A black and white photograph of the MIT Great Dome at night. The dome is illuminated from within, showing its tiered structure. Below the dome, a rectangular plaque reads "MCMXVI". In front of the dome, a horizontal stone tablet displays the text "MASSACHUSETTS INSTITUTE OF TECHNOLOGY". The building features classical columns and large windows. The foreground is a grassy area with some trees.

Contracts & Currencies

Blockchain - Next Gen Internet

Abel Sanchez, John R. Williams



Sumerian contract
Selling field & house
Circa 2600 BCE



Papyrus Contract Marriage 4th BCE

A photograph showing a close-up of a man's hands. He is wearing a brown leather strap watch on his left wrist. His hands are clasped together in a firm handshake over a silver laptop keyboard. In the bottom left corner, a clipboard with a white sheet of paper is visible, with the word "Contract" printed in green at the top of the page.

A contract is an agreement between two
or more parties that is enforceable by law

Building Block of Market Economy



We Live in a World of Paper

A close-up photograph of a massive pile of white paper, likely office documents or reports. The paper is held together by numerous black paperclips. The stacks are uneven and sprawling across the frame, with some papers tucked under others. In the background, a person's hand is visible, reaching towards the papers. To the right, there's a dark filing cabinet and some office supplies like a tape dispenser and a small plant.

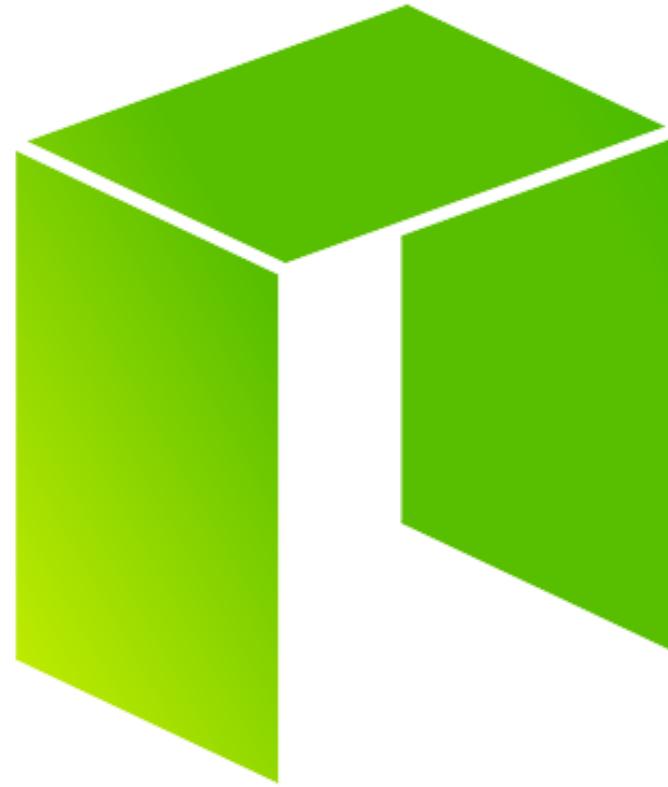
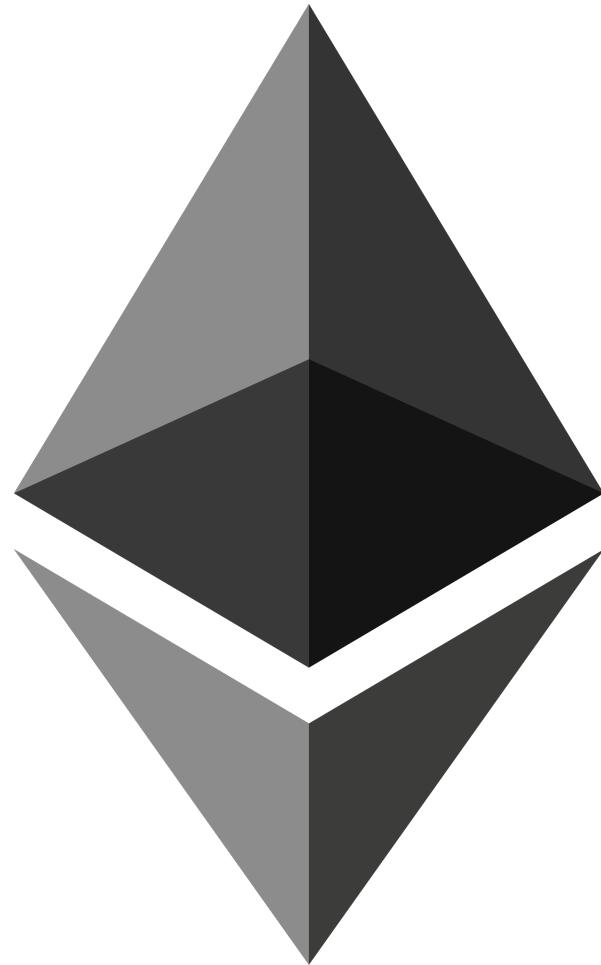
Connecting CONTRACT To Virtual WORLD



