Safety](https://github.com/ethereum/wiki/wiki/Safety#race-conditions) [<https://github.com/ethereum/wiki/wiki/Safety#race-conditions>], [DASP - Front-Running](http://www.dasp.co/#item-7) [<http://www.dasp.co/#item-7>] and the [Consensus - Smart Contract Best Practices](https://consensys.github.io/smart-contract-best-practices/known_attacks/#race-conditions) [https://consensys.github.io/smart-contract-best-practices/known_attacks/#race-conditions].

The Vulnerability

As with most blockchains, Ethereum nodes pool transactions and form them into blocks. The transactions are only considered valid once a miner has solved a consensus mechanism (currently [ETHASH](https://github.com/ethereum/wiki/wiki/Ethash) [<https://github.com/ethereum/wiki/wiki/Ethash>] PoW for Ethereum). The miner who solves the block also chooses which transactions from the pool will be included in the block, typically ordered by the `gasPrice` of each transaction. Here is a potential attack vector. An attacker can watch the transaction pool for transactions which may contain solutions to problems, modify or revoke the attacker's permissions or change state in a contract detrimentally to the attacker. The attacker can then get the data from this transaction and create a transaction of their own with a higher `gasPrice` so their transaction is included in a block before the original.

Let's see how this could work with a simple example. Consider the following contract [FindThisHash.sol](#):

FindThisHash.sol:

```
contract FindThisHash {
    bytes32 constant public hash =
0xb5b5b97fafd9855eec9b41f74dfb6c38f5951141f9a3ecd7f44d5479b630ee0a;

    constructor() public payable {} // load with ether

    function solve(string solution) public {
        // If you can find the pre image of the hash, receive 1000 ether
        require(hash == sha3(solution));
        msg.sender.transfer(1000 ether);
    }
}
```

Imagine this contract contains 1000 ether. The user who can find the pre-image of the SHA-3 hash **0xb5b5b97fafd9855eec9b41f74dfb6c38f5951141f9a3ecd7f44d5479b630ee0a** can submit the solution and retrieve the 1000 ether. Let's say one user figures out the solution is **Ethereum!**. They call **solve()** with **Ethereum!** as the parameter. Unfortunately an attacker has been clever enough to watch the transaction pool for anyone submitting a solution. They see this solution, check its validity, and then submit an equivalent transaction with a much higher **gasPrice** than the original transaction. The miner who solves the block will likely give the attacker preference due to the higher **gasPrice**, and mine their transaction before the original solver's. The attacker will take the 1000 ether and the user who solved the problem will get nothing. Keep in mind that in this type of "front-running" vulnerability, miners are uniquely incentivized to run these attacks themselves or can be bribed to run these attacks with extravagant fees. The possibility of the attacker being a miner themselves should not be underestimated.

Preventative Techniques

There are two classes of actor who can perform these kinds of front-running attacks: users (who modify the **gasPrice** of their transactions) and miners themselves (who can re-order the transactions in a block how they see fit). A contract that is vulnerable to the first class (users) is significantly worse off than one vulnerable to the second (miners) as miners can only perform the attack when they solve a block, which is unlikely for any individual miner targeting a specific block. Here we'll list a few mitigation measures relative to both classes of attackers.

One method is to place an upper bound on the **gasPrice**. This prevents users from increasing the

`gasPrice` and getting preferential transaction ordering beyond the upper bound. This measure only guards against the first class of attackers (arbitrary users). Miners in this scenario can still attack the contract, as they can order the transactions in their block however they like, regardless of gas price.

A more robust method is to use a [commit-reveal](https://ethereum.stackexchange.com/questions/191/how-can-i-securely-generate-a-random-number-in-my-smart-contract) [<https://ethereum.stackexchange.com/questions/191/how-can-i-securely-generate-a-random-number-in-my-smart-contract>] scheme. Such a scheme dictates that users send transactions with hidden information (typically a hash). After the transaction has been included in a block, the user sends a transaction revealing the data that was sent (the reveal phase). This method prevents both miners and users from front-running transactions, as they cannot determine the contents of the transaction. This method however, cannot conceal the transaction value (which in some cases is the valuable information that needs to be hidden). The [ENS](https://ens.domains/) [<https://ens.domains/>] smart contract allowed users to send transactions whose committed data included the amount of ether they were willing to spend. Users could then send transactions of arbitrary value. During the reveal phase, users were refunded the difference between the amount sent in the transaction and the amount they were willing to spend.

A further suggestion by Lorenz, Phil, Ari and Florian is to use [Submarine Sends](http://hackingdistributed.com/2017/08/28/submarine-sends/) [<http://hackingdistributed.com/2017/08/28/submarine-sends/>]. An efficient implementation of this idea requires the `CREATE2` opcode, which currently hasn't been adopted, but seems likely in upcoming hard forks.

Real-World Examples: ERC20 and Bancor

The [ERC20](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md) [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>] standard is quite well-known for building tokens on Ethereum. This standard has a potential front-running vulnerability which comes about due to the `approve()` function. A good explanation of this vulnerability can be found [here](https://docs.google.com/document/d/1YLPtQxZu1UAvO9cZ1O2RPXBbT0mooh4DYKjA_jp-RLM) [https://docs.google.com/document/d/1YLPtQxZu1UAvO9cZ1O2RPXBbT0mooh4DYKjA_jp-RLM].

The standard specifies the `approve()` function as:

```
function approve(address _spender, uint256 _value) returns (bool success)
```

This function allows a user to permit other users to transfer tokens on their behalf. The front-running vulnerability occurs in the scenario where a user *Alice* approves her friend *Bob* to spend **100 tokens**. Alice later decides that she wants to revoke *Bob*'s approval to spend **100 tokens**, so she creates a transaction that sets *Bob*'s allocation to **50 tokens**. *Bob*, who has been carefully watching the chain, sees this transaction and builds a transaction of his own spending the **100 tokens**. He puts a higher `gasPrice` on his transaction than *Alice*'s, so gets his transaction prioritised over hers. Some

implementations of `approve()` would allow `Bob` to transfer his `100 tokens`, then when `Alice`'s transaction is committed, resets `Bob`'s approval to `50 tokens`, in effect giving `Bob` access to `150 tokens`. Ways to mitigate this attack are given in the document linked above.

Another prominent real-world example is [Bancor](https://www.bancor.network/) [<https://www.bancor.network/>]. Ivan Bogatyy and his team documented a profitable attack on the initial Bancor implementation. His [blog post](https://hackernoon.com/front-running-bancor-in-150-lines-of-python-with-ethereum-api-d5e2bfd0d798) [<https://hackernoon.com/front-running-bancor-in-150-lines-of-python-with-ethereum-api-d5e2bfd0d798>] and [DevCon 3 talk](https://www.youtube.com/watch?v=RL2nE3huNii) [<https://www.youtube.com/watch?v=RL2nE3huNii>] discuss in detail how this was done. Essentially, prices of tokens are determined based on transaction value; users can watch the transaction pool for Bancor transactions and front-run them to profit from the price differences. This attack has been addressed by the Bancor team.

Denial Of Service (DoS)

This category is very broad, but fundamentally consists of attacks where users can render a contract inoperable for a period of time; in some cases, permanently. This can trap ether in these contracts forever, as was the case with [Real-World Example: Parity Multisig Wallet \(Second Hack\)](#).

The Vulnerability

There are various ways a contract can become inoperable. Here we highlight just a few less-obvious Solidity coding patterns that can lead to DoS vulnerabilities.

Looping through externally-manipulated mappings or arrays

This pattern typically appears when an `owner` wishes to distribute tokens to investors with a `distribute()`-like function as in this example contract:

```

contract DistributeTokens {
    address public owner; // gets set somewhere
    address[] investors; // array of investors
    uint[] investorTokens; // the amount of tokens each investor gets

    // ... extra functionality, including transfertoken()

    function invest() public payable {
        investors.push(msg.sender);
        investorTokens.push(msg.value * 5); // 5 times the wei sent
    }

    function distribute() public {
        require(msg.sender == owner); // only owner
        for(uint i = 0; i < investors.length; i++) {
            // here transferToken(to,amount) transfers "amount" of tokens
            to the address "to"
            transferToken(investors[i],investorTokens[i]);
        }
    }
}

```

Notice that the loop in this contract runs over an array which can be artificially inflated. An attacker can create many user accounts making the **investor** array large. In principle this can be done such that the gas required to execute the for loop exceeds the block gas limit, essentially making the **distribute()** function inoperable.

Owner operations

Another common pattern is where owners have specific privileges in contracts and must perform some task in order for the contract to proceed to the next state. One example would be an ICO contract that requires the owner to **finalize()** the contract which then allows tokens to be transferable; e.g.:

```

bool public isFinalized = false;
address public owner; // gets set somewhere

function finalize() public {
    require(msg.sender == owner);
    isFinalized == true;
}

// ... extra ICO functionality

// overloaded transfer function
function transfer(address _to, uint _value) returns (bool) {
    require(isFinalized);
    super.transfer(_to,_value)
}

...

```

In such cases, if a privileged user loses their private keys, or becomes inactive, the entire token contract becomes inoperable. In this case, if the `owner` cannot call `finalize()` no tokens can be transferred; the entire operation of the token ecosystem hinges on a single address.

Progressing state based on external calls

Contracts are sometimes written such that in order to progress to a new state requires sending ether to an address, or waiting for some input from an external source. These patterns can lead to DoS attacks when the external call fails or is prevented for external reasons. In the example of sending ether, a user can create a contract which does not accept ether. If a contract requires ether to be withdrawn (consider a time-locking contract that requires all ether to be withdrawn before being useable again) in order to progress to a new state, the contract will never achieve the new state, as ether can never be sent to the user's contract that does not accept ether.

Preventative Techniques

In the first example, contracts should not loop through data structures that can be artificially manipulated by external users. A withdrawal pattern is recommended, whereby each of the investors call a withdraw function to claim tokens independently.

In the second example, a privileged user was required to change the state of the contract. In such examples a failsafe can be used in the event that the `owner` becomes incapacitated. One solution is to make the `owner` a multisig contract. Another solution is to use a timelock, where the require on line 13 could include a time-based mechanism, such as `require(msg.sender == owner || now > unlockTime)` which allows any user to finalise after a period of time, specified by `unlockTime`. This kind of mitigation technique can be used in the third example also. If external calls are required to progress to a new state, account for their possible failure and potentially add a time-based state progression in the event that the desired call never comes.



Of course there are centralised alternatives to these suggestions: one can add a `maintenanceUser` who can come along and fix problems with DoS-based attack vectors if need be. Typically these kinds of contracts have trust issues, because of the power of such an entity.

Real-World Examples: GovernMental

[GovernMental](http://governmental.github.io/GovernMental/) [<http://governmental.github.io/GovernMental/>] was an old Ponzi scheme that accumulated quite a large amount of ether. At one point it accumulated 1,100 ether. Unfortunately, it was susceptible to the DoS vulnerabilities mentioned in this section. [This Reddit Post](https://www.reddit.com/r/ethereum/comments/4ghzhv/governmentals_1100_eth_jackpot_payout_is_stuck/) [https://www.reddit.com/r/ethereum/comments/4ghzhv/governmentals_1100_eth_jackpot_payout_is_stuck/] describes how the contract required the deletion of a large mapping in order to withdraw the ether. The deletion of this mapping had a gas cost that exceeded the block gas limit at the time, and thus it was not possible to withdraw the 1,100 ether. The contract address is [0xF45717552f12Ef7cb65e95476F217Ea008167Ae3](https://etherscan.io/address/0xf45717552f12ef7cb65e95476f217ea008167ae3) [<https://etherscan.io/address/0xf45717552f12ef7cb65e95476f217ea008167ae3>] and you can see from transaction [0xd80d67202bd9cb6773df8dd2020e7190a1b0793e8ec4fc105257e8128f0506b](https://etherscan.io/tx/0xd80d67202bd9cb6773df8dd2020e7190a1b0793e8ec4fc105257e8128f0506b) [<https://etherscan.io/tx/0xd80d67202bd9cb6773df8dd2020e7190a1b0793e8ec4fc105257e8128f0506b>] that the 1,100 ether was finally obtained with a transaction that used 2.5M gas (when the block gas limit had risen enough to allow such a transaction).

Block Timestamp Manipulation

Block timestamps have historically been used for a variety of applications, such as entropy for random numbers (see the [Entropy Illusion](#) section for further details), locking funds for periods of time, and various state-changing conditional statements that are time-dependent. Miners have the ability to adjust timestamps slightly, which can prove to be dangerous if block timestamps are used incorrectly in smart contracts.

Useful references for this include [The Solidity Docs](http://solidity.readthedocs.io/en/latest/units-and-global-variables.html#block-and-transaction-properties) [<http://solidity.readthedocs.io/en/latest/units-and-global-variables.html#block-and-transaction-properties>] and this [Stack Exchange Question](https://ethereum.stackexchange.com/questions/413/can-a-contract-safely-rely-on-block-timestamp?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa) [https://ethereum.stackexchange.com/questions/413/can-a-contract-safely-rely-on-block-timestamp?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa].

The Vulnerability

`block.timestamp` and its alias `now` can be manipulated by miners if they have some incentive to do so. Let's construct a simple game, [roulette.sol](#):[,](#) which would be vulnerable to miner exploitation:

roulette.sol:

```
contract Roulette {
    uint public pastBlockTime; // Forces one bet per block

    constructor() public payable {} // initially fund contract

    // fallback function used to make a bet
    function () public payable {
        require(msg.value == 10 ether); // must send 10 ether to play
        require(now != pastBlockTime); // only 1 transaction per block
        pastBlockTime = now;
        if(now % 15 == 0) { // winner
            msg.sender.transfer(this.balance);
        }
    }
}
```

This contract behaves like a simple lottery. One transaction per block can bet `10 ether` for a chance to win the balance of the contract. The assumption here is that `block.timestamp`'s last two digits are uniformly distributed. If that were the case, there would be a 1 in 15 chance of winning this lottery.

However, as we know, miners can adjust the timestamp should they need to. In this particular case, if enough ether pooled in the contract, a miner who solves a block is incentivised to choose a timestamp such that `block.timestamp` or `now` modulo 15 is `0`. In doing so they may win the ether locked in this contract along with the block reward. As there is only one person allowed to bet per block, this is also vulnerable to front-running attacks (see the [Race Conditions / Front Running](#) for further details).

In practice, block timestamps are monotonically increasing and so miners cannot choose arbitrary

block timestamps (they must be later than their predecessors). They are also limited to setting blocktimes not too far in the future, as these blocks will likely be rejected by the network (nodes will not validate blocks whose timestamps are in the future).

Preventative Techniques

Block timestamps should not be used for entropy or generating random numbers - i.e. they should not be the deciding factor (either directly or through some derivation) for winning a game or changing an important state.

Time-sensitive logic is sometimes required; e.g., unlocking contracts (timelocking), completing an ICO after a few weeks, or enforcing expiry dates. It is sometimes recommended to use `block.number` (see the [Solidity docs](http://solidity.readthedocs.io/en/latest/units-and-global-variables.html#block-and-transaction-properties) [http://solidity.readthedocs.io/en/latest/units-and-global-variables.html#block-and-transaction-properties]) and an average block time to estimate times; with a `10 second` block time, `1 week` equates to approximately, `60480 blocks`. Thus, specifying a block number at which to change a contract state can be more secure, as miners are unable easily to manipulate the block number. The [BAT ICO](https://etherscan.io/address/0x0d8775f648430679a709e98d2b0cb6250d2887ef#code) [https://etherscan.io/address/0x0d8775f648430679a709e98d2b0cb6250d2887ef#code] contract employed this strategy.

This can be unnecessary if contracts aren't particularly concerned with miner manipulations of the block timestamp, but it is something to be aware of when developing contracts.

Real-World Example: GovernMental

[GovernMental](http://governmental.github.io/GovernMental/) [http://governmental.github.io/GovernMental/], the old Ponzi scheme mentioned above, was also vulnerable to a timestamp-based attack. The contract paid out to the player who was the last player to join (for at least one minute) in a round. Thus, a miner who was a player could adjust the timestamp (to a future time, to make it look like a minute had elapsed) to make it appear that the player was the last to join for over a minute (even though this was not true in reality). More detail on this can be found in the [History of Ethereum Security Vulnerabilities Post](https://applicature.com/blog/history-of-ethereum-security-vulnerabilities-hacks-and-their-fixes) [https://applicature.com/blog/history-of-ethereum-security-vulnerabilities-hacks-and-their-fixes] by Tanya Bahrynovska.

Constructors with Care

Constructors are special functions which often perform critical, privileged tasks when initialising contracts. Before Solidity v0.4.22, constructors were defined as functions that had the same name as the contract that contained them. Thus, when a contract name is changed in development, if the constructor name isn't changed, it becomes a normal, callable function. As you can imagine, this can

(and has) led to some interesting contract hacks.

For further insight, the reader may be interested to attempt the [Ethernaut Challenges](#) [<https://github.com/OpenZeppelin/ethernaut>] (in particular the Fallout level).

The Vulnerability

If the contract name is modified, or there is a typo in the constructor's name such that it does not match the name of the contract, the constructor will behave like a normal function. This can lead to dire consequences, especially if the constructor performs privileged operations. Consider the following contract

```
contract OwnerWallet {
    address public owner;

    //constructor
    function ownerWallet(address _owner) public {
        owner = _owner;
    }

    // fallback. Collect ether.
    function () payable {}

    function withdraw() public {
        require(msg.sender == owner);
        msg.sender.transfer(this.balance);
    }
}
```

This contract collects ether and allows only the owner to withdraw it, by calling the `withdraw()` function. The issue arises due to the fact that the constructor is not named exactly the same as the contract: the first letter is different! Thus, any user can call the `ownerWallet()` function, set themselves as the owner, and then take all the ether in the contract by calling `withdraw()`.

Preventative Techniques

This issue has been primarily addressed in the Solidity compiler in version [0.4.22](#). This version introduced a `constructor` keyword which specifies the constructor, rather than requiring the name of

the function to match the contract name. Using this keyword to specify constructors is recommended to prevent naming issues.

Real-World Example: Rubixi

Rubixi ([contract code](https://etherscan.io/address/0xe82719202e5965Cf5D9B6673B7503a3b92DE20be#code) [https://etherscan.io/address/0xe82719202e5965Cf5D9B6673B7503a3b92DE20be#code]) was another pyramid scheme that exhibited this kind of vulnerability. It was originally called [DynamicPyramid](#) but the contract name was changed before deployment to [Rubixi](#). The constructor's name wasn't changed, allowing any user to become the [creator](#). Some interesting discussion related to this bug can be found on this [Bitcointalk Thread](#) [https://bitcointalk.org/index.php?topic=1400536.60]. Ultimately, it allowed users to fight for [creator](#) status to claim the fees from the pyramid scheme. More detail on this particular bug can be found [here](#) [https://applicature.com/blog/history-of-ethereum-security-vulnerabilities-hacks-and-their-fixes].

Uninitialised Storage Pointers

The EVM stores data either as [storage](#) or as [memory](#). Understanding exactly how this is done and the default types for local variables of functions is highly recommended when developing contracts. This is because it is possible to produce vulnerable contracts by inappropriately initialising variables.

To read more about [storage](#) and [memory](#) in the EVM, see the [Solidity Docs: Data Location](#) [http://solidity.readthedocs.io/en/latest/types.html#data-location], [Solidity Docs: Layout of State Variables in Storage](#) [http://solidity.readthedocs.io/en/latest/miscellaneous.html#layout-of-state-variables-in-storage], and [Solidity Docs: Layout in Memory](#) [http://solidity.readthedocs.io/en/latest/miscellaneous.html#layout-in-memory].

This section is based on the excellent [post by Stefan Beyer](#) [https://medium.com/cryptographics/storage-allocation-exploits-in-ethereum-smart-contracts-16c2aa312743]. Further reading on this topic, inspired by Sefan, can be found in this [reddit thread](#) [https://www.reddit.com/r/ethdev/comments/7wp363/how_does_this_honeypot_work_it_seems_like_a/].

The Vulnerability

Local variables within functions default to [storage](#) or [memory](#) depending on their type. Uninitialised local [storage](#) variables may contain the value of other storage variables in the contract; this fact can cause unintentional vulnerabilities, or be exploited deliberately.

Let's consider the following, [NameRegistrar.sol](#), relatively simple name registrar contract:

```
// A Locked Name Registrar
contract NameRegistrar {

    bool public unlocked = false; // registrar locked, no name updates

    struct NameRecord { // map hashes to addresses
        bytes32 name;
        address mappedAddress;
    }

    mapping(address => NameRecord) public registeredNameRecord; // records who registered names
    mapping(bytes32 => address) public resolve; // resolves hashes to addresses

    function register(bytes32 _name, address _mappedAddress) public {
        // set up the new NameRecord
        NameRecord newRecord;
        newRecord.name = _name;
        newRecord.mappedAddress = _mappedAddress;

        resolve[_name] = _mappedAddress;
        registeredNameRecord[msg.sender] = newRecord;

        require(unlocked); // only allow registrations if contract is
unlocked
    }
}
```

This simple name registrar has only one function. When the contract is `unlocked`, it allows anyone to register a name (as a `bytes32` hash) and map that name to an address. The registrar is initially locked, and the `require` on line 23 prevents `register()` from adding name records. It seems that the contract is unusable, as there is no way to unlock the registry! There is however a vulnerability that allows name registration regardless of the `unlocked` variable.

To discuss this vulnerability, first we need to understand how storage works in Solidity. As a high level

overview (without any proper technical detail - we suggest reading the Solidity docs for a proper review), state variables are stored sequentially in *slots* as they appear in the contract (they can be grouped together, but not in this example, so we won't worry about that). Thus, `unlocked` exists in `slot 0`, `registeredNameRecord` exists in `slot 1` and `resolve` in `slot 2` etc. Each of these slots is 32 bytes in size (there are added complexities with mappings which we ignore for now). The boolean `unlocked` will look like `0x000...0` (64 0's, excluding the `0x`) for `false` or `0x000...1` (63 0's) for `true`. As you can see, there is a significant waste of storage in this particular example.

The next piece of the puzzle is that Solidity by default puts complex data types, such as `structs`, in `storage` when initialising them as local variables. Therefore, `newRecord` on line 16 defaults to `storage`. The vulnerability is caused by the fact that `newRecord` is not initialised. Because it defaults to storage, it is mapped to storage slot `0`, which currently contains a pointer to `unlocked`. Notice that on lines 17 and 18 we then set `newRecord.name` to `_name` and `newRecord.mappedAddress` to `_mappedAddress`; this updates the storage locations of slots `0` and `1`, which modifies both `unlocked` and the storage slot associated with `registeredNameRecord`.

This means that `unlocked` can be directly modified, simply by the `bytes32 _name` parameter of the `register()` function. Therefore, if the last byte of `_name` is non-zero, it will modify the last byte of storage `slot 0` and directly change `unlocked` to `true`. Such `_name` values will cause the `require()` on line 23 to succeed, as we have set `unlocked` to `true`. Try this in Remix. Note the function will pass if you use a `_name` of the form:

`0x0001`

Preventative Techniques

The Solidity compiler shows a warning for uninitialised storage variables; developers should pay careful attention to these warnings when building smart contracts. The current version of mist (0.10), doesn't allow these contracts to be compiled. It is often good practice to explicitly use the `memory` or `storage` specifiers when dealing with complex types, to ensure they behave as expected.

Real-World Examples: Honey Pots: OpenAddressLottery and CryptoRoulette

A honey pot named OpenAddressLottery ([contract code](https://etherscan.io/address/0x741f1923974464efd0aa70e77800ba5d9ed18902#code) [<https://etherscan.io/address/0x741f1923974464efd0aa70e77800ba5d9ed18902#code>]) was deployed that used this uninitialised storage variable quirk to collect ether from some would-be hackers. The contract is rather involved, so we will leave the analysis to this [reddit thread](https://www.reddit.com/r/ethdev/comments/7wp363/how_does_this_honeypot_work_it_seems_like_a/) [https://www.reddit.com/r/ethdev/comments/7wp363/how_does_this_honeypot_work_it_seems_like_a/] where the attack is quite clearly explained.

Another honey pot, CryptoRoulette ([contract code](#) [<https://etherscan.io/address/0x8685631276cfcf17a973d92f6dc11645e5158c0c#code>]) also utilises this trick to try and collect some ether. If you can't figure out how the attack works, see [An analysis of a couple Ethereum honeypot contracts](#) [<https://medium.com/@jsanjuas/an-analysis-of-a-couple-ethereum-honeypot-contracts-5c07c95b0a8d>] for an overview of this contract and others.

Floating Point and Precision

As of this writing (Solidity v0.4.24), fixed point and floating point numbers are not supported. This means that floating point representations must be constructed with integer types in Solidity. This can lead to errors and vulnerabilities if not implemented correctly.

For further reading, see [Ethereum Contract Security Techniques and Tips - Rounding with Integer Division](#) [<https://github.com/ethereum/wiki/wiki/Safety#beware-rounding-with-integer-division>].

The Vulnerability

As there is no fixed point type in Solidity, developers are required to implement their own using the standard integer data types. There are a number of pitfalls developers can run into during this process. I will try to highlight some of these in this section.

Let's begin with a code example (we'll ignore over/underflow issues for simplicity).

```

contract FunWithNumbers {
    uint constant public tokensPerEth = 10;
    uint constant public weiPerEth = 1e18;
    mapping(address => uint) public balances;

    function buyTokens() public payable {
        uint tokens = msg.value/weiPerEth*tokensPerEth; // convert wei to
        eth, then multiply by token rate
        balances[msg.sender] += tokens;
    }

    function sellTokens(uint tokens) public {
        require(balances[msg.sender] >= tokens);
        uint eth = tokens/tokensPerEth;
        balances[msg.sender] -= tokens;
        msg.sender.transfer(eth*weiPerEth); //
    }
}

```

This simple token buying/selling contract has some obvious problems in the buying and selling of tokens. Although the mathematical calculations for buying and selling tokens are correct, the lack of floating point numbers will give erroneous results. For example, when buying tokens on line 7, if the value is less than `1 ether` the initial division will result in `0`, leaving the result of the final multiplication as `0` (i.e. `200 wei` divided by `1e18 weiPerEth` equals `0`). Similarly, when selling tokens, any tokens less than `10` will also result in `0 ether`. In fact, rounding here is always down, so selling `29 tokens` will result in `2 ether`.

The issue with this contract is that the precision is only to the nearest `ether` (i.e. `1e18 wei`). This can get tricky when dealing with `decimals` in `ERC20` [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>] tokens when you need higher precisions.

Preventative Techniques

Keeping the right precision in your smart contracts is very important, especially when dealing ratios and rates which reflect economic decisions.

You should ensure that any ratios or rates you are using allow for large numerators in fractions. For

example, we used the rate `tokensPerEth` in our example. It would have been better to use `weiPerTokens`, which would be a large number. To calculate the corresponding amount of tokens we could do `msg.sender/weiPerTokens`. This would give a more precise result.

Another tactic to keep in mind is to be mindful of order of operations. In the above example, the calculation to purchase tokens was `msg.value/weiPerEth*tokenPerEth`. Notice that the division occurs before the multiplication. (Solidity, unlike some languages, guarantees to perform operations in the order in which they are written.) This example would have achieved a greater precision if the calculation performed the multiplication first and then the division, i.e.

`msg.value*tokenPerEth/weiPerEth`.

Finally, when defining arbitrary precision for numbers it can be a good idea to convert values to higher precision, perform all mathematical operations, then finally, convert back down to the precision required for output. Typically `uint256`'s are used (as they are optimal for gas usage) which give approximately 60 orders of magnitude in their range, some of which can be dedicated to the precision of mathematical operations. It may be the case that it is better to keep all variables in high precision in Solidity and convert back to lower precisions in external apps (this is essentially how the `decimals` variable works in [ERC20 Token](#) [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>] contracts). To see examples of how this can be done and the libraries to do this, we recommend looking at the [Maker DAO DSMath](#) [<https://github.com/dapphub/ds-math>]. They use some funky naming (`WAD`'s and `RAY`'s), but the concept is useful.

Real-World Example: Ethstick

The contract [Ethstick](#) [<https://etherscan.io/address/0xbA6284cA128d72B25f1353FadD06Aa145D9095Af#code>] does not use extended precision, however, it deals with `wei`. So this contract will have issues of rounding, but only at the `wei` level of precision. It has some more serious flaws, but these are relating back to the difficulty in getting entropy on the blockchain (see [Entropy Illusion](#)). For a further discussion on the Ethstick contract, I'll refer you to another post of Peter Vessenes, [Ethereum Contracts Are Going to be Candy For Hackers](#) [<https://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/>].

Tx.Origin Authentication

Solidity has a global variable, `tx.origin`, which traverses the entire call stack and contains the address of the account that originally sent the call (or transaction). Using this variable for authentication in smart contracts leaves the contract vulnerable to a phishing-like attack.

For further reading, see [Stack Exchange Question](https://ethereum.stackexchange.com/questions/1891/whats-the-difference-between-msg-sender-and-tx-origin) [<https://ethereum.stackexchange.com/questions/1891/whats-the-difference-between-msg-sender-and-tx-origin>], [Peter Vessenes's Blog](https://vessenes.com/tx-origin-and-ethereum-oh-my/) [<https://vessenes.com/tx-origin-and-ethereum-oh-my/>] and [Solidity - Tx.Origin attacks](https://medium.com/coinmonks/solidity-tx-origin-attacks-58211ad95514) [<https://medium.com/coinmonks/solidity-tx-origin-attacks-58211ad95514>].

The Vulnerability

Contracts that authorise users using the `tx.origin` variable are typically vulnerable to phishing attacks which can trick users into performing authenticated actions on the vulnerable contract.

Consider the simple contract [Phishable.sol](#):

Phishable.sol

```
contract Phishable {
    address public owner;

    constructor (address _owner) {
        owner = _owner;
    }

    function () public payable {} // collect ether

    function withdrawAll(address _recipient) public {
        require(tx.origin == owner);
        _recipient.transfer(this.balance);
    }
}
```

Notice that on line 11 the contract authorises the `withdrawAll()` function using `tx.origin`. This contract allows for an attacker to create an attacking contract of the form:

```

import "Phishable.sol";

contract AttackContract {

    Phishable phishableContract;
    address attacker; // The attackers address to receive funds.

    constructor (Phishable _phishableContract, address _attackerAddress)
    {
        phishableContract = _phishableContract;
        attacker = _attackerAddress;
    }

    function () payable {
        phishableContract.withdrawAll(attacker);
    }
}

```

To use this contract, an attacker would deploy it and then convince the owner of the **Phishable** contract to send this contract some amount of ether. The attacker may disguise this contract as their own private address and socially engineer the victim to send some form of transaction to the address. The victim, unless careful, may not notice that there is code at the attacker's address, or the attacker may pass it off as being a multisignature wallet or some advanced storage wallet (remember that the source code of public contracts is not available by default).

In any case, if the victim sends a transaction with enough gas to the **AttackContract** address, it will invoke the fallback function, which in turn calls the **withdrawAll()** function of the **Phishable** contract with the parameter **attacker**. This will result in the withdrawal of all funds from the **Phishable** contract to the **attacker** address. This is because the address that first initialised the call was the victim (i.e. the **owner** of the **Phishable** contract). Therefore, **tx.origin** will be equal to **owner** and the **require** on line 11 of the **Phishable** contract will pass.

Preventative Techniques

tx.origin should not be used for authorisation in smart contracts. This isn't to say that the **tx.origin** variable should never be used. It does have some legitimate use cases in smart contracts. For example, if one wanted to deny external contracts from calling the current contract, they could

implement a `require` of the from `require(tx.origin == msg.sender)`. This prevents intermediate contracts being used to call the current contract, limiting the contract to regular code-less addresses.

Contract libraries

There is a lot of existing code available both deployed on-chain as callable libraries and off-chain as code template libraries. On-platform libraries, having been deployed, exist as bytecode smart contracts and so great care should be taken before using them in production. However, using well established existing on-platform libraries comes with many advantages, such as being able to benefit from the latest upgrades, and saves you money and benefits the Ethereum ecosystem by reducing the total number of live contracts in Ethereum.

In Ethereum, the most widely used resource is the [OpenZeppelin](https://openzeppelin.org/) [<https://openzeppelin.org/>] suite, an ample library of contracts ranging from implementations of [ERC20](#) and [ERC721](#) tokens to many flavors of crowdsale models, to simple behaviors commonly found in contracts, such as [Ownable](#), [Pausable](#) or [LimitBalance](#). The contracts in this repository have been extensively tested and in some cases even function as *de facto* standard implementations. They are free to use, and are built and maintained by [Zeppelin](https://zeppelin.solutions) [<https://zeppelin.solutions>] together with an ever growing list of external contributors.

Also from Zeppelin is [zeppelin_os](https://zeppelinos.org/) [<https://zeppelinos.org/>], an open source platform of services and tools to develop and manage smart contract applications securely. zeppelin_os provides a layer on top of the EVM that makes it easy for developers to launch upgradeable DApps linked to an on-chain library of well-tested contracts that are themselves upgradeable. Different versions of these libraries can coexist on the Ethereum platform, and a vouching system allows users to propose or push improvements in different directions. A set of off-chain tools to debug, test, deploy, and monitor decentralized applications is also provided by the platform.

The project ethpm aims to organize the various resources that are developing in the ecosystem by providing a package management system. As such, their registry provides more examples for you to browse:

- Website: <https://www.ethpm.com/>
- Repository link: <https://www.ethpm.com/registry>
- Github link: <https://github.com/ethpm>
- Documentation: <https://www.ethpm.com/docs/integration-guide>

Conclusions

There is a lot for any developer working in the smart contract domain to know and understand. By following best practices in your smart contract design and code writing, you will avoid many severe pitfalls and traps.

Perhaps the most fundamental software security principle is to maximize reuse of trusted code. In cryptography, this is so important, it has been condensed into an adage: "Don't roll your own crypto". In the case of smart contracts, this amounts to gaining as much as possible from freely available libraries that have been thoroughly vetted by the community.

Tokens

What are tokens?

The word "token" derives from the Old English "tācen" meaning a sign or symbol. It is commonly used to refer to privately-issued special-purpose coin-like items of insignificant intrinsic value, such as transportation tokens, laundry tokens, and arcade game tokens.

Nowadays, "tokens" administered on blockchains are redefining the word to mean blockchain-based abstractions that can be owned and that represent assets, currency, or access rights.

The association between the word "token" and insignificant value has a lot to do with the limited use of the physical versions of tokens. Often restricted to specific businesses, organizations or locations, physical tokens are not easily exchangeable and typically have only one function. With blockchain tokens, these restrictions are lifted, or more accurately, completely redefinable. Many blockchain tokens serve multiple purposes globally and can be traded for each other or for other currencies on global liquid markets. With the restrictions on use and ownership gone, the "insignificant value" expectation is also a thing of the past.

In this section, we look at various uses for tokens and how they are created. We also discuss attributes of tokens such as fungibility and intrinsicality. Finally, we examine the standards and technologies that they are based on, and experiment by building our own tokens.

How are tokens used?

The most obvious use of tokens is as digital private currencies. However, this is only one possible use. Tokens can be programmed to serve many different functions, often overlapping. For example, a token can simultaneously convey a voting right, an access right, and ownership of a resource. Currency is just the first "app".

Currency

A token can serve as a form of currency, with a value determined through private trade.

Resource

A token can represent a resource earned or produced in a sharing economy or resource-sharing environment; for example, a storage or CPU token representing resources that can be shared over a

network.

Asset

A token can represent ownership of an intrinsic or extrinsic, tangible or intangible asset. For example, gold, real estate, a car, oil, energy, MMOG items, etc.

Access

A token can represent access rights, and grant access to a digital or physical property, such as a discussion forum, an exclusive website, a hotel room, or a rental car.

Equity

A token can represent shareholder equity in a digital organization (e.g. a DAO) or legal entity (e.g. a corporation).

Voting

A token can represent voting rights in a digital or legal system.

Collectible

A token can represent a digital collectible (e.g. CryptoPunks) or physical collectible (e.g. a painting).

Identity

A token can represent a digital identity (e.g. avatar) or legal identity (e.g. national ID).

Attestation

A token can represent a certification or attestation of fact by some authority or by a decentralized reputation system (e.g. marriage record, birth certificate, college degree).

Utility

A token can be used to access or pay for a service.

Often, a single token encompasses several of these functions. Sometimes it is hard to discern between them, as the physical equivalents have always been inextricably linked. For example, in the physical world, a driver's license (attestation) is also an identity document (identity) and the two cannot be separated. In the digital realm, previously commingled functions can be separated and developed independently (e.g. an anonymous attestation).

Tokens and fungibility

Wikipedia says: "In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable."

Tokens are fungible when we can substitute any single unit of the token for another without any difference in its value or function.

Strictly speaking, if a token's historical provenance can be tracked, then it is not entirely fungible. The ability to track provenance can lead to blacklisting and whitelisting, reducing or eliminating fungibility. We will examine this further in [\[privacy\]](#).

Non-fungible tokens are tokens that each represent a unique tangible or intangible item and therefore are not interchangeable. For example, a token that represents ownership of a *specific* Van Gogh painting is not equivalent to another token that represents a Picasso, even though they might be part of the same "art ownership token" system. Similarly, a token representing a *specific* digital collectible such as a specific CryptoKitty (see [\[cryptoKitties\]](#)) is not interchangeable with any other CryptoKitty. Each non-fungible token is associated with a unique identifier, such as a serial number.

We will see examples of both fungible and non-fungible tokens later in this section.

Note that "fungible" is often used to mean "directly exchangeable for money" (for example, a casino token can be "cashed in", while laundry tokens typically cannot). This is *not* the sense in which we use the word here.

Counterparty risk

Counterparty risk is the risk that the *other* party in a transaction will fail to meet their obligations. Some types of transactions suffer additional counterparty risk because the transaction has more than two parties. For example, if you hold a certificate of deposit for a precious metal and you sell that to someone, there are at least three parties in that transaction: the seller, the buyer and the custodian of the precious metal. Someone holds the physical asset; by necessity they become party to the fulfillment of the transaction and add counterparty risk to any transaction involving that asset. In general, when an asset is traded indirectly through the exchange of a token of ownership, there is additional counterparty risk from the custodian of the asset. Do they have the asset? Will they recognize (or allow) the transfer of ownership based on the transfer of a token (such as a certificate, deed, title or digital token)? In the world of digital tokens representing assets, as in the non-digital world, it is important to understand who holds the asset that is represented by the token and what rules apply to

that underlying asset.

Tokens and intrinsicality

The word "intrinsic" derives from the Latin "intra", meaning "from within".

Some tokens represent digital items that are *intrinsic* to the blockchain. Those digital assets are governed by consensus rules, just like the tokens themselves. This has an important implication: tokens that represent intrinsic assets do not carry additional counterparty risk. If you hold the keys for a CryptoKitty, there is no other party holding that CryptoKitty for you - you own it directly. The blockchain consensus rules apply and your ownership (i.e. control) of the private keys is equivalent to ownership of the asset, without any intermediary.

Conversely, many tokens are used to represent *extrinsic* things, such as real estate, corporate voting shares, trademarks, and gold bars. The ownership of these items, which are not "within" the blockchain, is governed by law, custom and policy that are separate from the consensus rules that govern the token. In other words, token issuers and owners may still depend on real world non-smart contracts. As a result, these extrinsic assets carry additional counterparty risk because they are held by custodians, recorded in external registries, or controlled by laws and policies outside the blockchain environment.

One of the most important ramifications of blockchain-based tokens is the ability to convert extrinsic assets into intrinsic assets and thereby remove counterparty risk. A good example is moving from equity in a corporation (extrinsic) to an equity or voting token in a *decentralized autonomous organization* or similar (intrinsic) organization.

