Ethereum Fundamentals

History, Definition, Smart Contracts, ERC 20

History of Ethereum

Ethereum, a second-generation cryptocurrency which emerged after Bitcoin, was initially described in a white paper by **Vitalik Buterin**, a programmer and co-founder of Bitcoin Magazine, in late 2013 with a goal of building decentralized applications.Buterin had argued that Bitcoin needed a scripting language for application development. Failing to gain agreement, he proposed the development of a new platform with a more general scripting language.

- Vitalik was 19 when he wrote the Ethereum Whitepaper
- Development was funded by an online crowdsale that took place between July and August 2014
- The system then went live on 30 July 2015

Ethereum

- Ethereum is a decentralized open source blockchain featuring smart contract functionality. Ether (ETH) is the native cryptocurrency token of the Ethereum platform. It is the second-largest cryptocurrency by market capitalization, behind Bitcoin

- EVM - Ethereum Virtual Machine, which can execute scripts using an international network of public nodes
- EVM instruction set is Turing complete in contrst to Bitcoin

In computability theory, 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. This means that this system is able to recognize or decide other data-manipulation rule sets. Turing completeness is used as a way to express the power of such a data-manipulation rule set. Virtually all programming languages today are Turing-complete. The concept is named after English mathematician and computer scientist Alan Turing.

Difference between Bitcoin and Ethereum

- Bitcoin is the first stable POW Blockchain network – much more durable, more change-resistant
- Ethereum Introduces Smart contracts and ERC 20 Tokens
- Ethereum is more adaptive to change

Smart Contracts

- What is Smart contract?

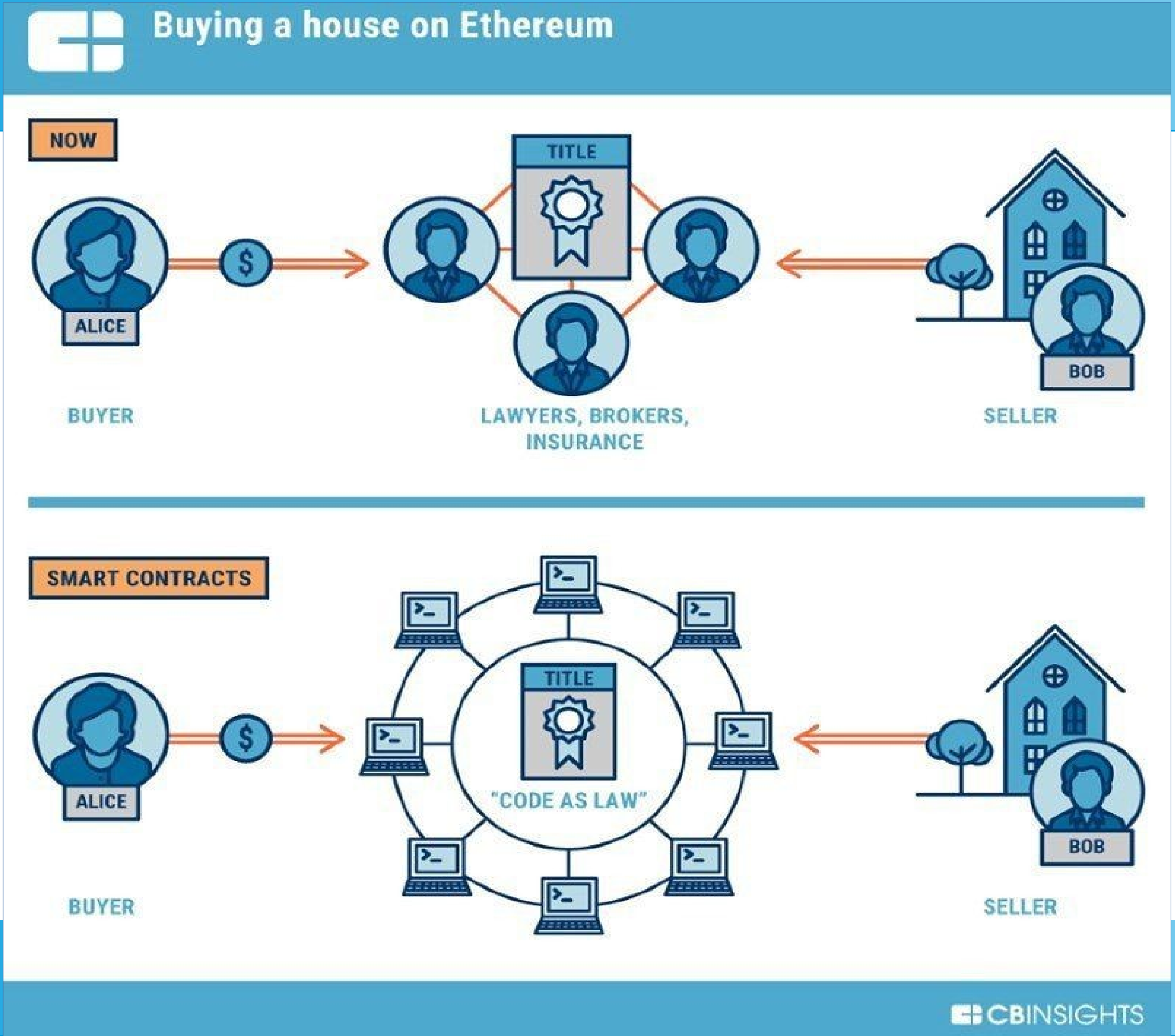
A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement. The objectives of smart contracts are the reduction of need in trusted intermediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions

Simply put, smart contracts work a lot like vending machines. You just drop a required amount of a cryptocurrency into the smart contract, and your escrow, house ownership right, driver's license, or whatever else drops into your account.

Smart Contracts Interdependence

A smart contract can work on its own, but it can also be implemented along with any number of other smart contracts. They can be set up in a way when they’ll be dependant on one another. For example, successful completion of one particular smart contract can trigger the start of another one, and so on. In theory, whole systems and organizations can run entirely on smart contracts. To some extent, this is already implemented in various cryptocurrency systems, where all the laws are pre-defined and because of that, the network itself can function autonomously and independently.

- Code as law principle!