SMART CONTRACTS



Smart contract platforms





POVERTY

MIT

Hernando de Soto



The formal, legal world

- Citizens can prove who they are
- People and businesses have legal addresses and identities
- Property titles and registries allow everyone to know who owns what
- Articles of incorporation enable investors and customers to know who they are buying and selling from
- Legal contracts are binding and enforceable



Free To
CHOOSE
NETWORK

Core Challenges

- Identity
- Contracts
- Payment

IDENTITY





Identity Explosion

- The average Web user maintains 50+ separate accounts with password reuse.
- Reuse spreads vulnerabilities
- I have over 100 passwords
- How many do you have?



Identities Today are Siloed and Vulnerable



Identity Silos Centralized Servers



- Education
- Car Insurance
- Health Care
- Tax Reports
- Social Media



* Within same institution
Multiple accounts



Challenges For Organizations

- Visibility
- Interoperability
- Cybersecurity



For Individuals

- Physical documents
- Management Burden
- Repetition of information
- Personal Information Leaks
- Identity Theft

Identity with blockchain contracts

- Blockchain identity
 - Managed by user
 - Data owned by user
 - Collection of credentials



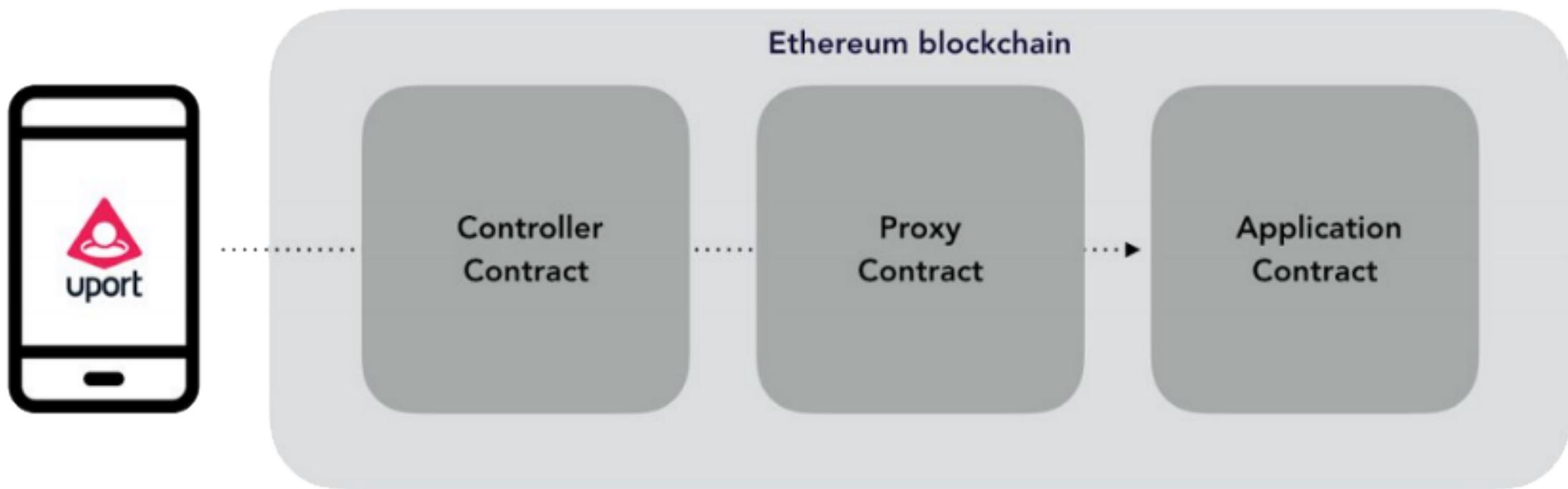
- Data
 - Verified claims/attestations (citizenship, visa, certificates)
 - Data standards, data schema
 - Granular disclosures
 - Possible to establish multiple identities/reputation