Using tokens: utility or equity

Almost all projects in Ethereum today are launching with some kind of token. But do all these projects really need a token? Are there any disadvantages to using a token, or will we see the slogan "tokenize all the things" come to fruition? In principle, the use of tokens can be seen as the ultimate management or organization tool. In practice, the integration of blockchain platforms, including Ethereum, into the existing structures of society mean that, so far, there are many limitations to their applicability.

First, let's start by clarifying the role of a token in a new project. The majority of projects are using tokens in one of two ways: either as "utility tokens" or as "equity tokens". Very often, those two roles are conflated.

Utility tokens are those where the use of the token is required to gain access to a service, application or resource. Examples of utility tokens include tokens that represent resources such as shared storage, or access to services such as social media networks.

Equity tokens are those that represent shares in the control or ownership of something, such as a startup. Equity tokens can be as limited as non-voting shares for distribution of dividends and profits, or as expansive as voting shares in a decentralized autonomous organization, where management of the platform is through some complex governance system based on votes by the token holders.

It's a duck!

Just because a token is used to fundraise for a startup doesn't mean it has to be used as payment for the service, and vice-versa. Many startups, however, face a difficult problem: tokens are a great fundraising mechanism, but offering securities (equity) to the public is a regulated activity in most jurisdictions. By disguising equity tokens as utility tokens, many startups hope to get around these regulatory restrictions and raise money from a public offering while presenting it as a pre-sale of "service access vouchers" or, as we call them, utility tokens. Whether these thinly disguised equity offerings will be able to skirt the regulators remains to be seen.

As the popular saying goes: "If it walks like a duck and quacks like a duck - it's a duck". Regulators are not likely to be distracted by these semantic contortions; quite the opposite, they are more likely to see such legal sophistry as an attempt to deceive the public.

Utility tokens: who needs them?

The real problem is that utility tokens introduce significant risks and adoption barriers for startups. Perhaps in a distant future "tokenize all the things" will become reality, but at present the number of people who have an understanding of and desire to use a token is a subset of the already small cryptocurrency market.

For a startup, each innovation represents a risk and a market filter. Innovation is taking the road least traveled, walking away from the path of tradition. It is already a lonely walk. If a startup is trying to innovate in a new area of technology, such as storage sharing over P2P networks, that is a lonely enough path. Adding a utility token to that innovation and requiring users to adopt tokens in order to use the service compounds the risk and increases the barriers to adoption. It's walking off the already lonely trail of P2P storage innovation and into the wilderness.

Think of each innovation as a filter. It limits adoption to the subset of the market that can become early adopters of this innovation. Adding a second filter compounds that effect, further limiting the

addressable market. You are asking your early adopters to adopt not one but two completely new technologies: the novel application/platform/service you built, and the token economy.

For a startup, each innovation introduces risks that increase the chance of failure of the startup. If you take your already risky startup idea and add a utility token, you are adding all the risks of the underlying platform (Ethereum), broader economy (exchanges, liquidity), regulatory environment (equity/commodity regulators) and technology (smart contracts, token standards). That's a lot of risk for a startup.

Advocates of "tokenize all the things" will likely counter that by adopting tokens they are also inheriting the market enthusiasm, early adopters, technology, innovation and liquidity of the entire token economy. That is true too. The question is whether the benefits and enthusiasm outweigh the risks and uncertainties.

Nevertheless, some of the most innovative business ideas are indeed taking place in the crypto realm. If regulators are not quick enough to adopt laws and support new business models, entrepreneurs and associated talent will seek to operate in other jurisdictions which are more crypto-friendly. This is already happening.

Finally, at the beginning of this chapter when introducing tokens we discussed the colloquial meaning of "token" as "something of insignificant value". The underlying reason for the insignificant value of most tokens is because they can only be used in a very narrow context: one bus company, one laundromat, one arcade, one hotel, or one company store. Limited liquidity, limited applicability, and high conversion costs reduce the value of tokens all the way down until it is only of "token" value. So when you add a utility token to your platform, but the token can only be used on your single platform with a small market, you are re-creating the conditions that made physical tokens worthless. This may indeed be the correct way to incorporate tokenization into your project. However, if in order to use your platform a user has to convert something into your utility token, use it and then convert the remainder back into something more generally useful, you've created a company scrip. The switching costs of a digital token are orders of magnitude lower than a physical token without a market, but they are not zero. Utility tokens that work across an entire industry sector will be very interesting and probably quite valuable. But if you set up your startup to have to bootstrap an entire industry standard in order to succeed, you may have already failed.

One of the benefits of deploying services on general-purpose platforms like Ethereum is exactly being able to connect smart contracts (and therefore the utility of tokens) across projects, increasing the potential for liquidity and utility of tokens.

Make this decision for the right reasons. Adopt a token because your application *cannot work without a*

token. Adopt it because the token solves a fundamental market barrier or access problem. Don't introduce a utility token because it is the only way you can raise money fast and you need to pretend it's not a public securities offering.

Tokens on Ethereum

Blockchain tokens existed before Ethereum. In some ways, the first blockchain currency, bitcoin, is a token itself. Many token platforms were also developed on Bitcoin and other cryptocurrencies before Ethereum. However, the introduction of the first token standard on Ethereum led to an explosion of tokens.

Vitalik Buterin suggested tokens as one of the most obvious and useful applications of a generalized programmable blockchain such as Ethereum. In fact, in the first year of Ethereum, it was common to see Vitalik and others wearing t-shirts emblazoned with the Ethereum logo and a smart contract sample on the back. There were several variations of this t-shirt, but the most common showed an implementation of a token.

Before we delve into the details of creating tokens on Ethereum, it is important to have an overview of how tokens work on Ethereum. Tokens are different from ether because the Ethereum protocol does not know anything about them. Sending ether is an intrinsic action of the Ethereum platform, but sending or even owning tokens is not. The ether balance of Ethereum accounts is handled at the protocol level, whereas the token balance of Ethereum accounts is handled at the smart contract level. In order to create a new token on Ethereum, you must create a new smart contract. Once deployed, the smart contract handles everything, including ownership, transfers and access rights. You can write your smart contract to perform all the necessary actions any way you want, but it is probably wisest to follow an existing standard. We will look at such standards next. We discuss the pros and cons of following standards at the end of the chapter.

ERC20 Token Standard

The first standard was introduced in November 2015 by Fabian Vogelsteller as an Ethereum Request for Comments (ERC). It was automatically assigned GitHub issue number 20, giving rise to the name "ERC20 token". The vast majority of tokens are currently based on the ERC20 standard. The ERC20 request for comments eventually became Ethereum Improvement Proposal EIP20 but it is mostly still referred to by the original name, "ERC20". You can read the standard here:

<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>

ERC20 is a standard for *fungible tokens*, meaning that different units of an ERC20 token are interchangeable and have no unique properties.

The ERC20 standard defines a common interface for contracts implementing a token, such that any compatible token can be accessed and used in the same way. The interface consists of a number of functions that must be present in every implementation of the standard, as well as some optional functions and attributes that may be added by developers.

ERC20 required functions & events

An ERC20-compliant token contract must provide at least the following functions and events:

totalSupply

Returns the total units of this token that currently exist. ERC20 tokens can have a fixed or a variable supply.

balanceOf

Given an address, returns the token balance of that address.

transfer

Given an address and amount, transfers that amount of tokens to that address, from the balance of the address that executed the transfer.

transferFrom

Given a sender, recipient and amount, transfers tokens from one account to another. Used in combination with approve below.

approve

Given a recipient address and amount, authorizes that address to execute several transfers up to that amount, from the account that issued the approval.

allowance

Given an owner address and a spender address, returns the remaining amount that the spender is approved to withdraw from the owner.

Transfer

Event triggered upon successful transfer (call to transfer or transferFrom) (even for zero value

transfers).

Approval

Event logged upon a successful call to approve.

ERC20 optional functions

In addition to the required functions listed above, the following optional functions are also defined by the standard:

name

Returns a human readable name (e.g. "US Dollars") of the token.

symbol

Returns a human readable symbol (e.g. "USD") for the token.

decimals

Returns the number of decimals used to divide token amounts. For example, if decimals is 2, then the token amount is divided by 100 to get its user representation.

The ERC20 interface defined in Solidity

Here's what an ERC20 interface specification looks like in Solidity:

```
contract ERC20 {  
    function totalSupply() constant returns (uint theTotalSupply);  
    function balanceOf(address _owner) constant returns (uint balance);  
    function transfer(address _to, uint _value) returns (bool success);  
    function transferFrom(address _from, address _to, uint _value) returns  
(bool success);  
    function approve(address _spender, uint _value) returns (bool  
success);  
    function allowance(address _owner, address _spender) constant returns  
(uint remaining);  
    event Transfer(address indexed _from, address indexed _to, uint  
_value);  
    event Approval(address indexed _owner, address indexed _spender, uint  
_value);  
}
```

ERC20 data structures

If you examine any ERC20 implementation, it will contain two data structures, one to track balances and one to track allowances. In Solidity, they are implemented with a *data mapping*.

The first data mapping implements an internal table of token balances, by owner. This allows the token contract to keep track of who owns the tokens. Each transfer is a deduction from one balance and an addition to another balance.

```
mapping(address => uint256) balances;
```

The second data structure is a data mapping of allowances. As we will see in [ERC20 workflows](#): "transfer" and "approve & transferFrom", with ERC20 tokens an owner of a token can delegate authority to a spender, allowing them to spend a specific amount (allowance) from the owner's balance. The ERC20 contract keeps track of the allowances with a two-dimensional mapping, with the primary key being the address of the token owner, mapping to a spender address and an allowance amount:

```
mapping (address => mapping (address => uint256)) public allowed;
```

ERC20 workflows: "transfer" and "approve & transferFrom"

The ERC20 token standard has two transfer functions. You might be wondering why.

ERC20 allows for two different workflows. The first is a single-transaction, straightforward workflow using the transfer function. This workflow is the one used by wallets to send tokens to other wallets. The vast majority of token transactions happen with the transfer workflow.

Executing the transfer contract is very simple. If Alice wants to send 10 tokens to Bob, her wallet sends a transaction to the token contract's address, calling the transfer function with Bob's address and "10" as the arguments. The token contract adjusts Alice's balance (-10) and Bob's balance (+10) and issues a +Transfer+ event.

The second workflow is a two-transaction workflow that uses approve followed by transferFrom. This workflow allows a token owner to delegate their control to another address. It is most often used to delegate control to a contract for distribution of tokens, but it can also be used by exchanges.

For example, if a company is selling tokens for an Initial Coin Offering or ICO, they can approve a crowdsale contract address to distribute a certain amount of tokens. The crowdsale contract can then transferFrom the token contract owner balance to each buyer of the token as illustrated in [The two-step approve & transferFrom workflow of ERC20 tokens](#).



An *Initial Coin Offering (ICO)* is a crowdfunding mechanism used by companies and organizations to raise money by selling tokens. The term is derived from the "Initial Public Offering (IPO)", which is the process by which a public company offers shares for sale to investors on a stock exchange. Unlike the highly regulated IPO markets, ICOs are open, global and messy. The examples and explanations of ICOs in this book are not an endorsement of this type of fundraising.

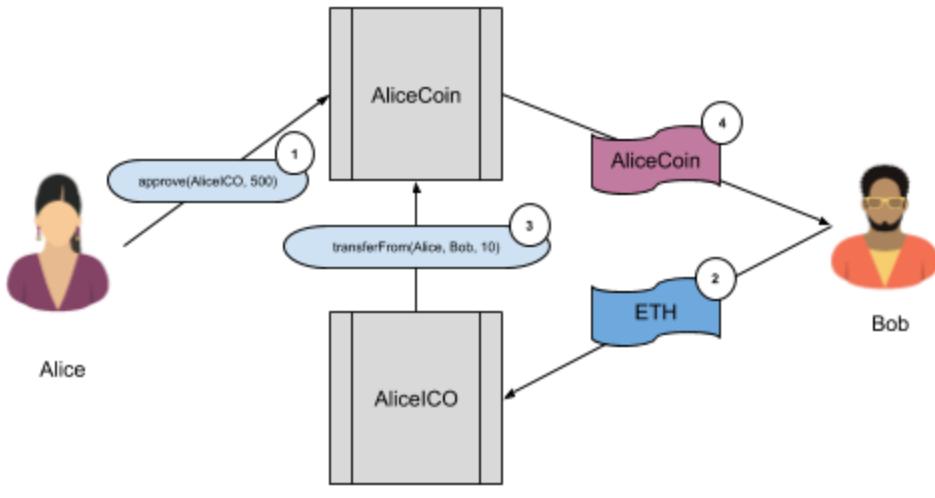


Figure 42. The two-step approve & transferFrom workflow of ERC20 tokens

For the approve & transferFrom workflow, two transactions are needed. Let's say that Alice wants to allow the AliceICO contract to sell 50% of all the AliceCoin tokens to buyers like Bob and Charlie. First, Alice launches the AliceCoin ERC20 contract, issuing all the AliceCoin to her own address. Then, Alice launches the AliceICO contract that can sell tokens for ether. Next, Alice initiates the approve & transferFrom workflow. She sends a transaction to the AliceCoin contract, calling `approve`, with the address of the AliceICO contract and 50% of the totalSupply as arguments. This will trigger the Approval event. Now, the AliceICO contract can sell AliceCoin.

When the AliceICO contract receives ether from Bob, it needs to send some AliceCoin to Bob in return. Within the AliceICO contract is an exchange rate between AliceCoin and ether. The exchange rate that Alice set when she created the AliceICO contract determines how many tokens Bob will receive for the amount of ether sent to the AliceICO contract. When the AliceICO contract calls the AliceCoin `transferFrom` function, it sets Alice's address as the sender, Bob's address as the recipient, and uses the exchange rate to determine how many AliceCoin tokens will be transferred to Bob in the "value" field. The AliceCoin contract transfers the balance from Alice's address to Bob's address and triggers a Transfer event. The AliceICO contract can call `transferFrom` an unlimited number of times, as long as it doesn't exceed the approval limit Alice set. The AliceICO contract can keep track of how many AliceCoin tokens it can sell by calling the `allowance` function.

ERC20 Implementations

While it is possible to implement an ERC20-compatible token in about thirty lines of Solidity code, most implementations are more complex. This is to account for potential security vulnerabilities. There are

two implementations mentioned in the EIP20 standard:

Consensys EIP20

A simple and easy to read implementation of an ERC20-compatible token. You can read the Solidity code for Consensys's implementation here: <https://github.com/ConsenSys/Tokens/blob/master/contracts/eip20/EIP20.sol>

OpenZeppelin StandardToken

This implementation is ERC20-compatible, with additional security precautions. It forms the basis of OpenZeppelin libraries implementing more complex ERC20-compatible tokens with fundraising caps, auctions, vesting schedules and other features. You can see the Solidity code for OpenZeppelin StandardToken here: <https://github.com/OpenZeppelin/zeppelin-solidity/blob/master/contracts/token/ERC20/StandardToken.sol>

Launching our own ERC20 token

Let's create and launch our own token. For this example, we will use the truffle framework (see [Truffle](#)). The example assumes you have already installed truffle, configured it, and are familiar with its basic operation.

We will call our token "Mastering Ethereum Token", with symbol "MET".

You can find this example in the book's GitHub repository: <https://github.com/ethereumbook/ethereumbook/blob/develop/code/truffle/METoken>

First, let's create and initialize a truffle project directory, the same way we did in [Creating a truffle project directory](#). Run these four commands and accept the default answers to any questions:

```
$ mkdir METoken  
$ cd METoken  
METoken $ truffle init  
METoken $ npm init
```

You should now have the following directory structure:

```
METoken/
+---- contracts
|   `---- Migrations.sol
+---- migrations
|   `---- 1_initial_migration.js
+---- package.json
+---- test
+---- truffle-config.js
`---- truffle.js
```

Edit the truffle.js or truffle-config.js configuration file to set up your truffle environment, or copy it from:

<https://github.com/ethereumbook/ethereumbook/blob/develop/code/truffle/METoken/truffle-config.js>

If you use the example truffle-config.js, remember to create a file .env in the METoken folder containing your test private keys for testing and deployment on public Ethereum test networks, such as Ropsten or Kovan. You can export your test network private key from MetaMask.

After that your directory should look like:

```
METoken/
+---- contracts
|   `---- Migrations.sol
+---- migrations
|   `---- 1_initial_migration.js
+---- package.json
+---- test
+---- truffle-config.js
+---- truffle.js
`---- .env *new file*
```



Only use test keys or test mnemonics that are *not* used to hold funds on the main Ethereum network. *Never* use keys that hold real money for testing.

For our example, we will import the OpenZeppelin StandardContract, which implements some

important security checks and is easy to extend. Let's import that library:

```
$ npm install zeppelin-solidity  
+ zeppelin-solidity@1.6.0  
added 8 packages in 2.504s
```

The zeppelin-solidity package will add about 250 files under the node_modules directory. The OpenZeppelin library includes a lot more than the ERC20 token, but we will only use a small part of it.

Next, let's write our token contract. Create a new file METoken.sol and copy the example code from GitHub:

<https://github.com/ethereumbook/ethereumbook/blob/develop/code/truffle/METoken/contracts/METoken.sol>

Our [METoken.sol : A Solidity contract implementing an ERC20 token](#) contract is very simple, as it inherits all its functionality from the OpenZeppelin StandardToken library:

METoken.sol : A Solidity contract implementing an ERC20 token

```
pragma solidity ^0.4.21;  
  
import 'zeppelin-solidity/contracts/token/ERC20/StandardToken.sol';  
  
contract METoken is StandardToken {  
    string public constant name = 'Mastering Ethereum Token';  
    string public constant symbol = 'MET';  
    uint8 public constant decimals = 2;  
    uint constant _initial_supply = 2100000000;  
  
    function METoken() public {  
        totalSupply_ = _initial_supply;  
        balances[msg.sender] = _initial_supply;  
        emit Transfer(address(0), msg.sender, _initial_supply);  
    }  
}
```

Here, we are defining the optional variables name, symbol, and decimals. We also define an _initial_supply variable, set to 21 million tokens; with two decimals of subdivision that gives 2.1 billion total units. In the contract's initialization (constructor) function we set the totalSupply to be equal to _initial_supply and allocate all of the _initial_supply to the balance of the account (msg.sender) that creates the METoken contract.

We now use truffle to compile the METoken code:

```
$ truffle compile
Compiling ./contracts/METoken.sol...
Compiling ./contracts/Migrations.sol...
Compiling zeppelin-solidity/contracts/math/SafeMath.sol...
Compiling zeppelin-solidity/contracts/token/ERC20/BasicToken.sol...
Compiling zeppelin-solidity/contracts/token/ERC20/ERC20.sol...
Compiling zeppelin-solidity/contracts/token/ERC20/ERC20Basic.sol...
Compiling zeppelin-solidity/contracts/token/ERC20/StandardToken.sol...
```

As you can see, truffle incorporated necessary dependencies from the OpenZeppelin libraries and compiled those contracts too.

Let's set up a migration script to deploy the METoken contract. Create a new file 2_deploy_contracts.js in the METoken/migrations folder. Copy the contents from the example on Github repository:

https://github.com/ethereumbook/ethereumbook/blob/develop/code/truffle/METoken/migrations/2_deploy_contracts.js

Here's what it contains:

2_deploy_contracts: Migration to deploy METoken

```
var METoken = artifacts.require("METoken");

module.exports = function(deployer) {
  // Deploy the METoken contract as our only task
  deployer.deploy(METoken);
};
```

Before we deploy on one of the Ethereum test networks, let's start a local blockchain to test everything. Start the ganache blockchain, either from the command-line with ganache-cli or from the graphical user interface.

Once ganache is started, we can deploy our METoken contract and see if everything works as expected:

```
$ truffle migrate --network ganache
Using network 'ganache'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
    ...
    ... 0xb2e90a056dc6ad8e654683921fc613c796a03b89df6760ec1db1084ea4a084eb
    Migrations: 0x8cdaf0cd259887258bc13a92c0a6da92698644c0
Saving successful migration to network...
  ...
  ... 0xd7bc86d31bee32fa3988f1c1eabce403a1b5d570340a3a9cdba53a472ee8c956
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying METoken...
  ...
  ... 0xbe9290d59678b412e60ed6aefedb17364f4ad2977cfb2076b9b8ad415c5dc9f0
  METoken: 0x345ca3e014aa5dca488057592ee47305d9b3e10
Saving successful migration to network...
  ...
  ... 0xf36163615f41ef7ed8f4a8f192149a0bf633fe1a2398ce001bf44c43dc7bdda0
Saving artifacts...
```

On the ganache console, we should see that our deployment has created 4 new transactions as depicted in [METoken deployment on Ganache](#):

ACCOUNTS	BLOCKS	TRANSACTIONS	LOGS	SEARCH FOR BLOCK NUMBERS OR TX HASHES	⚙️			
CURRENT BLOCK 4	GAS PRICE 100000000000	GAS LIMIT 6721975	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING			
TX HASH					CONTRACT CALL			
0xf36163615f41ef7ed8f4a8f192149a0bf633fe1a2398ce001bf44c43dc7bdda0					CONTRACT CREATION			
FROM ADDRESS 0x627306090abab3a6e1400e9345bc60c78a8bef57	TO CONTRACT ADDRESS 0x8cdaf0cd259887258bc13a92c0a6da92698644c0			GAS USED 26981	VALUE 0			
TX HASH					CONTRACT CREATION			
0xbe9290d59678b412e60ed6aefedb17364f4ad2977cfb2076b9b8ad415c5dc9f0					CONTRACT CALL			
FROM ADDRESS 0x627306090abab3a6e1400e9345bc60c78a8bef57	CREATED CONTRACT ADDRESS 0x345ca3e014aaaf5dca488057592ee47305d9b3e10			GAS USED 1475948	VALUE 0			
TX HASH					CONTRACT CALL			
0xd7bc86d31bee32fa3988f1c1eabce403a1b5d570340a3a9cdba53a472ee8c956					CONTRACT CREATION			
FROM ADDRESS 0x627306090abab3a6e1400e9345bc60c78a8bef57	TO CONTRACT ADDRESS 0x8cdaf0cd259887258bc13a92c0a6da92698644c0			GAS USED 41981	VALUE 0			
TX HASH					CONTRACT CREATION			
0xb2e90a056dc6ad8e654683921fc613c796a03b89df6760ec1db1084ea4a084eb					CONTRACT CALL			
FROM ADDRESS 0x627306090abab3a6e1400e9345bc60c78a8bef57	CREATED CONTRACT ADDRESS 0x8cdaf0cd259887258bc13a92c0a6da92698644c0			GAS USED 269607	VALUE 0			

Figure 43. METoken deployment on Ganache

Interacting with METoken using the truffle console

We can interact with our contract on the ganache blockchain, using the truffle console. This is an interactive JavaScript environment that provides access to the truffle environment and, via Web3, to the blockchain. In this case, we will connect the truffle console to the ganache blockchain:

```
$ truffle console --network ganache
truffle(ganache)>
```

The truffle(ganache)> prompt shows that we are connected to the ganache blockchain and are ready to type our commands. The truffle console supports all the truffle commands, so we could compile and migrate from the console. We've already run those commands, so let's go directly to the contract itself. The METoken contract exists as a JavaScript object within the truffle environment. Type METoken at the prompt and it will dump the entire contract definition:

```
truffle(ganache)> METoken
{ [Function: TruffleContract]
  _static_methods:

[...]

currentProvider:
HttpProvider {
  host: 'http://localhost:7545',
  timeout: 0,
  user: undefined,
  password: undefined,
  headers: undefined,
  send: [Function],
  sendAsync: [Function],
  _alreadyWrapped: true },
network_id: '5777' }
```

The METoken object also exposes several attributes, such as the address of the contract (as deployed by the migrate command):

```
truffle(ganache)> METoken.address
'0x345ca3e014aaf5dca488057592ee47305d9b3e10'
```

If we want to interact with the deployed contract, we have to use an asynchronous call, in the form of a JavaScript "promise". We use the deployed function to get the contract instance and then call the totalSupply function:

```
truffle(ganache)> METoken.deployed().then(instance =>
instance.totalSupply())
BigNumber { s: 1, e: 9, c: [ 2100000000 ] }
```

Next, let's use the accounts created by ganache to check our METoken balance and send some METoken to another address. First, let's get the account addresses:

```
truffle(ganache)> let accounts
undefined
truffle(ganache)> web3.eth.getAccounts((err,res) => { accounts = res })
undefined
truffle(ganache)> accounts[0]
'0x627306090abab3a6e1400e9345bc60c78a8bef57'
```

The accounts list now contains all the accounts created by ganache, and account[0] is the account that deployed the METoken contract. It should have a balance of METoken, because our METoken constructor gives the entire token supply to the address that created it. Let's check:

```
truffle(ganache)> METoken.deployed().then(instance => {
instance.balanceOf(accounts[0]).then(console.log) })
undefined
BigNumber { s: 1, e: 9, c: [ 2100000000 ] }
```

Finally, let's transfer 1000.00 METoken from account[0] to account[1], by calling the contract's transfer function:

```
truffle(ganache)> METoken.deployed().then(instance => {
instance.transfer(accounts[1], 100000) })
undefined
truffle(ganache)> METoken.deployed().then(instance => {
instance.balanceOf(accounts[0]).then(console.log) })
undefined
truffle(ganache)> BigNumber { s: 1, e: 9, c: [ 2099900000 ] }

undefined
truffle(ganache)> METoken.deployed().then(instance => {
instance.balanceOf(accounts[1]).then(console.log) })
undefined
truffle(ganache)> BigNumber { s: 1, e: 5, c: [ 100000 ] }
```



METoken has 2 decimals of precision, meaning that 1 METoken is 100 units in the contract. When we transfer 1000 METoken, we specify the value as 100,000 in the call to the transfer function.

As you can see, in the console, account[0] now has 20,999,000 MET, and account[1] has 1000 MET.

If you switch to the ganache graphical user interface, as shown in [METoken transfer on Ganache](#), you will see the transaction that called the transfer function:

Figure 44. METoken transfer on Ganache

Sending ERC20 tokens to contract addresses

So far we've set up an ERC20 token and transferred from one account to another. All the accounts we used for these demonstrations are externally-owned accounts (EOAs), meaning they are controlled by a private key, not a contract. What happens if we send MET to a contract address? Let's find out!

First, let's deploy another contract into our test environment. For this example, we will use our first contract, Faucet.sol. Let's add it to the METoken project by copying it to the contracts directory. Our directory should look like this:

```
METoken/
+---- contracts
|   +---- Faucet.sol
|   +---- METoken.sol
|   `---- Migrations.sol
```

We'll also add a migration, to deploy Faucet separately from METoken:

```
var Faucet = artifacts.require("Faucet");

module.exports = function(deployer) {
  // Deploy the Faucet contract as our only task
  deployer.deploy(Faucet);
};
```

Let's compile and migrate the contracts from the truffle console:

```
$ truffle console --network ganache
truffle(ganache)> compile
Compiling ./contracts/Faucet.sol...
Writing artifacts to ./build/contracts

truffle(ganache)> migrate
Using network 'ganache'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
    ...
    ... 0x89f6a7bd2a596829c60a483ec99665c7af71e68c77a417fab503c394fc7a0c9
      Migrations: 0xa1ccce36fb823810e729dce293b75f40fb6ea9c9
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Replacing METoken...
    ...
    ... 0x28d0da26f48765f67e133e99dd275fac6a25fdfec6594060fd1a0e09a99b44ba
      METoken: 0x7d6bf9d5914d37bcba9d46df7107e71c59f3791f
Saving artifacts...
Running migration: 3_deploy_faucet.js
  Deploying Faucet...
    ...
    ... 0x6fbf283bcc97d7c52d92fd91f6ac02d565f5fded483a6a0f824f66edc6fa90c3
      Faucet: 0xb18a42e9468f7f1342fa3c329ec339f254bc7524
Saving artifacts...
```

Great. Now let's send some MET to the Faucet contract:

```
truffle(ganache)> METoken.deployed().then(instance => {
  instance.transfer(Faucet.address, 100000) })
truffle(ganache)> METoken.deployed().then(instance => {
  instance.balanceOf(Faucet.address).then(console.log)})
truffle(ganache)> BigNumber { s: 1, e: 5, c: [ 100000 ] }
```

Alright, we have transferred 1000 MET to the Faucet contract. Now, how do we withdraw from the Faucet?

Remember, Faucet.sol is a pretty simple contract. It only has one function, withdraw, which is for

withdrawing *ether*. It doesn't have a function for withdrawing MET, or any other ERC20 token. If we use withdraw it will try to send ether, but since the faucet doesn't have a balance of ether yet, it will fail.

The METoken contract knows that Faucet has a balance, but the only way that it can transfer that balance is if it receives a transfer call from the address of the contract. Somehow we need to make the Faucet contract call the transfer function in METoken.

If you're wondering what to do next, don't. There is no solution to this problem. The MET sent to Faucet is stuck, forever. Only the Faucet contract can transfer it, and the Faucet contract doesn't have code to call the transfer function of an ERC20 token contract.

Perhaps you anticipated this problem. Most likely, you didn't. In fact, neither did hundreds of Ethereum users who accidentally transferred various tokens to contracts that didn't have any ERC20 capability. According to some estimates, tokens worth more than roughly \$2.5 million USD (at the time of writing) have been "stuck" like this and are lost forever.

One of the ways that users of ERC20 tokens can inadvertently lose their tokens in a transfer, is when they attempt to transfer to an exchange or another service. They copy an Ethereum address from the website of an exchange, thinking they can simply send tokens to it. However, many exchanges publish receiving addresses that are actually contracts! These contracts are only meant to receive ether, not ERC20 tokens, most often sweeping all funds sent to them to "cold storage" or another centralized wallet. Despite the many warnings saying "do not send tokens to this address", lots of tokens are lost this way.

Demonstrating the approve & transferFrom workflow

Our Faucet contract couldn't handle ERC20 tokens. Sending tokens to it using the transfer function results in the loss of those tokens. Let's rewrite the contract and make it handle ERC20 tokens. Specifically, we will turn it into a faucet that gives out MET to anyone who asks.

For this example, we make a copy of the truffle project directory, call it METoken_METFaucet, initialize truffle, npm, install OpenZeppelin dependencies and copy the METoken.sol contract. See our first example [Launching our own ERC20 token](#) for the detailed instructions.

Now, let's create a new faucet contract, call it METFaucet.sol. It will look like [METFaucet.sol: a faucet for METoken](#):

METFaucet.sol: a faucet for METoken

```
include ::code/truffle/METoken_METFaucet/contracts/METFaucet.sol
```

We've made quite a few changes to the basic faucet example. Since METFaucet will use the transferFrom function in METoken, it will need two additional variables. One will hold the address of the deployed METoken contract. The other will hold the address of the owner of MET who will approve the faucet withdrawals. The METFaucet will call METoken.transferFrom and instruct it to move MET from the owner to the address where the faucet withdrawal request came from.

We declare these two variables here:

```
StandardToken public METoken;
address public METOwner;
```

Since our faucet needs to be initialized with the correct addresses for METoken and METOwner we need to declare a custom constructor:

```
// METFaucet constructor, provide the address of METoken contract and
// the owner address we will be approved to transferFrom
function METFaucet(address _METoken, address _METOwner) public {

    // Initialize the METoken from the address provided
    METoken = StandardToken(_METoken);
    METOwner = _METOwner;
}
```

The next change is to the withdraw function. Instead of calling transfer, METFaucet uses the transferFrom function in METoken and asks METoken to transfer MET to the faucet recipient:

```
// Use the transferFrom function of METoken
METoken.transferFrom(METOwner, msg.sender, withdraw_amount);
```

Finally, since our faucet no longer sends ether, we should probably prevent anyone from sending ether

to METFaucet, as we wouldn't want it to get stuck. We change the fallback payable function to reject incoming ether, using the revert function to revert any incoming payments:

```
// REJECT any incoming ether
function () public payable { revert(); }
```

Now that our METFaucet.sol code is ready, we need to modify the migration script to deploy it. This migration script will be a bit more complex, as METFaucet depends on the address of METoken. We will use a JavaScript promise to deploy the two contracts in sequence. Create 2_deploy_contracts.js as follows:

```
var METoken = artifacts.require("METoken");
var METFaucet = artifacts.require("METFaucet");
var owner = web3.eth.accounts[0];

module.exports = function(deployer) {

    // Deploy the METoken contract first
    deployer.deploy(METoken, {from: owner}).then(function() {
        // then deploy METFaucet and pass the address of METoken
        // and the address of the owner of all the MET who will approve
        METFaucet
            return deployer.deploy(METFaucet, METoken.address, owner);
    });
}
```

Now, we can test everything in the truffle console. First, we use migrate to deploy the contracts. When METoken is deployed it will allocate all the MET to the account that created it, web3.eth.accounts[0]. Then, we call the approve function in METoken to approve METFaucet to send up to 1000 MET on behalf of web3.eth.accounts[0]. Finally, to test our faucet, we call METFaucet.withdraw from web3.eth.accounts[1] and try to withdraw 10 MET. Here are the console commands:

```
$ truffle console --network ganache
truffle(ganache)> migrate
Using network 'ganache'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
    ... 0x79352b43e18cc46b023a779e9a0d16b30f127bfa40266c02f9871d63c26542c7
  Migrations: 0xaa588d3737b611baf7bd713445b314bd453a5c8
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Replacing METoken...
    ... 0xc42a57f22cddf95f6f8c19d794c8af3b2491f568b38b96fef15b13b6e8ffff21
  METoken: 0xf204a4ef082f5c04bb89f7d5e6568b796096735a
  Replacing METFaucet...
    ... 0xd9615cae2fa4f1e8a377de87f86162832cf4d31098779e6e00df1ae7f1b7f864
  METFaucet: 0x75c35c980c0d37ef46df04d31a140b65503c0eed
Saving artifacts...
truffle(ganache)> METoken.deployed().then(instance => {
instance.approve(METFaucet.address, 100000) })
truffle(ganache)> METoken.deployed().then(instance => {
instance.balanceOf(web3.eth.accounts[1]).then(console.log) })
truffle(ganache)> BigNumber { s: 1, e: 0, c: [ 0 ] }
truffle(ganache)> METFaucet.deployed().then(instance => {
instance.withdraw(1000, {from:web3.eth.accounts[1]}) })
truffle(ganache)> METoken.deployed().then(instance => {
instance.balanceOf(web3.eth.accounts[1]).then(console.log) })
truffle(ganache)> BigNumber { s: 1, e: 3, c: [ 1000 ] }
```

As you can see from the results, we can use the approve and transferFrom workflow to authorize one contract to transfer tokens defined in another token. If properly used, ERC20 tokens can be used by externally-owned addresses and other contracts.

However, the burden of managing ERC20 tokens correctly is pushed to the user interface. If a user incorrectly attempts to transfer ERC20 tokens to a contract address and that contract is not equipped to receive ERC20 tokens, the tokens will be lost.

Issues with ERC20 tokens

The adoption of the ERC20 token standard has been truly explosive. Thousands of tokens have been launched, both to experiment with new capabilities and to raise funds in various "crowdfund" auctions and Initial Coin Offerings (ICOs). However there are some potential pitfalls, as we saw with the issue of transferring tokens to contract addresses.

One of the less obvious issues with ERC20 tokens is that they expose subtle differences between tokens and ether itself. Where ether is transferred by a transaction which has a recipient address as its destination, token transfers occur within the *specific token contract state* and have the token contract as their destination, not the recipient's address. The token contract tracks balances and issues events. In a token transfer, no transaction is actually sent to the recipient of the token. Instead, the recipient's address is added to a map within the token contract itself. A transaction sending ether to an address changes the state of an address. A transaction transferring a token to an address only changes the state of the token contract, not the state of the recipient address. Even a wallet that has support for ERC20 tokens does not become aware of a token balance unless the user explicitly adds a specific token contract to "watch". Some wallets watch the most popular token contracts to detect balances held by addresses they control, but that's limited to a small fraction of existing ERC20 contracts.

In fact, it's unlikely that a user would *want* to track all balances in all possible ERC20 token contracts. Many ERC20 tokens are more like email spam than usable tokens. They automatically create balances for accounts that have ether activity, in order to attract users. If you have an Ethereum address with a long history of activity, especially if it was created in the presale, you will find it full of "junk" tokens that appeared out of nowhere. Of course, the address isn't really full of tokens, it's the token contracts that have your address in them. You only see these balances if these tokens contracts are being watched by the block explorer or wallet you use to view your address.

Tokens don't behave the same way as ether. Ether is sent with the send function and accepted by any payable function in a contract or any externally owned address. Tokens are sent using transfer or approve & transferFrom functions that exist only in the ERC20 contract, and do not (at least in ERC20) trigger any payable functions in a recipient contract. Tokens are meant to function just like a cryptocurrency such as ether, but they come with certain differences that break that illusion.

Consider another issue. To send ether or use any Ethereum contract you need ether to pay gas. To send tokens, you *also need ether*. You cannot pay for a transaction's gas with a token and the token contract can't pay the gas for you. This may change at some point in the distant future, but in the meantime this can cause some rather strange user experiences. For example, let's say you use an exchange or Shapeshift to convert some bitcoin to a token. You "receive" the token in a wallet that tracks that

token's contract and shows your balance. It looks the same as any of the other cryptocurrencies you have in your wallet. Now try sending the token and your wallet will inform you that you need ether to do that. You might be confused - after all you didn't need ether to receive the token. Perhaps you have no ether. Perhaps you didn't even know the token was an ERC20 token on Ethereum, maybe you thought it was a cryptocurrency with its own blockchain. The illusion just broke.

Some of these issues are specific to ERC20 tokens. Others are more general issues that relate to abstraction and interface boundaries within Ethereum. Some can be solved by changing the token interface, others may need changes to fundamental structures within Ethereum (such as the distinction between EOAs and contracts, and between transactions and messages). Some may not be "solvable" exactly and may require user interface design to hide the nuances and make the user experience consistent regardless of the underlying distinctions.

In the next sections we will look at various proposals that attempt to address some of these issues.

ERC223 - a proposed token contract interface standard

The ERC223 proposal attempts to solve the problem of inadvertent transfer of tokens to a contract (that may or may not support tokens) by detecting whether the destination address is a contract or not. ERC223 requires that contracts designed to accept tokens implement a function named `tokenFallback`. If the destination of a transfer is a contract and the contract does not have support for tokens (i.e. does not implement `tokenFallback`), the transfer fails.

To detect whether the destination address is a contract, the ERC223 reference implementation uses a small segment of inline bytecode in a rather creative way:

```
function isContract(address _addr) private view returns (bool is_contract) {
    uint length;
    assembly {
        //retrieve the size of the code on target address, this needs
assembly
        length := extcodesize(_addr)
    }
    return (length>0);
}
```

You can see the discussion around the ERC223 proposal here:

<https://github.com/ethereum/EIPs/issues/223>

The ERC223 contract interface specification is:

```
interface ERC223Token {  
    uint public totalSupply;  
    function balanceOf(address who) public view returns (uint);  
  
    function name() public view returns (string _name);  
    function symbol() public view returns (string _symbol);  
    function decimals() public view returns (uint8 _decimals);  
    function totalSupply() public view returns (uint256 _supply);  
  
    function transfer(address to, uint value) public returns (bool ok);  
    function transfer(address to, uint value, bytes data) public returns  
(bool ok);  
    function transfer(address to, uint value, bytes data, string  
customFallback) public returns (bool ok);  
  
    event Transfer(address indexed from, address indexed to, uint value,  
bytes indexed data);  
}
```

ERC223 is not widely implemented and there is some debate in the ERC discussion thread about backwards compatibility and trade-offs between implementing changes at the contract interface level versus the user interface. The debate continues.