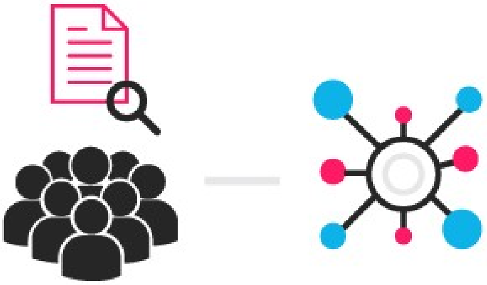
1

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

2

A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3



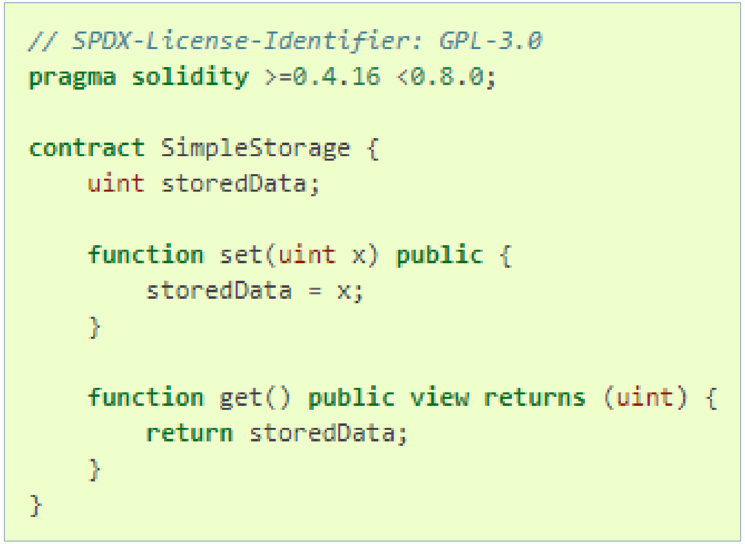
Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