Timestamp
Recipient ID
Claim Data
Issuer ID
Issuer Signature
History
Reputation

Swiss City of Zug, First self-sovereign government issued identity on blockchain



Architecture Overview



Decentralized Identity Foundation (DIF)

DECENTRALIZED IDENTITIES

anchored by

BLOCKCHAIN IDs

linked to

ZERO-TRUST DATASTORES

that are

UNIVERSALLY DISCOVERABLE

<http://identity.foundation>





ASHISH GADNIS - Co-FOUNDER / CEO
BANQU INC.

153016.16	202004061	22.67	13.73
239560.34	579188246	2.18	12.89
108831.55	187756713	20.15	15.76



LETS WRITE A CONTRACT



Remix - Solidity IDE

remix.ethereum.org/#optimize=false&version=soljson-v0.4.25+commit.59dbf8f1.js

Beautiful Patterns original abel DataStream

Compile Run Analysis Testing Debugger Settings Support

browser config

```
1 pragma solidity ^0.4.0;
2 contract Ballot {
3
4     struct Voter {
5         uint weight;
6         bool voted;
7         uint8 vote;
8         address delegate;
9     }
10
11     mapping(address &gt; Voter) voters;
12     uint8[] proposals;
13     uint proposalCount;
14
15     function Ballot(uint8 _numProposals) public {
16         chairperson = msg.sender;
17         voters[chairperson].weight = 1;
18         proposals.length = _numProposals;
19     }
20
21     /// Give $(toVoter) the right to vote on this ballot.
22     /// May only be called by $(chairperson).
23     function giveRightToVote(address toVoter) public {
24
25     }
26
27 }
```

Current version:0.4.25+commit.59dbf8f1.Emscripten clang

Select new compiler version

Auto compile Enable Optimization Hide warnings

Start to compile

http://remix.ethereum.org

```
19
20
21
22
23
24
25
26
27
```

[2] only remix transactions, script

Search transactions

- Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script.

Remix - Solidity IDE

remix.ethereum.org/#optimize=false&version=soljson-v0.4.25+commit.59dbf8f1.js

Beautiful Patterns original abel DataStream

browser config

browser/ballot.sol

```
pragma solidity ^0.4.25;
contract Hello{
    function get() public pure returns(string){
        return "Hello World!!!";
    }
}
```

StructDefinition Voter 4 reference(s)

Compile Run Analysis Testing Debugger Settings Support

Current version:0.4.25+commit.59dbf8f1.Emscripten.clang

Select new compiler version

Auto compile Enable Optimization Hide warnings

Start to compile

Hello World

Static Analysis raised 1 warning(s) that requires your attention. Click here  to show the warning(s).

Hello 

[2] only remix transactions, script Search transactions

- Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script.

Remix - Solidity IDE

remix.ethereum.org/#optimize=false&version=soljson-v0.4.25+commit.59dbf8f1.js

Beautiful Patterns original abel DataStream

browser config

browser/ballot.sol

```
pragma solidity ^0.4.25;
contract Hello{
    function get() public pure returns(string){
        return "Hello World!!!";
    }
}
```

StructDefinition Voter 4 reference(s)

Compile Run Analysis Testing Debugger Settings Support

Current version:0.4.25+commit.59dbf8f1.Emscripten clang

Select new compiler version

Auto compile Enable Optimization Hide warnings

Start to compile

Hello

Details ABI Bytecode

Static Analysis raised 1 warning(s) that requires your attention. Click here to show the warning(s).

Hello

[2] only remix transactions, script Search transactions

- Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script.

remix

Remix - Solidity IDE

remix.ethereum.org/#optimize=false&version=soljson-v0.4.25+commit.59dbf8f1.js

Beautiful Patterns original abel DataStream

Compile Run Analysis Testing Debugger Settings Support

browser config

StructDefinition Voter 4 reference(s)

pragma solidity ^0.4.25;

contract Hello{

function get() public pure returns(string){

return "Hello World!!!";}

}

}

Environment Injected Web3 Rinkeby (4)

Account 0x284...2d60e (2 ether)

Gas limit 3000000

Value 0 wei

Hello Deploy or At Address Load contract from Address

Transactions recorded: 0

Deployed Contracts

Currently you have no contract instances to interact with.