ERC777 - a proposed token contract interface standard

Another proposal for an improved token contract standard is ERC777. This proposal has several goals, including:

- To offer an ERC20 compatible interface
- To transfer tokens using a send function, similar to ether transfers
- To be compatible with ERC820 for token contract registration

- Contracts and addresses can control which tokens they send through a **tokensToSend** function that is called prior to sending
- Contracts and addresses are notified by calling a **tokensReceived** function in the recipient
- To reduce the probability of tokens being locked into contracts by requiring contracts to provide a **tokensReceived** function
- Existing contracts can use proxy contracts to provide the **tokensToSend** and **tokensReceived** functions
- To operate in the same way, whether sending to a contract or EOA
- To provide specific events for the minting and burning of tokens
- To add operators, trusted third parties, intended to be contracts, to move tokens on behalf of a token holder
- Token transfer transactions contain metadata in a **userData** and **operatorData** field

The specification of the standard can be found here: <https://eips.ethereum.org/EIPS/eip-777>

The ongoing discussion on ERC777 can be found here: <https://github.com/ethereum/EIPs/issues/777>

The ERC777 contract interface specification is:

```
interface ERC777Token {  
    function name() public constant returns (string);  
    function symbol() public constant returns (string);  
    function totalSupply() public constant returns (uint256);  
    function granularity() public constant returns (uint256);  
    function balanceOf(address owner) public constant returns (uint256);  
  
    function send(address to, uint256 amount, bytes userData) public;  
  
    function authorizeOperator(address operator) public;  
    function revokeOperator(address operator) public;  
    function isOperatorFor(address operator, address tokenHolder) public  
constant returns (bool);  
    function operatorSend(address from, address to, uint256 amount, bytes  
userData, bytes operatorData) public;  
  
    event Sent(address indexed operator, address indexed from, address  
indexed to, uint256 amount, bytes userData, bytes operatorData);  
    event Minted(address indexed operator, address indexed to, uint256  
amount, bytes operatorData);  
    event Burned(address indexed operator, address indexed from, uint256  
amount, bytes userData, bytes operatorData);  
    event AuthorizedOperator(address indexed operator, address indexed  
tokenHolder);  
    event RevokedOperator(address indexed operator, address indexed  
tokenHolder);  
}
```

ERC777 Hooks

The ERC777 tokens sender hook specification is:

```
interface ERC777TokensSender {  
    function tokensToSend(address operator, address from, address to,  
    uint value, bytes userData, bytes operatorData) public;  
}
```

The implementation of this interface is required for any address wishing to be notified of, to handle, or to prevent the debit of tokens. The address for which the contract implements this interface must be registered via ERC820, whether the contract implements the interface for itself or for another address.

The ERC777 tokens recipient hook specification is:

```
interface ERC777TokensRecipient {  
    function tokensReceived(address operator, address from, address to,  
    uint amount, bytes userData, bytes operatorData) public;  
}
```

The implementation of this interface is required for any address wishing to be notified of, to handle, or to reject the reception of tokens. The same logic and requirements as the tokens sender interface apply to the tokens recipient, with the added constraint that recipient contracts must implement this interface to prevent locking tokens. If the recipient contract does not register an address implementing this interface, the transfer of tokens will fail.

An important aspect is that only one single tokens sender and one tokens recipient can be registered per address. Hence the same hook functions are called upon the debit and the reception of every ERC777 token transfer. A specific token can be identified in these functions using the message's sender, which is the specific token contract address, to handle a particular use case.

On the other hand, the same tokens sender and tokens recipient hooks can be registered for multiple addresses and the hooks can distinguish who are the sender and the intended recipient using the `from` and `to` parameters.

A reference implementation of ERC777 is linked in the proposal. ERC777 depends on a parallel proposal for a registry contract, specified in ERC820. Some of the debate on ERC777 is about the complexity of adopting two big changes at once: a new token standard and a registry standard. The discussion continues.

ERC721 - non-fungible token (deed) standard

All the token standards we have looked at so far are *fungible* tokens, meaning that unit of a token are interchangeable. The ERC20 token standard only tracks the final balance of each account and does not (explicitly) track the provenance of any token.

The ERC721 proposal is for a standard for *non-fungible* tokens, also known as *deeds*.

From the Oxford Dictionary:

deed: A legal document that is signed and delivered, especially one regarding the ownership of property or legal rights.

The use of the word "deed" is intended to reflect the "ownership of property" part, even though these are not recognized as "legal documents" in any jurisdiction - yet. It is likely that at some point in the future, legal ownership based on digital signatures on a blockchain platform will be legally recognized.

Non-fungible tokens track ownership of a unique thing. The thing owned can be a digital item, such as an in-game item, or digital collectible; or the thing can be a physical item whose ownership is tracked by a token, such as a house, a car, or an artwork. A deed could also represent things with negative value, such as loans (debt), liens, easements, etc. The ERC721 standard places no limitation or expectation on the nature of the thing whose ownership is tracked by a deed, only that it can be uniquely identified, which in the case of this standard is achieved by a 256-bit identifier.

The details of the standard and discussion are tracked in two different GitHub locations:

Initial proposal: <https://github.com/ethereum/EIPs/issues/721>

Continued discussion: <https://github.com/ethereum/EIPs/pull/841>

To grasp the basic difference between ERC20 and ERC721, it is sufficient to look at the internal data structure used in ERC721:

```
// Mapping from deed ID to owner
mapping (uint256 => address) private deedOwner;
```

Whereas ERC20 tracks the balances that belong to each owner, with the owner being the primary key of the mapping, ERC721 tracks each deed ID and who owns it, with the deed ID being the primary key of the mapping. From this basic difference flow all the properties of a non-fungible token.

The ERC721 contract interface specification is:

```

interface ERC721 /* is ERC165 */ {
    event Transfer(address indexed _from, address indexed _to, uint256
_deedId);
    event Approval(address indexed _owner, address indexed _approved,
uint256 _deedId);
    event ApprovalForAll(address indexed _owner, address indexed
_operator, bool _approved);

    function balanceOf(address _owner) external view returns (uint256
_balance);
    function ownerOf(uint256 _deedId) external view returns (address
_owner);
    function transfer(address _to, uint256 _deedId) external payable;
    function transferFrom(address _from, address _to, uint256 _deedId)
external payable;
    function approve(address _approved, uint256 _deedId) external
payable;
    function setApprovalForAll(address _operator, boolean _approved)
payable;
    function supportsInterface(bytes4 interfaceID) external view returns
(bool);
}

```

ERC721 also supports two *optional* interfaces, one for metadata and one for enumeration of deeds and owners.

The ERC721 optional interface for metadata is:

```

interface ERC721Metadata /* is ERC721 */ {
    function name() external pure returns (string _name);
    function symbol() external pure returns (string _symbol);
    function deedUri(uint256 _deedId) external view returns (string
_deedUri);
}

```

The ERC721 optional interface for enumeration is:

```
interface ERC721Enumerable /* is ERC721 */ {
    function totalSupply() external view returns (uint256 _count);
    function deedByIndex(uint256 _index) external view returns (uint256
_deedId);
    function countOfOwners() external view returns (uint256 _count);
    function ownerByIndex(uint256 _index) external view returns (address
_owner);
    function deedOfOwnerByIndex(address _owner, uint256 _index) external
view returns (uint256 _deedId);
}
```

Token standards

In this section, we've reviewed several proposed standards and a couple of widely-deployed standards for token contracts. What exactly do these standards do? Should you use these standards? How should you use them? Should you add functionality beyond these standards? Which standards should you use? We will examine all those questions next.

What are token standards? What is their purpose?

Token standards are a *minimum* specification for an implementation. What that means is that in order to be compliant with, say ERC20, you need to at minimum implement the functions and behavior specified by ERC20. You are also free to *add* to the functionality by implementing functions that are not part of the standard.

The primary purpose of these standards is to encourage *interoperability* between contracts. Thus, all wallets, exchanges, user interfaces and other infrastructure components can *interface* in a predictable manner with any contract that follows the specification. In other words, if you deploy a contract that follows the ERC20 standard, all existing wallet users can seamlessly start trading your token without any wallet upgrade or effort on your part.

The standards are meant to be *descriptive*, rather than *prescriptive*. How you choose to implement those functions is up to you - the internal function of the contract is not relevant to the standard. They have some functional requirements, which govern the behavior under specific circumstances, but they do not prescribe an implementation. An example of this is the behavior of a transfer function if the value is set to zero.

Should you use these standards?

Given all these standards, each developer faces a dilemma: use the existing standards or innovate beyond the restrictions they impose?

This dilemma is not easy to resolve. Standards necessarily restrict your ability to innovate, by creating a narrow "rut" that you have to follow. On the other hand, the basic standards have emerged from the experience with hundreds of applications and often fit well with the vast majority of use cases.

As part of this consideration is an even bigger issue: the value of interoperability and broad adoption. If you choose to use an existing standard, you gain the value of all the systems designed to work with that standard. If you choose to depart from the standard, you have to consider the cost of building all of the support infrastructure on your own, or persuading others to support your implementation as a new standard. The tendency to forge your own path and ignore existing standards is known as "Not Invented Here" and is antithetical to open source culture. On the other hand, progress and innovation depends on departing from tradition sometimes. It's a tricky choice, so consider it carefully!



Not invented here is a stance adopted by social, corporate, or institutional cultures that avoid using or buying already existing products, research, standards, or knowledge because of their external origins and costs, such as royalties. See https://en.wikipedia.org/wiki/Not_invented_here.

Security by maturity

Beyond the choice of standard, there is the parallel choice of *implementation*. When you decide to use a standard such as ERC20, you have to then decide how to implement a compatible design. There are a number of existing "reference" implementations that are widely used in the Ethereum ecosystem, or you could write your own from scratch. Again, this choice represents a dilemma that can have serious security implications.

Existing implementations are "battle tested". While it is impossible to prove that they are secure, many of them underpin millions of dollars of tokens. They have been attacked, repeatedly and vigorously. So far, no significant vulnerabilities have been discovered. Writing your own is not easy - there are many subtle ways that a contract can be compromised. It is much safer to use a well-tested widely-used implementation. In our examples above, we used the OpenZeppelin implementation of the ERC20 standard, as this implementation is security-focused from the ground up.

If you use an existing implementation you can also extend it. Again, be careful with this impulse.

Complexity is the enemy of security. Every single line of code you add expands the *attack surface* of your contract and could represent a vulnerability lying in wait. You may not notice a problem until you put a lot of value on top of the contract and someone breaks it.



Standards and implementation choices are important parts of overall secure smart contract design, but they're not the only considerations. See [Smart contract security](#).

Extensions to token interface standards

The token standards discussed in this section start with a very minimal interface, with limited functionality. Many projects have created extended implementations to support features that they need for their application. Some of these include:

Owner Control

Specific addresses, or sets of addresses (i.e. multi-sig) are given special capabilities, such as blacklisting, whitelisting, minting, recovery, etc.

Burning

A token burn is when tokens are deliberately destroyed by transfer to an unspendable address or by erasing a balance and reducing the supply.

Minting

The ability to add to the total supply of tokens, at a predictable rate, or by "fiat" of the creator of the token.

Crowdfunding

The ability to offer tokens for sale, for example through an auction, market sale, reverse auction, etc.

Caps

Pre-defined and immutable limits on the total supply, the opposite of the "minting" feature.

Recovery "Back Doors"

Functions to recover funds, reverse transfers, or dismantle the token that can be activated by a designated address or sets of addresses.

Whitelisting

The ability to restrict actions (such as token transfers) to specific addresses. Most commonly used to offer tokens to "accredited investors" after vetting by the rules of different jurisdictions. There is usually a mechanism for updating the whitelist.

Blacklisting

The ability to restrict token transfers by disallowing specific addresses. There is usually a function for updating the blacklist.

There are reference implementations for many of these functions, for example in the OpenZeppelin library. Some of these are use case-specific and only implemented in a few tokens. There are, as of now, no widely accepted standards for the interfaces to these functions.

As previously discussed, the decision to extend a token standard with additional functionality represents a trade-off between innovation/risk and interoperability/security.

Tokens and ICOs

Tokens have been an explosive development in the Ethereum ecosystem. It is likely that they will be a very important, foundational component of all smart contract platforms like Ethereum.

Nevertheless, the importance and future impact of these standards should not be confused with an endorsement of current token offerings. As in any early stage technology, the first wave of products and companies will almost all fail, and some will fail spectacularly. Many of the tokens on offer in Ethereum today are barely-disguised scams, pyramid schemes and money grabs.

The trick is to separate the long-term vision and impact of this technology, which is likely to be huge, from the short term bubble of token ICOs, which is rife with fraud. Token standards and the platform will survive the current token mania, and then they will likely change the world.

Oracles

In this chapter, we discuss *Oracles*, which are systems that can provide external data sources to Ethereum smart contracts. The term "oracle", comes from Greek mythology, where it referred to a person in communication with the gods who could see visions of the future. In the context of blockchains, an oracle is a system that can answer questions that are external to Ethereum. Ideally oracles are systems that are *trustless*, meaning that they do not need to be trusted because they operate on decentralized principles.

Why are oracles needed

A key component of the Ethereum platform is the Ethereum Virtual Machine, with its ability to execute programs and update the state of Ethereum, constrained by consensus rules, on any node in the decentralized network. In order to maintain consensus, EVM execution must be totally deterministic and based only on the shared context of the Ethereum state and signed transactions. This has two particularly important consequences: the first is that there can be no intrinsic source of randomness for the EVM and smart contracts to work with; the second is that extrinsic data can only be introduced as the data payload of a transaction.

Let's unpack those two consequences further. To understand the prohibition of a true random function in the EVM to provide randomness for smart contracts, consider the effect on attempts to achieve consensus after the execution of such a function: node A would execute the command and store 3 on behalf of the smart contract in its storage, while node B, executing the same smart contract, would store 7 instead. Thus, nodes A and B would come to different conclusions about what the resulting state should be, despite having run exactly the same code in the same context. Indeed, it could be that a different resulting state would be achieved every time that the smart contract is evaluated. As such, there would be no way for the network, with its multitude of nodes running independently around the world, to ever come to a decentralized consensus on what the resulting state should be. In practice, it would get much worse than this example very quickly, because knock-on effects, including ether transfers, would build up exponentially.

Note that pseudo-random functions, such as cryptographically secure hash functions (which are deterministic and therefore can be, and indeed are, part of the EVM), are not enough for many applications. Take a gambling game that simulates coin flips to resolve bet payouts, which needs to randomize heads or tails - a miner can gain an advantage by playing the game and only including their transactions in blocks for which they will win. So how do we get around this problem? Well, all nodes can agree on the contents of signed transactions, so extrinsic information, including sources of

randomness, price information, weather forecasts, etc, can be introduced as the data part of transactions sent to the network. However, such data simply can not be trusted, because it comes from unverifiable sources. As such, we have just deferred the problem. We use Oracles to attempt to solve these problems, which we will discuss in detail, in the rest of this chapter.

Oracle use cases and examples

Oracles, ideally, provide a trustless (or at least near-trustless) way of getting extrinsic (i.e. "real world" or off-chain) information, such as the result of football games, the price of gold, or truly random numbers, on to the Ethereum platform for smart contracts to use. They can also be used to relay data securely to DApp front-ends directly. They can be thought of as a *bridge*, i.e. a mechanism for bridging the gap between the off-chain world and smart contracts. Allowing smart contracts to enforce contractual relationships based on real-world events and data broadens their scope dramatically. However, this can also introduce external risks to Ethereum's security model. Consider a "smart will" contract that distributes assets when a person dies. This is something frequently discussed in the smart contract space, and highlights the risks of a trusted oracle. If the inheritance amount controlled by such a contract is high enough, the incentives to hack the oracle and trigger distribution of assets *before* the owner dies is very high.

Note that some oracles provide data that is particular to a specific private data source, such as academic certificates or government IDs. Even though that is a fully trusted data source, it is so by definition. Such subjective data can't be given "trustlessly" - the provider of such information, such as a university, is the sole arbiter of this information, so it only makes sense to go to the single source of this information to obtain it. As such, we include these data sources in our definitions of what counts as "oracles" because they also provide a data bridge for smart contracts with the characteristic of the data being provided. The kind of subjective data generally takes the form of attestations, such as passports or records of achievement. Attestations will become a big part of the success of blockchain platforms, particularly in relation to the related issues of verifying identity or reputation, so it is important to explore how they can be served by blockchain platforms.

Let's look at some more examples of data that might be provided by oracles:

- Random numbers/entropy from physical sources such as quantum/thermal processes: e.g. to fairly select a winner in a lottery smart contract
- Parametric triggers indexed to natural hazards: e.g. triggering of catastrophe bond smart contracts, such as Richter scale measurement for an earthquake bond

- Exchange rate data: e.g. for accurate pegging of cryptocurrencies to fiat currency
- Capital markets data: e.g. pricing baskets of tokenized assets/securities
- Benchmark reference data: e.g. incorporating interest rates into smart financial derivatives
- Static/pseudo-static data: security identifiers, country codes, currency codes, etc.
- Time and interval data: for event triggers grounded in precise time measurement
- Weather data: e.g. insurance premium calculations based on weather forecasts
- Political events: for prediction market resolution
- Sporting events: for prediction market resolution and fantasy sports contracts
- Geo-location data: e.g. as used in supply chain tracking
- Damage verification: for insurance contracts
- Events occurring on other blockchains: interoperability functions
- Ether market price: e.g. for fiat gas price oracles
- Flight statistics: e.g. as used by groups and clubs for flight ticket pooling
- Attestation/Certification: e.g. academic achievements or government-issued licenses and identification documents

In this section, we will examine some of the ways oracles can be implemented, including basic oracle patterns, computation oracles, decentralized oracles, and oracle client implementations in Solidity.

Oracle design patterns

All oracles provide a few key functions, by definition:

- Collecting data from an off-chain source
- Transferring the data on-chain with a signed message
- Making the data available by putting it in a smart contract's storage

Once the data is available in a smart contract's storage, it can be accessed by other smart contracts via message calls that invoke a "retrieve" function of the oracle's smart contract; and it can also be accessed by Ethereum nodes or network-enabled clients directly by "looking" into the oracle's storage.

The three main ways to set up an oracle can be categorized as: *request-response*, *publish-subscribe* and *immediate-read*.

Starting with the simplest, *immediate-read* oracles are those that provide data which is only needed for an immediate decision, like "What is the address for ethrerumbook.info?" or "Is this person over 18?". Those wishing to query this kind of data tend to do so on a "just-in-time" basis, i.e. the look-up is made when it is needed and possibly never again. Examples of such oracles include those that hold data about or issued by organizations, such as academic certificates, dial codes, institutional memberships, airport identifiers, self-sovereign IDs, etc. This type of oracle stores data once in its contract storage, whence any other smart contract can look it up using a request call to the oracle contract. It may be updated. The data in the oracle's storage is also available for direct look-up by blockchain-enabled (i.e. Ethereum client-connected) applications without having to go through the palaver and incurring the gas costs of issuing a transaction. A shop wanting to check the age of a customer wishing to purchase alcohol could use an oracle in this way. This type of oracle is attractive to an organization or company that might otherwise have to run and maintain servers to answer such data requests. Note that the data stored by the oracle is likely not to be the raw data that the oracle is serving, e.g. for efficiency or privacy reasons. A university may set up an oracle for the certificates of academic achievement of past students. However, storing the full details of the certificate (which may run to pages of courses taken and grades achieved) would be excessive. Instead, a hash of the certificate is sufficient. Likewise, a government might wish to put citizen IDs on to the Ethereum platform, where clearly the details included need to be kept private. Again, hashing the data (more carefully, in Merkle trees with salts) and only storing the root hash in the smart contract's storage is an efficient way to organize such a service.

The next setup is *publish-subscribe*, where an oracle that effectively provides a broadcast service for data that is expected to change (perhaps both regularly and frequently), is either polled by a smart contract on-chain, or watched by an off-chain daemon for updates. This category has a pattern similar to RSS feeds, WebSub, and the like, where the oracle is updated with new information and a flag signals that new data is available to those who consider themselves "subscribed". Interested parties must either poll the oracle to check whether the latest information has changed, or listen for updates to oracle contracts and act when they occur. Examples include price feeds, weather information, economic or social statistics, traffic data, etc. Polling is very inefficient in the world of web servers, but not so in the peer-to-peer context of blockchain platforms: Ethereum clients have to keep up with all state changes, including changes to contract storage, so polling for data changes is a local call to a synced client. Ethereum event logs make it particularly easy for applications to look out for oracle updates, and so this pattern can in some ways be even considered a "push" service. However, if the polling is done from a smart contract, which might be necessary for some decentralized applications (e.g. where activation incentives are not possible), then significant gas expenditure may be incurred.

The *request-response* category is the most complicated: this is where the data space is too huge to be stored in a smart contract and users are expected to only need a small part of the overall data set at a time. It is also an applicable model for data provider businesses. In practical terms, such an oracle might be implemented as a system of on-chain smart contracts and off-chain infrastructure used to monitor requests, retrieve and return data. A request for data from a decentralized application would typically be an asynchronous process involving a number of steps. In this pattern, firstly, an EOA would transact with a decentralized application, resulting in an interaction with a function defined in the oracle smart contract. This function initiates the request to the oracle, with the associated arguments detailing the data requested in addition to supplementary information that might include callback functions and scheduling parameters. Once this transaction has been validated, the oracle request can be observed as an EVM event emitted by the oracle contract, or as a state change; the arguments can be retrieved and used to perform the actual query of the off-chain data source. The oracle may also require payment for processing the request, gas payment for the callback, and permissions to access the requested data. Finally, the resulting data is signed by the oracle owner, attesting to the validity of the data at a given time, and delivered in a transaction to the decentralized application that made the request—either directly or via the oracle contract. Depending on the scheduling parameters, the oracle may broadcast further transactions updating the data at regular intervals, e.g. end of day pricing information.

The steps for a *request-response* oracle may be summarized as follows:

1. Receive a query from a DApp
2. Parse the query
3. Check that payment and data access permissions are provided
4. Retrieve relevant data from an off-chain source (and encrypt it if necessary)
5. Sign transaction(s) with the data included
6. Broadcast transactions to the network
7. Schedule any further necessary transactions, such as notifications, etc.

A range of other schemes are also possible; for example, data can be requested from and returned directly by an EOA, removing the need for an oracle smart contract. Similarly, the request and response could be made to and from an Internet of Things–enabled hardware sensor. Therefore, oracles can be human, software, or hardware.

The request–response pattern described above is commonly seen in client–server architectures. While

this is a useful messaging pattern which allows applications to have a two-way conversation, it is perhaps inappropriate under certain conditions. For example, a smart bond requiring an interest rate from an oracle might have to request the data on a daily basis under a request-response pattern in order to ensure the rate is always correct. Given that interest rates change infrequently, a publish-subscribe pattern may be more appropriate here—especially when taking into consideration Ethereum’s limited bandwidth.

Publish–subscribe is a pattern where publishers (in this context, oracles) do not send messages directly to receivers, but instead categorize published messages into distinct classes. Subscribers are able to express an interest in one or more classes and retrieve only those messages which are of interest. Under such a pattern, an oracle might write the interest rate to its own internal storage each time it changes. Multiple subscribed DApps can simply read it from the oracle contract, thereby reducing the impact on network bandwidth while minimizing storage costs.

In a broadcast or multicast pattern, an oracle would post all messages to a channel and subscribing contracts would listen to the channel under a variety of subscription modes. For example, an oracle might publish messages to a cryptocurrency exchange rate channel. A subscribing smart contract could request the full content of the channel if it required the time series for, e.g., a moving average calculation; another might require only the latest rate for a spot price calculation. A broadcast pattern is appropriate where the oracle does not need to know the identity of the subscribing contract.

Data authentication

If we assume that the source of data being queried by a DApp is both authoritative and trustworthy (a not insignificant assumption), an outstanding question remains: given that the oracle and the request–response mechanism may be operated by distinct entities, how are we able trust this mechanism? There is a distinct possibility that data may be tampered with in transit, so it is critical that off-chain methods are able to attest to the returned data’s integrity. Two common approaches to data authentication are *authenticity proofs* and *Trusted Execution Environments* (TEEs).

Authenticity proofs are cryptographic guarantees that data has not been tampered with. Based on a variety of attestation techniques (e.g. digitally-signed proofs), they effectively shift the trust from the data carrier to the attestor, i.e. the provider of the attestation. By verifying the authenticity proof on-chain, smart contracts are able to verify the integrity of the data before operating upon it. Oraclize is an example of an oracle service leveraging a variety of authenticity proofs. One such proof that is currently available for data queries from the Ethereum main network is the TLSNotary Proof. TLSNotary Proofs allow a client to provide evidence to a third party that HTTPS web traffic occurred between the client and a server. While HTTPS is itself secure, it doesn’t support data signing. As a result, TLSNotary Proofs

rely on TLSNotary (via PageSigner) signatures. TLSNotary Proofs leverage the Transport Layer Security (TLS) protocol, enabling the TLS master key, which signs the data after it has been accessed, to be split between three parties: the server (the oracle), an auditee (Oraclize), and an auditor. Oraclize uses an Amazon Web Services (AWS) virtual machine instance as the auditor, which can be verified as having been unmodified since instantiation. This AWS instance stores the TLSNotary secret, allowing it to provide honesty proofs. Although it offers higher assurances against data tampering than a pure request-response mechanism, this approach does require the assumption that Amazon itself will not tamper with the VM instance.

TownCrier is an authenticated data feed oracle system based on the TEE approach; such methods utilize hardware-based secure enclaves to ensure data integrity. TownCrier uses Intel's SGX (Software Guard eXtensions) to ensure that responses from HTTPS queries can be verified as authentic. SGX provides guarantees of integrity, ensuring that applications running within an enclave are protected by the CPU against tampering by any other process. It also provides confidentiality, ensuring that an application's state is opaque to other processes when running within the enclave. And finally, SGX allows attestation, by generating a digitally signed proof that an application—securely identified by a hash of its build—is actually running within an enclave. By verifying this digital signature, it is possible for a decentralized application to prove that a TownCrier instance is running securely within an SGX enclave. This, in turn, proves that the instance has not been tampered with and that the data emitted by TownCrier is therefore authentic. The confidentiality property additionally enables TownCrier to handle private data by allowing data queries to be encrypted using the TownCrier instance's public key. By operating an oracle's query/response mechanism within an enclave such as SGX, it can effectively be thought of as running securely on trusted third party hardware, ensuring that the requested data is returned untampered (assuming that we trust Intel/SGX).

Computation oracles

So far, we have only discussed oracles in the context of requesting and delivering data. However, oracles can also be used to perform arbitrary computation, a function which can be especially useful given Ethereum's inherent block gas limit and comparatively expensive computation costs. Rather than just relaying the results of a query, computation oracles can be used to perform computation on a set of inputs and return a calculated result that may have been infeasible to calculate on-chain. For example, one might use a computation oracle to perform a computationally-intensive regression calculation in order to estimate the yield of a bond contract.

If you are willing to trust a centralized but auditable service, you can go again to Oraclize. They provide a service that allows decentralized applications to request the output of a computation performed in a sandboxed AWS virtual machine. The AWS instance creates an executable container from a user-

configured Dockerfile packed in an archive that is uploaded to IPFS. On request, Oraclize retrieves this archive using its hash, and then initializes and executes the Docker container on AWS, passing any arguments that are provided to the application as environment variables. The containerized application performs the calculation, subject to a time constraint, and writes the result to standard output where it can be retrieved by Oraclize and returned to the decentralized application. Oraclize currently offers this service on an auditable t2.micro AWS instance, so if the computation is of some non-trivial value, it is possible to check that the correct Docker container was executed. Nonetheless, this is not a truly decentralized solution.

The concept of a 'cryptlet' as a standard for verifiable oracle truths has been formalized as part of Microsoft's wider ESC Framework. Cryptlets execute within an encrypted capsule that abstracts away the infrastructure, such as I/O, and has the CryptoDelegate attached so incoming and outgoing messages are signed, validated, and proven automatically. Cryptlets support distributed transactions so that contract logic can take on complex multi-step, multi-blockchain and external system transactions in an ACID manner. This allows developers to create portable, isolated, and private resolutions of the truth for use in smart contracts. Cryptlets follow the format below:

```
public class SampleContractCryptlet : Cryptlet
{
    public SampleContractCryptlet(Guid id, Guid bindingId, string
name, string address,.IContainerServices hostContainer, bool contract)
        : base(id, bindingId, name, address, hostContainer, contract)
    {
        MessageApi =
            new CryptletMessageApi(GetType().FullName, new
SampleContractConstructor())
```

For a more decentralized solution, we can turn to TrueBit, who offer a solution for scalable and verifiable off-chain computation. They use a system of solvers and verifiers, who are incentivized to perform computations and verification of those computations, respectively. Should a solution be challenged, an iterative verification process on subsets of the computation are performed on-chain—a kind of 'verification game'. The game proceeds through a series of rounds, each recursively checking a smaller and smaller subset of the computation. The game eventually reaches a final round, where the challenge is sufficiently trivial such that the judges—Ethereum miners—can make a final ruling on whether the challenge was met, on-chain. In effect, TrueBit is an implementation of a computation market, allowing decentralized applications to pay for verifiable computation to be performed outside of the network, but relying on Ethereum to enforce the rules of the verification game. In theory, this

enables trustless smart contracts to securely perform any computation task.

A broad range of applications exist for systems like TrueBit, ranging from machine learning to verification of proof-of-work. An example of the latter is the Doge–Ethereum bridge, which uses TrueBit to verify Dogecoin's proof-of-work (Scrypt), which is a memory-hard and computationally-intensive function that cannot be computed within the Ethereum block gas limit. By performing this verification on TrueBit, it has been possible to securely verify Dogecoin transactions within a smart contract on Ethereum's Rinkeby testnet.

Decentralized oracles

While centralized data or computation oracles suffice for many applications, they represent single points of failure in the Ethereum network. A number of schemes have been proposed around the idea of decentralized oracles as a means of ensuring data availability, and the creation of a network of individual data providers with an on-chain data aggregation system.

ChainLink have proposed a decentralized oracle network consisting of three key smart contracts: a reputation contract, an order-matching contract, an aggregation contract, and an off-chain registry of data providers. The reputation contract is used to keep track of data providers' performance. Scores in the reputation contract are used to populate the off-chain registry. The order-matching contract selects bids from oracles using the reputation contract. It then finalizes a Service Level Agreement, which includes query parameters and the number of oracles required. This means that the purchaser needn't transact with the individual oracles directly. The aggregation contract collects responses, submitted using a commit-reveal scheme, from multiple oracles, and then calculates the final collective result of the query, and finally feeds the results back into the reputation contract.

One of the main challenges with such a decentralized approach is the formulation of the aggregation function. ChainLink proposes calculating a weighted response, allowing a validity score to be reported for each oracle response. Detecting an 'invalid' score here is non-trivial, since it relies on the premise that outlying data points, measured by deviations from responses provided by peers, are incorrect. Calculating a validity score based on the location of an oracle response amongst a distribution of responses risks penalizing correct answers over average ones. Therefore, ChainLink offers a standard set of aggregation contracts, but also allows customized aggregation contracts to be specified.

A related idea is the SchellingCoin protocol. Here, multiple participants report values and the median is taken as the 'correct' answer. Reporters are required to provide a deposit which is redistributed in favor of values that are closer to the median, therefore incentivizing the reporting of values that are similar to others. A common value, also known as the Schelling Point, which respondents might consider as the

natural and obvious target around which to coordinate, is expected to be close to the actual value.

Teutsch recently proposed a new design for a decentralized off-chain data availability oracle. This design leverages a dedicated proof-of-work blockchain which is able to correctly report on whether or not registered data is available during a given epoch. Miners attempt to download, store, and propagate all currently registered data, thereby guaranteeing data is available locally. While such a system is expensive in the sense that every mining node stores and propagates all registered data, the system allows storage to be reused by releasing data after the registration period ends.

Oracle client interfaces in Solidity

Below is a Solidity example demonstrating how Oraclize can be used to continuously poll for the ETH/USD price from an API and store the result in a usable manner.

```
/*
ETH/USD price ticker leveraging CryptoCompare API

This contract keeps in storage an updated ETH/USD price,
which is updated every 10 minutes.

*/
pragma solidity ^0.4.1;
import "github.com/oraclize/ethereum-api/oraclizeAPI.sol";

/*
    "oracilize_" prepended methods indicate inheritance from
"usingOraclize"
*/
contract EthUsdPriceTicker is usingOraclize {

    uint public ethUsd;

    event newOraclizeQuery(string description);
    event newCallbackResult(string result);

    function EthUsdPriceTicker() payable {
        // signals TLSN proof generation and storage on IPFS
        oracilize_setProof(proofType_TLSNotary | proofStorage_IPFS);
```

```

        // requests query
        queryTicker();
    }

    function __callback(bytes32 _queryId, string _result, bytes _proof)
public {
    if (msg.sender != oraclize_cbAddress()) throw;
    newCallbackResult(_result);

    /*
     * parse the result string into an unsigned integer for on-chain
use
     * uses inherited "parseInt" helper from "usingOraclize",
allowing for
     * a string result such as "123.45" to be converted to uint 12345
     */
    ethUsd = parseInt(_result, 2);

    // called from callback since we're polling the price
    queryTicker();
}

function queryTicker() public payable {
    if (oraclize_getPrice("URL") > this.balance) {
        newOraclizeQuery("Oraclize query was NOT sent, please add
some ETH to cover for the query fee");
    } else {
        newOraclizeQuery("Oraclize query was sent, standing by for
the answer..");

        // query params are (delay in seconds, datasource type,
datasource argument)
        // specifies JSONPath, to fetch specific portion of JSON API
result
        oraclize_query(60 * 10, "URL", "json(https://min-
api.cryptocompare.com/data/price?fsym=ETH&tsyms=USD,EUR,GBP).USD");
    }
}

```



To integrate with Oraclize, the contract EthUsdPriceTicker must be a child of usingOraclize; the usingOraclize contract is defined in the oraclizeAPI file. The data request is made using the oraclize_query() function, which is inherited from the usingOraclize contract. This is an overloaded function that expects at least two arguments:

- The supported datasource to use, such as URL, WolframAlpha, IPFS, or computation
- The argument for the given datasource, which may include the use of JSON or XML parsing helpers

The price query is performed in the queryTicker() function. In order to perform the query, Oraclize requires the payment of a small fee in ether, covering the gas cost for transmitting and processing the result to the __callback() function and accompanying surcharge for the service. This amount is dependent on the data source, and, where specified, the type of authenticity proof that is required. Once the data has been retrieved, the __callback() function is called by an Oraclize-controlled account permissioned to do the callback; it passes in the response value and a unique queryId argument, which, for example, can be used to handle and track multiple pending callbacks from Oraclize.

Financial data provider Thomson Reuters also provides an oracle service for Ethereum, called BlockOne IQ, allowing market and reference data to be requested by smart contracts running on private or permissioned networks. Below is the interface for the oracle, and a client contract that will make the request.

```
pragma solidity ^0.4.11;

contract Oracle {
    uint256 public divisor;
    function initRequest(uint256 queryType, function(uint256) external
onSuccess, function(uint256) external onFailure) public returns (uint256
id);
    function addArgumentToRequestUInt(uint256 id, bytes32 name, uint256
arg) public;
    function addArgumentToRequestString(uint256 id, bytes32 name, bytes32
arg) public;
    function executeRequest(uint256 id) public;
    function getResponseUInt(uint256 id, bytes32 name) public constant
returns(uint256);
```

```

        function getResponseString(uint256 id, bytes32 name) public constant
    returns(bytes32);
        function getResponseError(uint256 id) public constant
    returns(bytes32);
        function deleteResponse(uint256 id) public constant;
    }

contract OracleB1IQClient {

    Oracle private oracle;
    event LogError(bytes32 description);

    function OracleB1IQClient(address addr) public payable {
        oracle = Oracle(addr);
        getIntraday("IBM", now);
    }

    function getIntraday(bytes32 ric, uint256 timestamp) public {
        uint256 id = oracle.initRequest(0, this.handleSuccess,
this.handleFailure);
        oracle.addArgumentToString(id, "symbol", ric);
        oracle.addArgumentToInt(id, "timestamp", timestamp);
        oracle.executeRequest(id);
    }

    function handleSuccess(uint256 id) public {
        assert(msg.sender == address(oracle));
        bytes32 ric = oracle.getResponseString(id, "symbol");
        uint256 open = oracle.getResponseInt(id, "open");
        uint256 high = oracle.getResponseInt(id, "high");
        uint256 low = oracle.getResponseInt(id, "low");
        uint256 close = oracle.getResponseInt(id, "close");
        uint256 bid = oracle.getResponseInt(id, "bid");
        uint256 ask = oracle.getResponseInt(id, "ask");
        uint256 timestamp = oracle.getResponseInt(id, "timestamp");
        oracle.deleteResponse(id);
        // Do something with the price data..
    }
}

```

```

function handleFailure(uint256 id) public {
    assert(msg.sender == address(oracle));
    bytes32 error = oracle.getResponseError(id);
    oracle.deleteResponse(id);
    emit LogError(error);
}

}

```

The data request is initiated using the `initRequest()` function, which allows the query type (in this example, a request for an intraday price) to be specified, in addition to two callback functions. This returns a `uint256` identifier which can then be used to provide additional arguments. The `addArgumentToString()` function is used to specify the RIC (Reuters Instrument Code), here for IBM stock, and `addArgumentToRequestUint()` allows the timestamp to be specified. Now, passing in an alias for `block.timestamp` will retrieve the current price for IBM. The request is then executed by the `executeRequest()` function. Once the request has been processed, the oracle contract will call the `onSuccess` callback function with the query identifier, allowing the resulting data to be retrieved; in the event of retrieval failure, the `onFailure` callback with an error code instead. The available fields that can be retrieved on success include open, high, low, close (OHLC) and bid/ask prices.

Reality Keys allows requests for facts to be made off-chain using POST requests. Responses are cryptographically signed, allowing them to be verified on-chain. Here, a request is made to check the balance of an account on the Bitcoin blockchain at a specific time using the `blockr.io` API:

```

wget -qO- https://www.realitykeys.com/api/v1/blockchain/new --post
-data="chain=XBT&address=1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX&which_total=t
otal_received&comparison=ge&value=1000&settlement_date=2015-09-
23&objection_period_secs=604800&accept_terms_of_service=current&use_exist
ing=1"

```

In this example, arguments allow the blockchain to be specified, the amount to be queried (total received or final balance) and the result to be compared with a provided value, allowing a true or false response. The resulting JSON object includes the returned value, in addition to the `signature_v2` field, which allows the result to be verified in a smart contract using the `ecrecover()` function:

To verify the signature, `ecrecover()` can determine that the data was indeed signed by `ethereum_address` as follows: the `fact_hash` and `signed_value` are hashed, and passed to `ecrecover()` with the three signature parameters:

```
bytes32 result_hash = sha3(fact_hash, signed_value);
address signer_address = ecrecover(result_hash, sig_v, sig_r, sig_s);
assert(signer_address == ethereum_address);
uint256 result = uint256(signed_value) / base_unit;
// Do something with the result..
```

Conclusions

As you can see, oracles provide a crucial service to smart contracts: they bring external facts to contract execution. With that, of course, oracles also introduce a significant risk - if they are trusted sources and can be compromised, they can result in compromised execution of the smart contracts they feed.

Generally, when considering the use of an oracle be very careful about the *trust model*. If you assume the oracle can be trusted, you may be undermining the security of your smart contract by exposing it to potentially false inputs. Oracles can be very useful, if the security assumptions are carefully considered.

Decentralized oracles can resolve some of these concerns and offer Ethereum smart contracts trustless

external data. Choose carefully and you can start exploring the bridge between Ethereum and the "real world" that oracles offer.