Smart Contracts in Ethrereum

Smart Contracts in Ethereum use Solidity language

Remix IDE – Web based IDE for writing smart contracts

https://remix.ethereum.org/



```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.16 <0.8.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

DAPPs

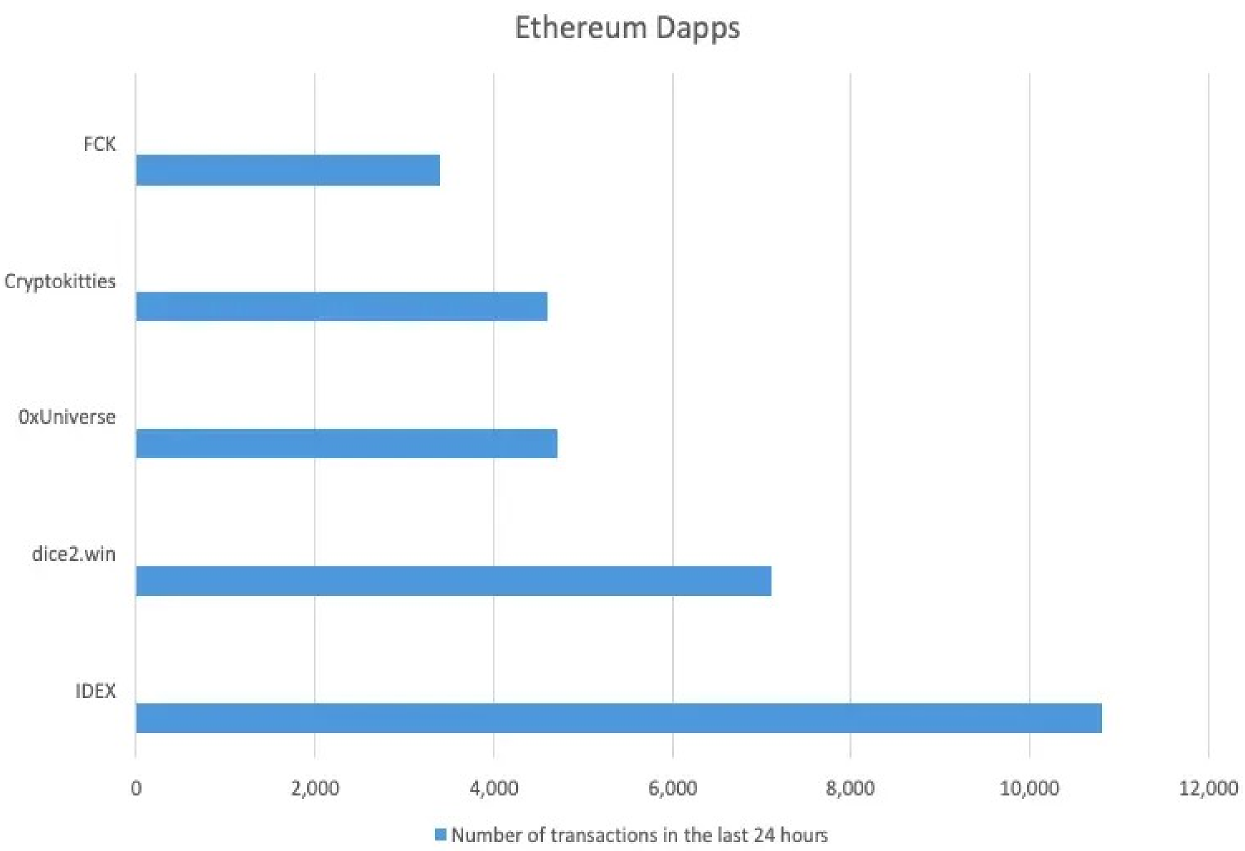
DAPPs – what are they?

Dapp – Decentralized Application

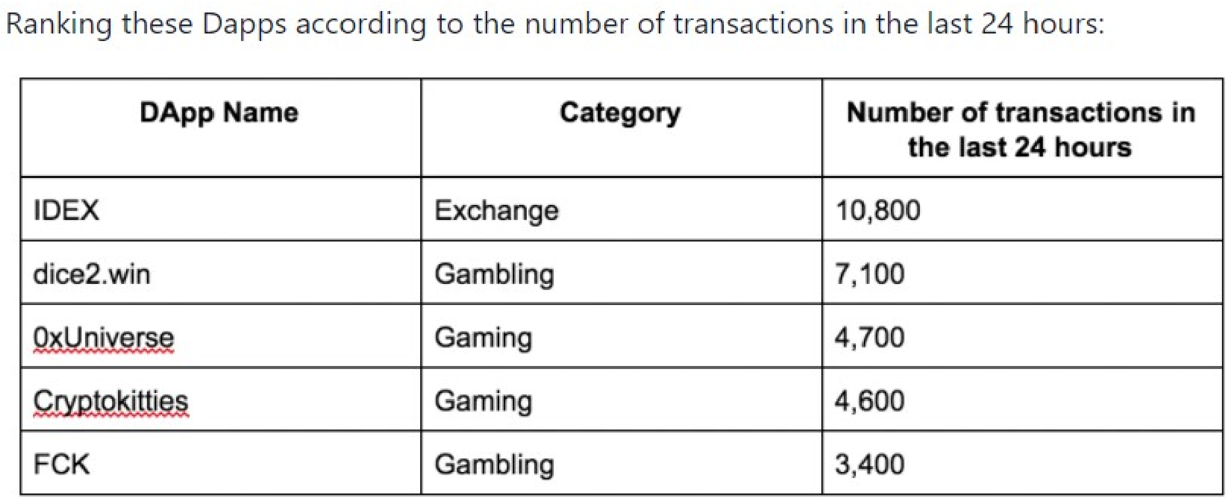
Dapp is a computer application that runs on a distributed computing system. DApps have been popularized by distributed ledger technologies (DLT) such as the Ethereum Blockchain, where DApps are often referred to as smart contracts.

DApps have their backend code running on a decentralized peer-to-peer network, as opposed to typical applications where the backend code is running on centralized servers. A DApp can have frontend code and user interfaces written in any language that can make calls to its backend.

DAPPs Examples



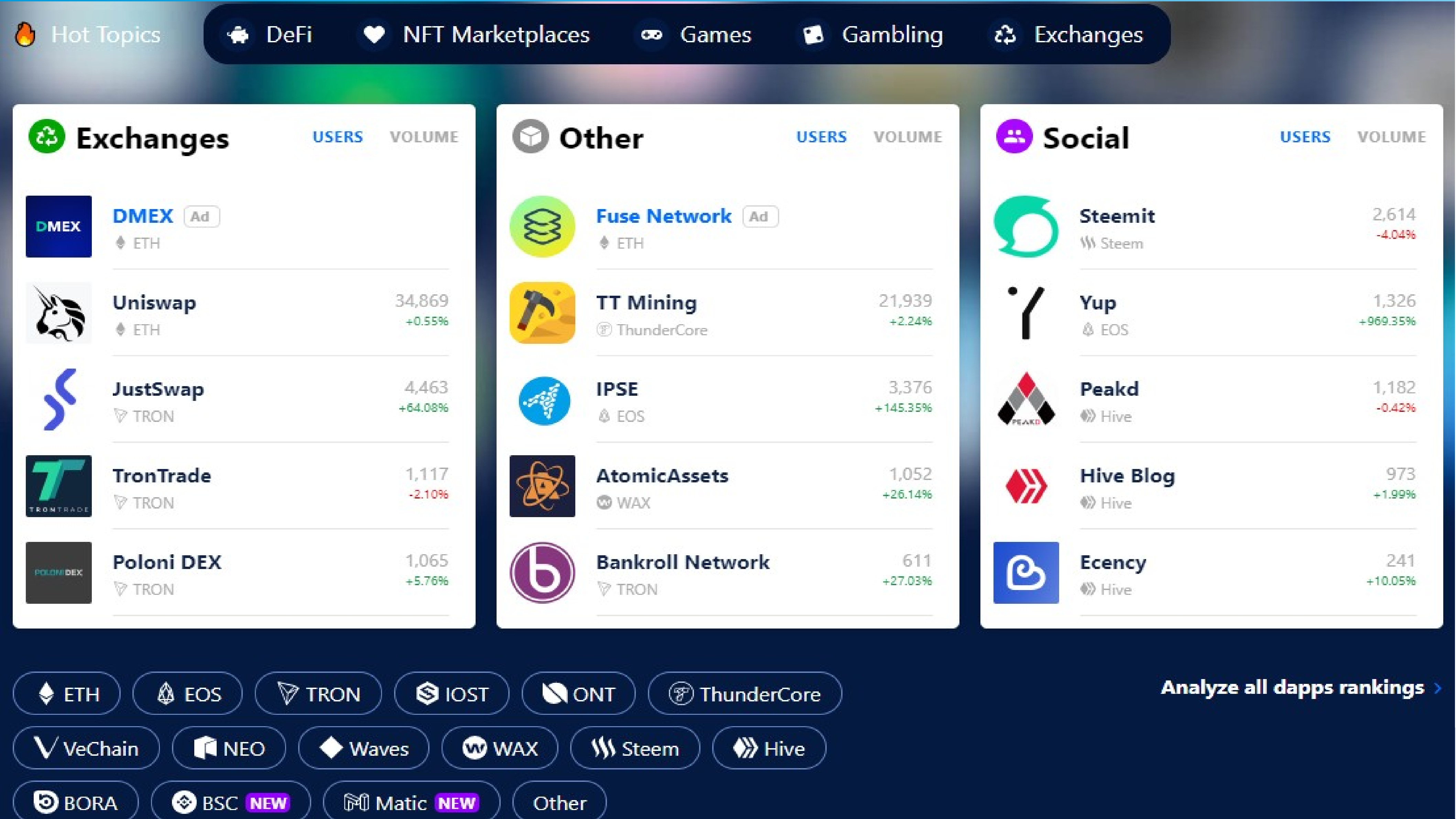
DAPPs Examples



Ranking these Dapps according to the number of transactions in the last 24 hours:

DApp Name	Category	Number of transactions in the last 24 hours
IDEX	Exchange	10,800
dice2.win	Gambling	7,100
0xUniverse	Gaming	4,700
Cryptokitties	Gaming	4,600
FCK	Gambling	3,400

https://dappradar.com/



Exchanges

USERS VOLUME

Dapp	Chain	Users	Change
DMEX Ad	ETH		
Uniswap	ETH	34,869	+0.55%
JustSwap	TRON	4,463	+64.08%
TronTrade	TRON	1,117	-2.10%
Poloni DEX	TRON	1,065	+5.76%

Other

USERS VOLUME

Dapp	Chain	Users	Change
Fuse Network Ad	ETH		
TT Mining	ThunderCore	21,939	+2.24%
IPSE	EOS	3,376	+145.35%
AtomicAssets	WAX	1,052	+26.14%
Bankroll Network	TRON	611	+27.03%

Social

USERS VOLUME

Dapp	Chain	Users	Change
Steemit	Steem	2,614	-4.04%
Yup	EOS	1,326	+969.35%
Peakd	Hive	1,182	-0.42%
Hive Blog	Hive	973	+1.99%
Ecency	Hive	241	+10.05%

Useful DAPP links

CryptoKitties

https://www.cryptokitties.co/

OpenSea

https://opensea.io/

Augur

https://augur.net/

Uniswap

https://app.uniswap.org/

The “DAO Hack”

The most infamous DAO project was the DAO created by the Slock.it and went live on 30 April 2016. It was a virtual venture capital fund that is governed by the investors of the DAO.