[2] only remix transactions, script Search transactions

- Executing common command to interact with the Remix interface (see list of commands above). Note that these commands can also be included and run from a JavaScript script.

remix

Remix - Solidity IDE | Rinkeby Transaction 0x2ac0ff | +

rinkeby.etherscan.io/tx/0x2ac0ff4eed4e85127310ccf398718d0827e950dadaccbc2affacd07188721f96

Beautiful Patterns original abel DataStream

RINKEBY (CLIQUE) TESTNET Search by Address / Txhash / Block / Token / Ens GO Language

HOME BLOCKCHAIN TOKEN MISC

Transaction 0x2ac0ff4eed4e85127310ccf398718d0827e950dadaccbc2affacd07188721f96 

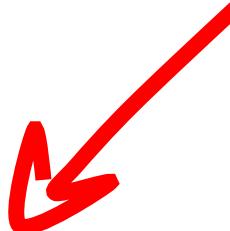
Home / Transactions / Tx Info

Overview

Transaction Information   Tools & Utilities 

[This is a Rinkeby Testnet Transaction Only]

TxHash:	0x2ac0ff4eed4e85127310ccf398718d0827e950dadaccbc2affacd07188721f96
TxReceipt Status:	Success
Block Height:	3180550 (11 Block Confirmations)
TimeStamp:	3 mins ago (Oct-18-2018 04:21:35 AM +UTC)
From:	0x83ef5fc005e4092a719b8df9793a3f216016a3ef
To:	[Contract 0x760384468faf53da01ece05ddcf3ed1a24c0ec76 Created] 
Value:	0 Ether (\$0.00)
Gas Limit:	136491
Gas Used By Transaction:	136491
Gas Price:	0.000000001 Ether (1 Gwei)



Remix - Solidity IDE | Rinkeby Accounts, Address A | +

rinkeby.etherscan.io/address/0x760384468faf53da01ece05ddcf3ed1a24c0ec76

Beautiful Patterns original abel DataStream

RINKEBY (CLIQUE) TESTNET Search by Address / Txhash / Block / Token / Ens GO Language

HOME BLOCKCHAIN TOKEN MISC

Contract 0x760384468FAf53DA01EcE05dDCf3ED1A24C0ec76

Home / Accounts / Address

Contract Overview

Balance: 0 Ether

Transactions: 1 txn

Misc:

Contract Creator: 0x83ef5fc005e4092... at txn 0x2ac0ff4eed4e851...

More Options

Transactions Code Events

Latest 1 txn

TxHash	Block	Age	From	To	Value	[TxFee]
0x2ac0ff4eed4e851...	3180550	4 mins ago	0x83ef5fc005e4092...	IN Contract Creation	0 Ether	0.000136491

[Download CSV Export]

Remix - Solidity IDE

remix.ethereum.org/#optimize=false&version=soljson-v0.4.25+commit.59dbf8f1.js

Beautiful Patterns original abel DataStream

Compile Run Analysis Testing Debugger Settings Support

browser config

StructDefinition Voter 4 reference(s)

pragma solidity ^0.4.25;

contract Hello{

function get() public pure returns(string){

return "Hello World!!!";}

}

}

Environment Injected Web3 Rinkeby (4)

Account 0x83e...6a3ef (3.999819877 ether)

Gas limit 3000000

Value 0 wei

Hello

Deploy

or

At Address Load contract from Address

Transactions recorded: 1

Deployed Contracts

Hello at 0x760...0ec76 (blockchain)

get

0: string: Hello World!!!

creation of Hello pending...

<https://rinkeby.etherscan.io/tx/0x2ac0ff4eed4e85127310ccf398718d0827e950dadaccbc2affac07188721f96>

[block:3180550 txIndex:47] from:0x83e...6a3ef to:Hello.(constructor) value:0 wei data:0x608...b0029 logs:0 hash:0x2ac...21f96

call to Hello.get

[call] from:0x83ef5fc005e4092a719b8df9793a3f216016a3ef to:Hello.get() data:0x6d4...ce63c