Decentralized Applications (DApps)

In this chapter we will explore the world of *Decentralized Applications* or *DApps*. From the early days of Ethereum, the founders' vision was much broader than "smart contracts": no less than reinventing the web and creating a new world of DApps, aptly called *web3*. Smart contracts are a way to decentralize the controlling logic and payment functions of applications. Web3 DApps are about decentralizing all other aspects of an application: storage, messaging, naming etc (see [Web3: A decentralized web using smart contracts and P2P Technologies](#)).

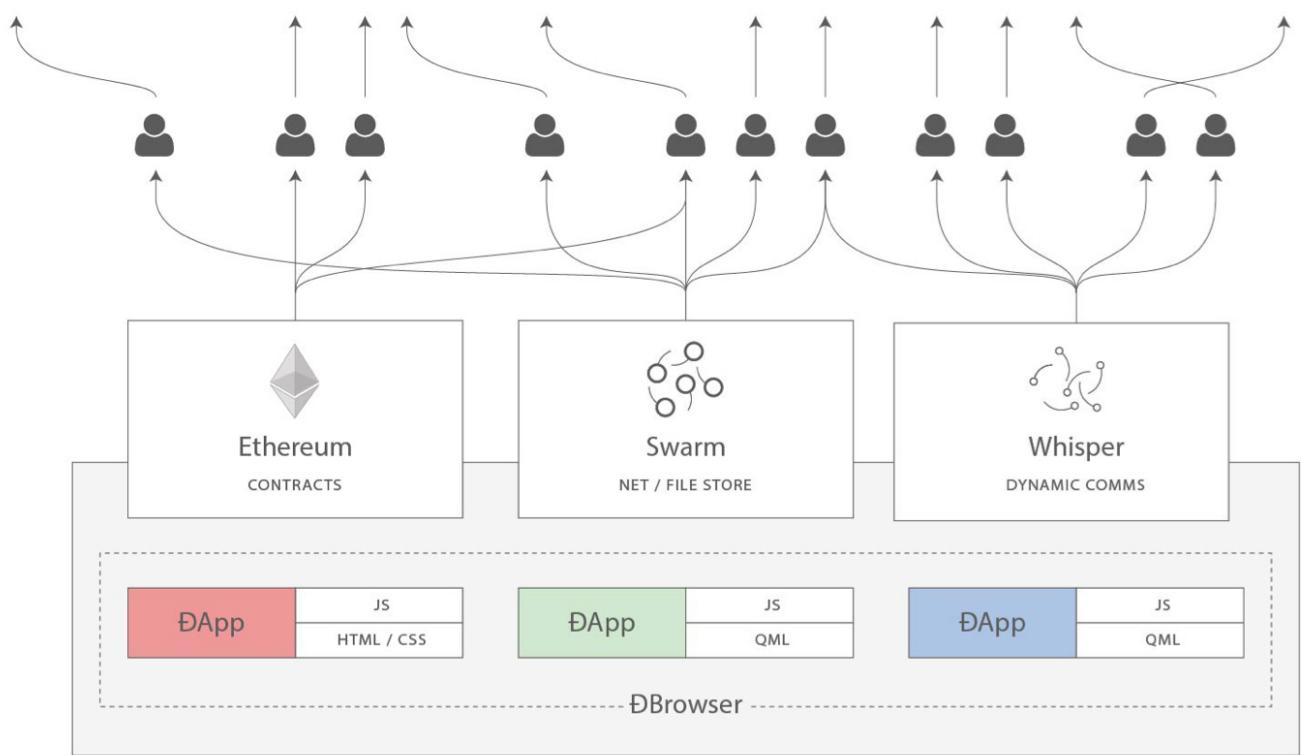


Figure 45. *Web3: A decentralized web using smart contracts and P2P Technologies*

While "decentralized apps" are an audacious vision of the future, the term "DApp" is often applied to any smart contract with a web front end. Some of these so-called DApps are highly centralized applications (CApps?). Beware of false DApps!

In this section we will develop and deploy a DApp: an auction platform. You can find the source code in the book's repository under `code/auction_dapp`. We will look at each aspect of an auction application

and see how we can decentralize the application as much as possible.

What is a DApp?

A Decentralized Application, or *DApp*, is an application which is mostly or entirely decentralized.

Consider all the possible aspects of an application that may be decentralized:

- Front-end software
- Back-end software (application logic)
- Data storage
- Name resolution
- Message communications

Each of these can be somewhat centralized or somewhat decentralized. For example, a front-end can be developed as a web app that runs on a centralized server, or as a mobile app that runs on your device. The back-end and storage can be on private servers and proprietary databases, or a smart contract and P2P storage.

There are many advantages to creating a DApp that a typical centralized architecture can not provide:

1) Resiliency: by having the business-logic controlled by a smart contract, a DApp back-end will be fully distributed and managed on a blockchain platform. Unlike deploying an application on a centralized server, a DApp will have no downtime and will continue to be available as long as the platform is still operating.

2) Transparency: the on-chain nature of a DApp allows everyone to inspect the code and be more sure about its function. Any interaction with the DApp will be stored forever in the blockchain.

3) Censorship Resistance: as long as a user has access to an Ethereum node (running one if necessary), the user will always be able to interact with a DApp without interference from any centralized control. No service provider, or even the owner of the smart contract, can alter the code once it is deployed on the network.

In the Ethereum ecosystem as it stands today, there are very few truly decentralized apps - most still rely on centralized services and servers for some part of their operation. In the future, we expect that it will be possible for every part of any DApp to be operated in a fully decentralized way.

Smart contracts "back end"

In a DApp, smart contracts are used to store the business logic (program code) and the related state of your application. You can think of a smart contract replacing a server-side (a.k.a. "back-end") component in a regular application. This is an oversimplification, of course. One of the main differences is that any computation executed in a smart contract is very expensive and so should be kept as minimal as possible. It is therefore important to identify which aspects of the application need a trusted and decentralized execution platform.

Ethereum smart contracts allow you to build architectures in which a network of smart contracts call and pass data between each other, reading and writing their own state variables as they go, their complexity restricted only by the block gas limit. After deploying your smart contract, your business logic could well be used by many other developers in the future.

One major consideration of smart contract architecture design is the inability to change the code of a smart contract once it is deployed. It can be deleted if it is programmed with an accessible SELFDESTRUCT opcode, but other than complete removal, the code cannot be changed in any way.

The second major consideration of smart contract architecture design is DApp size; a really large monolithic smart contract may cost a lot of gas to deploy and use. Therefore, some applications may choose to have off-chain computation and an external data source. Keep in mind, however, that having the core business logic of the DApp be dependent on external data (e.g. from a centralized server) means your users will have to trust these external resources.

Front end (Web User Interface)

Unlike the business logic of the DApp, which requires a developer to understand the EVM and new languages such as Solidity, the client side interface of a DApp can use standard web technologies (HTML, CSS, JavaScript, etc). This allows a traditional web developer to use familiar tools, libraries and frameworks. Interactions with Ethereum, such as signing messages, sending transactions and key management are often conducted through the web browser, via an extension such as MetaMask.

Although it is possible to create a mobile DApp as well, currently there are few resources to help create mobile DApp front-ends, mainly due to the lack of mobile clients that can serve as a light client with key management functionality.

The front-end is usually linked to Ethereum via the web3.js JavaScript library, which is bundled with the front-end resources and served to a browser by a web server.

Data storage

Due to high gas costs and the currently low block gas limit, smart contracts are not suited to store or process large amounts of data. Hence, most DApps will utilize off-chain data storage services, meaning they store the bulky data off the Ethereum chain, on a data storage platform. That data storage platform can be centralized, for example a typical cloud database. Or, the data can be decentralized, stored on a P2P platform such as the *Interplanetary File System (IPFS)*, or Ethereum's own *Swarm* platform.

Decentralized P2P storage is ideal for storing and distributing large static assets such as images, videos, and the resources of the application's front-end web interface (HTML, CSS, JavaScript, etc).

Inter-Planetary File System (IPFS)

The *Inter-Planetary File System (IPFS)* is a decentralized content-addressable storage system that distributes stored objects among peers in a P2P network. "Content Addressable" means that each piece of content (file) is hashed and the hash is used to identify that file. You can then retrieve any file from any IPFS node, by requesting it by its hash.

IPFS aims to replace HTTP as the protocol of choice for delivery of web applications. Instead of storing a web application on a single server, the files are stored on IPFS and can be retrieved from any IPFS node.

More information about IPFS can be found at <https://ipfs.io>

Swarm

Swarm is another content-addressable P2P storage system, similar to IPFS. Swarm is built by the Ethereum Foundation, as part of the Go-Ethereum suite of tools. Like IPFS, Swarm allows you to store files that get disseminated and replicated by Swarm nodes. You can access any Swarm file by referring to it by a hash. Swarm allows you to access a web site from a decentralized P2P system, instead of a central web server.

The home page for Swarm is itself stored on Swarm and accessible on your Swarm node or a gateway: <https://swarm-gateways.net/bzz:theswarm.eth/>

Decentralized message communications protocols

Another major component of any application is inter-process communication. That means being able to exchange messages between applications, between different instances of the application, or between users of the application. Traditionally, this is achieved by reliance on a centralized server.

There are a variety of decentralized alternatives to a server-based protocols, offering messaging over a P2P network. The most notable P2P messaging protocol for DApps is *Whisper*, which is part of the Ethereum Foundation's Go-Ethereum suite of tools. More information about Whisper can be found here: <https://github.com/ethereum/wiki/wiki/Whisper>

A basic DApp example: Auction DApp

In this section we will start building an example DApp, to explore the various decentralization tools. Our DApp will implement a decentralized auction.

The Auction DApp allows a user to register a "deed" token, which represents some unique asset, such as a house, a car, a trademark, etc. Once a token has been registered, the ownership of the token is transferred to the Auction DApp, allowing it to be listed for sale. The Auction DApp lists each of the registered tokens, allowing other users to place bids. During the auction, users can join a chat room, created specifically for each auction. Once an auction is finalized, the deed token ownership is transferred to the winner of the auction.

The overall auction process can be seen in [Auction DApp: A simple example auction DApp](#):

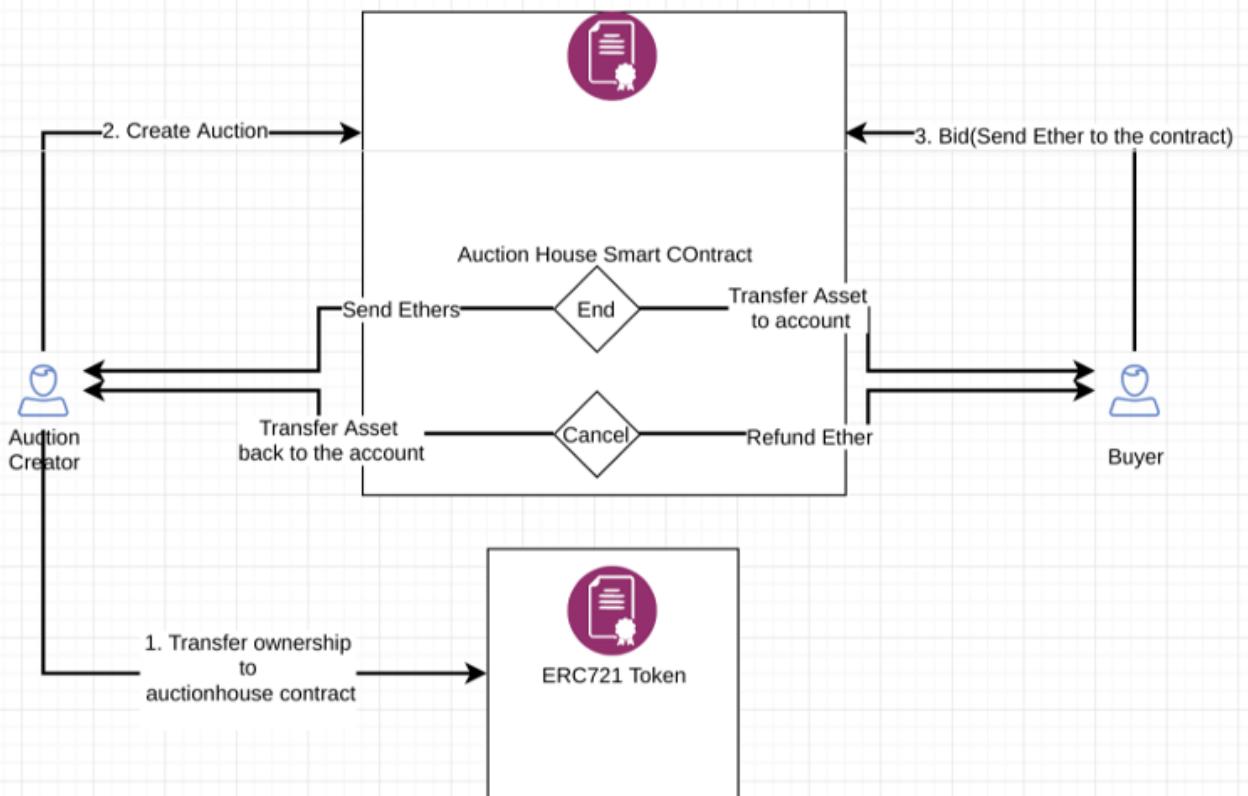


Figure 46. Auction DApp: A simple example auction DApp

The main components of our Auction DApp are:

- A smart contract implementing ERC721 non-fungible "deed" tokens (DeedRepository).
- A smart contract implementing an Auction (AuctionRepository) to sell the deeds.
- A web front-end using the Vue/Vuetify JavaScript framework.
- The web3.js library to connect to Ethereum chains (via MetaMask or other clients).

- A Swarm client, to store resources such as images.
- A Whisper client, to create per-auction chat rooms for all participants.

You can find the source code for the auction DApp in the book's repository: https://github.com/ethereumbook/ethereumbook/tree/develop/code/auction_dapp

Auction DApp: Back-end smart Contracts

Our Auction DApp example is supported by two smart contracts that we need to deploy on an Ethereum blockchain in order to support the application: AuctionRepository and DeedRepository.

Let's start by looking at DeedRepository, shown in [DeedRepository.sol : An ERC721 deed token for use in an auction](#). This contract is an ERC-721 compatible "non-fungible token" (See [ERC721 - non-fungible token \(deed\) standard](#)).

DeedRepository.sol : An ERC721 deed token for use in an auction

```
pragma solidity ^0.4.17;
import "./ERC721/ERC721Token.sol";

/**
 * @title Repository of ERC721 Deeds
 * This contract contains the list of deeds registered by users.
 * This is a demo to show how tokens(deeds) can be mint and add to the
repository
 */
contract DeedRepository is ERC721Token {

    /**
     * @dev Created a DeedRepository with a name and symbol
     * @param _name string represents the name of the repository
     * @param _symbol string represents the symbol of the repository
     */
    function DeedRepository(string _name, string _symbol) public
ERC721Token(_name, _symbol) {}

    /**
     * @dev Public function to register a new deed
     * @dev Call the ERC721Token Minter
}
```

```

* @param _tokenId uint256 represents a specific deed
* @param _uri string containing metadata/uri
*/
function registerDeed(uint256 _tokenId, string _uri) public {
    _mint(msg.sender, _tokenId);
    addDeedMetadata(_tokenId, _uri);
    emit DeedRegistered(msg.sender, _tokenId);
}

/**
* @dev Public function to add metadata to a deed
* @param _tokenId represents a specific deed
* @param _uri text which describes the characteristics of a given
deed
* @return whether the deed metadata was added to the repository
*/
function addDeedMetadata(uint256 _tokenId, string _uri) public
returns(bool){
    _setTokenURI(_tokenId, _uri);
    return true;
}

/**
* @dev Event is triggered if deed/token is registered
* @param _by address of the registrar
* @param _tokenId uint256 represents a specific deed
*/
event DeedRegistered(address _by, uint256 _tokenId);
}

```

As you can see, the DeedRepository contract is a straightforward implementation of an ERC721-compatible token.

Our Auction DApp uses the DeedRepository contract to issue and track tokens for each auction. The auction itself is orchestrated by the AuctionRepository contract, which can be found here:

https://github.com/ethereumbook/ethereumbook/tree/develop/code/auction_dapp/backend/contracts/AuctionRepository.sol

The AuctionRepository contract is too long to include here in full, but [AuctionRepository.sol : The main Auction DApp smart contract](#) is the main definition of the contract and data structures:

AuctionRepository.sol : The main Auction DApp smart contract

```
contract AuctionRepository {  
  
    // Array with all auctions  
    Auction[] public auctions;  
  
    // Mapping from auction index to user bids  
    mapping(uint256 => Bid[]) public auctionBids;  
  
    // Mapping from owner to a list of owned auctions  
    mapping(address => uint[]) public auctionOwner;  
  
    // Bid struct to hold bidder and amount  
    struct Bid {  
        address from;  
        uint256 amount;  
    }  
  
    // Auction struct which holds all the required info  
    struct Auction {  
        string name;  
        uint256 blockDeadline;  
        uint256 startPrice;  
        string metadata;  
        uint256 deedId;  
        address deedRepositoryAddress;  
        address owner;  
        bool active;  
        bool finalized;  
    }  
}
```

The AuctionRepository contract manages all auctions with the following functions:

```
getCount()
getBidsCount(uint _auctionId)
getAuctionsOf(address _owner)
getCurrentBid(uint _auctionId)
getAuctionsCountOfOwner(address _owner)
getAuctionById(uint _auctionId)
createAuction(address _deedRepositoryAddress, uint256 _deedId, string
_auctionTitle, string _metadata, uint256 _startPrice, uint
_blockDeadline)
approveAndTransfer(address _from, address _to, address
_deedRepositoryAddress, uint256 _deedId)
cancelAuction(uint _auctionId)
finalizeAuction(uint _auctionId)
bidOnAuction(uint _auctionId)
```

We can deploy these contracts to the Ethereum blockchain of our choice (e.g. Ropsten), using truffle in the book's repository:

```
cd code/auction_dapp/backend
truffle init
truffle compile
truffle migrate --network ropsten
```

DApp governance

If you read through the two smart contracts of the Auction DApp you will notice something important:

There is no special account or role that has special privileges over the DApp. Each auction has an owner with some special capabilities, but the Auction DApp itself has no privileged user.

This is a deliberate choice to decentralize the governance of the DApp and relinquish any control once it has been deployed. Some DApps, by comparison, have one or more privileged accounts, with special capabilities, such as the ability to terminate the DApp contract, to override or change its configuration, or to "veto" certain operations. Usually, these governance functions are introduced in the DApp in order to avoid unknown problems that might arise due to a bug.

The issue of governance is a particularly difficult one to solve. It represents a double-edged sword: On one side, privileged accounts are dangerous - if compromised they can subvert the security of the DApp. On the other side, without any privileged account, there are no recovery options if a bug is found. We have seen both of these risks manifest in Ethereum DApps. In the case of The DAO, there were some privileged accounts called the "curators", but they were very limited in their capabilities. Those accounts were not able to override the DAO attacker's withdrawal of the funds. In a more recent case, the decentralized exchange Bancor experienced a massive theft because a privileged management account was compromised. Turns out, Bancor was not as decentralized as initially assumed.

When building a DApp, you have to decide if you want to make the smart contracts truly independent, launching them and then having no control, or creating privileged accounts and running the risk of those being compromised. Either choice carries risk, but in the long run, true DApps cannot have specialized access for privileged accounts - that's not decentralized.

Auction DApp: Front-end user interface

Once the Auction DApp contracts are deployed, you can interact with them using your favorite JavaScript console and web3.js, or another web3 library. However, most users will need an easy-to-use interface. Our Auction DApp user interface is built using the as Vue.js JavaScript framework and Vuetify library of UI components.

You can find the user interface code in the `code/auction_dapp/frontend` folder in the book's repository. The directory has the following structure and contents:

```
frontend/
|-- build
|   |-- build.js
|   |-- check-versions.js
|   |-- logo.png
|   |-- utils.js
|   |-- vue-loader.conf.js
|   |-- webpack.base.conf.js
|   |-- webpack.dev.conf.js
|   `-- webpack.prod.conf.js
|-- config
|   |-- dev.env.js
|   |-- index.js
|   `-- prod.env.js
|-- index.html
|-- package.json
|-- package-lock.json
|-- README.md
|-- src
|   |-- App.vue
|   |-- components
|   |   |-- Auction.vue
|   |   `-- Home.vue
|   |-- config.js
|   |-- contracts
|   |   |-- AuctionRepository.json
|   |   `-- DeedRepository.json
|   |-- main.js
|   |-- models
|   |   |-- AuctionRepository.js
|   |   |-- ChatRoom.js
|   |   `-- DeedRepository.js
|   |-- router
|   |   `-- index.js
```

Once you have deployed the contracts, edit the front-end configuration in `frontend/src/config.js` and enter the address of the `DeedRepository` and `AuctionRepository` contracts, as deployed. The front-end

application also needs access to an Ethereum node offering a JSON-RPC and websockets interface. Once you've configured the front-end, launch it with a web server on your local machine:

```
npm install  
npm run dev
```

The Auction DApp front-end will launch and will be accessible via any web browser at:

<http://localhost:8080>

If all goes well, you should see [Auction DApp User interface](#) which illustrates the Auction DApp running in your web browser:

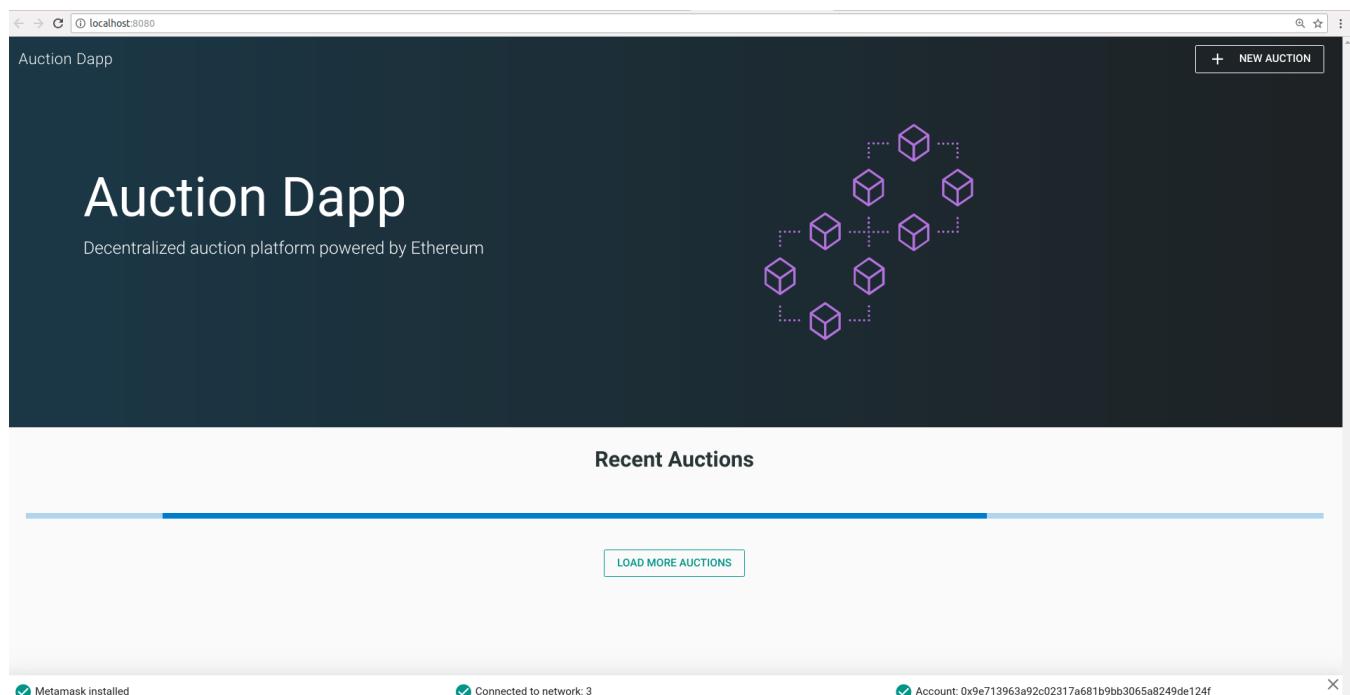


Figure 47. Auction DApp User interface

Further Decentralizing the Auction DApp

Our DApp is already quite decentralized, but we can improve things.

The AuctionRepository contract operates independently of any oversight, open to anyone. Once deployed it cannot be stopped, nor can any auction be censored. Each auction has a separate chat room that allows anyone to communicate about the auction without censorship or identification. The various auction assets, such as the description and associated image, are stored on Swarm, making them hard to censor or block.

Anyone can interact with the DApp by constructing transactions manually or by running the Vue frontend on their local machine. The DApp code itself is open source and developed collaboratively on a public repository.

But we can do more to make this DApp decentralized and resilient:

- Store all the application code on Swarm or IPFS
- Access the DApp by reference to a name, using the Ethereum Name Service

In the next sections we will further decentralize the Auction DApp.

Storing the Auction DApp on Swarm

We introduced Swarm in [\[swarm\]](#), earlier in this chapter. Our Auction DApp already uses Swarm to store the icon image for each auction. This is a much more efficient solution than attempting to store data on Ethereum, which is expensive. It is also a lot more resilient than if these images were stored on a centralized service like a web server or file server.

But we can take things one step further. We can store the entire front-end of the DApp itself in Swarm and run it from a Swarm node directly, instead of running a web server.

Preparing Swarm

To get started, we need to install Swarm and initialize our Swarm node. Swarm is part of the Ethereum Foundation's Go-Ethereum suite of tools. Refer to the instructions for installing go-ethereum in [Go-Ethereum \(Geth\)](#), or to install a Swarm binary release, follow these instructions:

<https://swarm-guide.readthedocs.io/en/latest/installation.html>

Once you have installed Swarm, you can check that it is working correctly by running it with the version command:

```
$ swarm version
Version: 0.3
Git Commit: 37685930d953bcbe023f9bc65b135a8d8b8f1488
Go Version: go1.10.1
OS: linux
```

To start running Swarm, you must tell it how to connect to an instance of Geth, to access the JSON-RPC API. Get it started by following the instructions here:

<https://swarm-guide.readthedocs.io/en/latest/gettingstarted.html>

When you start swarm, you should see something like this:

```
Maximum peer count
Starting peer-to-peer node
225171a4/linux-amd64/go1.10
connecting to ENS API
swarm[5955]: [189B blob data]
Starting P2P networking
UDP listener up
self=enode://f50c8e19ff841bcd5ce7d2d...
Updated bzz local addr
oaddr=9c40be8b83e648d50f40ad3d35f... uaddr=e
Starting Swarm service
9c40be8b hive starting
detected an existing store. trying to load peers
hive 9c40be8b: peers loaded
Swarm network started on bzz address: 9c40be8b83e648d50f40ad3d35f...
Pss started
Streamer started
IPC endpoint opened
url=/home/ubuntu/.ethereum/bzzd.ipc
RLPx listener up
self=enode://f50c8e19ff841bcd5ce7d2d...
```

You can confirm that your Swarm node is running correctly by connecting to the local Swarm gateway

web interface: <http://localhost:8500>

You should see a [Swarm gateway on localhost](#) and be able to query any Swarm hash or ENS name:

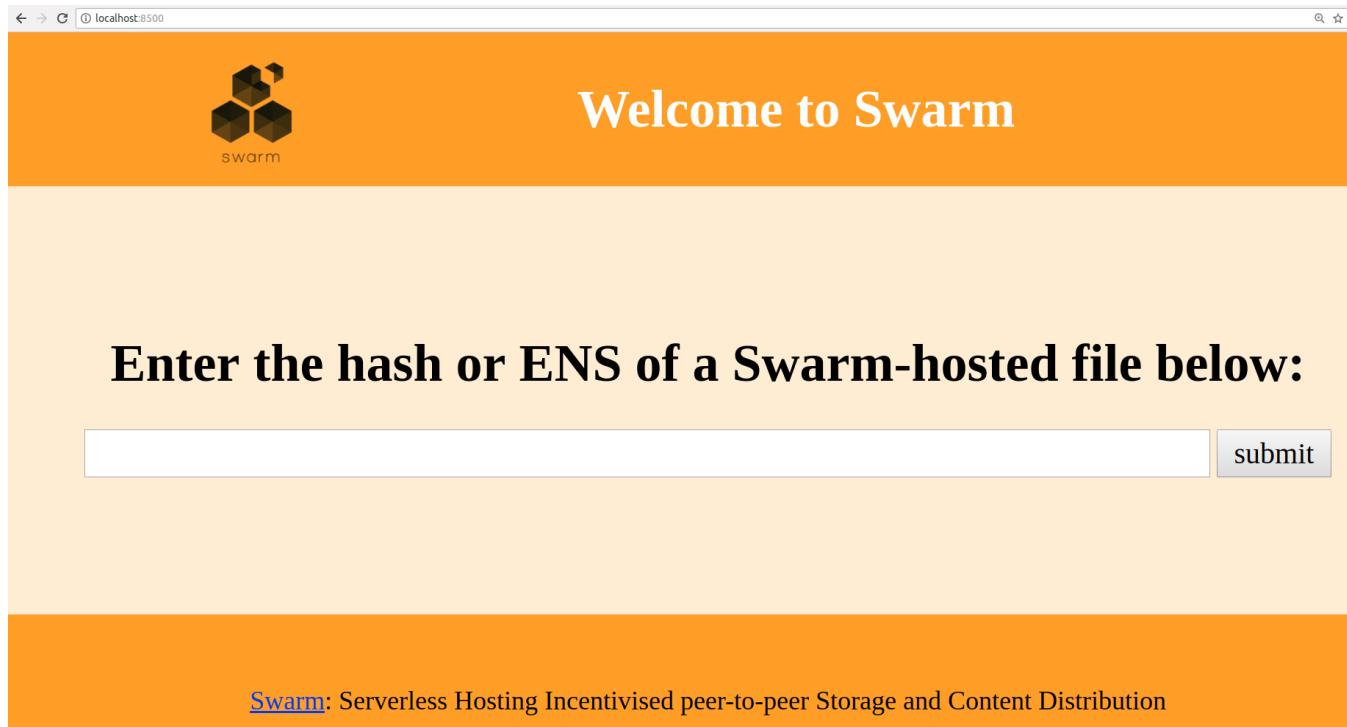


Figure 48. Swarm gateway on *localhost*

Uploading files to Swarm

Once you have your local Swarm node and gateway running, you can upload to Swarm and the files will be accessible on any Swarm node, simply by reference to the file hash.

Let's test this by uploading a file!

```
$ swarm up code/auction_dapp/README.md  
ec13042c83ffc2fb5cb0aa8c53f770d36c9b3b35d0468a0c0a77c97016bb8d7c
```

Swarm has uploaded the README.md file, and returned a hash. We can now use this hash to access the README.md from any Swarm node. For example, we could use the public Swarm gateway:

<https://swarm-gateways.net/bzz:/ec13042c83ffc2fb5cb0aa8c53f770d36c9b3b35d0468a0c0a77c97016bb8d7c/>

While uploading one file is relatively straightforward, it is a bit more complex to upload an entire DApp front-end. That's because the various DApp resources (HTML, CSS, JavaScript, libraries etc.) have embedded references to each other. Normally, a web server translates URLs to local files and serves the correct resources. We can achieve the same for Swarm by packaging our DApp.

In the Auction DApp, there's a script for packaging all the resources:

```
$ cd code/auction_dapp/frontend
$ npm run build

> frontend@1.0.0 build
/home/aantonop/Dev/ethereumbook/code/auction_dapp/frontend
> node build/build.js

Hash: 9ee134d8db3c44dd574d
Version: webpack 3.10.0
Time: 25665ms
Asset      Size  Chunks             Chunk Names
static/js/vendor.77913f316aaf102cec11.js   1.25 MB      0 [emitted]
[big] vendor
static/js/app.5396ead17892922422d4.js     502 kB       1 [emitted]  [big]
app
static/js/manifest.87447dd4f5e60a5f9652.js  1.54 kB       2 [emitted]
manifest
static/css/app.0e50d6a1d2b1ed4daa03d306ced779cc.css  1.13 kB       1
[emitted]           app
static/css/app.0e50d6a1d2b1ed4daa03d306ced779cc.css.map  2.54 kB
[emitted]
static/js/vendor.77913f316aaf102cec11.js.map  4.74 MB      0 [emitted]
vendor
static/js/app.5396ead17892922422d4.js.map    893 kB       1 [emitted]
app
static/js/manifest.87447dd4f5e60a5f9652.js.map  7.86 kB       2
[emitted]           manifest
index.html 1.15 kB           [emitted]

Build complete.
```

The result of this command will be a new directory `code/auction_dapp/frontend/dist` that contains the entire Auction DApp frontend, packed together:

```
dist/
|-- index.html
`-- static
  |-- css
  |   |-- app.0e50d6a1d2b1ed4daa03d306ced779cc.css
  |   `-- app.0e50d6a1d2b1ed4daa03d306ced779cc.css.map
  '-- js
    |-- app.5396ead17892922422d4.js
    |-- app.5396ead17892922422d4.js.map
    |-- manifest.87447dd4f5e60a5f9652.js
    |-- manifest.87447dd4f5e60a5f9652.js.map
    |-- vendor.77913f316aaaf102cec11.js
    `-- vendor.77913f316aaaf102cec11.js.map
```

Now we can upload the entire DApp to Swarm, by using the `up` command and the recursive option. We will also tell Swarm that `index.html` is the defaultpath for loading this DApp:

```
swarm --bzzapi http://localhost:8500 --recursive --defaultpath
dist/index.html up dist/
ab164cf37dc10647e43a233486cdeffa8334b026e32a480dd9cbd020c12d4581
```

Now, our entire Auction DApp is hosted on Swarm and accessible by the Swarm URL:

`bzz://ab164cf37dc10647e43a233486cdeffa8334b026e32a480dd9cbd020c12d4581`

We've made some progress in decentralizing our DApp, but we've made it harder to use. A URL like that is much harder to use than a web server with a nice name like `auction_dapp.com`. Are we forced to sacrifice usability in order to gain decentralization? Not necessarily. In the next section we will examine the *Ethereum Naming System (ENS)*, which allows us to use easy-to-read names but still preserves the decentralized nature of our application.

Ethereum Naming System (ENS)

You can design the best smart contract in the world, but if you don't provide a good interface for users, they won't be able to access it.

On the traditional internet, the Domain Name system (DNS), allows us to use human-readable names in the browser, while resolving those names to IP addresses or other identifiers behind the scenes. On the Ethereum blockchain, the *Ethereum Naming System (ENS)* solves the same problem, but in a decentralized manner.

For example, the Ethereum Foundation donation address is 0xb6916095ca1df60bB79Ce92cE3Ea74c37c5d359; in a wallet that supports ENS, it's simply ethereum.eth.

ENS is more than a smart contract. ENS is a fundamental DApp itself, offering a decentralized name service. Furthermore, ENS is supported by a number of DApps for registration, management, and auctions of registered names. ENS demonstrates how DApps can work together: A DApp built to serve other DApps, supported by an ecosystem of DApps, embedded in other DApps, etc.

In this section we will look at how ENS works, how we can set up our own name and link it to a wallet or Ethereum address, how we can embed ENS in another DApp and how we can use ENS to name our DApp resources to make them easier to use.

History of Ethereum name services

Name registration was the first non-currency application of blockchains, pioneered by Namecoin. The Ethereum whitepaper gave a two-line Namecoin-like registration system as one of its example applications.

Early releases of Geth and the C++ Ethereum client had a built-in namereg contract (*not used any more*), and many proposals and ERCs for name services were made, but it was only when Nick Johnson started working for Ethereum Foundation in 2016 and took the project under his wing that serious work on a registrar started.

ENS was launched on Star Wars day, May 4, 2017 (after a failed attempt to launch it on Pi Day, March 15).

The ENS specification

ENS is specified mainly in three Ethereum Improvement Proposals (EIPs), namely ERC137, which specifies the basic functions of ENS, ERC162, which describes the auction system for the .eth root, and ERC181, which specifies reverse registration of addresses.

ENS follows a "sandwich" design philosophy: a very simple layer on the bottom, followed by layers of

more complex but replaceable code, with a very simple top layer that keeps all the funds in separate accounts.

Bottom layer: Name Owners and resolvers

The ENS operates on "nodes" instead of human-readable names: a human-readable name is converted to a node using the "Namehash" algorithm.

The base layer of the ENS is a cleverly simple contract (less than 50 lines of code) defined by ERC137 that allows only nodes' owners to set information about their names and to create subnodes (the ENS equivalent of DNS subdomains).

The only functions on the base layer are those that enable a node owner to set information about their own node (specifically the resolver, time to live or transferring the ownership) and to create owners of new subnodes.

Namehash algorithm

Namehash is a recursive algorithm that can convert any name into a hash that identifies the name.

"Recursive" means that we solve the problem by solving a sub-problem that is a smaller problem of the same type, and then use the solution to the sub-problem to solve the original problem.

Namehash recursively hashes components of the name, producing a unique, fixed-length string for any valid input domain, or "node".

For example, the Namehash node of subdomain.example.eth is: `keccak('example.eth' node) + keccak('subdomain')`. The sub-problem we must solve is to compute the node for example.eth, which is: `keccak('.eth' node) + keccak('example')`. In turn, we must compute the node for eth, which is: `keccakRoot Node) + keccak('eth')`.

The root node is what we call the "base case" of our recursion, and we obviously can't define it recursively, or the algorithm will never terminate! The root node is defined as:

Putting this all together, the node of `subdomain.example.eth` is therefore: `keccak(keccak(keccak(0x0_0 + keccak('eth')) + keccak('example')) + keccak('subdomain'))`

Generalizing, we can define the Namehash function as follows (the base case for the root node, or

(empty name, followed by the recursive step):

```
namehash([]) =  
0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000  
namehash([label, ...]) = keccak256(namehash(...) + keccak256(label))
```

In Python this becomes:

```
def namehash(name):
    if name == '':
        return '\0' * 32
    else:
        label, _, remainder = name.partition('.')
        return sha3(namehash(remainder) + sha3(label))
```

Thus, `mastering-ethereum.eth` will be processed as follows:

```
namehash('mastering-ethereum.eth')  
⇒ sha3(namehash('eth') + sha3('mastering-ethereum'))  
⇒ sha3(sha3(namehash('') + sha3('eth')) + sha3('mastering-ethereum'))  
⇒ sha3(sha3(( '\0' * 32) + sha3('eth'))) + sha3('mastering-ethereum'))
```

Of course, subdomains can themselves have subdomains: after `subdomain.example.eth` there could be a `sub.subdomain.example.eth`, then a `sub.sub.subdomain.example.eth` and so on. To avoid expensive recomputation, since Namehash depends only on the name itself, the node for a given name can be precomputed and inserted into a contract, removing the need for string manipulation, and permitting immediate lookup of ENS records regardless of the number of components in the raw name.

How to choose a valid name

Names consist of a series of dot-separated labels. Although upper and lower case letters are allowed, all labels should follow a UTS46 normalization process that case-folds labels before hashing them, so names with different case but identical spelling will end up with the same Namehash.

You could use labels and domains of any length, but for the sake of compatibility with legacy DNS, the

following rules are recommended:

- Labels should be no more than 64 characters each.
- Complete ENS names should be no more than 255 characters.
- Labels should not start or end with hyphens, or start with digits.

Root node ownership

One of the results of this hierarchical system is that it relies on the owners of the root node, who are able to create top level domains.

While the eventual goal is to adopt a decentralized decision-making process for new top level domains, right now the root node is controlled by a 4 out of 7 multisig, held by people in different countries (built as a reflection of the seven keyholders of the DNS system). As a result, a majority of at least 4 of the 7 keyholders is required to effect any change.