During the initial offering took place in May 2016, the only requirement for being an investor was to invest Ether into the system. In exchange, participants were given DAO Tokens, 100 DAO Tokens for 1 Ether, which give voting rights to be used during the selection of projects that would be funded. The DAO raised 12.7 million Ether, which was equal to more than 150 million USD back then and became the biggest crowdfunding project until its time.

On 16 June 2016, the attacker managed to retrieve approximately 3.6 million Ether from the DAO fund abusing this loophole, which is known as a “recursive call exploit”.

The “DAO Hack”

The DAO can be considered as the first big-scale application of Ethereum-based smart contracts.

The hard fork was completed on 20 July and the funds were returned to the investors. Ironically, victims of the hack were able to get their funds back since the so-called immutability was not absolute.

Decision was made that the funds will be returned to their owners by implementing Hard-fork.

The Ethereum hard-fork did not prevent all participants from following the old main branch. Thus, the branch created with the hard-fork continued as the Ethereum whereas the old branch kept going as the Ethereum Classic

ERC 20 Tokens

- What is ERC ?

In Ethereum, an ERC is an Ethereum Request for Comments. These are technical documents that outline standards for programming on Ethereum. They’re not to be confused with Ethereum Improvement Proposals (EIPs)

Authored by Vitalik Buterin and Fabian Vogelsteller in 2015, ERC-20 proposes a relatively simple format for Ethereum-based tokens. By following the outline, developers don’t need to reinvent the wheel.

It should be noted that the ERC-20 standard was developed into an EIP (specifically, EIP-20). This happened a couple of years after the original proposal due to its widespread use. However, even years later, the name “ERC-20” has stuck.

ERC 20 Tokens

- What is ERC 20 ?

ERC-20 has emerged as the technical standard used for all smart contracts on the Ethereum blockchain for token implementation.

They follow a list of standards so that they can be shared, exchanged for other tokens, or transferred to a crypto-wallet.

ERC 20 Tokens

- How ERC 20 emmerges