remix

The screenshot shows the Remix Solidity IDE interface. On the left, the code editor displays a simple Hello World contract named 'Hello'. In the center, the transaction history shows the deployment of the contract, with a red arrow pointing to the transaction log entry for the constructor call. To the right, the deployed contract details are shown, including its address (Hello at 0x760...0ec76) and the result of the 'get' function call, which is '0: string: Hello World!!!'. A second red arrow points from the deployed contract details to this function call result.





```
pragma solidity ^0.4.18;

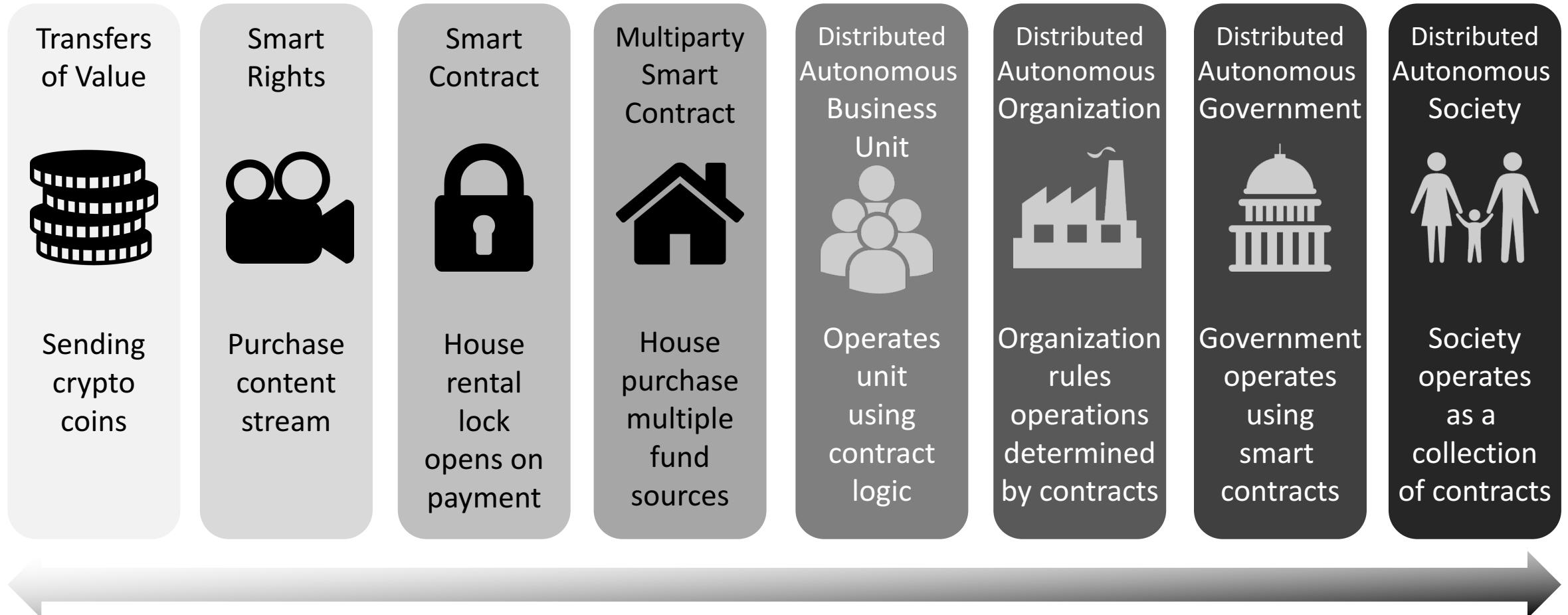
// -----
// 'coco' 'Example Coco Supply Token' token contract
//
// Symbol      · coco
```

<http://abel.mit.edu/erc20.sol>

```
// -----
// Safe maths
// -----
library SafeMath {
    function add(uint a, uint b) internal pure returns (uint c) {
        c = a + b;
        require(c >= a);
    }
```

0.0000000000000000253
123456789012345678
25000000000000000000

Smart Contracts



Simple

Complex

Dr. Gavin Wood

- https://youtu.be/U_LK0t_qaPo?t=757

Send me some ether

0x72ac0213dCbe1F1970e583Cbb4894da3e88eCa1b



"The most important book about technology today,
with implications that go far beyond programming."
—Guy Kawasaki

Revised & Expanded

THE CATHEDRAL & THE BAZAAR

MUSINGS ON LINUX AND OPEN SOURCE
BY AN ACCIDENTAL REVOLUTIONARY



ERIC S. RAYMOND

WITH A FOREWORD BY BOB YOUNG, CHAIRMAN & CEO OF RED HAT, INC.

The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary

by [Eric S. Raymond](#)