Currently the purpose and goal of these keyholders is to work in consensus with the community to:

- Migrate and upgrade the temporary ownership of the .eth TLD (Top Level Domain) to a more permanent contract once the system is evaluated.
- Allow adding new TLDs, if the community agrees they are needed.
- Migrate the ownership of the root multisig to a more decentralized contract, when such a system is agreed upon, tested and implemented.
- Serve as a last resort way to deal with any bugs or vulnerabilities in the top-level registries.

Resolvers

The basic ENS contract can't add metadata to names; that is the job of "resolver contracts". These are user-created contracts that can answer questions about the name, such as "What's the Swarm address associated with this app?", "What is the Ethereum address that receives payments in ether and tokens?", or "What's the hash of the app?" (to verify its integrity).

Middle layer: the ".eth" nodes

At the moment, the only top level domain that is uniquely registrable in a smart contract is .eth.

There's work on enabling traditional DNS domain owners to claim ENS ownership. While in theory this

could work for .com the only domain that this has been implemented for so far is [.xyz, and only on Ropsten testnet](<https://medium.com/the-ethereum-name-service/how-to-claim-your-dns-domain-on-ens-e600ef2d92ca>).

.eth domains are distributed via an auction system. There is no reserved list or priority, and the only way to acquire a name is to use the system. The auction system is a complex piece of code (over 500 lines); most of the early development efforts (and bugs!) in ENS were in this part of the system, but it's also replaceable and upgradeable (without risk to the funds—more on that later).

Vickrey Auctions

Names are distributed via a modified Vickrey Auction. In a traditional Vickrey auction, every bidder submits a sealed bid, and all of them are revealed simultaneously, at which point the highest bidder wins the auction, but only pays the second-highest bid. Therefore bidders are incentivized not to bid less than the true value of the name to them, since bidding their true value increases the chance they will win but does not affect the price they will eventually pay.

On a blockchain, some changes are required:

- To ensure bidders don't submit bids they have no intention of paying, they must lock up a value equal or higher than their bid beforehand, to guarantee the bid is valid.
- Because you can't hide secrets on a blockchain, bidders must execute at least two transactions (a commit-reveal process), in order to hide the original value and name they bid on.
- Since you can't reveal all bids simultaneously in a decentralized system, bidders must reveal their own bids themselves; if they don't, they forfeit their locked-up funds. Without this forfeit, one could make many bids and choose to reveal only one or two, turning a sealed-bid auction into a traditional increasing price auction.

Therefore, the auction is a four-step process:

1. Start the auction. This is required to broadcast the intent to register a name. This creates all auction deadlines. The names are hashed, so that only those who have the name in their dictionary will know which auction was opened. This allows some privacy, useful if you are creating a new project and don't want to share details about it. You can open multiple dummy auctions at the same time, so if someone is following you they cannot simply bid on all auctions you open.
2. Make a sealed bid: you must do this before the bidding deadline, by tying a given amount of ether

to the hash of a secret message (containing, among others, the hash of the name, the actual amount of the bid, and a salt). You can lock up more ether than you are actually bidding in order to mask your true valuation.

3. Reveal the bid: during the reveal period, you must make a transaction that reveals the bid, which will then calculate the highest bid, the second higher bid and send ether back to unsuccessful bidders. Every time the bid is revealed the current winner is recalculated, therefore the last one to be set before the revealing deadline expires becomes the overall winner.
4. Clean up after: if you are the winner, you can finalize the auction in order to get back the difference between your bid and the second highest. If you forgot to reveal you can make a late reveal and recover a little of your bid.

Top layer of the ENS: the Deeds

The top layer of the ENS is yet another super-simple contract with a single purpose: to hold the funds.

When you win a name, the funds are not actually sent anywhere, but are just locked up for the period you want to hold the name (at least a year). This works like a guaranteed buy-back: if the owner does not want the name any more they can sell it back to the system and recover their ether (so the cost of holding the name is the opportunity cost of doing something with a return greater than zero).

Of course, having a single contract hold millions of dollars in ether has proven to be very risky, so instead ENS creates a Deed Contract for each new name. The Deed Contract is very simple (about 50 lines of code) and it only allows the funds to be transferred back to a single account (the deed owner) and to be called by a single entity (the registrar contract). This approach drastically reduces the attack surface where bugs can put the funds at risk.

Registering a name

Registering a name in ENS is a four-step process, as we saw in [Vickrey Auctions](#). First we place a bid for any available name, then we reveal our bid after 48 hours to secure the name. [ENS timeline for registration](#) is a diagram showing the timeline of registration:

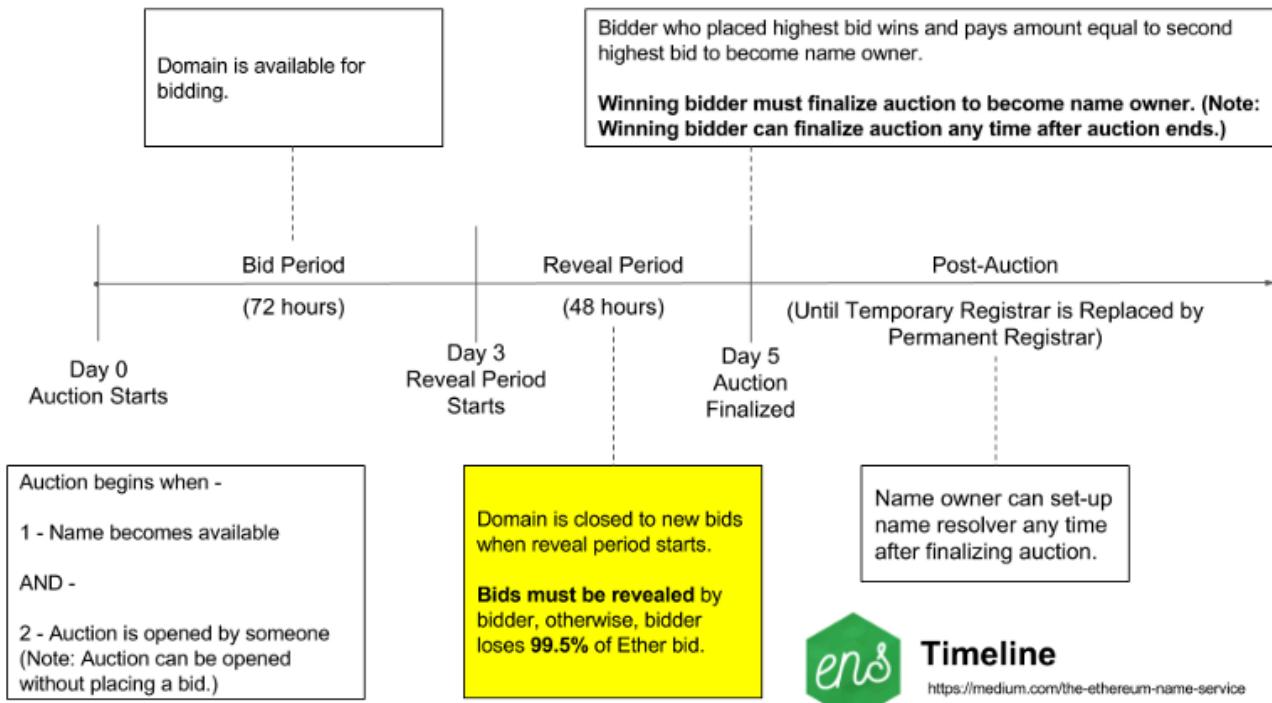


Figure 49. ENS timeline for registration

Let's register our first name!

We will use one of several available user-friendly interfaces to search for available names, place a bid on the name ethereumbook.eth, reveal the bid and secure the name.

There are a number of web-based interfaces to ENS that allow us to interact with the ENS DApp. For this example, we will use the mycrypto.com interface, in conjunction with MetaMask as our wallet.

First, we need to make sure the name we want is available. While writing this book, we really wanted to register the name mastering.eth, but alas, [Searching for ENS names on MyCrypto.com](#) revealed it was already taken! Because ENS registrations only last one year, it might become possible to secure that name in the future. In the mean time, let's search for ethereumbook.eth:

ENS

The Ethereum Name Service is a distributed, open, and extensible naming system based on the Ethereum blockchain. Once you have a name, you can tell your friends to send ETH to `mewtopia.eth` instead of `0x4bbeEB066eD09B.....`.

ethereumbook

.eth

Check ENS Name

ethereumbook.eth is available!

- Do you want ethereumbook.eth? [Unlock your Wallet to Start an Auction](#)

Figure 50. Searching for ENS names on MyCrypto.com

Great! The name is available. In order to register it, we need to move forward with [Starting an auction for an ENS name](#). Let's unlock MetaMask and start an auction for ethereumbook.eth:

Name

Actual Bid Amount

You must remember this to claim your name later.

Bid Mask

*This is the amount of ETH you send when placing your bid. It has no bearing on the *actual* amount you bid (above). It is simply to hide your real bid amount. It must be \geq to your actual bid.*

Secret Phrase

*You must remember this to claim your name later (feel free to change this)

Figure 51. Starting an auction for an ENS name



As mentioned in [Vickrey Auctions](#), you must reveal your bid within 48hrs after the auction is complete, or you **lose the funds in your bid**. Did we forget to do this and lose 0.1 ETH ourselves? You bet we did. Put a reminder on your calendar.

Let's make our bid. In order to do that we need to follow the steps in [Placing a bid for an ENS name](#):

You are about to start an auction & place a bid. ×

Screenshot & save first!

You cannot claim your name unless you have this information during the reveal process.



->
0.01



Name	ethereumbook.eth
Actual Bid Amount	0.01 ETH
Bid Mask	0.01 ETH
Secret Phrase	parent year thought
From Account	0x5ab7a6abe87f295224f517537dF760A894E81Afc
△ Reveal Date △	Wed Apr 18 2018 09:05:29 GMT-0500 (CDT)
Auction Ends	Fri Apr 20 2018 09:05:29 GMT-0500 (CDT)

Copy and save this:

```
{"name": "ethereumbook", "nameSHA3": "0x9c93995aece88698383037a9bd20857e8ec81a0da1f2c132bdc99c1d2454d1e5", "owner": "0x5ab7a6abe87f295224f517537df760a894e81afc", "value": "10000000000000000000", "secret": "parent year thought", "secretSHA3": "0xb7022c370a9d54b38bbc236fdff54786642ab1556d418"}▲ ▼
```

The ETH node you are sending through is provided by mycryptoapi.com.

Are you sure you want to do this?

No, get me out of here!

Yes, I am sure! Make transaction.

Figure 52. Placing a bid for an ENS name

Take a screenshot, save your secret phrase (as a backup for your bid), and **add a reminder in your calendar for the reveal date and time**, so you don't forget and lose your funds.

When you're ready, select the big green submit button in the [MetaMask transaction containing your bid](#):

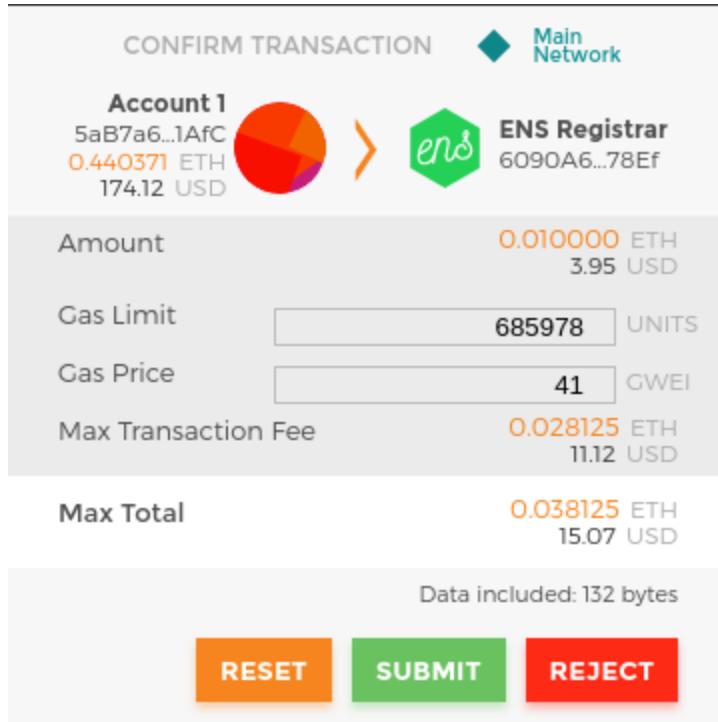


Figure 53. MetaMask transaction containing your bid

If all goes well, return and reveal the bid in 48 hours and the name is now registered to your Ethereum address.

Managing your ENS name

Now that we have registered an ENS name, we can manage it using another user-friendly interface, by visiting: <https://manager.ens.domains/>

Once there, enter the name you want to manage in the search box. You need to have your Ethereum wallet (e.g. MetaMask) unlocked, so that the ENS manager DApp can manage the name on your behalf using the [The ENS Manager web interface](#):



Figure 54. The ENS Manager web interface

From this interface, we can create subdomains, set a resolver contracts (more on that later) and connect each name to the appropriate resource, such as the Swarm address of a DApp front-end.

Creating an ENS subdomain

First, let's create a subdomain for our example Auction DApp, (see [Adding the subdomain auction.ethereumbook.eth](#)). We will name the subdomain auction, so the fully qualified name will be auction.ethereumbook.eth:

ENS Manager

ethereumbook.eth

Get Details

Node Details

Resolver Details

Name: ethereumbook.eth

Owner: 0x5ab7a6abe87f295224f517537df760a894e81afc

Resolver: 0x1da022710df5002339274aadee8d58218e9d6ab5

0x...

Update owner

Set Resolver

Use default resolver

Check for subdomain

auction

Create new subdomain



Figure 55. Adding the subdomain auction.ethereumbook.eth

Once you create the subdomain, you enter auction.ethereumbook.eth in the search box and now you can manage the subdomain, just as we managed the domain ethereumbook.eth previously.

ENS Resolvers

In ENS, resolving a name is a two-step process:

1. The ENS registry is called with the name to resolve after hashing it. If the record exists, the registry returns the address of its resolver.
2. The resolver is called, using the method appropriate to the resource being requested. The resolver returns the desired result.

This two-step process has several benefits. By separating the functionality of resolvers from the naming system itself, we have a lot more flexibility. The owners of names can use custom resolvers to resolve any type or resource, extending the functionality of ENS. For example, if in the future you wanted to link a geolocation resource (longitude/latitude) to an ENS name, you could create a new resolver that answers a geolocation query. Who knows what applications might be useful in the future? With custom resolvers, the only limitation is your imagination.

For convenience, there is a default public resolver that can resolve a variety of resources including:

- Address (for wallets or contracts)
- Content (a Swarm hash for DApps or contract source code)

Since we want to link our Auction DApp to a Swarm hash, we can use the public resolver, which supports content resolution, and don't need to code or deploy a custom resolver. See [Set the default public resolver for auction.ethereumbook.eth](#).

Let's set our auction.ethereumbook.eth name to use the public resolver:

ENS Manager

auction.ethereumbook.eth

Get Details

Node Details

Resolver Details

Name: ethereumbook.eth

Owner: 0x5ab7a6abe87f295224f517537df760a894e81afc

Resolver: 0x1da022710df5002339274aaddee8d58218e9d6ab5

0x...

Update owner

0x5ffc014343cd971b7eb70732021e26c35t

Set Resolver

Use default resolver



Figure 56. Set the default public resolver for auction.ethereumbook.eth

Resolving a name to a Swarm hash (content)

Once the resolver for auction.ethereumbook.eth is set to be the public resolver, we can set it to return the Swarm hash as the content of our name, see [Set the 'content' return for auction.ethereumbook.eth](#):

ENS Manager

auction.ethereumbook.eth

Get Details

Node Details

Resolver Details

Name: auction.ethereumbook.eth

Owner: 0x5ab7a6abe87f295224f517537df760a894e81afc

Resolver: 0x5ffc014343cd971b7eb70732021e26c35b744cc4

Address: 0x000

Content: 0x000

Set Addr

0x512ada039e1fb518e4ba50b130ff99ad47

Set Content



Figure 57. Set the 'content' return for auction.ethereumbook.eth

Wait a short time for your transaction to be confirmed and you should be able to resolve the name

correctly. Before setting a name, our Auction DApp could be found on a Swarm gateway by its hash:

<https://swarm-gateways.net/>

bzz:ab164cf37dc10647e43a233486cdeffa8334b026e32a480dd9cbd020c12d4581

or by searching in a DApp browser or Swarm gateway for the Swarm URL:

bzz://ab164cf37dc10647e43a233486cdeffa8334b026e32a480dd9cbd020c12d4581

Now that we have attached it to a name, it is much easier:

<http://swarm-gateways.net/bzz:/auction.ethereumbook.eth/>

or, by search for "auction.ethereumbook.eth" in any ENS compatible wallet or DApp browser (e.g. Mist).

From App to DApp

Over the past several sections, we have gradually built a Decentralized Application. We started with a pair of smart contracts to run an auction for ERC721 deeds. These contracts were designed to have no governing or privileged accounts, so that their operation is truly decentralized. We added a front-end, implemented in JavaScript, that offers a convenient and user friendly interface to our DApp. We added a decentralized storage system with Swarm, to store application resources such as images. We added a decentralized communication system using Whisper, to deliver a chat room function for each auction, without any central servers.

Next, we uploaded the entire front-end to Swarm, so that our DApp doesn't rely on any web servers to serve the files. Finally, we use allocated a name for our DApp using ENS, connecting it to the Swarm hash of the front-end, so that users can access it with a simple and easy-to-remember human-readable name.

With each of these steps, we increased the decentralization of our application. The final result is a DApp that has no central point of authority, no central point of failure and expresses the "web3" vision.

Here's the final [Auction DApp architecture](#):

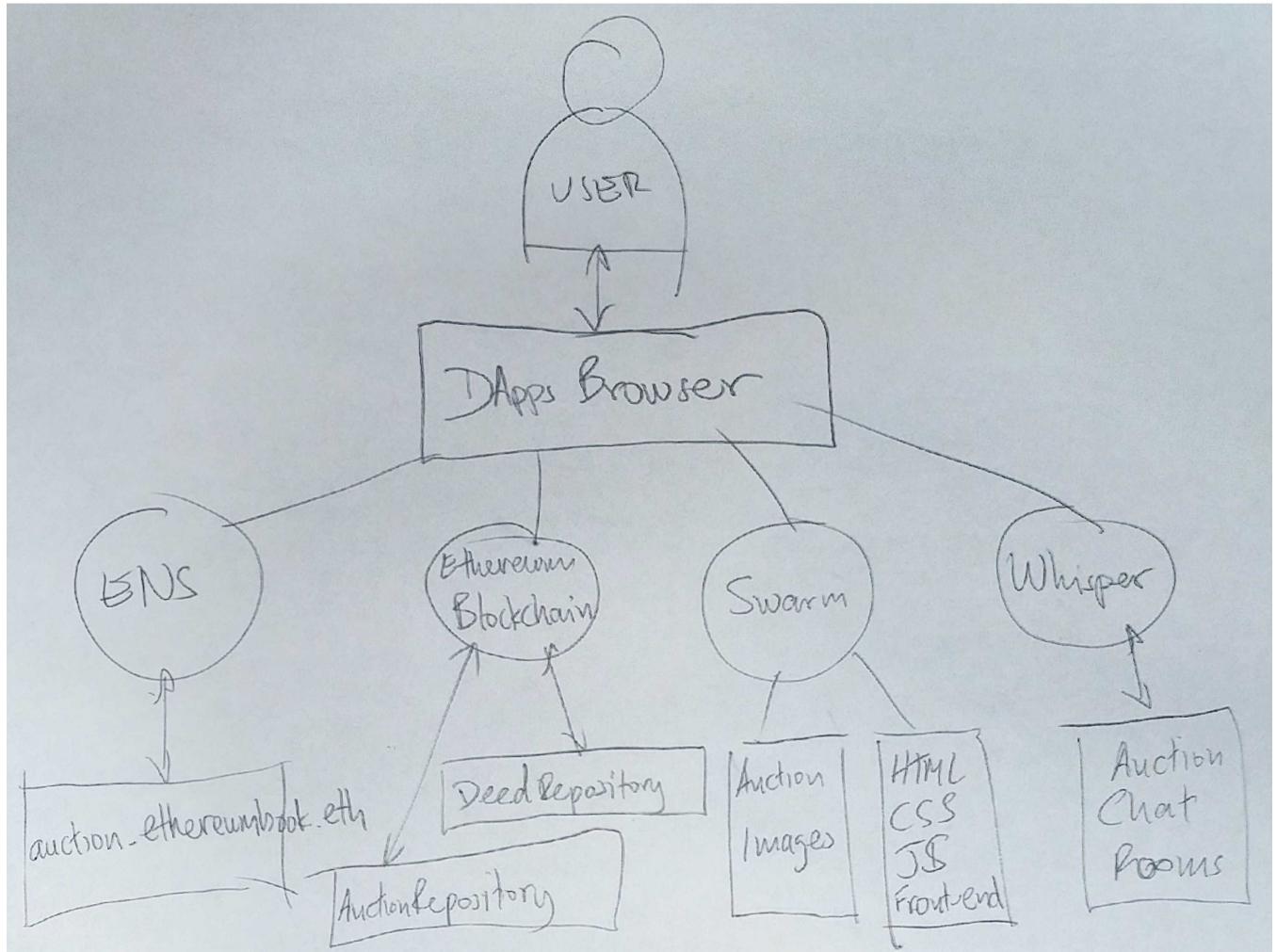


Figure 58. Auction DApp architecture

Conclusions

Decentralized applications are the culmination of the Ethereum vision, as expressed by the founders from the very earliest designs. While a lot of applications call themselves "DApps" today, most are not fully decentralized. However, it is already possible to construct applications that are almost completely decentralized. Over time, as the technology matures further, more and more of our applications can be decentralized, resulting in a more resilient, censorship resistant and free web.

The Ethereum Virtual Machine

At the heart of the Ethereum protocol and operation is the Ethereum Virtual Machine, or EVM for short. As you might guess from the name, it is a computation engine, not hugely dissimilar to the virtual machines of Microsoft's .NET framework or LLVM, or interpreters of other byte-code-compiled programming languages, such as Java. In this chapter we take a detailed look at the EVM, including its instruction set, structure and operation within the context of Ethereum state updates.

What is it?

The EVM is the part of Ethereum that handles smart contract deployment and execution. Simple value transfer transactions from one EOA to another don't need to involve it, practically speaking, but everything else will involve a state update computed by the EVM. At a high level, the EVM running on the Ethereum blockchain can be thought of as a global decentralized computer containing millions of executable objects, each with its own permanent data store.

The EVM is a quasi-Turing-complete state machine; "quasi" because all execution processes are limited to a finite number of computational steps by the amount of gas available for any given smart contract execution. As such, the halting problem is "solved" (all program executions will halt) and the situation where execution might (accidentally or maliciously) run forever (thus bringing the Ethereum platform to halt in its entirety) is avoided.

The EVM has a stack-based architecture, storing all in-memory values on a stack. It works with a word size of 256 bits (mainly to facilitate native hashing and elliptic curve operations) and has several addressable data components:

1. An immutable program code ROM, loaded with the bytecode of the smart contract to be executed
2. A volatile *memory*, with every location explicitly initialized to zero
3. A permanent *storage* that is part of the Ethereum state, also zero-initialized

There is also a set of environment variables and data that are available during execution. We will go through these in more detail in this chapter.

[The Ethereum Virtual Machine \(EVM\) Architecture and Execution Context](#) shows the EVM architecture and execution context:

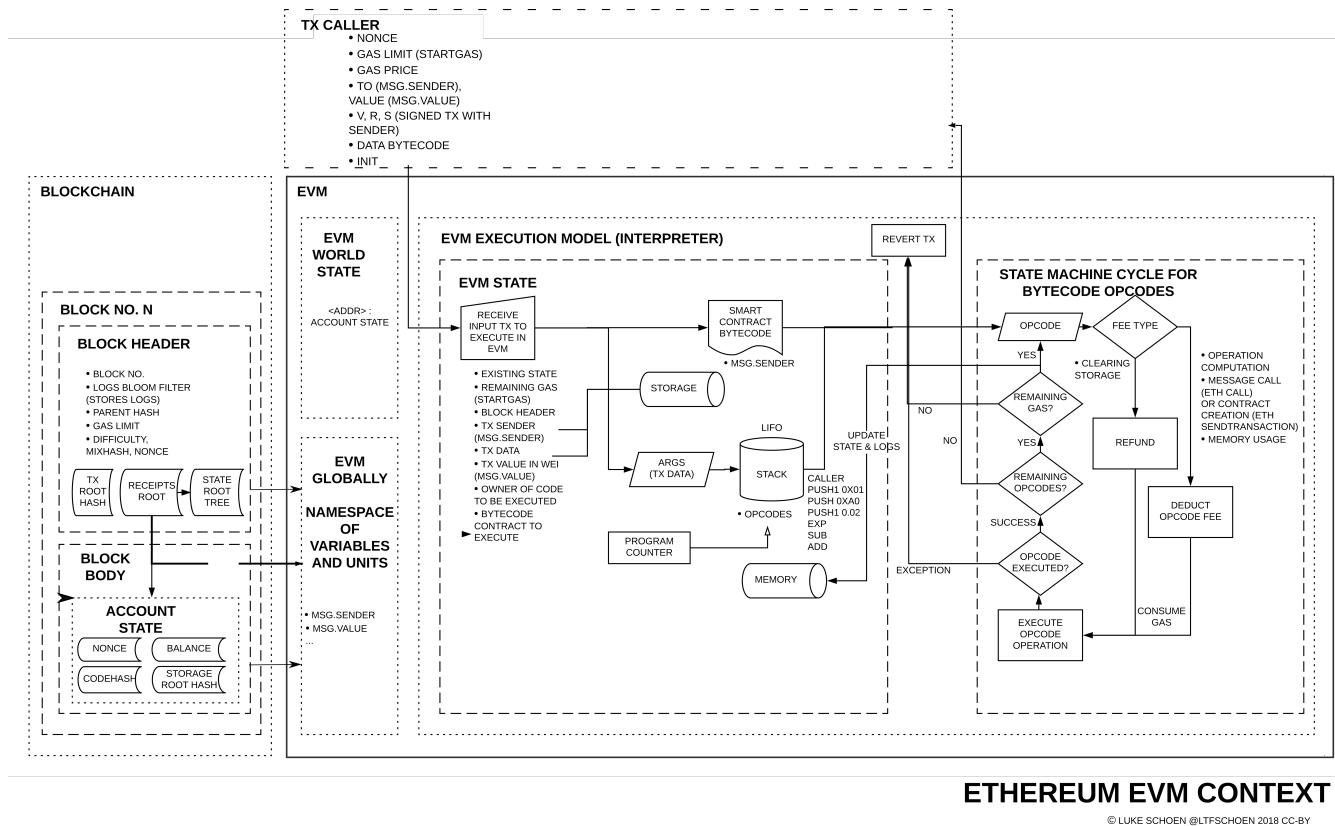


Figure 59. The Ethereum Virtual Machine (EVM) Architecture and Execution Context

Comparison with Existing Technology

The term "virtual machine" is often applied to the virtualization of a real computer, typically by a "hypervisor" such as VirtualBox or QEMU, or of an entire operating system instance, such as Linux's KVM. These must provide a software abstraction, respectively, of actual hardware, and of system calls and other kernel functionality.

The EVM operates in a much more limited domain: it is just a computation engine, and as such provides an abstraction of just computation and storage, similar to the Java Virtual Machine (JVM) specification, for example. From a high-level viewpoint, the JVM is designed to provide a runtime environment that is agnostic of the underlying host OS or hardware, enabling compatibility across a wide variety of systems. High level programming languages such as Java or Scala (that use the JVM), or C# (that uses .NET) are compiled into the bytecode instruction set of their respective virtual machine. In the same way, the EVM executes its own bytecode instruction set (which we will look at below) which higher level

smart contract programming languages, such as LLL, Serpent, Mutan or Solidity, are compiled into.

The EVM, therefore, has no scheduling capability, because execution ordering is organized externally to it - Ethereum clients run through verified block transactions to determine which smart contracts need executing and in which order. In this sense, the Ethereum world computer is single-threaded, like JavaScript. Neither does the EVM have any "system interface" handling or "hardware support" - there is no physical machine to interface with. The Ethereum world computer is completely virtual.

The EVM Instruction Set (Bytecode Operations)

The EVM instruction set offers most of the operations you might expect, including:

- arithmetic and bitwise logic operations
- execution context inquiries
- stack, memory, and storage access
- control flow operations
- logging, calling and other operators

In addition to the typical bytecode operations, the EVM also has access to account information (e.g. address and balance), and block information (such as block number and current gas price).

Let's start our exploration of the EVM in more detail by looking at the available opcodes and what they do. As you might expect, all operands are taken from the stack, and the result (where applicable) is often put back on the top of the stack.

Arithmetic Operations

Arithmetic opcode instructions:

```
ADD      //Add the top two stack items
MUL      //Multiply the top two stack items
SUB      //Subtract the top two stack items
DIV      //Integer division
SDIV     //Signed integer division
MOD      //Modulo (remainder) operation
SMOD     //Signed modulo operation
ADDMOD   //Addition modulo any number
MULMOD   //Multiplication modulo any number
EXP      //Exponential operation
SIGNEXTEND //Extend the length of a two's complement signed integer
SHA3      //Compute the Keccak-256 hash of a block of memory
```

Note that all arithmetic is performed modulo 2^{256} (unless otherwise noted), and that the zero-th power of zero, 0^0 , is taken to be one.

Stack Operations

Stack, memory and storage management:

```
POP      //Remove the top item from the stack
MLOAD   //Load a word from memory
MSTORE  //Save a word to memory
MSTORE8 //Save a byte to memory
SLOAD   //Load a word from storage
SSTORE  //Save a word to storage
MSIZE   //Get the size of the active memory in bytes
PUSHx   //Place x-byte item on the stack, where x can be any integer from
        //1 to 32 (full word) inclusive
DUPx    //Duplicate the x-th stack item, where x can be any integer from
        //1 to 16 inclusive
SWAPx   //Exchange 1st and (x+1)-th stack items, where x can be any
        //integer from 1 to 16 inclusive
```

Process Flow Operations

Instructions for control flow:

```
STOP      //Halts execution
JUMP     //Set the program counter to any value
JUMPI    //Conditionally alter the program counter
PC       //Get the value of the program counter (prior to the increment
corresponding to this instruction)
JUMPDEST //Mark a valid destination for jumps
```

System Operations

Opcodes for the system executing the program:

```
LOGx      //Append a log record with +xx topics, where xx is any
integer from 0 to 4 inclusive
CREATE     //Create a new account with associated code
CALL       //Message-call into another account, i.e. run another
account's code
CALLCODE   //Message-call into this account with an another account's
code
RETURN     //Halt execution and return output data
DELEGATECALL //Message-call into this account with an alternative
account's code, but persisting the current values for sender and value
STATICCALL //Static message-call into an account
REVERT     //Halt execution reverting state changes but returning data
and remaining gas
INVALID    //The designated invalid instruction
SELFDESTRUCT //Halt execution and register account for deletion
```

Logic Operations

Opcodes for comparisons and bitwise logic:

```
LT      //Less-than comparison
GT      //Greater-than comparison
SLT     //Signed less-than comparison
SGT     //Signed greater-than comparison
EQ      //Equality comparison
ISZERO  //Simple not operator
AND     //Bitwise AND operation
OR      //Bitwise OR operation
XOR     //Bitwise XOR operation
NOT     //Bitwise NOT operation
BYTE    //Retrieve a single byte from a full-width 256 bit word
```

Environmental Operations

Opcodes dealing with execution environment information:

```

GAS           //Get the amount of available gas (after the reduction for
this instruction)
ADDRESS        //Get the address of the currently executing account
BALANCE        //Get the account balance of any given account
ORIGIN         //Get the address of the EOA that initiated this EVM
execution
CALLER         //Get the address of the caller immediately responsible
for this execution
CALLVALUE      //Get the ether amount deposited by the caller responsible
for this execution
CALLDATALOAD   //Get the input data sent by the caller responsible for
this execution
CALLDATASIZE   //Get the size of the input data
CALLDATACOPY   //Copy the input data to memory
CODESIZE       //Get the size of code running in the current environment
CODECOPY        //Copy the code running in the current environment to
memory
GASPRICE       //Get the gas price specified by the originating
transaction
EXTCODESIZE   //Get the size of any account's code
EXTCODECOPY    //Copy any account's code to memory
RETURNDATASIZE //Get the size of the output data from the previous call
in the current environment
RETURNDATACOPY //Copy of data output from the previous call to memory

```

Block Operations

Opcodes for accessing information on the current block:

```

BLOCKHASH     //Get the hash of one of the 256 most recently completed
blocks
COINBASE      //Get the block's beneficiary address for the block reward
TIMESTAMP     //Get the block's timestamp
NUMBER        //Get the block's number
DIFFICULTY    //Get the block's difficulty
GASLIMIT      //Get the block's gas limit

```

Ethereum State

The job of the EVM is to update the Ethereum state by computing valid state transitions as a result of smart contact code execution, as defined by the Ethereum protocol. This aspect leads to the description of Ethereum as a *transaction-based state machine*, which reflects the fact that external actors (i.e. account holders and miners) initiate state transitions by creating, accepting and ordering transactions. It is useful at this point to consider what constitutes the Ethereum state.

At the top level, we have the Ethereum *world state*. The world state is a mapping of Ethereum addresses (160 bit values) to *accounts*. At the lower level, each Ethereum address represents an account comprising an ether *balance* (stored as the number of Wei owned by the account), a *nonce* (representing the number of transactions successfully sent from this account if it is an EOA, or the number of contracts created by it if it is a contract account), the account's *storage* (which is a permanent data store, only used by smart contracts), and the account's *program code* (again, only if the account is a smart contract account). An EOA will always have no code and an empty storage.

When a transaction results in smart contract code execution, an EVM is instantiated with all the information required in relation to the current block being created and the specific transaction being processed. In particular, the EVM's program code ROM is loaded with the code of the contract account being called, the program counter is set to zero, the storage is loaded from the contract account's storage, the memory is set to all zeros and all the block and environment variables are set. A key variable is the gas supply for this execution, and it is set to the amount of gas paid for by the sender at the start of the transaction (see [Gas](#) for more details). As code execution progresses, the gas supply is reduced according to the gas cost of the operations executed. If at any point the gas supply is reduced to zero we get an "*Out of Gas*" (OOG) exception; execution immediately halts and the transaction is abandoned. No changes to the Ethereum state are applied, except for the sender's nonce being incremented and their ether balance going down to pay the block's beneficiary for the resources used to execute the code to the halting point. At this point, you can think of the EVM running on a sand-boxed copy of the Ethereum world state, with this sand-boxed version being discarded completely if execution cannot complete for whatever reason. However, if execution does complete successfully, then the real world state is updated to match the sand-boxed version, including any changes to the called contract's storage data, any new contracts created and any ether balance transfers that were initiated.

Note that because a smart contract can itself effectively initiate transactions, code execution is a recursive process. A contract can call other contracts, with each call resulting in another EVM being instantiated around the new target of the call. Each instantiation has its sand-box world state initialized from the sand-box of the EVM at the level above. Each instantiation is also given a specified amount of

gas for its gas supply (not exceeding the amount of gas remaining in the level above, of course), and so may itself halt with an exception due to being given too little gas to complete its execution. Again, in such cases, the sand-box state is discarded, and execution returns to the EVM at the level above.

Compiling Solidity to EVM bytecode

Compiling a Solidity source file to EVM bytecode can be accomplished via several methods. In [Ethereum Basics](#) we used the online Remix compiler. In this chapter, we will use the solc executable at the command line. For a list of options, run the following command:

```
$ solc --help
```

Generating the raw opcode stream of a Solidity source file is easily achieved with the `--opcodes` command line option. This opcode stream leaves out some information (the `--asm` option produces the full information), but it is sufficient for this discussion. For example, compiling an example Solidity file `Example.sol` and sending the opcode output into a directory named `BytecodeDir` is accomplished with the following command:

```
$ solc -o BytecodeOutputDir --opcodes Example.sol
```

or

```
$ solc -o BytecodeOutputDir --asm Example.sol
```

The following command will produce the bytecode binary for our example program:

```
$ solc -o BytecodeOutputDir --bin Example.sol
```

The output opcode files generated will depend on the specific contracts contained within the Solidity source file. Our simple Solidity file `Example.sol` [[simple_solidity_example](#)] has only one contract, named "example".

```

pragma solidity ^0.4.19;

contract example {

    address contractOwner;

    function example() {
        contractOwner = msg.sender;
    }
}

```

As you can see, all this contract does is hold one persistent state variable, which is set as the address of the last account to run this contract.

If you look in the BytecodeDir directory, you will see the opcode file example.opcode (see [\[simple_solidity_example\]](#)) which contains the EVM opcode instructions of the "example" contract. Opening the example.opcode file in a text editor will show the following:

```

PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE ISZERO PUSH1 0xE JUMPI PUSH1 0x0
DUP1 REVERT JUMPDEST CALLER PUSH1 0x0 DUP1 PUSH2 0x100 EXP DUP2 SLOAD
DUP2 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFF MUL NOT AND SWAP1
DUP4 PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFF AND MUL OR SWAP1
SSTORE POP PUSH1 0x35 DUP1 PUSH1 0x5B PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN
STOP PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0x0 DUP1 REVERT STOP LOG1 PUSH6
0x627A7A723058 KECCAK256 JUMP 0xb9 SWAP14 0xcb 0x1e 0xdd RETURNDATACOPY
0xec 0xe0 0x1f 0x27 0xc9 PUSH5 0x9C5ABCC14A NUMBER 0x5e INVALID
EXTCODESIZE 0xdb 0xcf EXTCODESIZE 0x27 EXTCODESIZE 0xe2 0xb8 SWAP10 0xed
0x

```

Compiling the example with the --asm option produces a file named example.evm in our BytecodeDir directory. This contains a slightly higher level description of the EVM bytecode instructions, together with some helpful annotations:

```

/* "Example.sol":26:132  contract example {... */
    mstore(0x40, 0x60)
/* "Example.sol":74:130  function example() {... */

```

```
jumpi(tag_1, iszero(callvalue))
0x0
dup1
revert
tag_1:
    /* "Example.sol":115:125 msg.sender */
caller
    /* "Example.sol":99:112 contractOwner */
0x0
dup1
    /* "Example.sol":99:125 contractOwner = msg.sender */
0x100
exp
dup2
sload
dup2
0xffffffffffffffffffffffffffff
mul
not
and
swap1
dup4
0xffffffffffffffffffff
and
mul
or
swap1
sstore
pop
    /* "Example.sol":26:132 contract example {... */
dataSize(sub_0)
dup1
dataOffset(sub_0)
0x0
codecopy
0x0
return
stop
```

```
sub_0: assembly {
    /* "Example.sol":26:132 contract example {... */
    mstore(0x40, 0x60)
    0x0
    dup1
    revert

    auxdata:
0xa165627a7a7230582056b99dcb1edd3eece01f27c9649c5abcc14a435efe3bdbcf3b273
be2b899eda90029
}
```

The --bin-runtime option produces the machine readable hexadecimal bytecode:

```
60606040523415600e57600080fd5b336000806101000a81548173
ffffffffffffffffffffffffff
021916908373
ffffffffffffffffffff
160217905550603580605b6000396000f3006060604052600080fd00a165627a7a7230582
056b99dcb1e
```

You can investigate what's going on here in detail using the opcode list given above in [The EVM Instruction Set \(Bytecode Operations\)](#). However, that's quite a task, so let's just start by examining the first four instructions as listed in [\[opcode_output\]](#):

```
PUSH1 0x60 PUSH1 0x40 MSTORE CALLVALUE
```

Here we have PUSH1 followed with a raw byte of value 0x60. This corresponds to the EVM instruction which takes the single byte following the opcode in the program code (as a literal value) and pushing it onto the stack. It is possible to push values of size up to 32 bytes onto the stack, e.g.: PUSH32 0x436f6e67726174756c6174696f6e732120536f6f6e20746f206d617374657221.