ERC20 was created by ethereum developers on behalf of the broader ethereum network and community in 2015 and officially recognized in September 2017. To create a standard of this type for ethereum, a developer or group of developers must submit what is known as an Ethereum Improvement Proposal (EIP) with specific protocols and standards. A committee then approves, amends, and finalizes that EIP, at that point it becomes an ERC.

Smart contracts are then obligated to conform to one of the standards. ERC20 is the best known of all of these ERC standards, but it is not the only one in existence.

ERC 20 Tokens

To put this with simple wording – using the ERC 20 Standart anyone with sufficient technical background can create their own blockchain network using Ethereum blockchain as an infrastructure!

Plenty of well-known digital currencies use the ERC-20 standard, including Maker (MKR), Basic Attention Token (BAT), Augur (REP), and OmiseGO (OMG). If you are planning on purchasing any digital currency that's issued as an ERC-20 token, you must also have a wallet that is compatible with these tokens. Luckily, because ERC-20 tokens are so popular, there are many different options for wallets.

ERC 20 Tokens

- Contents of the ERC20 Standard

ERC20 contains several functions, meaning that a compliant token must be able to implement this list (descriptions of each function are in parentheses):

- totalSupply (provide information about the total token supply)
- balanceOf (provide account balance of the owner's account)
- transfer (execute transfer of a specified number of tokens to a specified address)
- transferFrom (execute transfer of a specified number of tokens from a specified address)
- approve (allow a spender to withdraw a set number of tokens from a specified account)
- allowance (return a set number of tokens from a spender to the owner)

ERC 20 Tokens

- Example of ERC 20 Tokens

Most popular ERC 20 Tokens -
https://etherscan.io/tokens

Tehter (USDT) -
https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7

ChainLink -
https://etherscan.io/token/0x514910771af9ca656af840dff83e8264ecf986ca

Wrapped BTC
https://https://etherscan.io/token/0x2260fac5e5542a773aa44fbcfedf7c193bc2c599

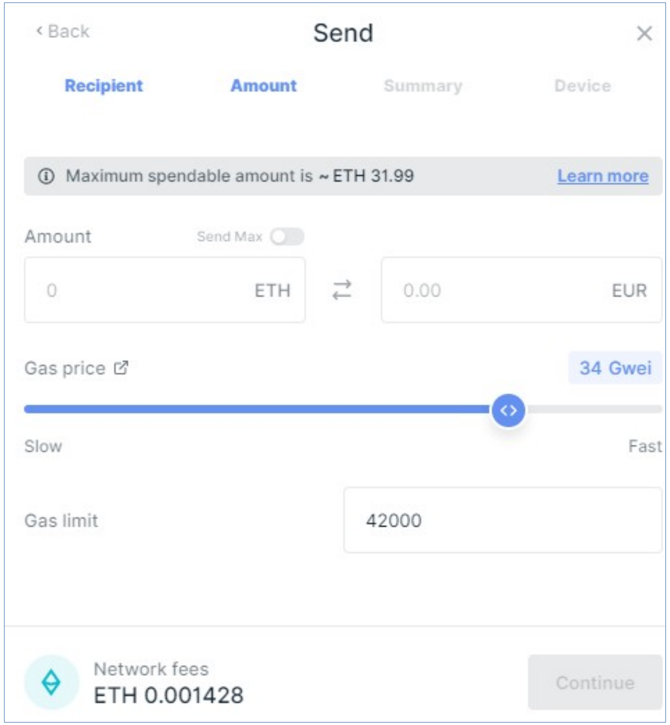
Ethereum GAS