The second PUSH1 opcode from [\[opcode_output\]](#) stores 0x40 onto the top of the stack (pushing the 0x60 already present there down one slot).

Next is MSTORE, which is a memory store operation that saves a value to the EVM's memory. It takes

two arguments and, like most EVM operations, obtains them from on the stack. For each argument the stack is popped, i.e. the top value on the stack is taken off and all the other values on the stack are shifted up one position. The first argument for MSTORE is the address of the word in memory where the value to be saved will be put. For this program we have 0x40, so that is removed from the stack and used as the memory address. The second argument is the value to be saved, which is 0x60 here. After the MSTORE is executed, our stack is empty again, but we have the value 0x60 (96 in decimal) at the memory location 0x40.

The next opcode is CALLVALUE, which is an environmental opcode that pushes onto the top of the stack the amount of ether (measured in Wei) sent with the message call that initiated this execution.

We could continue to step through this program in this way until we had a full understanding of the low level state changes that this code effects, but it wouldn't help us at this stage. We'll come back to it later in the chapter.

Contract Deployment Code

There is an important but subtle difference between the code used when creating and deploying a new contract on the Ethereum platform and the code of the contract itself. In order to create a new contract, a special transaction is needed that has its to field set to the special 0x0 address and its data field set to the contract's *initiation code*. When such a contract creation transaction is processed, the code for the new contract account is *not* the code in the data field of the transaction. Instead, an EVM is instantiated with the code in the data field of the transaction loaded into its program code ROM, and then the output of the execution of that deployment code is taken as the code for the new contract account. This is so that new contracts can be programmatically initialized using the Ethereum world state at the time of deployment, setting values in the contract's storage and even sending ether or creating further new contracts.

When compiling a contract offline, e.g. using solc on the command line, you can either get the *deployment bytecode* or the *runtime bytecode*.

The deployment bytecode is used for every aspect of the initialization of a new contract account, including the bytecode of what will actually end up being executed when transactions call this new contract (i.e. the runtime bytecode), and the code to initialize everything based on the contract's constructor.

The runtime bytecode, on the other hand, is exactly *the bytecode that ends up being executed when the new contract is called* and nothing more, i.e. it does not include the bytecode needed to initialize the contract during deployment.

Let's take the simple `Faucet.sol` contract we created earlier as an example.

```
// Version of Solidity compiler this program was written for
pragma solidity ^0.4.19;

// Our first contract is a faucet!
contract Faucet {

    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {

        // Limit withdrawal amount
        require(withdraw_amount <= 10000000000000000);

        // Send the amount to the address that requested it
        msg.sender.transfer(withdraw_amount);
    }

    // Accept any incoming amount
    function () public payable {}

}
```

To get the deployment bytecode, we would run `solc --bin Faucet.sol`. If we instead wanted just the runtime bytecode, we would run `solc --bin-runtime Faucet.sol`.

If you compare the output of these commands, you will see that the runtime bytecode is a subset of the deployment bytecode. In other words, the runtime bytecode is entirely contained within the deployment bytecode.

Disassembling the Bytecode

Disassembling EVM bytecode is a great way to understand how high-level Solidity acts in the EVM. There are a few disassemblers you can use to do this:

- **Porosity** is a popular open source decompiler: <https://github.com/comaeio/porosity>

- **Ethersplay** is an EVM plugin for Binary Ninja, a disassembler: <https://github.com/trailofbits/ethersplay>
 - **IDA-Evm** is an EVM plugin for IDA, another disassembler: <https://github.com/trailofbits/ida-evm>

In this section, we will be using the Ethersplay plugin for Binary Ninja and using it to start [Disassembling the Faucet runtime bytecode](#).

After getting the runtime bytecode of `Faucet.sol`, we can feed it into Binary Ninja (after loading the Ethersplay plugin) to see what the EVM instructions look like.

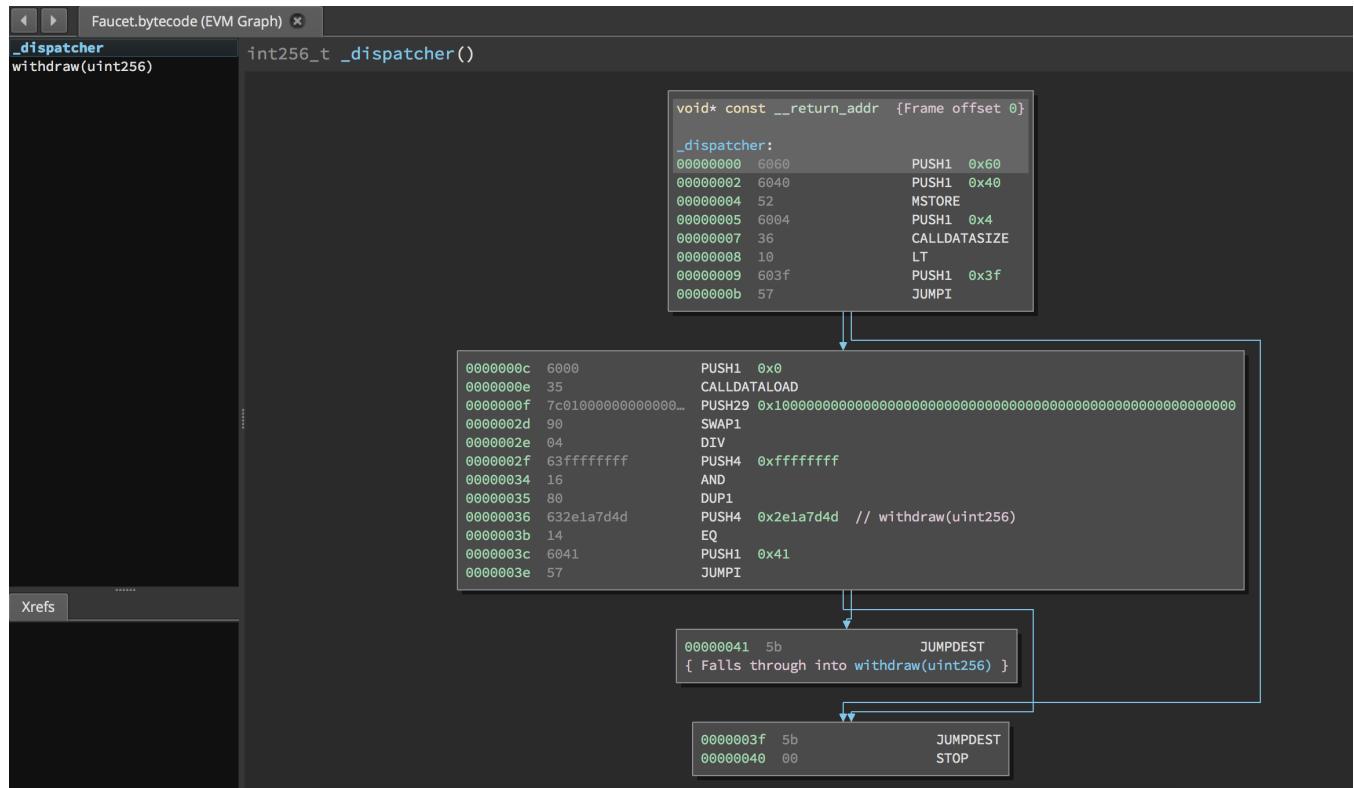


Figure 60. Disassembling the Faucet runtime bytecode

When you send a transaction to an ABI-compatible smart contract (which you can assume all contracts are), the transaction first interacts with that smart contract's *dispatcher*. The dispatcher reads in the data field of the transaction and sends the relevant part to the appropriate function. We can see an example of a dispatcher at the beginning of our disassembled Faucet.sol runtime bytecode. After the familiar MSTORE instruction, we see the following instructions:

```
PUSH1 0x4
CALLDATASIZE
LT
PUSH1 0x3f
JUMPI
```

As we have seen, PUSH1 0x4 places 0x4 onto the top of the stack, which is otherwise empty. CALLDATASIZE gets the size in bytes of the data sent with the transaction (known as the *calldata*) and pushes that number onto the stack. After these operations have been executed the stack looks like this:

Stack

<length of calldata from tx>

0x4

This next instruction is LT, short for “less than”. The LT instruction checks whether the top item on the stack is less than the next item on the stack. In our case, it checks to see if the result of CALLDATASIZE is less than 4 bytes.

Why does the EVM check to see that the calldata of the transaction is at least 4 bytes? Because of how function identifiers work. Each function is identified by the first four bytes of its keccak256 hash. By placing the function’s name and what arguments it takes into a keccak256 hash function, we can deduce its function identifier. In our case, we have:

```
keccak256("withdraw(uint256)") = 0x2e1a7d4d...
```

Thus, the function identifier for the withdraw(uint256) function is 0x2e1a7d4d, since these are the first four bytes of the resulting hash. A function identifier is always 4 bytes long, so if the entire data field of the transaction sent to the contract is less than 4 bytes, then there’s no function with which the transaction could possibly be communicating, unless a *fallback function* is defined. Because we implemented such a fallback function in Faucet.sol, the EVM jumps to this function when the calldata’s length is less than 4 bytes.

LT pops the top two values off the stack and, if the transaction’s data field is less than 4 bytes, pushes 1 onto it. Otherwise, it pushes 0. In our example, let’s assume the data field of the transaction sent to our contract was less than 4 bytes.

The PUSH1 0x3f instruction pushes the byte 0x3f onto the stack. After this instruction, the stack looks like this:

Stack

0x3f

1

The next instruction is JUMPI, which stands for "jump if". It works like so:

```
jumpi(label, cond) // Jump to "label" if "cond" is true
```

In our case, "label" is 0x3f, which is where our fallback function lives in our smart contract. The "cond" argument is 1, which was the result of the LT instruction earlier. To put this entire sequence into words, the contract jumps to the fallback function if the transaction data is less than 4 bytes.

At 0x3f, only a "STOP" instruction follows, because, although we declared a fallback function, we kept it empty. As you can see in [JUMPI instruction leading to fallback function](#), had we not implemented a fallback function, the contract would throw an exception instead.

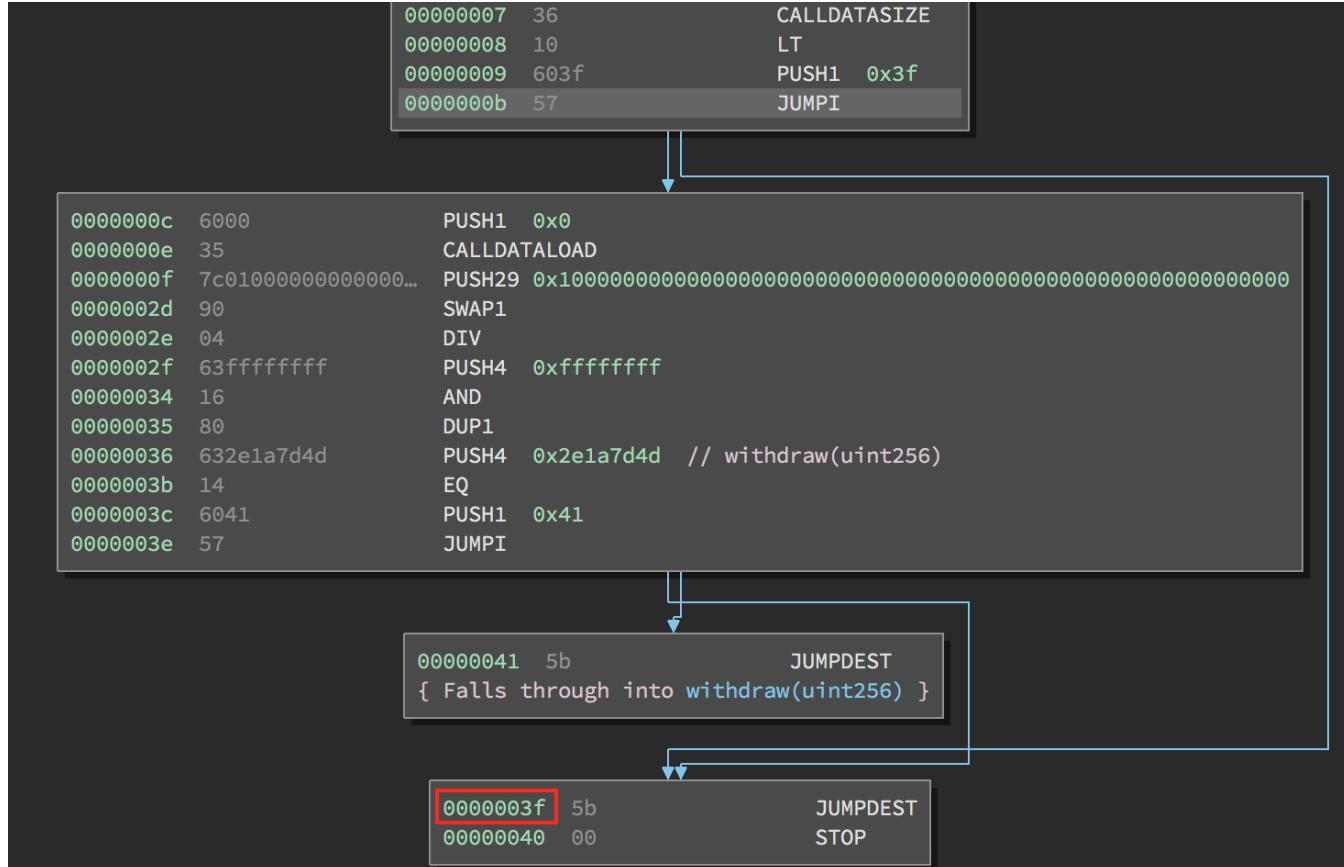


Figure 61. JUMPI instruction leading to fallback function

Let's examine the central block of the dispatcher. Assuming we received calldata that was greater than 4 bytes in length, the JUMPI instruction would not jump to the fallback function. Instead, code execution would proceed to the following instructions:

```
PUSH1 0x0
CALLDATALOAD
PUSH29 0x1000000...
SWAP1
DIV
PUSH4 0xffffffff
AND
DUP1
PUSH4 0x2e1a7d4d
EQ
PUSH1 0x41
JUMPI
```

PUSH1 0x0 pushes 0 onto the stack, which is now otherwise empty again. CALLDATALOAD accepts as an argument an index within the calldata sent to the smart contract and reads 32 bytes from that index, like so:

```
calldataload(p) //load 32 bytes of calldata starting from byte position p
```

Since 0 was the index passed to it from the PUSH1 0x0 command, CALLDATALOAD reads 32 bytes of calldata starting at byte 0, and then pushes it to the top of the stack (after popping the original 0x0). After the PUSH29 0x1000000... instruction, the stack is then:

Stack

0x1000000... (29 bytes in length)

32 bytes of calldata starting at byte 0

SWAP1 switches the top element on the stack with the *i*th element after it. In this case, it swaps 0x1000000... with the calldata. The new stack is:

Stack

32 bytes of calldata starting at byte 0

0x1000000... (29 bytes in length)

The next instruction is DIV, which works as follows:

```
div(x, y) // integer division x / y
```

In this case, $x = 32$ bytes of calldata starting at byte 0, and $y = 0x100000000\dots$ (29 bytes total). Can you think of why the dispatcher is doing the division? Here's a hint: we read 32 bytes from calldata earlier starting at index 0. The first four bytes of that calldata is the function identifier.

The $0x100000000\dots$ we pushed earlier is 29 bytes long, consisting of a 1 at the beginning, followed by all 0s. Dividing our 32 bytes of calldata by this $0x100000000\dots$ will leave us only the *topmost 4 bytes* of our calldata load starting at index 0. These four bytes—the first four bytes in the calldata starting at index 0—are the function identifier, and this is how the EVM extracts that field.

If this part isn't clear to you, think of it like this: in base_{10} , $1234000 / 1000 = 1234$. In base_{16} , this is no different. Instead of every place being a multiple of 10, it is a multiple of 16. Just as dividing by 10^3 (1000) in our smaller example kept only the topmost digits, dividing our 32 byte base_{16} value by 16^{29} does the same.

The result of the DIV (the function identifier) gets pushed on the stack, and our stack is now:

Stack

```
function identifier sent in data
```

Since the PUSH4 `0xffffffff` and AND instructions are redundant, we can ignore them entirely, as the stack will remain the same after they are done. The DUP1 instruction duplicates the 1st item on the stack, which is the function identifier. The next instruction, PUSH4 `0x2e1a7d4d`, pushes the pre-calculated function identifier of the withdraw(uint256) function onto the stack. The stack is now:

Stack

```
0x2e1a7d4d
```

```
function identifier sent in data
```

```
function identifier sent in data
```

The next instruction, EQ, pops off the top two items of the stack and compares them. This is where the dispatcher does its main job: it compares whether the function identifier sent in the msg.data field of the transaction matches that of withdraw(uint256). If they are equal, EQ pushes 1 onto the stack, which

will ultimately be used to jump to the withdraw function. Otherwise, EQ pushes 0 onto the stack.

Assuming the transaction sent to our contract indeed began with the function identifier for withdraw (uint256), our stack has become:

Stack

1

function identifier sent in data (now known to be 0x2e1a7d4d)

Next, we have PUSH1 0x41, which is the address at which the withdraw(uint256) function lives in the contract. After this instruction, the stack looks like this:

Stack

0x41

1

function identifier sent in msg.data

The JUMPI instruction is next, and it once again accepts the top two elements on the stack as arguments. In this case, we have jumpi(0x41, 1), which tells the EVM to execute the jump to the location of the withdraw(uint256) function, and the execution of that function's code can proceed.

Turing completeness and Gas

As we have already touched on, in simple terms, a system or programming language is *Turing complete* if it can run any program. This capability, however, comes with an very important caveat: some programs take forever to run. An important aspect of this is that we can't tell, just by looking at a program, whether it will take forever or not to execute. We have to actually go through with the execution of the program and wait for it to finish to find out. Of course, if it is going to take forever to execute, we will have to wait forever to find out. This is called "the halting problem" and would be a huge problem for Ethereum if it were not addressed.

Because of the halting problem, the Ethereum world computer is at risk of being asked to execute a program that never stops. This could be by accident or malice. We have discussed that Ethereum acts like a single-threaded machine, without any scheduler, and so if it became stuck in an infinite loop, this would mean it would become unusable.

However, with gas, there is a solution: if after a pre-specified maximum amount of computation has been performed, the execution hasn't ended, the execution of the program is halted by the EVM. This makes the EVM a *quasi-Turing* complete machine: it can run any program you feed into it, but only if the program terminates within a particular amount of computation. That limit isn't fixed in Ethereum - you can pay to increase it up to a maximum (called the "block gas limit") and everyone can agree to increase that maximum over time. Nevertheless, at any one time, there is a limit in place, and transactions that consume too much gas while executing are halted.

In the following sections, we will look at gas and examine how it works in detail.

Gas

Gas is Ethereum's unit for measuring the computational and storage resources required to perform actions on the Ethereum blockchain. In contrast to Bitcoin, whose transaction fees only take into account the size of a transaction in kilobytes, Ethereum must account for every computational step performed by transactions and smart contract code execution.

Each operation performed by a transaction or contract costs a fixed amount of gas. Some examples, from the Ethereum yellow paper:

- Adding two numbers costs 3 gas
- Calculating a Keccak256 hash costs 30 gas + 6 gas for each 256 bits of data being hashed
- Sending a transaction costs 21,000 gas

Gas is a crucial component of Ethereum, and serves a dual role: as a buffer between the (volatile) price of Ethereum and the reward to miners for the work they do, and as a defense against denial of service attacks. To prevent accidental or malicious infinite loops or other computational wastage in the network, the initiator of each transaction is required to set a limit to the amount of computation they are willing to pay for. The gas system thereby disincentivizes attackers from sending "spam" transactions, as they must pay proportionately for the computational, bandwidth, and storage resources that they consume.

Gas Accounting During Execution

When an EVM is needed to complete a transaction, in the first instance it is given a gas supply equal to the amount specified by the gas limit in the transaction. Every opcode that is executed has a cost in gas, and so the EVM's gas supply is reduced as the EVM steps through the program. Before each operation,

the EVM checks that there is enough gas to pay for the operation's execution. If there isn't enough gas, execution is halted and the transaction is reverted. The originator of the transaction still pays for all the gas used at the specified gas price, however.

If the EVM reaches the end of execution successfully, without running out of gas, the gas cost used is paid to the miner as a transaction fee, converted to ether based on the gas price specified in the transaction:

```
miner fee = gas cost * gas price
```

The gas remaining in the gas supply is refunded to the sender, again converted to ether based on the gas price specified in the transaction:

```
remaining gas = gas limit - gas cost  
refunded ether = remaining gas * gas price
```

If the gas used exceeds the specified gas limit at any point, i.e. if the transaction "runs out of gas" during execution, the operation is immediately terminated, raising the exception "Out of Gas". The transaction is reverted and all changes to the state are rolled back.

Although the transaction was unsuccessful, the sender will be charged a transaction fee, as miners have already performed the computational work up to that point, and must be compensated for doing so.

Gas accounting considerations

The relative gas costs of the various operations that can be performed by the EVM have been carefully chosen to best protect the Ethereum blockchain from attack. You can see a detailed table of gas costs for different EVM opcodes in [EVM OpCodes and Gas Cost](#).

More computationally intensive operations cost more gas. For example, executing the SHA3 function is ten times more expensive (30 gas) than the ADD operation (3 gas). More importantly, some operations such as EXP require an additional payment based on the size of the operand. There is also a gas cost to using EVM memory and for storing data in a contract's on-chain storage.

The importance of matching gas cost to the real-world cost of resources was demonstrated in 2016 when an attacker found and exploited a mismatch in costs. The attack generated transactions that were

very computationally expensive, and made the Ethereum mainnet almost grind to a halt. This mismatch was resolved by a hard fork (codenamed "Tangerine Whistle") that tweaked the relative gas costs.

Gas cost vs. gas price

While the gas *cost* is a measure of computation and storage used in the EVM, the gas itself also has a *price* measured in ether. When performing a transaction, the sender specifies the gas price they are willing to pay (in ether) for each unit of gas, allowing the market to decide the relationship between the price of ether and the cost of computing operations (as measured in gas).

transaction fee = total gas used * gas price paid (in ether)

When constructing a new block, miners on the Ethereum network can choose among pending transactions by selecting those which offer to pay a higher gas price. Offering a higher gas price will therefore incentivize miners to include your transaction and get it confirmed faster.

In practice, the sender of a transaction will set a gas limit that is higher than or equal to the gas expected to be used. If the gas limit is set higher than the amount of gas consumed, the sender will receive a refund of the excess amount, as miners are only compensated for the work they actually perform.

At the end of

It is important to be clear about the distinction between the *gas cost* and the *gas price*:

gas cost - the number of units of gas required to perform a particular operation

gas price - the amount of ether you are willing to pay per unit of gas when you send your transaction to the Ethereum network



While gas has a price, it cannot be "owned" nor "spent". Gas exists only inside the Ethereum Virtual Machine (EVM) as a count of how much computational work is being performed. The sender is charged a transaction fee in ether, which is then converted to gas for EVM accounting and then back to ether as a transaction fee paid to the miners.

Negative gas cost

Ethereum encourages the deletion of used storage variables and accounts by refunding some of the gas used during contract execution.

There are 2 operations in the EVM with negative gas costs:

1. Deleting a contract (SELFDESTRUCT) is worth a refund of 24,000 gas
2. Changing a storage address from a non-zero value to zero (SSTORE[x] = 0) is worth a refund of 15,000 gas

To avoid exploitation of the refund mechanism, the maximum refund for a transaction is set to half the total amount of gas used (rounded down).

Block gas limit

The block gas limit is the maximum amount of gas that may be consumed by all the transactions in a block, and constrains how many transactions can fit into a block.

For example, let's say we have 5 transactions whose gas limits have been set to 30,000, 30,000, 40,000, 50,000 and 50,000. If the block gas limit is 180,000, then any four of those transactions can fit in a block, while the fifth will have to wait for a future block. As previously discussed, miners decide which transactions to include in a block. Different miners are likely to select different combinations, mainly because they receive transactions from the network in a different order.

If a miner tries to include a transaction that requires more gas than the current block gas limit, the block will be rejected by the network. Most Ethereum clients will stop you from issuing such a transaction by giving a warning along the lines of "transaction exceeds block gas limit". The block gas limit on the Ethereum mainnet is 8 million gas at the time of writing according to <https://etherscan.io>, meaning that around 380 basic transactions (each consuming 21,000 gas) could fit into a block.

Who decides what the block gas limit is?

The miners on the network collectively decide the block gas limit. Individuals who want to mine on the Ethereum network use a mining program, such as ethminer, which connects to a Geth or Parity Ethereum client. The Ethereum protocol has a built-in mechanism where miners can vote on the gas limit so capacity can be increased or decreased in subsequent blocks. The miner of a block can vote to adjust the block gas limit by a factor of 1/1024 (0.0976%) in either direction. The result of this is an

adjustable block size based on the needs of the network at the time. This mechanism is coupled with a default mining strategy where miners vote on a gas limit which is at least 4.7 million gas, but which targets a value of 150% of the average of recent total gas usage per block (using a 1024-block exponential moving average).

Conclusions

In this chapter we have worked with the Ethereum Virtual Machine, tracing the execution of various smart contracts and looking at how the EVM executes bytecode. We also look at gas, the EVM's accounting mechanism and how it solves the halting problem and protects Ethereum from denial of service attacks. Next, in [Consensus](#), we look at the mechanism used by Ethereum to achieve decentralized consensus.

Consensus

Throughout this book we have talked about the "consensus rules" that are the rules that everyone must agree to, for the system to operate in a decentralized, yet deterministic, manner. In computer science, the term *consensus* predates blockchains and is related to the broader problem of synchronizing state in distributed systems, such that different participants in a distributed system all (eventually) agree on a single system-wide state. This is called "reaching consensus".

When it comes to the core function of decentralized record keeping and verification, it can become problematic to rely on trust alone to ensure that information derived from state updates is correct. This rather general challenge is particularly pronounced in decentralized networks because there is no central entity to decide what is true. The lack of a central decision-making entity is one of the main attractions of blockchain platforms, because of the resulting capacity to resist censorship and the lack of dependence on authority for permission to access information. However, these benefits come at a cost: without a trusted arbitrator, any disagreements, deceptions or differences need to be reconciled using other means. Consensus algorithms are the mechanism used to reconcile security and decentralization.

In blockchains, consensus is a critical property of the system. Simply put, there is money at stake! So, in the context of blockchains, *consensus* is about being able to arrive at a common state, while maintaining decentralization. In other words, consensus is intended to produce a system of *strict rules without rulers*. There is no one person, organization or group "in charge", rather power and control is diffused across a broad network of participants, whose self interest is served by following the rules and behaving honestly.

The ability to come to consensus across a distributed network, under adversarial conditions, without centralizing control, is the core principle of all open public blockchains. To address this challenge and maintain the valued property of decentralization, the community continues to experiment with different models of consensus. This chapter explores these consensus models and their expected impact on smart contract blockchains such as Ethereum.



While consensus algorithms are an important part of how blockchains work, they operate at a foundational layer, far below the abstraction of smart contracts. In other words, most of the details of consensus are hidden from the writers of smart contracts. You don't need to know how they work to use Ethereum, anymore than you need to know how routing works to use the internet.

Consensus via proof of work (PoW)

The creator of the original blockchain, Bitcoin, invented a *consensus algorithm* called *Proof of Work (PoW)*. Arguably, PoW is the most important invention underpinning Bitcoin. The colloquial term for PoW is "mining", which creates a misunderstanding about the primary purpose of consensus. Often people assume that the purpose of mining is the creation of new currency, since the purpose of real-world mining is the extraction of precious metals or other resources. Rather, the real purpose of mining (and all other consensus models) is to **secure the blockchain**, while keeping control over the system decentralized and diffused across as many participants as possible. The reward of newly minted currency is an incentive system whose purpose is to reward those who contribute to the security of the system: a means to an end. In that sense, the reward is the means and decentralized security is the end. In PoW consensus there is also a corresponding "punishment", which is the cost of energy required to participate in mining. If participants do not follow the rules and earn the reward, they risk the funds they have already spent on electricity to mine. Thus, PoW consensus is a careful balance of risk and reward that drives participants to behave honestly out of self interest.

Ethereum is currently a PoW blockchain, in that it uses a PoW algorithm with the same basic incentive system for the same basic goal: securing the blockchain while decentralizing control. Ethereum's PoW algorithm is slightly different than Bitcoin's and is called *Ethash*. We will examine the function and design characteristics of *Ethash* in [Ethash: Ethereum's proof of work](#).

Consensus via proof of stake (PoS)

Historically, proof of work was not the first consensus algorithm proposed. Preceding the introduction of proof of work, many researchers had proposed variations of consensus algorithms based on financial stake, now called *Proof of Stake (PoS)*. In some respect, proof of work was invented as an alternative to proof of stake. After the success shown by Bitcoin, many blockchains have emulated proof of work. Yet, the explosion of research into consensus algorithms has also resurrected proof of stake, significantly advancing the state of the technology. From the beginning, Ethereum founders were hoping to eventually migrate Ethereum's consensus algorithm to proof of stake. In fact, there is a deliberate handicap on Ethereum's proof of work called the *difficulty bomb*, intended to gradually make proof of work mining of Ethereum more and more difficult, thereby forcing the transition to proof of stake.

At the time of publication of this book, Ethereum is still using proof of work, but the ongoing research towards a proof of stake alternative is nearing completion. Ethereum's planned proof of stake algorithm is called *Casper*. The introduction of Casper as a replacement of Ethash has been postponed several times over the past 2 years, necessitating interventions to defuse the difficulty bomb and postpone its

forced obsolescence of proof of work.

In general, a PoS algorithm works as follows. The blockchain keeps track of a set of validators, and anyone who holds the blockchain's base cryptocurrency (in Ethereum's case, ether) can become a validator by sending a special type of transaction that locks up their ether into a deposit. The validators take turns proposing and voting on the next valid block, and the weight of each validator's vote depends on the size of its deposit (i.e. stake). Importantly, a validator risks losing their deposit if the block they staked it on is rejected by the majority of validators. Conversely, validators earn a small reward, proportional to their deposited stake, for every block that is accepted by the majority. Thus, PoS forces validators to act honestly and follow the consensus rules, by a system of reward and punishment. The major difference between PoS and PoW is that the punishment in PoS is intrinsic to the blockchain (e.g. loss of staked ether), whereas in PoW the punishment is extrinsic (e.g. loss of funds spent on electricity).

Ethash: Ethereum's proof of work

Ethash is the Ethereum Proof-of-Work (PoW) algorithm and uses an evolution of the Dagger–Hashimoto Algorithm, which is a combination of Vitalik Buterin's Dagger algorithm and Thaddeus Dryja's Hashimoto algorithm. Ethash is dependent on the generation and analysis of a large dataset, known as a *Directed Acyclic Graph* or more simply *the DAG*. The DAG had an initial size of about 1GB and will continue to slowly and linearly grow in size, being updated once every *epoch* (30,000 blocks, or roughly 125 hours).

The purpose of the DAG is to make the Ethash PoW algorithm dependent on maintaining a large, frequently accessed data structure. This in turn is intended to make Ethash "ASIC resistant", which means that it is more difficult to make *Application Specific Integrated Circuits (ASIC)* mining equipment that is orders of magnitude faster than a fast *Graphics Processing Unit (GPU)*. Ethereum's founders wanted to avoid centralization in PoW mining, where those with access to specialized silicon fabrication factories and big budgets could dominate the mining infrastructure and undermine the security of the consensus algorithm.

Use of consumer-level GPUs for carrying out the PoW on the Ethereum network means that more people around the world can participate in the mining process. The more independent miners there are, the more decentralized the mining power and we can avoid a situation like Bitcoin's mining, where much of the mining power is concentrated in the hands of a few large industrial mining operations. The downside of the use of GPUs for mining is that it precipitated a worldwide shortage GPUs in 2017, causing their price to skyrocket and an outcry from gamers. This led to purchase restrictions at retailers limiting buyers to a one or two GPUs per customer.

Until recently, the threat of Application-Specific Integrated Circuit (ASIC) miners on the Ethereum network was largely non-existent. To use ASICs for Ethereum requires the design, manufacture, and distribution of highly customized hardware. Producing them requires considerable investment of time and money. The Ethereum developers' long-expressed plans to move to a PoS consensus algorithm likely kept ASIC suppliers away from targeting the Ethereum network for a long time. As soon as Ethereum moves to PoS, ASICs designed for the PoW algorithm will be rendered useless—that is, unless miners can use them to mine other cryptocurrencies instead. The latter possibility is now a reality with a range of other Ethash-based consensus coins available, such as PIRL, Ubiq, and of course Ethereum Classic, which has pledged to remain a PoW blockchain for the foreseeable future. This means that we will likely see ASIC mining begin to become a force on the Ethereum network while it is still operating on PoW consensus.

Casper: Ethereum's proof of stake

Casper is the proposed name for Ethereum's proof of stake consensus algorithm. It is still under active research and development and is not implemented on the Ethereum blockchain at the time of publication of this book. Casper is being developed in two competing "flavors":

- Casper FFG: "The Friendly Finality Gadget"
- Casper CBC: "The Friendly GHOST / Correct-By-Construction"

Initially, Casper FFG was proposed as a hybrid PoW/PoS algorithm to be implemented first, as a transition to a more permanent "pure PoS" algorithm, later. In June 2018, Vitalik Buterin, who was leading the research work on Casper FFG decided to "scrap" the hybrid model in favor of a pure PoS algorithm. Now, Casper FFG and Casper CBC are both being developed in parallel. As Vitalik explains:

The main tradeoff between FFG and CBC is that CBC seems to have nicer theoretical properties, but FFG seems to be easier to implement.

More information about Casper's history, ongoing research and future plans can be found at the following links:

<https://twitter.com/i/moments/1036281460704112645> https://medium.com/@Vlad_Zamfir/the-history-of-casper-part-1-59233819c9a9 https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-2-8e09b9d3b780 https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-3-70fefb1182fc https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-4-3855638b5f0e

Principles of consensus

The principles and assumptions of consensus algorithms can be more clearly understood by asking a few key questions:

- Who can change the past and how, also known as *immutability*.
- Who can change the future and how, also known as *finality*.
- What is the cost to make such changes?
- How decentralized is the power to make such changes?
- Who will know if something has changed and how will they know?

Consensus algorithms are evolving rapidly, attempting to answer these questions in increasingly innovative ways.

Consensus controversy and competition

At this point you might be wondering: why do we need so many different consensus algorithms? Which one works better? The answer to that question is at the center of the most exciting area of research in distributed systems of the past decade. It all boils down to what you consider "better", which in the context of computer science is about assumptions, goals, and the unavoidable tradeoffs.

It is likely that no algorithm can optimize across all dimensions of the problem of decentralized consensus. When someone suggests that a consensus algorithm is "better", you should start asking questions that clarify: Better at what? Immutability, finality, decentralization, cost? There is no clear answer to these questions, at least not yet. Furthermore, the design of consensus algorithms is at the center of a multi-billion dollar industry and generates enormous controversy and heated arguments. In the end, there might not be a "correct" answer, as much as there might be different answers for different applications.

The entire blockchain industry is one giant experiment where these questions will be tested under adversarial conditions, with enormous monetary value at stake. In the end, history will answer the controversy.

Appendix A: Ethereum Fork History

Most hard forks are planned as part of an upgrade roadmap and consist of updates that the community generally agrees to (i.e. there is social consensus). However, some hard forks lack consensus, which leads to multiple distinct blockchains. The events that lead to the Ethereum / Ethereum Classic split is one such case, and are discussed in this section.



The opinions expressed in this section are controversial. Contributions were made by, and are presented from the perspective of, the Ethereum Classic community.

Ethereum Classic (ETC)

Ethereum Classic came to be after members of the Ethereum community implemented a time-sensitive hard fork ("DAO Hard Fork"). On 20th July 2016, at a block height of 1.92 million, Ethereum introduced an irregular state change via a hard fork in an effort to return approximately 3.6 million ether that had been taken from a smart contract known as The DAO. Almost everyone agreed that the ether taken had been stolen and that leaving it all in the hands of the thief would be of significant detriment to development of the Ethereum ecosystem as well as the platform itself.

Returning the ether to its respective owners before The DAO even existed was technically easy, if rather politically controversial. A number of people in the ecosystem disagreed with this change, believing immutability should be a fundamental principle of the Ethereum blockchain without exception; they elected to continue the original chain under the moniker of Ethereum Classic. While the split itself was initially ideological both chains have since evolved into separate entities.

The Decentralized Autonomous Organization (The DAO)

The DAO was created by Slock.it aiming to provide community-based funding and governance for projects. The core idea was that proposals would be submitted, curators would manage proposals, funds would be raised from investors within the Ethereum community, and if the project proves successful then investors would receive a share of the profits.

The DAO was also one of the first experiments in an Ethereum token. Rather than funding projects directly with Ether, participants would trade their ether for DAO tokens, use them to vote on project funding, and would later be able to trade them back for Ether.

DAO tokens were available to purchase in a crowdsale that ran from 5th April through 30th April 2016, amassing nearly 14% <<[1]>> of the total ether in existence, which was worth ~\$150 million USD at the time.

The Re-Entrancy Bug

On 9th June, developers Peter Vessenes and Chriseth reported that most Ethereum-based contracts which manage funds were potentially vulnerable to an exploit <<[2]>> that can empty contract funds. A few days later (12th June) Stephen Tual (Co-founder of Slock.it), reported that The DAO's code was not vulnerable <<[3]>> to the bug described by Peter and Chriseth. Worried DAO contributors temporarily breathed a sigh of relief until 5 days later, when an unknown attacker ("the DAO Attacker") started draining The DAO <<[4]>> using an exploit similar to the one described on 9th June. Ultimately the DAO Attacker siphoned ~3.6 million ether out of The DAO.

Simultaneously an assemblage of volunteers calling themselves the Robinhood Group (RHG) started using the same exploit to withdraw the remaining funds in order to save them from being stolen by the DAO Attacker. On the 21st June, the RHG announced <<[5]>> that they had secured about 70% of The DAO's funds (roughly 7.2 million ether), with plans to return it to the community (which they successfully did on the ETC network, and didn't need to do on the Ethereum network after the fork). Many thanks and commendations are given to the RHG for their quick thinking and fast actions that helped secure the bulk of the community's ether.

Re-Entrancy Technicals

While a more detailed and thorough explanation of the bug is given by Phil Daian <<[6]>>, the short explanation is that a crucial function in the DAO had two lines of code in the wrong order, meaning that the Attacker could have requests to withdraw ether acted upon repeatedly, before the check of whether the Attacker was entitled to the withdrawal was completed. This type of vulnerability is described in [Re-Entrancy](#).

Re-Entrancy Attack Flow

Imagine you had \$100 in your bank account and you could bring your bank teller any number of withdrawal slips. The bank teller gives you money for each slip in order, and only at the end of all the slips do they record your withdrawal. What if you brought them three slips to each withdraw \$100? What if you brought them three thousand?

The attack worked like this:

1. DAO Attacker asks the DAO Contract to withdraw DAO tokens (DAO).
2. DAO Attacker asks the contract to withdraw DAO *again*, before the contract updates its records that DAO was withdrawn.
3. Repeat step two as much as possible.
4. The contract finally logs a single DAO withdrawal, losing track of the withdrawals that happened in the interim.

The DAO Hard Fork

Fortunately, there were several safeguards built into The DAO: all withdrawal requests were subject to a 28 day delay. This gave the community a little while to discuss what to do about the exploit. From roughly 17th June to 20th July the DAO Attacker would be unable to convert their DAO tokens into Ether.

Several developers focused on finding a viable solution, and multiple avenues were explored in this short space of time. Among them was the DAO Soft Fork, announced on 24th June, to delay DAO withdrawals until consensus was reached <<[7]>>, and a DAO Hard Fork, announced on 15th July, to reverse the effects of the DAO Attack with an exceptional state change <<[8]>>.

On 28th June, developers discovered a DoS exploit in the DAO Soft Fork <<[9]>>, and concluded that the DAO Hard Fork would be the only viable option to fully resolve the situation. The DAO Hard Fork would transfer all ether that had been invested in the DAO into a new refund smart contract, allowing the original owners of the ether to claim a full refund. This provided a solution for returning the hacked funds, but also meant interfering with the balances of specific addresses on the network, however isolated they were. There would also be some leftover ether in portions of The DAO known as childDAOs <<[12]>>. A group of trustees would manually authorize the leftover ether, worth ~\$6-7 million at the time <<[8]>>.

With time running out, multiple Ethereum development teams created clients that allowed a user to decide whether they wanted to enable this fork. However, the client creators wanted to decide whether to make this choice opt-in (don't fork by default), or opt-out (fork by default). On the 15th July, a vote was opened on carbonvote.com <<[10]>>. The next day, at block height 1,894,000 <<[11]>> it was closed. Of the 5.5% of the total ether supply that voted, ~80% of the votes (~4.5% of the total ether supply) voted for opt-out. One quarter of the opt-out vote came from a single address <<[12]>>.

Ultimately the decision became opt-out, and those who opposed the DAO Hard Fork would need to

explicitly state that they opposed by changing a configuration option in the software they were running.

On the 20th July, at block height 1,920,000 <<[13]>> Ethereum implemented the DAO Hard Fork <<[14]>> and thus two Ethereum networks were created, one including the state change, and the other ignoring it.

When the DAO Hard Forked Ethereum (present-day Ethereum) gained a majority of the mining power, many assumed that consensus was achieved and the minority chain would fade away; as in previous forks. Despite this, a sizable portion of the Ethereum community (roughly 10% by value and mining power) started supporting the non-forked chain, which came to be known as Ethereum Classic with the symbol ETC.

Within days, several exchanges began to list both Ethereum ("ETH") and Ethereum Classic ("ETC"). Due to the nature of hard forks, all Ethereum users holding ether at the time of the split then held funds on both of the chains and a market value for ETC was soon established with Poloniex listing ETC on the 24th July <<[15]>>.

Timeline of The DAO Hard Fork

- 2016 April 5: Slock.it creates The DAO following a security audit by Dejavu Security <<[16]>>
- 2016 April 30: The DAO crowdsale launches <<[17]>>
- 2016 May 27: The DAO crowdsale ends
- 2016 June 9: A generic recursive call bug is discovered and believed to affect many Solidity contracts that track user's balances <<[2]>>
- 2016 June 12: Stephen Tual declares that DAO funds are not at risk <<[3]>>
- 2016 June 17: The DAO is exploited and a variant of the discovered bug (termed the "re-entry bug") is used to start draining the funds; eventually nabbing ~30% of the funds <<[6]>>
- 2016 June 21: The RHG announces it has secured the other ~70% of the ether stored within The DAO <<[5]>>
- 2016 June 24: A soft fork vote is announced via opt-in signaling through Geth and Parity clients, designed to temporarily withhold funds until the community can better decide what to do <<[7]>>
- 2016 June 28: A vulnerability is discovered in the soft fork and it's abandoned <<[9]>>
- 2016 June 28 to July 15: Users debate whether or not to hard fork; most of the vocal public debate

occurs on the /r/ethereum subreddit

- 2016 July 15: The DAO Hard Fork is proposed, to return the funds taken in The DAO Attack <<[8]>>
- 2016 July 15: A vote is held on carbonvote to decide if the DAO Hard Fork is opt-in (don't fork by default) or opt-out (fork by default) <<[10]>>
- 2016 July 16: 5.5% of the total ether supply votes, ∼80% of the votes (∼4.5% of the total supply) are pro the opt-out hard fork; one quarter of the pro-vote comes from a single address <<[11]>> <<[12]>>
- 2016 July 20: The hard fork occurs at block 1,920,000 <<[13]>> <<[14]>>
- 2016 July 20: Those against the DAO Hard Fork continue running the old non-hard fork client software; this leads to issues with transactions being replayed on both chains <<[18]>>
- 2016 July 24: Poloniex lists the original Ethereum chain under the ticker symbol ETC, the first exchange to do so <<[15]>>
- 2016 August 10: The RHG transfers 2.9 million of the recovered ETC to Poloniex in order to convert it to ETH on the advice of Bity SA; 14% of the total RHG holdings are converted from ETC to ETH and other cryptocurrencies; Poloniex freezes the other 86% of deposited ETH <<[19]>>
- 2016 August 30: The frozen funds are sent by Poloniex back to the RHG, which then sets up a refund contract on the ETC chain <<[20]>> <<[21]>>
- 2016 December 11: IOHK's ETC development team forms, led by Ethereum founding member Charles Hoskinson
- 2017 January 13: The ETC network is updated to resolve transaction replay issues; the chains are now functionally separate <<[22]>>
- 2017 February 20: ETCDEVTeam forms, led by early ETC developer Igor Artamonov (splix)

Ethereum and Ethereum Classic

While the initial split was centered around The DAO, the two networks, Ethereum and Ethereum Classic, are now separate projects, although most development is still done by the Ethereum community and simply ported to Ethereum Classic codebases. Nevertheless, the full set of differences is constantly evolving and too extensive to cover in this chapter. However, it is worth noting that the chains do differ significantly in their core development and community structure.

Technical Differences

The EVM

For the most part (as of April 2018) the two networks remain highly compatible: contract code produced for one chain runs as expected on the other; but there are some small differences in EVM OPCODES (see EIPs [140](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-140.md) [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-140.md>], [145](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-145.md) [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-145.md>], and [214](https://github.com/ethereum/EIPs/blob/master/EIPS/eip-214.md) [<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-214.md>]).

Core Network Development

Being open projects, blockchain platforms often have many users and contributors. However, the core network development (code that runs the network) is often done by small groups due to the expertise and knowledge required to develop this type of software. As such the code that these groups produce is very closely tied to the code that actually runs the network.

Ethereum	Ethereum Classic
Ethereum Foundation, and volunteers.	ETCDEV, IOHK, and volunteers.

thereum_forks]] === A timeline of notable Ethereum forks

Ellaism is an Ethereum-based network, and intends to use exclusively Proof-of-Work to secure the blockchain. It has a zero pre-mine and has no mandatory developer fees, with all support and development donated freely by the community. Its developers believe this makes their coin one of the most honest pure Ethereum projects, and something that is uniquely interesting as a platform for serious developers, educators, and enthusiasts. Ellaism is a pure smart contract platform. Its goal is to create a smart contract platform that is both fair and trustworthy.

Principles:

1. All changes and upgrades to the protocol should strive to maintain and reinforce these Principles of Ellaism.
2. Monetary Policy: 280 million coins.
3. No censorship: Nobody should be able to prevent valid txs from being confirmed.
4. Open-Source: Ellaism source code should always be open for anyone to read, modify, copy, share.

5. Permissionless: No arbitrary gatekeepers should ever prevent anybody from being part of the network (user, node, miner, etc).
6. Pseudonymous: No ID should be required to own, use Ellaism.
7. Fungible: All coins are equal and should be equally spendable.
8. Irreversible Transactions: Confirmed blocks should be set in stone. Blockchain History should be immutable.
9. No Contentious Hard Forks: Never hard fork without consensus from the whole community. Only break the existing consensus when necessary.
10. Many feature upgrades can be carried out without a hard fork, such as improving the performance of the EVM.

Several other forks have occurred on Ethereum as well. Some of these are hard forks in the sense that they split directly off of the pre-existing Ethereum network. Others are software forks: they use Ethereum's client/node software but run entirely separate networks without any history shared with Ethereum. There will likely be more forks over the life of Ethereum.

There are also several other projects that claim to be Ethereum forks but are actually based on ERC20 tokens and run on the Ethereum network. Two examples of these are EtherBTC (ETHB) and Ethereum Modification (EMOD). These are not forks in the traditional sense, and may sometimes be called airdrops.

- Expanse was the first fork of the Ethereum blockchain to gain traction. It was announced via the Bitcoin Talk forum on September 7 2015. The actual fork occurred a week later on September 14 2015 at a block height of 800,000. It was originally founded by Christopher Franko and James Clayton. Their stated vision was to create an advanced chain for: "identity, governance, charity, commerce, and equity".
- EthereumFog (ETF) was launched on December 14 2017 and forked at a block height of 4,730,660. Their stated aims are to develop "World Decentralized Fog Computing" by focusing on fog computing and decentralized storage. There is still little information on what this will actually entail.
- EtherZero (ETZ) was launched on January 19 2018 at block height of 4,936,270. Its notable innovations were the introduction of a masternode architecture and the removal of transaction fees for smart contracts to enable a wider diversity of DApps. There have been some criticism from some prominent members of the Ethereum community, MyEtherWallet and MetaMask, due to the

lack of clarity surrounding development and some accusations of possible phishing.

- EtherInc (ETI) was launched on February 13 2018 at a block height of 5,078,585 with a focus on building decentralized organizations. They also announced the reduction of block times, increased miner rewards, the removal of uncle rewards and set a cap on mineable coins. They use the same private keys as Ethereum and have implemented replay protection to protect ether on the original non-forked chain.

References

- [[[1]]] <https://www.economist.com/news/finance-and-economics/21699159-new-automated-investment-fund-has-attracted-stacks-digital-money-dao>
- [[[2]]] <https://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/>
- [[[3]]] <https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b>
- [[[4]]] <http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit>
- [[[5]]] https://www.reddit.com/r/ethereum/comments/4p7mhc/update_on_the_white_hat_attack/
- [[[6]]] <http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>
- [[[7]]] <https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma/>
- [[[8]]] <https://blog.slock.it/hard-fork-specification-24b889e70703>
- [[[9]]] <https://blog.ethereum.org/2016/06/28/security-alert-dos-vulnerability-in-the-soft-fork/>
- [[[10]]] <https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/>
- [[[11]]] <https://etherscan.io/block/1894000>
- [[[12]]] <https://elaineou.com/2016/07/18/stick-a-fork-in-ethereum/>
- [[[13]]] <https://etherscan.io/block/1920000>
- [[[14]]] <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>
- [[[15]]] <https://twitter.com/poloniex/status/757068619234803712>
- [[[16]]] <https://blog.slock.it/deja-vu-dao-smart-contracts-audit-results-d26bc088e32e>

- [[[17]]] <https://blog.slock.it/the-dao-creation-is-now-live-2270fd23affc>
- [[[18]]] <https://gastracker.io/block/0x94365e3a8c0b35089c1d1195081fe7489b528a84b22199c916180db8b28ade7f>
- [[[19]]] <https://bitcoinmagazine.com/articles/millions-of-dollars-worth-of-etc-may-soon-be-dumped-on-the-market-1472567361/>
- [[[20]]] <https://medium.com/@jackfru1t/the-robin-hood-group-and-etc-bdc6a0c111c3>
- [[[21]]] https://www.reddit.com/r/EthereumClassic/comments/4xauca/follow_up_statement_on_the_etc_salvaged_from/
- [[[22]]] https://www.reddit.com/r/EthereumClassic/comments/5nt4qm/diehard_etc_protocol_upgrade_successful_nethash/
- [[[23]]] <https://web.archive.org/web/20160429141714/https://daohub.org/explainer.html/>
- [[[24]]] <https://ethereumclassic.github.io/blog/2016-12-12-TeamGrothendieck/>

Appendix B: Ethereum Standards

Ethereum Improvement Proposals (EIPs)

<https://github.com/ethereum/EIPs/>

<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md>

From EIP-1:

EIP stands for Ethereum Improvement Proposal. An EIP is a design document providing information to the Ethereum community, or describing a new feature for Ethereum or its processes or environment. The EIP should provide a concise technical specification of the feature and a rationale for the feature. The EIP author is responsible for building consensus within the community and documenting dissenting opinions.

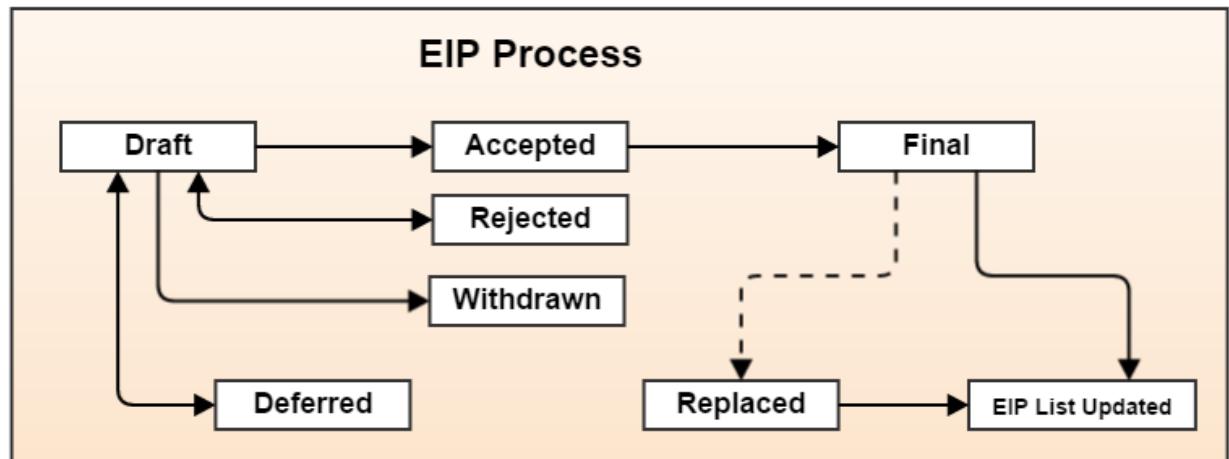


Figure 62. Ethereum Improvement Proposal Workflow

Table of Most Important EIPs and ERCs

Table 8. Important EIPs and ERCs

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-1 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1.md]	EIP Purpose and Guidelines	Martin Becze, Hudson Jameson	Meta	Final	
EIP-2 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-2.md]	Homestead Hard-fork Changes	Vitalik Buterin	Core	Final	
EIP-5 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-5.md]	Gas Usage for RETURN and CALL	Christian Reitwiessner	Core	Draft	
EIP-6 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-6.md]	Renaming Suicide Opcode	Hudson Jameson	Interface	Final	
EIP-7 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-7.md]	DELEGATECALL	Vitalik Buterin	Core	Final	
EIP-8 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-8.md]	devp2p Forward Compatibility Requirements for Homestead	Felix Lange	Networking	Final	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-20 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md]	ERC-20 Token Standard. Describes standard functions a token contract may implement to allow DApps and Wallets to handle tokens across multiple interfaces/DAps. Methods include: <code>totalSupply()</code> , <code>balanceOf(address)</code> , <code>transfer</code> , <code>transferFrom</code> , <code>approve</code> , <code>allowance</code> . Events include: <code>Transfer</code> (triggered when tokens are transferred), <code>Approval</code> (triggered when <code>approve</code> is called).	Fabian Vogelsteller, Vitalik Buterin	ERC	Final	Frontier
EIP-55 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-55.md]	ERC-55 Mixed-case checksum address encoding	Vitalik Buterin	ERC	Final	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-86 [https://github.com/ethereum/EIPs/blob/bd136e662fca4154787b44cded8d2a29b993be66/EIPS/abstraction.md]	Setting the stage for "abstracting out" account security, and allowing users creation of "account contracts" toward a model where in the long-term all accounts are contracts that can pay for gas, and users are free to define their own security model (that perform any desired signature verification and nonce checks instead of using the in-protocol mechanism where ECDSA and default nonce scheme are the only "standard" way to secure an account, which is currently hard-coded into transaction processing).	Vitalik Buterin	Core	Deferred (to be replaced)	Constantinople

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-96 [https://github.com/ethereum/EIPs/pull/210]	Setting the Blockhash and state root refactoring to store blockhashes in the state to reduce protocol complexity and need for client implementation complexity necessary to process the BLOCKHASH opcode. Extends range of how far back blockhash checking may go, with the side effect of creating direct links between blocks with very distant block numbers to facilitate much more efficient initial Light Client syncing.	Vitalik Buterin	Core	Deferred	Constantinople
EIP-100 [https://github.com/ethereum/EIPs/issues/100]	Change formula that computes the difficulty of a block (difficulty adjustment algorithm) to target mean block time and take uncles into account.	Vitalik Buterin	Core	Final	Metropolis Byzantium

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-101 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-101.md]	Serenity Currency and Crypto Abstraction. Abstracting Ether up a level with the benefit of allowing Ether and sub- Tokens to be treated similarly by contracts, reducing level of indirection required for custom-policy accounts such as Multisigs, and purifying the underlying Ethereum protocol by reducing the minimal consensus implementation complexity	Vitalik Buterin	Active	Serenity feature	Serenity Casper
EIP-105 [https://blog.ethereum.org/2016/03/05/serenity-poc2/]	"Sharding scaffolding" EIP to allow Ethereum transactions to be parallelised using a binary tree sharding mechanism, and to set the stage for a later sharding scheme. Research in progress: https://github.com/ethereum/sharding	Vitalik Buterin	Active	Serenity feature	Serenity Casper

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-137 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-137.md]	Ethereum Domain Name Service - Specification	Nick Johnson	ERC	Final	
EIP-140 [https://github.com/ethereum/EIPs/pull/206]	Add REVERT opcode instruction, which stops execution and rolls back the EVM execution state changes without consuming all provided gas (instead the contract only has to pay for memory) or losing logs, and returning to the caller a pointer to the memory location with the error code or message.	Alex Beregszaszi, Nikolai Mushegian	Core	Final	Metropolis Byzantium
EIP-141 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-141.md]	Designated invalid EVM instruction	Alex Beregszaszi	Core	Final	
EIP-145 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-145.md]	Bitwise shifting instructions in EVM	Alex Beregszaszi, Paweł Bylica	Core	Deferred	
EIP-150 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-150.md]	Gas cost changes for IO-heavy operations	Vitalik Buterin	Core	Final	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-155 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-155.md]	Simple Replay Attack Protection. Replay Attack allows any transaction using a pre-EIP155 Ethereum Node or Client to become signed so it is valid and executed on both the Ethereum and Ethereum Classic chains.	Vitalik Buterin	Core	Final	Homestead
EIP-158 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-158.md]	State clearing	Vitalik Buterin	Core	Superseded	
EIP-160 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-160.md]	EXP cost increase	Vitalik Buterin	Core	Final	
EIP-161 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-161.md]	State trie clearing (invariant-preserving alternative[EIP-161])	Gavin Wood	Core	Final	
EIP-162 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-162.md]	ERC-162 ENS support for reverse resolution of Ethereum addresses	Maurelian, Nick Johnson	ERC	Final	
EIP-165 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-165.md]	ERC-165 Standard Interface Detection	Christian Reitwiessner	Interface	Draft	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-170 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-170.md]	Contract code size limit	Vitalik Buterin	Core	Final	
EIP-181 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-181.md]	ERC-181 ENS support for reverse resolution of Ethereum addresses	Nick Johnson	ERC	Final	
EIP-190 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-190.md]	ERC-190 Ethereum Smart Contract Packaging Standard	Merriam, Coulter, Erfurt, Catalano, Matias	ERC	Final	
EIP-196 [https://github.com/ethereum/EIPs/pull/213]	Precompiled contracts for addition and scalar multiplication operations on the elliptic curve alt_bn128, which are required in order to perform zkSNARK verification within the block gas limit	Christian Reitwiessner	Core	Final	Metropolis Byzantium
EIP-197 [https://github.com/ethereum/EIPs/pull/212]	Precompiled contracts for optimal Ate pairing check of a pairing function on a specific pairing-friendly elliptic curve alt_bn128 and is combined with EIP 196	Vitalik Buterin, Christian Reitwiessner	Core	Final	Metropolis Byzantium

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-198 [https://github.com/ethereum/EIPs/pull/198]	Precompile to support big integer modular exponentiation enabling RSA signature verification and other cryptographic applications	Vitalik Buterin	Core	Final	Metropolis Byzantium
EIP-211 [https://github.com/ethereum/EIPs/pull/211]	New opcodes: RETURNDATASIZE and RETURNDATACOPY . Support for returning variable-length values inside the EVM with simple gas charging and minimal change to calling opcodes using new opcodes RETURNDATASIZE and RETURNDATACOPY . Handles similar to existing calldata , whereby after a call, return data is kept inside a virtual buffer from which the caller can copy it (or parts thereof) into memory, and upon the next call, the buffer is overwritten.	Christian Reitwiessner	Core	Final	Metropolis Byzantium

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-214 [https://github.com/ethereum/EIPs/pull/214]	New opcode: STATICCALL . Permits non-state-changing calls to itself or other contracts whilst disallowing any modifications to state during the call (and its sub-calls, if present) to increase smart contract security and assure developers that re-entrancy bugs cannot arise from the call. Calls the child with STATIC flag set true for execution of child, causing exception to be thrown upon any attempts to make state-changing operations inside an execution instance where STATIC is set true , and resets flag once call returns.	Vitalik Buterin, Christian Reitwiessner	Core	Final	Metropolis Byzantium
EIP-225 [https://github.com/ethereum/EIPs/issues/225]	Rinkeby Testnet using Proof-of-Authority where blocks only mined by trusted signers				Homestead

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-234 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-234.md]	Add blockHash to JSON-RPC filter options	Micah Zoltu	Interface	Draft	
EIP-615 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-615.md]	Subroutines and Static Jumps for the EVM	Greg Colvin	Core	Draft	
EIP-616 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-616.md]	SIMD Operations for the EVM	Greg Colvin	Core	Draft	
EIP-681 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-681.md]	ERC-681 URL Format for Transaction Requests	Daniel A. Nagy	Interface	Draft	
EIP-649 [https://github.com/ethereum/EIPs/pull/669]	Metropolis Difficulty Bomb Delay and Block Reward Reduction - Delay of the Ice Age (aka the Difficulty Bomb) by 1 year, and reduction of the block reward from 5 to 3 ether.	Afri Schoedon, Vitalik Buterin	Core	Final	Metropolis Byzantium

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-658 [https://github.com/ethereum/EIPs/pull/658]	Embedding transaction status code in receipts. Fetch and embed status field indicative of success or failure state to transaction receipts for callers, as was no longer able to assume the transaction failed if and only if it consumed all gas after the introduction of the REVERT opcode in EIP-140.	Nick Johnson	Core	Final	Metropolis Byzantium
EIP-706 [https://github.com/ethereum/EIPS/blob/master/EIPS/eip-706.md]	DEVp2p snappy compression	Péter Szilágyi	Networking	Final	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-721 [https://github.com/ethereum/EIPs/issues/721]	ERC-721 Non-Fungible Token (NFT) Standard. A standard API that would allow smart contracts to operate as unique tradable non-fungible tokens (NFT) that may be tracked in standardised wallets and traded on exchanges as assets of value, similar to ERC-20. CryptoKitties was the first popularly-adopted implementation of a digital NFT in the Ethereum ecosystem.	William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs	Standard	Draft	
EIP-758 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-758.md]	Subscriptions and filters for transaction return data	Jack Peterson	Interface	Draft	
EIP-801 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-801.md]	ERC-801 Canary Standard	ligi	Interface	Draft	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-827 [https://github.com/ethereum/EIPs/issues/827]	ERC-827 A extension of the standard interface ERC20 for tokens with methods that allows the execution of calls inside transfer and approvals. This standard provides basic functionality to transfer tokens, as well as allow tokens to be approved so they can be spent by another on-chain third party. Also it allows to execute calls on transfers and approvals.	Augusto Lemble	ERC	Draft	

EIP/ERC #	Title	Author	Layer	Status	Created
EIP-930 [https://github.com/ethereum/EIPs/issues/930]	ERC-930 The ES (Eternal Storage) contract is owned by an address that have write permissions. The storage is public, which means everyone has read permissions. It store the data on mappings, using one mapping per type of variable. The use of this contract allows the developer to migrate the storage easily to another contract if needed.	Augusto Lemble	ERC	Draft	

Appendix C: Ethereum EVM Opcodes and gas consumption

This appendix is based on the consolidation work done by the people of <https://github.com/trailofbits/evm-opcodes> as a Reference for Ethereum VM (EVM) Opcodes and Instruction information with the following LICENSE <https://github.com/trailofbits/evm-opcodes/blob/master/LICENSE>.

Table 9. EVM Opcodes and Gas Cost

Opcode	Name	Description	Extra Info	Gas
0x00	STOP	Halts execution	-	0
0x01	ADD	Addition operation	-	3
0x02	MUL	Multiplication operation	-	5
0x03	SUB	Subtraction operation	-	3
0x04	DIV	Integer division operation	-	5
0x05	SDIV	Signed integer division operation (truncated)	-	5
0x06	MOD	Modulo remainder operation	-	5
0x07	SMOD	Signed modulo remainder operation	-	5
0x08	ADDMOD	Modulo addition operation	-	8
0x09	MULMOD	Modulo multiplication operation	-	8
0x0a	EXP	Exponential operation	-	10***
0x0b	SIGNEXTEND	Extend length of two's complement signed integer	-	5
0x0c - 0x0f	Unused	Unused	-	

Opcode	Name	Description	Extra Info	Gas
0x10	LT	Less-than comparison	-	3
0x11	GT	Greater-than comparison	-	3
0x12	SLT	Signed less-than comparison	-	3
0x13	SGT	Signed greater-than comparison	-	3
0x14	EQ	Equality comparison	-	3
0x15	ISZERO	Simple not operator	-	3
0x16	AND	Bitwise AND operation	-	3
0x17	OR	Bitwise OR operation	-	3
0x18	XOR	Bitwise XOR operation	-	3
0x19	NOT	Bitwise NOT operation	-	3
0x1a	BYTE	Retrieve single byte from word	-	3
0x1b - 0x1f	Unused	Unused	-	
0x20	SHA3	Compute Keccak-256 hash	-	30
0x21 - 0x2f	Unused	Unused	-	
0x30	ADDRESS	Get address of currently executing account	-	2
0x31	BALANCE	Get balance of the given account	-	400
0x32	ORIGIN	Get execution origination address	-	2
0x33	CALLER	Get caller address	-	2

Opcode	Name	Description	Extra Info	Gas
0x34	CALLVALUE	Get deposited value by the instruction/transaction responsible for this execution	-	2
0x35	CALLDATALOAD	Get input data of current environment	-	3
0x36	CALLDATASIZE	Get size of input data in current environment	-	2
0x37	CALLDATACOPY	Copy input data in current environment to memory	-	3
0x38	CODESIZE	Get size of code running in current environment	-	2
0x39	CODECOPY	Copy code running in current environment to memory	-	3
0x3a	GASPRICE	Get price of gas in current environment	-	2
0x3b	EXTCODESIZE	Get size of an account's code	-	700
0x3c	EXTCODECOPY	Copy an account's code to memory	-	700
0x3d	RETURNDATASIZE	Pushes the size of the return data buffer onto the stack	EIP 211 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-211.md]	2
0x3e	RETURNDATACOPY	Copies data from the return data buffer to memory	EIP 211 [https://github.com/ethereum/EIPs/blob/master/EIPS/eip-211.md]	3
0x3f	Unused	-	-	

Opcode	Name	Description	Extra Info	Gas
0x40	BLOCKHASH	Get the hash of one of the 256 most recent complete blocks	-	20
0x41	COINBASE	Get the block's beneficiary address	-	2
0x42	TIMESTAMP	Get the block's timestamp	-	2
0x43	NUMBER	Get the block's number	-	2
0x44	DIFFICULTY	Get the block's difficulty	-	2
0x45	GASLIMIT	Get the block's gas limit	-	2
0x46 - 0x4f	Unused	-	-	
0x50	POP	Remove word from stack	-	2
0x51	MLOAD	Load word from memory	-	3
0x52	MSTORE	Save word to memory	-	3*
0x53	MSTORE8	Save byte to memory	-	3
0x54	SLOAD	Load word from storage	-	200
0x55	SSTORE	Save word to storage	-	0*
0x56	JUMP	Alter the program counter	-	8
0x57	JUMPI	Conditionally alter the program counter	-	10
0x58	GETPC	Get the value of the program counter prior to the increment	-	2

Opcode	Name	Description	Extra Info	Gas
0x59	MSIZE	Get the size of active memory in bytes	-	2
0x5a	GAS	Get the amount of available gas, including the corresponding reduction the amount of available gas	-	2
0x5b	JUMPDEST	Mark a valid destination for jumps	-	1
0x5c - 0x5f	Unused	-	-	
0x60	PUSH1	Place 1 byte item on stack	-	3
0x61	PUSH2	Place 2-byte item on stack	-	3
0x62	PUSH3	Place 3-byte item on stack	-	3
0x63	PUSH4	Place 4-byte item on stack	-	3
0x64	PUSH5	Place 5-byte item on stack	-	3
0x65	PUSH6	Place 6-byte item on stack	-	3
0x66	PUSH7	Place 7-byte item on stack	-	3
0x67	PUSH8	Place 8-byte item on stack	-	3
0x68	PUSH9	Place 9-byte item on stack	-	3
0x69	PUSH10	Place 10-byte item on stack	-	3
0x6a	PUSH11	Place 11-byte item on stack	-	3
0x6b	PUSH12	Place 12-byte item on stack	-	3

Opcode	Name	Description	Extra Info	Gas
0x6c	PUSH13	Place 13-byte item on stack	-	3
0x6d	PUSH14	Place 14-byte item on stack	-	3
0x6e	PUSH15	Place 15-byte item on stack	-	3
0x6f	PUSH16	Place 16-byte item on stack	-	3
0x70	PUSH17	Place 17-byte item on stack	-	3
0x71	PUSH18	Place 18-byte item on stack	-	3
0x72	PUSH19	Place 19-byte item on stack	-	3
0x73	PUSH20	Place 20-byte item on stack	-	3
0x74	PUSH21	Place 21-byte item on stack	-	3
0x75	PUSH22	Place 22-byte item on stack	-	3
0x76	PUSH23	Place 23-byte item on stack	-	3
0x77	PUSH24	Place 24-byte item on stack	-	3
0x78	PUSH25	Place 25-byte item on stack	-	3
0x79	PUSH26	Place 26-byte item on stack	-	3
0x7a	PUSH27	Place 27-byte item on stack	-	3
0x7b	PUSH28	Place 28-byte item on stack	-	3
0x7c	PUSH29	Place 29-byte item on stack	-	3
0x7d	PUSH30	Place 30-byte item on stack	-	3

Opcode	Name	Description	Extra Info	Gas
0x7e	PUSH31	Place 31-byte item on stack	-	3
0x7f	PUSH32	Place 32-byte (full word) item on stack	-	3
0x80	DUP1	Duplicate 1st stack item	-	3
0x81	DUP2	Duplicate 2nd stack item	-	3
0x82	DUP3	Duplicate 3rd stack item	-	3
0x83	DUP4	Duplicate 4th stack item	-	3
0x84	DUP5	Duplicate 5th stack item	-	3
0x85	DUP6	Duplicate 6th stack item	-	3
0x86	DUP7	Duplicate 7th stack item	-	3
0x87	DUP8	Duplicate 8th stack item	-	3
0x88	DUP9	Duplicate 9th stack item	-	3
0x89	DUP10	Duplicate 10th stack item	-	3
0x8a	DUP11	Duplicate 11th stack item	-	3
0x8b	DUP12	Duplicate 12th stack item	-	3
0x8c	DUP13	Duplicate 13th stack item	-	3
0x8d	DUP14	Duplicate 14th stack item	-	3
0x8e	DUP15	Duplicate 15th stack item	-	3

Opcode	Name	Description	Extra Info	Gas
0x8f	DUP16	Duplicate 16th stack item	-	3
0x90	SWAP1	Exchange 1st and 2nd stack items	-	3
0x91	SWAP2	Exchange 1st and 3rd stack items	-	3
0x92	SWAP3	Exchange 1st and 4th stack items	-	3
0x93	SWAP4	Exchange 1st and 5th stack items	-	3
0x94	SWAP5	Exchange 1st and 6th stack items	-	3
0x95	SWAP6	Exchange 1st and 7th stack items	-	3
0x96	SWAP7	Exchange 1st and 8th stack items	-	3
0x97	SWAP8	Exchange 1st and 9th stack items	-	3
0x98	SWAP9	Exchange 1st and 10th stack items	-	3
0x99	SWAP10	Exchange 1st and 11th stack items	-	3
0x9a	SWAP11	Exchange 1st and 12th stack items	-	3
0x9b	SWAP12	Exchange 1st and 13th stack items	-	3
0x9c	SWAP13	Exchange 1st and 14th stack items	-	3
0x9d	SWAP14	Exchange 1st and 15th stack items	-	3
0x9e	SWAP15	Exchange 1st and 16th stack items	-	3
0x9f	SWAP16	Exchange 1st and 17th stack items	-	3
0xa0	LOG0	Append log record with no topics	-	375

Opcode	Name	Description	Extra Info	Gas
0xa1	LOG1	Append log record with one topic	-	750
0xa2	LOG2	Append log record with two topics	-	1125
0xa3	LOG3	Append log record with three topics	-	1500
0xa4	LOG4	Append log record with four topics	-	1875
0xa5 - 0xaf	Unused	-	-	
0xb0	JUMPTO	Tentative libevmasm has different numbers [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xb1	JUMPIF	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xb2	JUMPSUB	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xb4	JUMPSUBV	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xb5	BEGINSUB	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	

Opcode	Name	Description	Extra Info	Gas
0xb6	BEGINDATA	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xb8	RETURNSUB	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xb9	PUTLOCAL	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xba	GETLOCAL	Tentative	EIP 615 [https://github.com/ethereum/EIPs/blob/606405b5ab7aa28d8191958504e8aad4649666c9/EIPS/eip-615.md]	
0xbb - 0xe0	Unused	-	-	
0xe1	SLOADBYTES	Only referenced in pyethereum	-	-
0xe2	SSTOREBYTES	Only referenced in pyethereum	-	-
0xe3	SSIZE	Only referenced in pyethereum	-	-
0xe4 - 0xef	Unused	-	-	
0xf0	CREATE	Create a new account with associated code	-	32000
0xf1	CALL	Message-call into an account	-	Complicated
0xf2	CALLCODE	Message-call into this account with alternative account's code	-	Complicated

Opcode	Name	Description	Extra Info	Gas
0xf3	RETURN	Halt execution returning output data	-	0
0xf4	DELEGATECALL	Message-call into this account with an alternative account's code, but persisting into this account with an alternative account's code	-	Complicated
0xf5	CALLBLACKBOX	-	-	40
0xf6 - 0xf9	Unused	-	-	
0xfa	STATICCALL	Similar to CALL, but does not modify state	-	40
0xfb	CREATE2	Create a new account and set creation address to sha3(sender + sha3(init code)) % 2**160	-	
0xfc	TXEXECGAS	Not in yellow paper FIXME	-	-
0xfd	REVERT	Stop execution and revert state changes, without consuming all provided gas and providing a reason	-	0
0xfe	INVALID	Designated invalid instruction	-	0
0xff	SELFDESTRUCT	Halt execution and register account for later deletion	-	5000*

Appendix D: Development Tools, Frameworks and Libraries

Frameworks

Frameworks can be used to ease Ethereum smart contracts development. By doing everything yourself you get a better understanding of how everything fits together, but it's a lot of tedious, repetitive work. The frameworks described in this section can automate certain tasks and make development easier.

Truffle

Github: <https://github.com/trufflesuite/truffle>

Website: <https://truffleframework.com>

Documentation: <https://truffleframework.com/docs>

Truffle Boxes: <http://truffleframework.com/boxes/>

npm package repository: <https://www.npmjs.com/package/truffle>

Installing the truffle framework

The truffle framework comprises several Node.js packages. Before we install truffle, we need to have an up-to-date and working installation of Node.js and the Node Package Manager (npm).

The recommended way to install Node.js and npm is to use the Node Version Manager (NVM), nvm. Once we install nvm, it will handle all the dependencies and updates for us. We'll follow the instructions found at <http://nvm.sh>

Once nvm is installed on your operating system, installing Node.js is simple. We use the --lts flag to tell nvm that we want the most recent "Long Term Support (LTS)" version of Node.js:

```
$ nvm install --lts
```

Confirm you have node and npm installed:

```
$ node -v  
v8.9.4  
$ npm -v  
5.6.0
```

Create a hidden file `.nvmrc` that contains the Node.js version supported by your DApp so developers just need to run `nvm install` in the root of the project directory and it will automatically install and switch to using that version.

```
$ node -v > .nvmrc  
$ nvm install
```

Looking good. Now to install truffle:

```
$ npm -g install truffle  
+ truffle@4.0.6  
installed 1 package in 37.508s
```

Integrating a pre-built Truffle project (Truffle Box)

If we want to use or create a DApp that builds upon a pre-built boilerplate, then at the Truffle Boxes link we can choose an existing Truffle project, and then run the following to download and extract it:

```
$ truffle unbox <BOX_NAME>
```

Creating a truffle project directory

For each project where we will use truffle, we create a project directory and initialize truffle within that directory. Truffle will create the necessary directory structure inside our project directory. Customarily, we give the project directory a name that describes our project. For this example, we will use truffle to deploy our faucet contract from [A simple contract: a test ether faucet](#), and therefore we will name the project folder `Faucet`.

```
$ mkdir Faucet  
$ cd Faucet  
Faucet $
```

Once inside the Faucet directory, we initialize truffle:

```
Faucet $ truffle init
```

Truffle creates a directory structure and some default files:

```
Faucet  
+---- contracts  
|   `---- Migrations.sol  
+---- migrations  
|   `---- 1_initial_migration.js  
+---- test  
+---- truffle-config.js  
`---- truffle.js
```

We will also use a number of JavaScript (Node.js) support packages, in addition to truffle itself. We can install these with npm. We initialize the npm directory structure and accept the defaults suggested by npm:

```
$ npm init

package name: (faucet)
version: (1.0.0)
description:
entry point: (truffle-config.js)
test command:
git repository:
keywords:
author:
license: (ISC)
About to write to Faucet/package.json:
```

```
{
  "name": "faucet",
  "version": "1.0.0",
  "description": "",
  "main": "truffle-config.js",
  "directories": {
    "test": "test"
  },
  "scripts": {
    "test": "echo \\\"Error: no test specified\\\" && exit 1"
  },
  "author": "",
  "license": "ISC"
}
```

Is this ok? (yes)

Now, we can install the dependencies that we will use to make working with truffle easier:

```
$ npm install dotenv truffle-wallet-provider ethereumjs-wallet
```

You now have a node_modules directory with several thousand files inside your Faucet directory.

Prior to deploying the DApp to a cloud production or continuous integration environment it is important to specify the engines field so that your DApp is built with the correct Node.js version and its associated dependencies are installed.