The exchangeable unit on the network is called “Ether” (ETH)

Gas is used to submit transactions. Gas can be converted to Ethereum

- Gas Limit
- Gas Price

The total cost of a transaction (the “transaction fee”) is the Gas Limit * Gas Price.



Maximum spendable amount is ~ ETH 31.99 Learn more

Amount: 0 ETH ⇄ 0.00 EUR

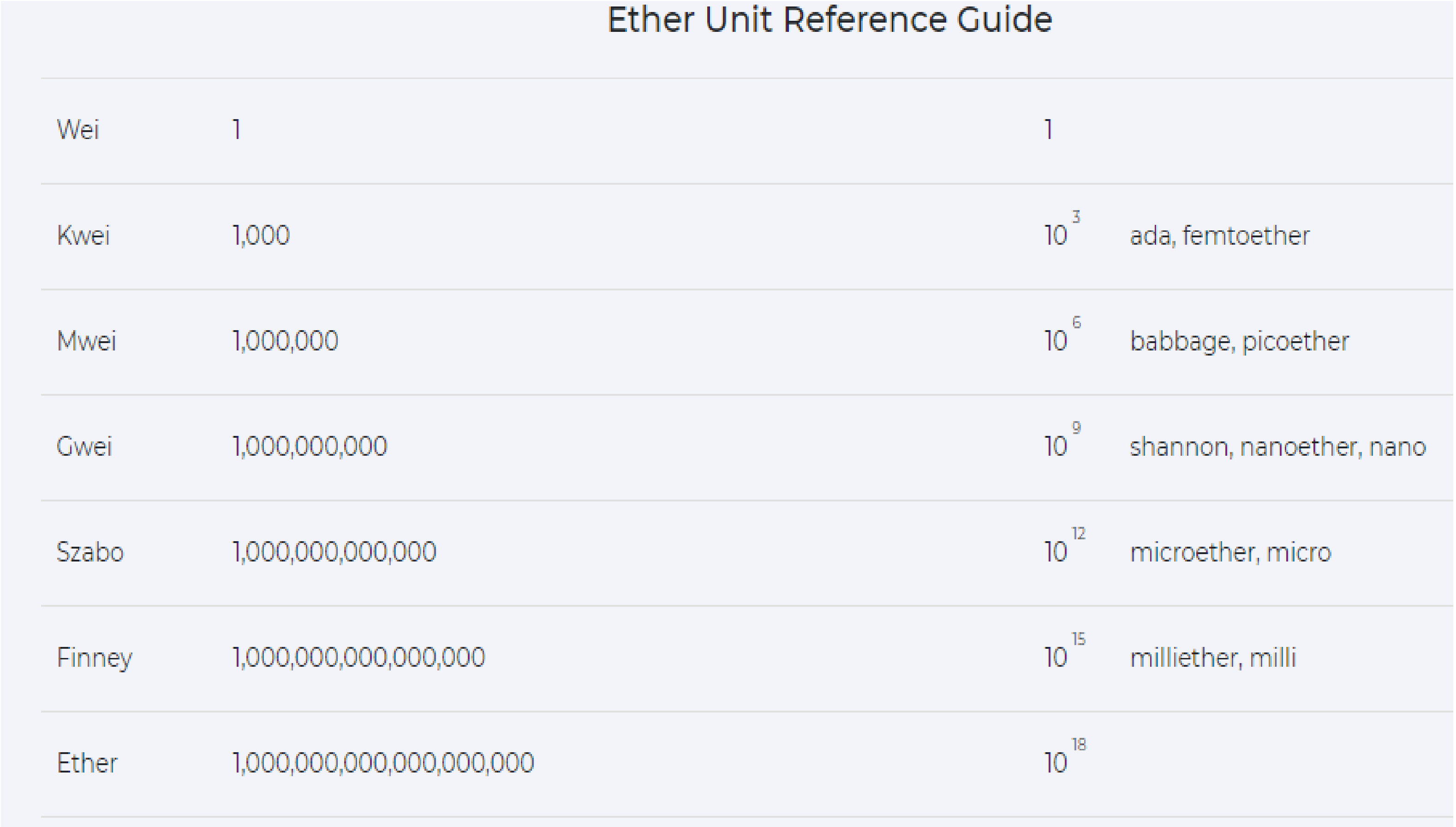
Gas price: 34 Gwei

Gas limit: 42000

Network fees
ETH 0.001428

GAS Unit reference

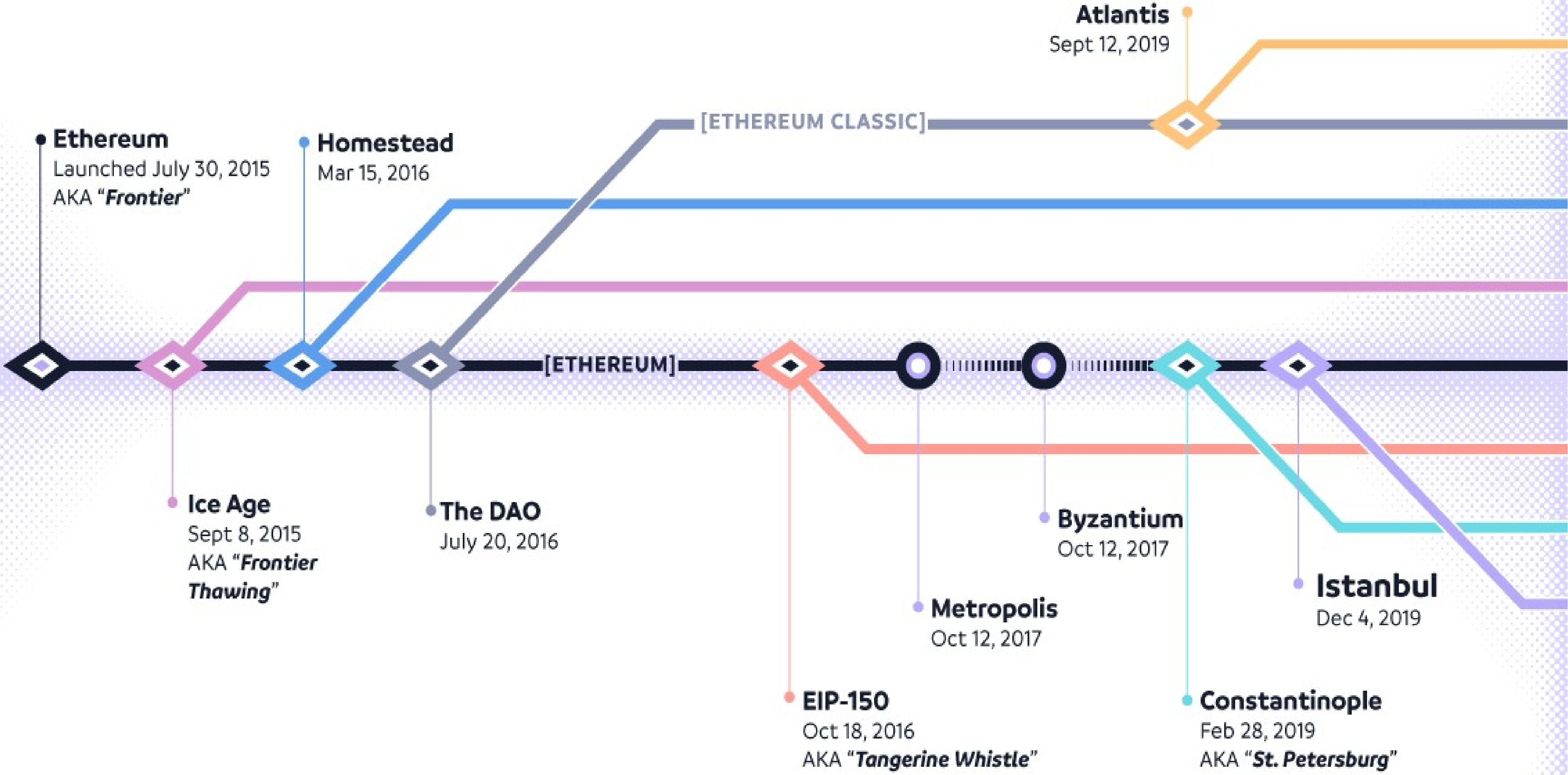
Wei Dai is a computer engineer known for contributions to cryptography and cryptocurrencies. He developed the Crypto++ cryptographic library, created the b-money cryptocurrency system. The smallest subunit of Ether, the wei, is named after him



Ether Unit Reference Guide

Wei	1	1	
Kwei	1,000	10^{3}	ada, femtoether
Mwei	1,000,000	10^{6}	babbage, picoether
Gwei	1,000,000,000	10^{9}	shannon, nanoether, nano
Szabo	1,000,000,000,000	10^{12}	microether, micro
Finney	1,000,000,000,000,000	10^{15}	milliether, milli
Ether	1,000,000,000,000,000,000	10^{18}	

https://gwei.io/



Ethereum
Launched July 30, 2015
AKA "*Frontier*"

Ice Age
Sept 8, 2015
AKA "*Frontier Thawing*"

Homestead
Mar 15, 2016

The DAO
July 20, 2016

EIP-150
Oct 18, 2016
AKA "*Tangerine Whistle*"

Metropolis
Oct 12, 2017

Byzantium
Oct 12, 2017

Constantinople
Feb 28, 2019
AKA "*St. Petersburg*"

Atlantis
Sept 12, 2019

Istanbul
Dec 4, 2019

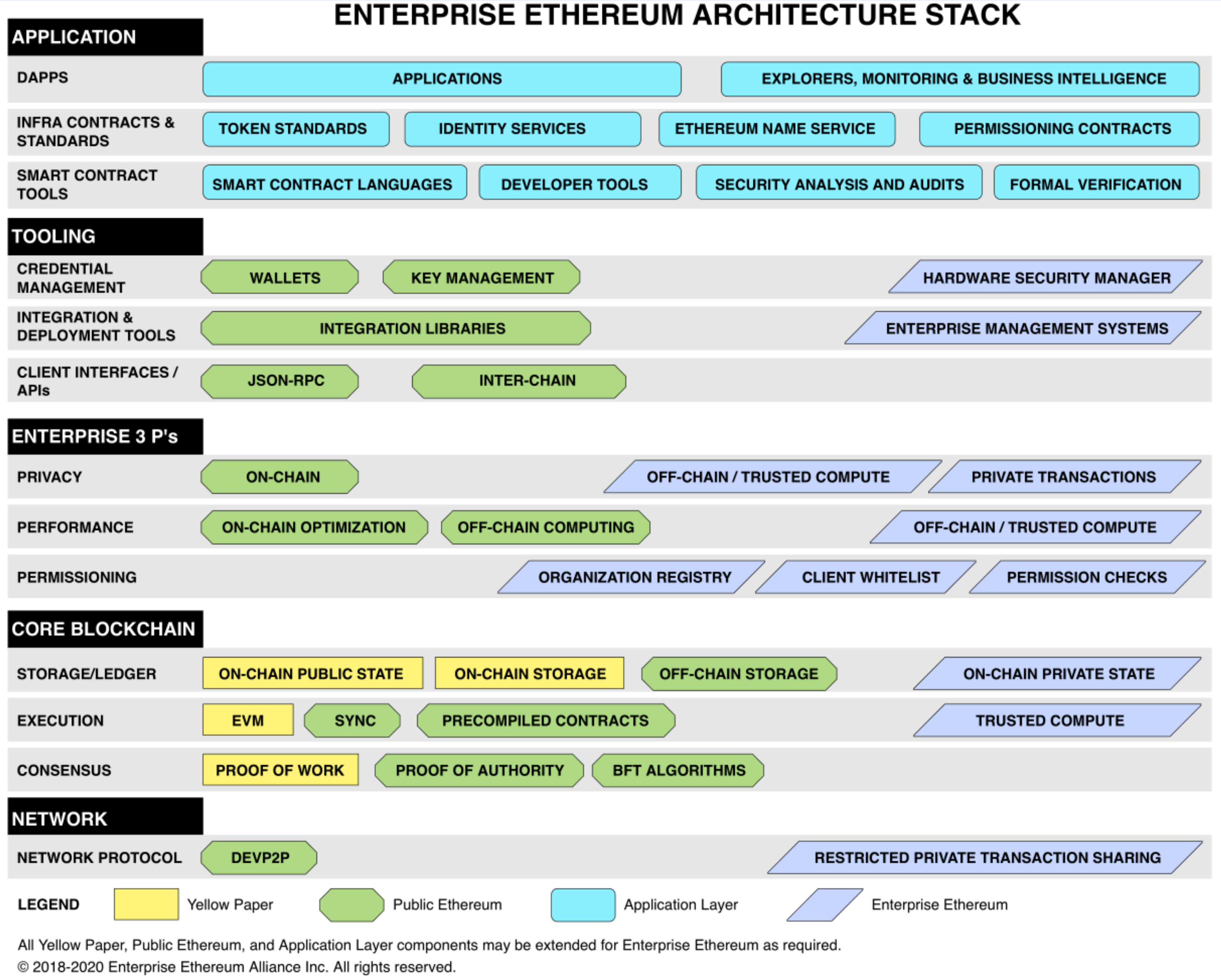
Ethereum for Corporate needs

- https://entethalliance.org/
- The Largest Enerprise Ecosystem For Ethereum

Members like Microsoft, Vmware, Baidu, Web3 Labs -

https://entethalliance.org/eea-members/

Architecture stack -
https://entethalliance.org/wp-content/uploads/2020/08/EEA_Architecture_Stack.pdf



ENTERPRISE ETHEREUM ARCHITECTURE STACK

APPLICATION

DAPPS: APPLICATIONS; EXPLORERS, MONITORING & BUSINESS INTELLIGENCE

INFRA CONTRACTS & STANDARDS: TOKEN STANDARDS; IDENTITY SERVICES; ETHEREUM NAME SERVICE; PERMISSIONING CONTRACTS

SMART CONTRACT TOOLS: SMART CONTRACT LANGUAGES; DEVELOPER TOOLS; SECURITY ANALYSIS AND AUDITS; FORMAL VERIFICATION

TOOLING

CREDENTIAL MANAGEMENT: WALLETS; KEY MANAGEMENT; HARDWARE SECURITY MANAGER

INTEGRATION & DEPLOYMENT TOOLS: INTEGRATION LIBRARIES; ENTERPRISE MANAGEMENT SYSTEMS