Package.json engines field configuration: <https://docs.npmjs.com/files/package.json#engines>

Configuring truffle

Truffle creates some empty configuration files, truffle.js and truffle-config.js. On Windows systems the truffle.js name may cause a conflict when you try to run the command truffle and Windows attempts to run truffle.js instead. To avoid this, we will delete truffle.js and use truffle-config.js, in support of Windows users who, honestly, suffer enough already.

```
$ rm truffle.js
```

Now we edit truffle-config.js and replace the contents with the sample configuration below, which will help to get us started:

```
module.exports = {
  networks: {
    localnode: { // Whatever network our local node connects to
      network_id: "*", // Match any network id
      host: "localhost",
      port: 8545,
    }
  }
};
```

The configuration above is a good starting point. It sets up one default Ethereum network (named localnode), which assumes you are running an Ethereum client (such as parity), either as a full node, or as a light client. This configuration will instruct truffle to communicate with the local node over RPC, on port 8545. Truffle will use whatever Ethereum network the local node is connected to, such as the Ethereum main network, or a test network like Ropsten. The local node will also be providing the wallet functionality.

In following sections, we will configure additional networks for truffle to use, such as the ganache local

test blockchain, and Infura, a hosted network provider. As we add more networks, the configuration file will get more complex, but it will also give us more options for our testing and development workflow.

Using truffle to deploy a contract

We now have a basic working directory for our Faucet project, and we have truffle and its dependencies configured. Contracts go in the contracts subdirectory of our project. The directory already contains a "helper" contract, Migrations.sol, which manages contract upgrades for us. We'll examine the use of Migrations.sol in a later section.

Let's copy the Faucet.sol contract (from [Faucet.sol : A Solidity contract implementing a faucet](#)) into the contracts subdirectory, so that the project directory looks like this:

```
Faucet
+---- contracts
|   +---- Faucet.sol
|   `---- Migrations.sol
...
...
```

We can now ask truffle to compile the contract for us:

```
$ truffle compile
Compiling ./contracts/Faucet.sol...
Compiling ./contracts/Migrations.sol...
Writing artifacts to ./build/contracts
```

Truffle migrations - understanding deployment scripts

Truffle offers a deployment system called a *migration*. If you have worked in other frameworks, you may have seen something similar: Ruby on Rails, Python Django and many other languages and frameworks have a migrate command.

In all those frameworks, the purpose of a migration is to handle changes in the data schema between different versions of the software. The purpose of migrations in Ethereum is slightly different. Because Ethereum contracts are immutable and cost gas to deploy, truffle offers a migration mechanism to keep track of which contracts (and which versions) have already been deployed. In a complex project with

dozens of contracts and complex dependencies, you would not want to have to pay to redeploy contracts that haven't changed. You would also not want to manually track which versions of which contracts have been deployed already. The truffle migration mechanism does all that by deploying the smart contract Migrations.sol, which then keeps track of all other contract deployments.

We have only one contract, Faucet.sol, which means that the migration system is overkill, to say the least. Unfortunately, we have to use it. But, by learning how to use it for one contract, we can start practicing some good habits for our development workflow. The effort will pay off as things get more complicated.

Truffle's migrations directory is where the migration scripts are found. Right now, there's only one script 1_initial_migration.js, which deploys the Migrations.sol contract itself:

[[1_initial_migration]]

```
var Migrations = artifacts.require("./Migrations.sol");

module.exports = function(deployer) {
  deployer.deploy(Migrations);
};
```

We need a second migration script, to deploy Faucet.sol. Let's call it 2_deploy_contracts.js. It is very simple, just like 1_initial_migration.js, with only a few small changes. In fact, you can copy the contents of 1_initial_migration.js and simply replace all instances of Migrations with Faucet:

```
var Faucet = artifacts.require("./Faucet.sol");

module.exports = function(deployer) {
  deployer.deploy(Faucet);
};
```

The script initializes a variable Faucet, identifying the Faucet.sol Solidity source code as the artifact that defines Faucet. Then, it calls the deploy function to deploy this contract.

We're all set. Let's use truffle migrate to deploy the contract. We have to specify on which network to deploy the contract, using the --network argument. We only have one network specified in the

configuration file, which we named localnode. Make sure your local Ethereum client is running and then type:

```
Faucet $ truffle migrate --network localnode
```

Because we are using a local node to connect to the Ethereum network and manage our wallet, we have to authorize the transaction that truffle creates. I'm running parity connected to the Ropsten test blockchain, so during the truffle migration I will see a pop-up on parity's web console:

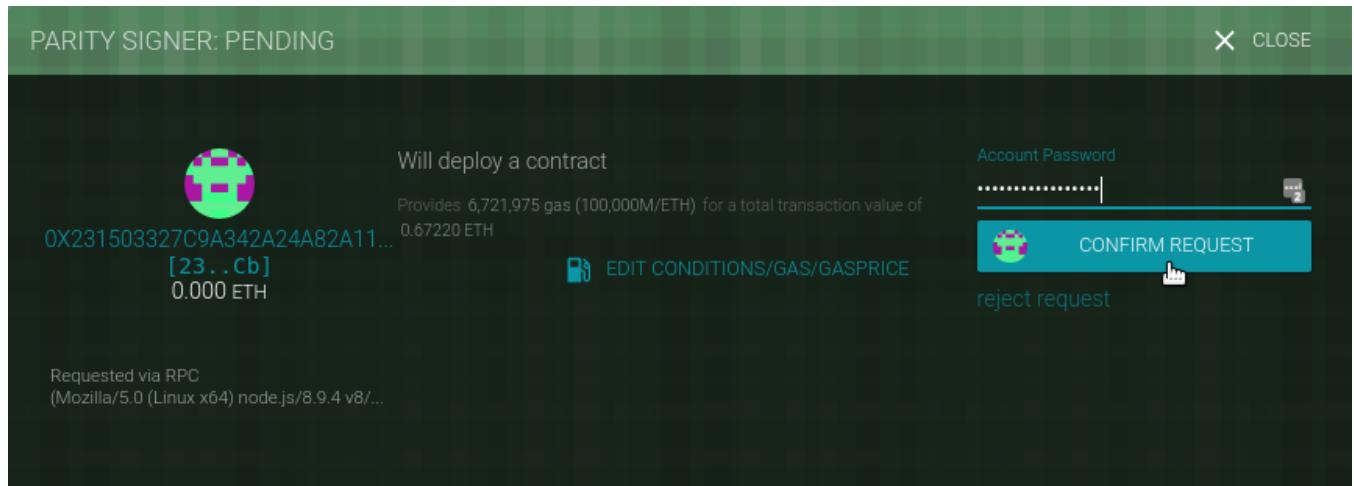


Figure 63. Parity asking for confirmation to deploy Faucet

You will see four transactions, total. One to deploy Migrations, one to update the deployments counter to 1, one to deploy Faucet and one to update the deployments counter to 2.

Truffle will show the migrations completing, show each of the transactions and show the contract addresses:

```
$ truffle migrate --network localnode
Using network 'localnode'.

Running migration: 1_initial_migration.js
  Deploying Migrations...
    ... 0xfa090db179d023d2abae543b4a21a1479e70ca7d35a469a5d1a98bfc6bd80fe8
      Migrations: 0x8861c27715550bed8362c0345add158489df6db0
Saving successful migration to network...
  ... 0x985c4a32716826ddbe4eae284104bef8bc69e959899f62246a1b27c9dfcd6c03
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying Faucet...
    ... 0xecdbeef77f0558edc689440e34b7bba0a3ba7a45e4b680b071b47c30a930e9d6
      Faucet: 0xd01cd8e7bd29e4bff8c1693f59eee46137a9f300
Saving successful migration to network...
  ... 0x11f376bd7307edddfd40dc4a14c3f7cb84b6c921ac2465602060b67d08f9fd8a
Saving artifacts...
```

Using the truffle console

Truffle offers a JavaScript console that we can use to interact with the Ethereum network (via the local node), interact with deployed contracts, and interact with the wallet provider. In our current configuration (localnode), the node and wallet provider is our local parity client.

Let's start the truffle console and try some commands:

```
$ truffle console --network localnode
truffle(localnode)>
```

Truffle presents a prompt, showing the selected network configuration (localnode). It's important to remember and be aware of which network we are using. You wouldn't want to accidentally deploy a test contract or make a transaction on the Ethereum main network. That could be an expensive mistake!

The truffle console offers an auto-complete function that makes it easy for us to explore the environment. If we press Tab after a partially-completed command, truffle will complete the command

for us. Pressing Tab twice will show all possible completions if more than one command matches our input. In fact, if we press Tab twice on an empty prompt, truffle lists all commands:

```
truffle(localnode)>
Array Boolean Date Error EvalError Function Infinity JSON Math NaN Number
Object RangeError ReferenceError RegExp String SyntaxError TypeError
URIError decodeURI decodeURIComponent encodeURI encodeURIComponent eval
isFinite isNaN parseFloat parseInt undefined

ArrayBuffer Buffer DataView Faucet Float32Array Float64Array GLOBAL
Int16Array Int32Array Int8Array Intl Map Migrations Promise Proxy Reflect
Set StateManager Symbol Uint16Array Uint32Array Uint8Array
Uint8ClampedArray WeakMap WeakSet WebAssembly XMLHttpRequest _ assert
async_hooks buffer child_process clearImmediate clearInterval
clearTimeout cluster console crypto dgram dns domain escape events fs
global http http2 https module net os path perf_hooks process punycode
querystring readline repl require root setImmediate setInterval
setTimeout stream string_decoder tls tty unescape url util v8 vm web3
zlib

__defineGetter__ __defineSetter__ __lookupGetter__ __lookupSetter__
__proto__ constructor hasOwnProperty isPrototypeOf propertyIsEnumerable
toLocaleString toString valueOf
```

The vast majority of the wallet and node related functions are provided by the web3 object, which is an instance of the web3.js library. The web3 object abstracts the RPC interface to our parity node. You will also notice two objects with familiar names: Migrations and Faucet. Those represent the contracts we just deployed. We will use the truffle console to interact with a contract. First, let's check our wallet via the web3 object:

```
truffle(localnode)> web3.eth.accounts
[ '0x9e713963a92c02317a681b9bb3065a8249de124f',
  '0xdb5dc1a13e3a55cf3b4587cd8d1e5fdeb6738145' ]
```

Our parity client has two wallets, with some test ether on Ropsten. The web3.eth.accounts attribute contains a list of all the accounts. We can check the balance of the first account, using the getBalance

function:

```
truffle(localnode)> web3.eth.getBalance(web3.eth.accounts[0]).toNumber()
191198572800000000
truffle(localnode)>
```

The web3.js is a large JavaScript library that offers a comprehensive interface to the Ethereum system, via a provider such as a local client. We will examine web3.js in more detail in [\[web3js\]](#). Now let's try to interact with our contracts:

```
truffle(localnode)> Faucet.address
'0xd01cd8e7bd29e4bff8c1693f59eee46137a9f300'
truffle(localnode)> web3.eth.getBalance(Faucet.address).toNumber()
0
truffle(localnode)>
```

Next, we'll use sendTransaction to send some test ether to fund the Faucet. Note the use of web3.toWei to convert ether units for us. Typing eighteen zeros without making a mistake is both difficult and dangerous, so it's always better to use a unit converter for values. Here's how we send the transaction:

```
truffle(localnode)> web3.eth.sendTransaction({from:web3.eth.accounts[0],
  to:Faucet.address, value:web3.toWei(0.5, 'ether')});
'0xf134c75b985dc0e0c27c2f0412251e0860eb530a5055e660f21e7483ab336808'
```

Switch to the web console on parity, where you will see a pop-up asking you to confirm this transaction. Wait a minute and once the transaction is mined, you will be able to see the balance of our Faucet contract:

```
truffle(localnode)> web3.eth.getBalance(Faucet.address).toNumber()
500000000000000000
```

Let's call the withdraw function now, to withdraw some test ether from the Faucet:

```
truffle(localnode)> Faucet.deployed().then(instance =>
{instance.withdraw(web3.toWei(0.1, 'ether'))}).then(console.log)
```

Again, you will need to approve the transaction in the parity web console. The balance of the Faucet has decreased, and our test wallet has received 0.1 ether:

```
truffle(localnode)> web3.eth.getBalance(Faucet.address).toNumber()
4000000000000000
```

```
truffle(localnode)> Faucet.deployed().then(instance =>
{instance.withdraw(web3.toWei(1, 'ether'))})
```

```
StatusError: Transaction:
0xe147ae9e3610334ada8d863c9028c12bd0501be2d0cf05865c18612b92d3f9c exited
with an error (status 0).
```

Embark

Embark is a framework built to allow developers to easily develop and deploy Decentralized Applications. Embark integrates with Ethereum, IPFS, whisper and Swarm to offer the following features:

- * Automatically deploy contracts and make them available in JS code.
- * Watch for changes and update contracts to redeploy if needed.
- * Manage and interact with different chains (e.g testnet, local, mainnet).
- * Manage complex systems of interdependent contracts.
- * Store and Retrieve data, including uploading and retrieving files hosted in IPFS.
- * Ease the process of deploying the full application to IPFS or Swarm.
- * Send and receive messages through Whisper.

Github: <https://github.com/embark-framework/embark/>

Documentation: <https://embark.status.im/docs/>

npm package repository: <https://www.npmjs.com/package/embark>

```
$ npm -g install embark
```

OpenZeppelin

[OpenZeppelin](https://openzeppelin.org/) [https://openzeppelin.org/] is an open framework of reusable and secure smart contracts in the Solidity language.

It is community-driven, led by the [Zeppelin](https://zeppelin.solutions/) [https://zeppelin.solutions/] team, with over a hundred external contributors. The main focus of the framework is security, achieved by applying industry-standard contract security patterns and best practices, taking advantage of all the experience the Zeppelin devs have gained from [auditing](https://blog.zeppelin.solutions/tagged/security) [https://blog.zeppelin.solutions/tagged/security] a huge number of contracts, and through constant testing and auditing from the community that uses the framework as a base for their real-world applications.

The OpenZeppelin framework is the most widely used solution for Ethereum smart contracts. The framework currently has an ample library of contracts including implementations of [ERC20](#) and [ERC721](#) tokens, many flavors of crowdsale models, and simple behaviors commonly found in contracts such as [Ownable](#), [Pausable](#) or [LimitBalance](#). The contracts in this repository in some cases function as *de facto* standard implementations.

The framework is licensed under an MIT license, and all the contracts have been designed with a modular approach to guarantee ease of reuse and extension. These are clean and basic building blocks, ready to be used on your next Ethereum project. Let's set up the framework and build a simple crowdsale using the OpenZeppelin contracts, to demonstrate how easy it is to use. This example also stresses the importance of reusing secure components instead of writing them by yourself.

First, we will need to install the `openzeppelin-solidity` library into our workspace. The latest release as of the time of this writing is [v1.9.0](#), so we will use that one.

```
mkdir sample-crowdsale
cd sample-crowdsale
npm install openzeppelin-solidity@1.9.0
mkdir contracts
```

At the time of writing, OpenZeppelin includes multiple basic token contracts that follow the ERC20, ERC721 and ERC827 standards, with different characteristics for emission, limits, vesting, lifecycle, etc.

Let's make an ERC20 token that's mintable, meaning that the initial supply starts at 0 and new tokens can be created by the token owner (in our case, the crowdsale contract) and sold to buyers. In order to

do this, create a `contracts/SampleToken.sol` file with the following contents:

```
pragma solidity 0.4.23;

import 'openzeppelin-solidity/contracts/token/ERC20/MintableToken.sol';

contract SampleToken is MintableToken {
    string public name = "SAMPLE TOKEN";
    string public symbol = "SAM";
    uint8 public decimals = 18;
}
```

OpenZeppelin already provides a `MintableToken` contract that we can use as a base for our token, so we only define the details that are specific to our case. Next, let's make the crowdsale contract. Just like with tokens, OpenZeppelin already provides a wide variety of crowdsale flavors. Currently, you will find contracts for various scenarios involving distribution, emission, price, and validation. So, let's say that you want to set a goal for your crowdsale and if it's not met by the time the sale finishes, you want to refund all your investors. For that, you can use the [RefundableCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/distribution/RefundableCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/distribution/RefundableCrowdsale.sol>] contract. Maybe you want to define a crowdsale with an increasing price to incentivize early buyers; there is the [IncreasingPriceCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/price/IncreasingPriceCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/price/IncreasingPriceCrowdsale.sol>] contract just for that. Or maybe end the crowdsale when a specified amount of ether has been received by the contract ([CappedCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/validation/CappedCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/validation/CappedCrowdsale.sol>]), or set a finishing time with the [TimedCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/validation/TimedCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/validation/TimedCrowdsale.sol>] contract, or a whitelist of buyers with the [WhitelistedCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/validation/WhitelistedCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/validation/WhitelistedCrowdsale.sol>] contract.

As we said before, the OpenZeppelin contracts are basic building blocks. These crowdsale contracts have been designed to be combined; just read the source code of the base [Crowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/Crowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/Crowdsale.sol>] contract for directions on how to extend it. For the crowdsale of our token, we need to mint tokens when ether is received by the crowdsale contract, so let's use [MintedCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/emission/MintedCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/emission/MintedCrowdsale.sol>] as a base. And to make it more interesting, let's make it also a [PostDeliveryCrowdsale](https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/distribution/PostDeliveryCrowdsale.sol) [<https://github.com/OpenZeppelin/openzeppelin-solidity/blob/v1.9.0/contracts/crowdsale/distribution/PostDeliveryCrowdsale.sol>] so the tokens can only be withdrawn after the

crowdsale ends. Write the following into `contracts/SampleCrowdsale.sol`:

```
pragma solidity 0.4.23;

import './SampleToken.sol';
import 'openzeppelin-solidity/contracts/crowdsale/emission/MintedCrowdsale.sol';
import 'openzeppelin-solidity/contracts/crowdsale/distribution/PostDeliveryCrowdsale.sol';

contract SampleCrowdsale is PostDeliveryCrowdsale, MintedCrowdsale {

    constructor(
        uint256 _openingTime,
        uint256 _closingTime
        uint256 _rate,
        address _wallet,
        MitableToken _token
    )
        public
        Crowdsale(_rate, _wallet, _token)
        PostDeliveryCrowdsale(_openingTime, _closingTime)
    {
    }
}
```

Again, we barely had to write any code, just reuse the battle-tested code that the OpenZeppelin community made available. However, it is important to note that this case is different than that of our `SampleToken` contract. If you go to the [Crowdsale automated tests](https://github.com/OpenZeppelin/openzeppelin-solidity/tree/v1.9.0/test/crowdsale) [<https://github.com/OpenZeppelin/openzeppelin-solidity/tree/v1.9.0/test/crowdsale>] you will see that they are tested in isolation. When you integrate different units of code into a bigger component, it's not enough to test all the units separately, because the interactions between them might cause behaviors that you didn't expect. In particular, you will see that here we introduced multiple inheritance, which can surprise the developer if they don't understand the details of Solidity. Our `SampleCrowdsale` is simple, and it will work just as we expect because the framework was designed to make cases like these straightforward; but do not relax your vigilance because of the simplicity that this framework introduces. Every time you integrate parts of the OpenZeppelin framework to build a more complex solution, you must fully test every aspect of your

solution to ensure that all the interactions of the units work as you intend.

Finally, when we are happy with our solution and have tested it thoroughly, we need to deploy it. OpenZeppelin integrates well with Truffle, so we can just write a migrations file as explained in the Truffle section above. Write the following in migrations/2_deploy_contracts.js:

```
const SampleCrowdsale = artifacts.require('./SampleCrowdsale.sol');
const SampleToken = artifacts.require('./SampleToken.sol');

module.exports = function(deployer, network, accounts) {
  const openingTime = web3.eth.getBlock('latest').timestamp + 2; // two
  secs in the future
  const closingTime = openingTime + 86400 * 20; // 20 days
  const rate = new web3.BigNumber(1000);
  const wallet = accounts[1];

  return deployer
    .then(() => {
      return deployer.deploy(SampleToken);
    })
    .then(() => {
      return deployer.deploy(
        SampleCrowdsale,
        openingTime,
        closingTime,
        rate,
        wallet,
        SampleToken.address
      );
    });
};
```

This was just a quick overview of a few of the contracts that are part of the OpenZeppelin framework. You are welcome to join the OpenZeppelin development community to learn and contribute.

Github: <https://github.com/OpenZeppelin/openzeppelin-solidity>

Website: <https://openzeppelin.org/>

zeppelin_os

[zeppelin_os](https://github.com/zeppelinos) [https://github.com/zeppelinos] is an open source, distributed platform of tools and services on top of the EVM to develop and manage smart contract applications securely.

Unlike OpenZeppelin's code, which needs to be re-deployed with each application every time, zeppelin_os's code lives on-chain. Applications that need a given functionality, say, an ERC20 token, not only do not have to re-design and re-audit its implementation (something that OpenZeppelin solved) but do not even need to deploy it. With zeppelin_os, an application interacts with the token's on-chain implementation directly, in much the same way as a desktop application interacts with the components of its underlying OS.

At the core of zeppelin_os sits a very clever contract known as a "proxy". A proxy is a contract that is capable of wrapping any other contract, exposing its interface without having to manually implement setters and getters for it, and can upgrade it without losing state. In Solidity terms, it can be seen as a normal contract whose business logic is contained within a library, which can be swapped for a new library at any time without losing its state. The way in which the proxy links to its implementation is completely automated and encapsulated for the developer. Practically any contract can be made upgradeable with little to no change in its code. More about zeppelin_os's proxy mechanism can be found in zeppelin_os's blog: [upgradeability-using-unstructured-storage](https://blog.zeppelinos.org/) [https://blog.zeppelinos.org/], and an example of how to use it can be found here: <https://github.com/zeppelinos/zos-lib/tree/master/examples/single>.

Developing applications using zeppelin_os is similar to developing JavaScript applications using NPM. An AppManager handles an application package for each version of the application. A package is simply a directory of contracts, each of which can have one or more upgradeable proxies. The AppManager not only provides proxies for application-specific contracts, but also does so for zeppelin_os implementations, in the form of a standard library. To see a full example of this, please visit: [examples/complex](https://github.com/zeppelinos/zos-lib/tree/master/examples/complex) [https://github.com/zeppelinos/zos-lib/tree/master/].

Although currently in development, zeppelin_os aims to provide a wide set of additional features, such as developer tools, a scheduler that automates background operations within contracts, development bounties, a marketplace that facilitates communication and exchange of value between applications, and much more. All of this is described in zeppelin_os's [whitepaper](https://zeppelinos.org/zeppelin_os_.pdf) [https://zeppelinos.org/zeppelin_os_.pdf].

Utilities

EthereumJS helpeth: A command line utility

helpeth is a command line tool for key and transaction manipulation that makes a developer's job a lot easier.

It is part of the EthereumJS collection of JavaScript based libraries and tools.

<https://github.com/ethereumjs/helpeth>

Usage: helpeth [command]

Commands:

signMessage <message>	Sign a message
verifySig <hash> <sig>	Verify signature
verifySigParams <hash> <r> <s> <v>	Verify signature parameters
createTx <nonce> <to> <value> <data>	Sign a transaction
<gasLimit> <gasPrice>	
assembleTx <nonce> <to> <value> <data>	Assemble a transaction from
its	
<gasLimit> <gasPrice> <v> <r> <s>	components
parseTx <tx>	Parse raw transaction
keyGenerate [format] [icapdirect]	Generate new key
keyConvert	Convert a key to V3 keystore
format	
keyDetails	Print key details
bip32Details <path>	Print key details for a given
path	
addressDetails <address>	Print details about an
address	
unitConvert <value> <from> <to>	Convert between Ethereum
units	

Options:

```
-p, --private      Private key as a hex string
[string]
--password       Password for the private key
[string]
--password-prompt Prompt for the private key password
[boolean]
-k, --keyfile    Encoded key file
[string]
--show-private   Show private key details
[boolean]
--mnemonic      Mnemonic for HD key derivation
[string]
--version        Show version number
[boolean]
--help           Show help
[boolean]
```

dapp.tools

Dapp.Tools is a comprehensive suite of blockchain-oriented developer tools created in the spirit of the Unix philosophy.

The documentation and installation instructions are found at <https://dapp.tools/>

Dapp

Dapp is all you need to start developing for Ethereum. It creates new DApps, runs Solidity unit tests, debugs, deploys, launches testnets, and more.

Seth

Seth is a handy tool for slicing and dicing transactions, querying the blockchain, converting between data formats, performing remote calls, and other everyday tasks.

Hevm

Hevm is a Haskell EVM implementation with a nimble terminal-based Solidity debugger. It's used to test and debug DApps.

Evmdis

Evmdis is an EVM disassembler. It performs static analysis on the bytecode to provide a higher level of abstraction for the bytecode than raw EVM operations.

Features include:

- Separates bytecode into basic blocks.
- Jump target analysis, assigning labels to jump targets and replacing addresses with label names.
- Composes individual operations into compound expressions where possible.
- Provides insight into the state of the stack at the start of each block.

Github: <https://github.com/arachnid/evmdis>

SputnikVM

SputnikVM is a standalone pluggable virtual machine for different Ethereum-based blockchains. It's written in Rust, can be used as a binary, cargo crate, shared library, or integrated through FFI, Protobuf and JSON interface. It has a separate binary sputnikvm-dev intended for testing purposes, which emulates most of the JSON RPC API and block mining.

Github: <https://github.com/etcdevteam/sputnikvm>

Libraries

web3.js

web3.js is the Ethereum-compatible JS API for communicating with clients via JSON RPC, developed by the Ethereum Foundation.

Github: <https://github.com/ethereum/web3.js>

npm package repository: <https://www.npmjs.com/package/web3>

Documentation link for web3.js API 0.2x.x; <https://github.com/ethereum/wiki/wiki/JavaScript-API>

Documentation link for web3.js API 1.0.0-beta.xx; <https://web3js.readthedocs.io/en/1.0/web3.html>

web3.py

web3.py is a Python library for interacting with the Ethereum blockchain, maintained by the Ethereum Foundation.

Github: <https://github.com/ethereum/web3.py>

PyPi: <https://pypi.python.org/pypi/web3/4.0.0b9>

Documentation: <https://web3py.readthedocs.io/>

EthereumJS

A collection of libraries and utilities for Ethereum.

Github: <https://github.com/ethereumjs>

Website: <https://ethereumjs.github.io/>

web3j

web3j is the Java and Android library for integrating with Ethereum clients and working with smart contracts.

Github: <https://github.com/web3j/web3j>

Website: <https://web3j.io>

Documentation: <https://docs.web3j.io>

Etherjar

Etherjar is another Java library for integrating with Ethereum and working with smart contracts. It's designed for server side projects based on Java 8+, provides low-level access and a high-level wrapper around RPC, Ethereum data structures and Smart Contract access.

Github: <https://github.com/infinitape/etherjar>

Nethereum

Nethereum is the .Net integration library for Ethereum.

Github: <https://github.com/Nethereum/Nethereum>

Website: <http://nethereum.com/>

Documentation: <https://nethereum.readthedocs.io/en/latest/>

ethers.js

The ethers.js library is a compact, complete, full-featured, extensively tested MIT-licensed Ethereum library, which has received a DevEx grant from the Ethereum Foundation towards its extension and maintenance.

GitHub link: <https://github.com/ethers-io/ethers.js>

Documentation: <https://docs.ethers.io>

Emerald Platform

Emerald Platform provides libraries and UI components to build DApps on top of Ethereum. Emerald JS and Emerald JS UI provides set of modules and React components to build JavaScript applications and websites; Emerald SVG Icons is a set of blockchain related icons. In addition to JavaScript libraries it has a Rust library to operate private keys and transaction signatures. All Emerald libraries and components are licensed under the Apache License, version 2.0.

Github: <https://github.com/etcdevteam/emerald-platform>

Documentation: <https://docs/etcdevteam.com>

Testing smart contracts

There are several commonly-used test frameworks for smart contract development, summarized in [Smart Contract Test Frameworks](#), below.

Table 10. Smart Contract Test Frameworks

Framework	Test Language(s)	Testing Framework	Chain Emulator	Website
Truffle	JavaScript/Solidity	Mocha	TestRPC/Ganache	truffleframework.com
Embark	JavaScript	Mocha	TestRPC/Ganache	embark.readthedocs.io
DApp	Solidity	ds-test (custom)	Ethrun (Parity)	dapp.readthedocs.io
Populus	Python	Pytes	Python chain emulator	populus.readthedocs.io

Truffle Test

Part of the Truffle framework, Truffle allows for unit tests to be written in JavaScript (Mocha based) or Solidity. These tests are run against Ganache.

Embark Framework Testing

Embark integrates with Mocha to run unit tests written in JavaScript. The tests are in turn run against contracts deployed on TestRPC/Ganache. The Embark Framework automatically deploys smart contracts, and will automatically redeploy the contracts when they are changed. It also keeps track of deployed contracts and deploys contracts only when truly needed. Embark includes a testing library to rapidly run and test your contracts in an EVM, with functions like assert.equal(). The command embark test will run any test files under directory test.

DApp

DApp uses native Solidity code (a library called ds-test) and a Parity-built Rust library called Ethrun to execute Ethereum bytecode and then assert correctness. The ds-test library provides assertion functions for validating correctness and events for logging data in the console.

Assertions functions include:

```
assert(bool condition)
assertEq(address a, address b)
assertEq(bytes32 a, bytes32 b)
assertEq(int a, int b)
assertEq(uint a, uint b)
assertEq0(bytes a, bytes b)
expectEventsExact(address target)
```

Logging commands will log information to the console, making them useful for debugging:

```
logs(bytes)
log_bytes32(bytes32)
log_named_bytes32(bytes32 key, bytes32 val)
log_named_address(bytes32 key, address val)
log_named_int(bytes32 key, int val)
log_named_uint(bytes32 key, uint val)
log_named_decimal_int(bytes32 key, int val, uint decimals)
log_named_decimal_uint(bytes32 key, uint val, uint decimals)
```

Populus

Populus uses Python and its own chain emulator to run contracts written in Solidity. Unit tests are written in Python with the pytest library. Populus supports writing contracts specifically for testing. These contract filenames should match the glob pattern `Test*.sol` and be located anywhere under the project tests directory `tests`.

On-Blockchain Testing

Although most testing shouldn't occur on deployed contracts, a contract's behavior can be checked via Ethereum clients. The following commands can be used to assess a smart contract's state. These commands should be typed at the '`geth`' terminal, although any web3 console will also support these commands.

```
eth.getTransactionReceipt(txhash);
```

Gets the address of a contract at `txhash`.

```
eth.getCode(contractaddress)
```

Gets the code of a contract deployed at `contractaddress`. This can be used to verify proper deployment.

```
eth.getPastLogs(options)
```

Gets the full logs of the contract located at the address specified in options. This is helpful for viewing the history of a contract's calls.

```
eth.getStorageAt(address, position)
```

Gets the storage located at address with an offset of position.

Ganache: A local test blockchain

Ganache is a local test blockchain that you can use to deploy contracts, develop your applications, and run tests. It is available as a desktop application (with a graphical user interface) for Windows, Mac, and Linux. It is also available as a command-line utility called ganache-cli. For more details and installation instructions for the Ganache desktop application, see:

<https://truffleframework.com/ganache>

The ganache-cli code can be found here:

<https://github.com/trufflesuite/ganache-cli/>

To install the command line ganache-cli, use npm:

```
$ npm install -g ganache-cli
```

We can use ganache-cli to start a local blockchain for testing.

```
$ ganache-cli \
--networkId=3 \
--port="8545" \
--verbose \
--gasLimit=8000000 \
--gasPrice=4000000000;
```

- ☒ Check the `--networkId` and `--port` flag values match your configuration in truffle.js
- ☒ Check the `--gasLimit` flag value matches the latest mainnet Gas Limit (i.e. 8000000 gas) shown at <https://ethstats.net> to avoid encountering `out of gas` exceptions unnecessarily. Note that a `--gasPrice` of 4000000000 represents a Gas Price of 4 gwei.
- ☒ Optionally enter a `--mnemonic` flag value to restore a previous HD wallet and associated addresses

Appendix E: web3.js tutorial

Description

This tutorial is based on web3@1.0.0-beta.29 web3.js. It is intended as an introduction to web3.js.

The web3.js JavaScript library is a collection of modules which contain specific functionality for the Ethereum ecosystem, and an Ethereum compatible JavaScript API, which implements the Generic JSON RPC spec.

To run this script you don't need to run your own local node, because it uses the [Infura services](#) [<https://infura.io>].

web3.js contract basic interaction in a non-blocked (async) fashion

Check you have a valid npm version:

```
$ npm -v  
5.6.0
```

If you haven't initialize npm:

```
$ npm init
```

Install basic dependences:

```
npm i command-line-args  
npm i web3  
npm i node-rest-client-promise
```

This will update your package.json configuration file with your new dependences.

Node.js script execution

Basic execution

```
code/web3js/web3-contract-basic-interaction.js
```

Use your own Infura Token

```
code/web3js/web3-contract-basic-interaction.js --infuraFileToken  
/path/to/file/with/infura_token
```

or

```
code/web3js/web3-contract-basic-interaction.js  
/path/to/file/with/infura_token
```

Reviewing the demo script

Next, let's review our demo script web3-contract-basic-interaction.

We use the Web3 object to obtain a basic web3 provider:

```
var web3 = new Web3(infura_host);
```

Next, let's interact with web3 and try some basic functions. Let's see the protocol version:

```
web3.eth.getProtocolVersion().then(function(protocolVersion) {  
    console.log(`Protocol Version: ${protocolVersion}`);  
})
```

Now let's look at the current gas price:

```
web3.eth.getGasPrice().then(function(gasPrice) {  
    console.log(`Gas Price: ${gasPrice}`);  
})
```

What's the last mined block in the current chain?

```
web3.eth.getBlockNumber().then(function(blockNumber) {  
    console.log(`Block Number: ${blockNumber}`);  
})
```

Contract interaction

Now let's try some basic interactions with a contract.

We will use the contract at: <https://kovan.etherscan.io/address/0xd0a1e359811322d97991e03f863a0c30c2cf029c#code>

First, let's initialize our contract address:

```
var our_contract_address = "0xd0A1E359811322d97991E03f863a0C30C2cF029C";
```

Let's see its balance:

```
web3.eth.getBalance(our_contract_address).then(function(balance) {  
    console.log(`Balance of ${our_contract_address}: ${balance}`);  
})
```

Now let's see its byte code:

```
web3.eth.getCode(our_contract_address).then(function(code) {  
    console.log(code);  
})
```

We prepare our environment to interact with the Etherscan explorer API.

Let's initialize our contract url in the Etherscan explorer API for the Kovan chain:

```
var etherscan_url =  
`https://kovan.etherscan.io/api?module=contract&action=getabi&address=${o  
ur_contract_address}`
```

And let's initialize a REST client to interact with the Etherscan API:

```
var client = require('node-rest-client-promise').Client();
```

Let's get a client promise:

```
client.getPromise(etherscan_url)
```

Once we've got a valid client promise, we can get our contract ABI from the Etherscan API:

```
.then((client_promise) => {  
  our_contract_abi = JSON.parse(client_promise.data.result);
```

And now we create our contract object as a promise to consume later.

```
return new Promise((resolve, reject) => {
    var our_contract = new web3.eth.Contract(our_contract_abi,
our_contract_address);
    try {
        // If all goes well
        resolve(our_contract);
    } catch (ex) {
        // If something goes wrong
        reject(ex);
    }
});
})
```

If our contract promise returns successfully we can start interacting with it:

```
.then((our_contract) => {
```

Let's see our contract address:

```
console.log(`Our Contract address: ${our_contract._address}`);
```

or alternatively:

```
console.log(`Our Contract address in other way:
${our_contract.options.address}`);
```

Now let's query our contract abi:

```
console.log("Our contract abi: " +
JSON.stringify(our_contract.options.jsonInterface));
```

Now let's see our contract total supply using a callback:

```
our_contract.methods.totalSupply().call(function(err, totalSupply) {  
  if (!err) {  
    console.log(`Total Supply with a callback: ${totalSupply}`);  
  } else {  
    console.log(err);  
  }  
});
```

Or we can use the returned Promise instead of passing in the callback:

```
our_contract.methods.totalSupply().call().then(function(totalSupply){  
  console.log(`Total Supply with a promise: ${totalSupply}`);  
}).catch(function(err) {  
  console.log(err);  
});
```

Asynchronous operation with await

Now that you've seen the basic tutorial, we can try the same interactions using an asynchronous await construct. Review the web3-contract-basic-interaction-async-await.js script in code/web3js and compare it to this tutorial to see how they differ. Async-await is easier to read, as it makes the asynchronous interaction behave more like a sequence of blocking calls.

Index

@

\$ symbol, 83
.eth' node) + keccak('example', 373
'example.eth' node) + keccak('subdomain', 373

A

asymmetric cryptography, 99
attribution, 3

B

Bitcoin improvement proposals
 Hierarchical Deterministic Wallets (BIP-32/BIP-44), 125
 Mnemonic Code Words (BIP-39), 127
 Multipurpose HD Wallet Structure (BIP-43), 127
bitcoin improvement proposals
 Mnemonic Code Words (BIP-39), 128
blockchain applications
 warnings and cautions, 4
brainwallets, 129

C

code examples, obtaining and using, 3
cold storage, 139
comments and questions, 5
contact information, 5
cryptography
 asymmetric, 99
 defined, 97
 elliptic curve cryptography
 id=Celliptic04, 103
 see=also keys and addresses, 97

D

Dual_EC_DRBG, 113
deterministic wallets
 seealso=wallets, 122
digital currencies
 cryptocurrency, 98
digital fingerprint, 111
digital signatures
 algorithm used, 162
 asymmetric cryptography and, 99
 defined, 163
 how they work, 163
 purposes of, 163
 verifying, 164

E

Edward Snowden, 112
Elliptic Curve Digital Signature Algorithm (ECDSA), 162, 164
elliptic curve cryptography
 id=elliptic04, 103
encryption, 97
 see=also keys and addresses, 97
entropy
 random number generation, 102

F

FIPS, 112
FIPS-202, 112

G

generator point, 102, 108
getting started
 warnings and cautions, 4

H

hardened derivation, 139
hardware wallets, 128, 139
 seealso=wallets, 128
hash function, 111
hierarchical deterministic (HD) wallets, 125, 135, 140
 seealso=wallets, 122

I

intended audience, 1

J

JBOK wallets
 seealso=wallets, 122

K

Keccak Hash Function, 112
Keccak-256, 112
key derivation methods, 122
key-stretching function, 131
keychains, 121
keys and addresses
 overview of
 elliptic curve cryptography, 103
 key pairs, 100
 private key generation, 100
 public key calculation, 102
 public key cryptography, 98
 public key generation, 108
 seealso public and private keys, 142
warnings and cautions, 4

L

libsecp256k1 cryptographic library, 110

M

mnemonic code words, 122, 127, 128

N

NIST, 112
nondeterministic wallets
 seealso=wallets, 122

O

OpenSSL cryptographic library, 110
open source licenses, 3

P

PBKDF2 function, 131
passphrases, 131, 133
pre image, 111
public and private keys
 hardened child key derivation, 139
 key pairs, 98
 ephemeral, 164
 seealso keys and addresses, 98

Q

QR codes
 warnings and cautions, 4

R

Root Node) + keccak('eth', 373
random numbers
 random number generation, 102
root seeds, 135

S

SHA-3 Hash Function, 112

salts, 131

shell commands, 83

storage

 cold storage, 139

T

terminal applications, 83

transactions

 digital signatures and, 162

 warnings and cautions, 4

typographical conventions, 2

W

wallets

 best practices for, 127

 contents of, 121

 defined, 121

 technology of

 creating HD wallets from root seed, 135

 mnemonic code words, 128

 seeds and mnemonic codes, 127

 types of

 JBOK wallets, 122

 deterministic (seeded) wallets, 125

 hierarchical deterministic (HD) wallets, 125

 nondeterministic (random) wallets, 122

 primary distinctions, 122

warnings and cautions

 avoid sending money to addresses appearing

 in book, 4

 private key protection, 100