CLIENT INTERFACES / APIs: JSON-RPC; INTER-CHAIN

ENTERPRISE 3 P's

PRIVACY: ON-CHAIN; OFF-CHAIN / TRUSTED COMPUTE; PRIVATE TRANSACTIONS

PERFORMANCE: ON-CHAIN OPTIMIZATION; OFF-CHAIN COMPUTING; OFF-CHAIN / TRUSTED COMPUTE

PERMISSIONING: ORGANIZATION REGISTRY; CLIENT WHITELIST; PERMISSION CHECKS

CORE BLOCKCHAIN

STORAGE/LEDGER: ON-CHAIN PUBLIC STATE; ON-CHAIN STORAGE; OFF-CHAIN STORAGE; ON-CHAIN PRIVATE STATE

EXECUTION: EVM; SYNC; PRECOMPILED CONTRACTS; TRUSTED COMPUTE

CONSENSUS: PROOF OF WORK; PROOF OF AUTHORITY; BFT ALGORITHMS

NETWORK

NETWORK PROTOCOL: DEVP2P; RESTRICTED PRIVATE TRANSACTION SHARING

LEGEND 🟨 Yellow Paper ⬢ Public Ethereum 🟦 Application Layer ▱ Enterprise Ethereum

All Yellow Paper, Public Ethereum, and Application Layer components may be extended for Enterprise Ethereum as required.

Baseline Protocol

What is Baseline Protocol?

The Baseline Protocol initiative was announced on March 4, 2020 and launched as an OASIS open source project on March 19, 2020, supported by fourteen founding companies. More companies joined the effort shortly thereafter and continue to do so.

The Baseline Protocol is an open-source initiative aimed at the synchronization of private business processes, like document exchange, via a public blockchain. It leverages cryptography techniques like zero-knowledge proofs and signatures, peer-to-peer messaging protocols, and the blockchain to achieve its goals.

Baseline Protocol

Official website

https://www.baseline-protocol.org/

Members of baseline protocol:

Microsoft, ConsenSys, Enterprise Ethereum Alliance,

Ethereum Foundation, Unibright, Chainlink

Current Baseline version 0.1 Baseline examples can be found here:

https://github.com/ethereum-oasis/baseline

Different Ethereum Networks

Mainnet (public, PoW) – uses ETH, block explorer: etherscan.io

- Test networks:

Ropsten (public, Pow)
Rinkeby (authenticated, PoA)

Kovan Testnet (authenticated, PoA) – uses KETH - https://kovan.etherscan.io/

https://kovan-testnet.github.io/website/

Blockchain use in Business Domain

Use cases for Blockchain in Business Domain

link

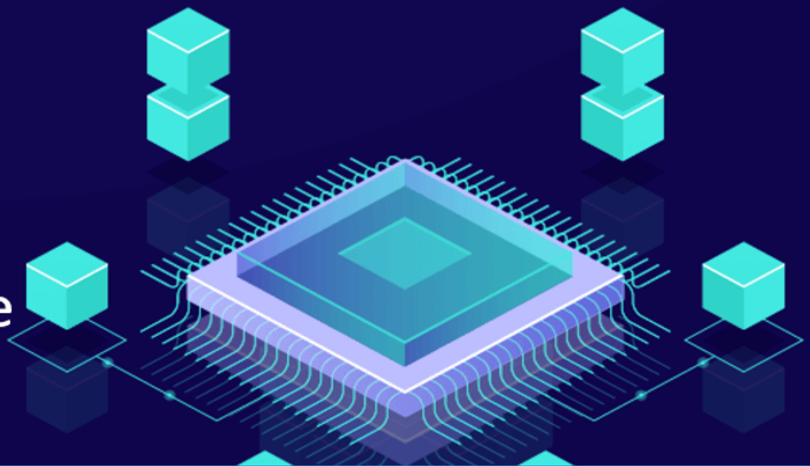
- Blockchain for Insurance
- Blockchain for Digital Rights
- Blockchain for Internet-of-Things
- Blockchain for Medical Records
- Blockchain for Banking
- Blockchain for Legal & Regtech
- Blockchain for e-Tickets

10+ MUST KNOW ENTERPRISE BLOCKCHAIN USE CASES

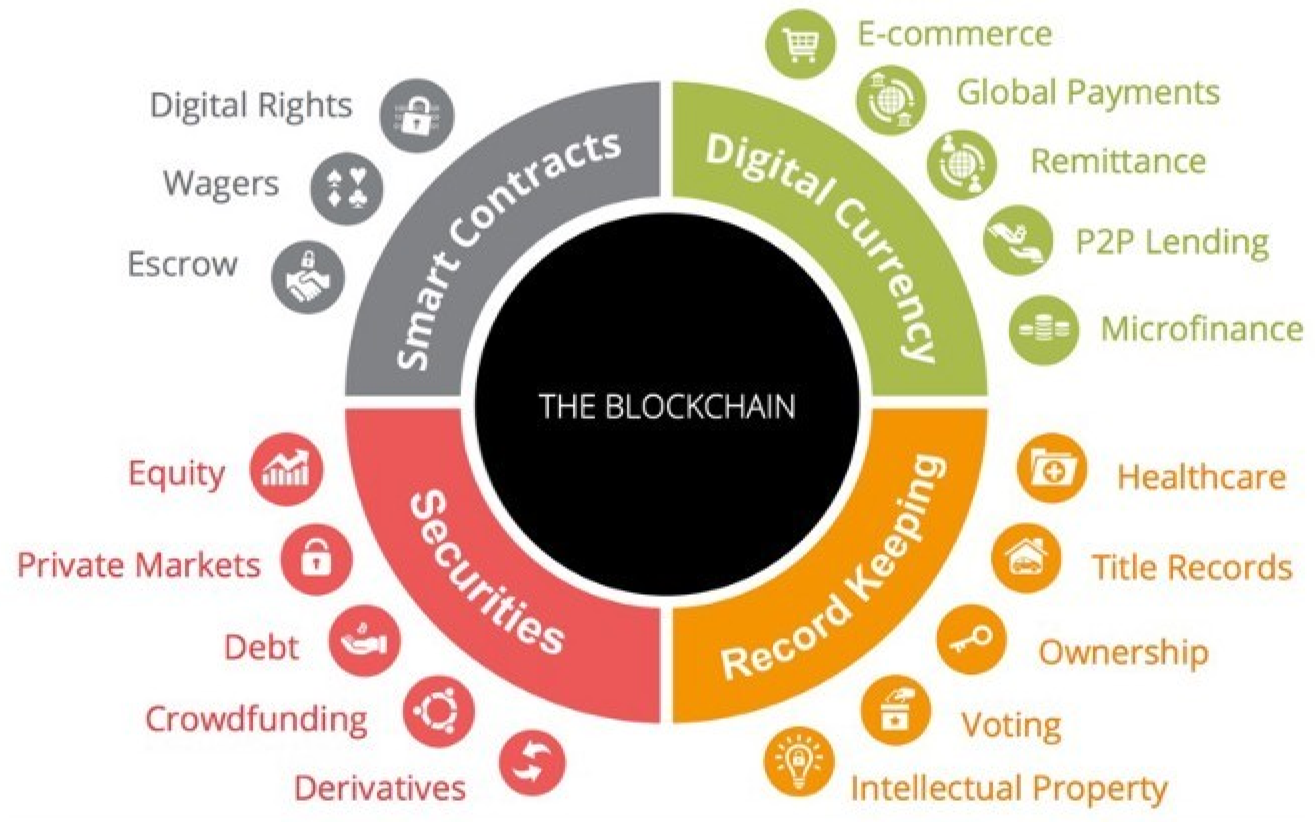
- Banking and Finance
- Food Safety
- Supply Chain
- Retail
- Automobiles
- Government Services
- Healthcare
- Insurance
- Energy
- Real Estate
- International Trade
- Sports

Key Features of Enterprise Blockchains

- Decentralization
- Immutability
- Transparency
- Cheaper
- Faster



Blockchain use in Business Domain



Form your team for the course project

Choose subject of your project

- Describe your business case and the real world problem you want to resolve!
- The team can consist of 5-7 members
- Write on a peace of paper of your Blockchain project and your team member names and faculty number

Form your team for the course project

Use the following link to register: https://365.uni-sofia.bg/register

- Login into Office 365 and join Team
- Use the following code: **91uy1bs**

Homework

Download and install **Metamask or other wallet.**
Make sure you secure your seed phrase (words) or private key.
Check your Public address

How to Get Test Ether – KETH

https://gitter.im/kovan-testnet/faucet - 5 KETH

https://faucet.kovan.network – max 1 KETH per day

Send Test Ether to your team members. Submit transactions using Kovan Test Network.
If your team consist of 5 members – you should submit 4 Transactions

Post one Transaction Id of the transactions in FB Group (we'll create a Post under which you will post you will post it) :)

Usefull Links

Enterprise Blockchain news - www.ledgerinsights.com

Gas convert units - https://www.myetherwallet.com/convert-units

Wei Dai - https://gwei.io/

Gas convert units - https://www.myetherwallet.com/convert-units

ERC 20 - https://academy.binance.com/en/articles/an-introduction-to-erc-20-tokens
https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

DAO Hack -
https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562

DAPPS - https://blockgeeks.com/guides/dapps/

Baseline protocol info - https://limechain.tech/blog/the-baseline-protocol-explained/

https://www.baseline-protocol.org/

Questions ?

- Thank you for your attention!