Blockchain and smart contracts: infrastructure and platforms

Claudio Di Ciccio | http://diciccio.net | claudio.diciccio@uniroma1.it

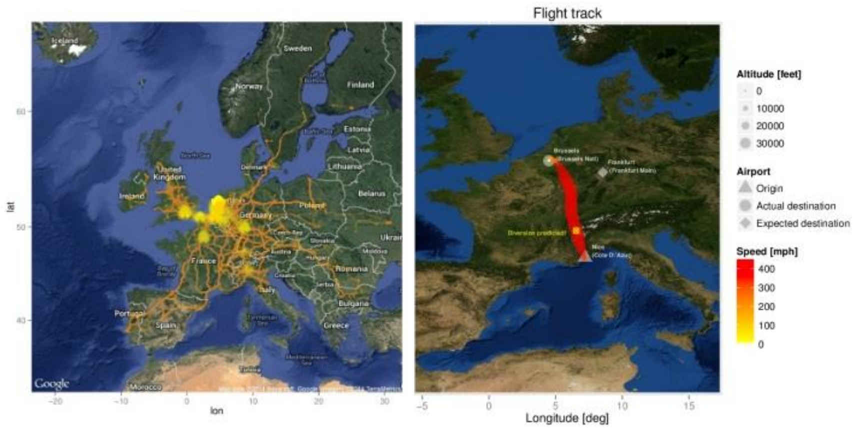
Sapienza, University of Rome, Italy

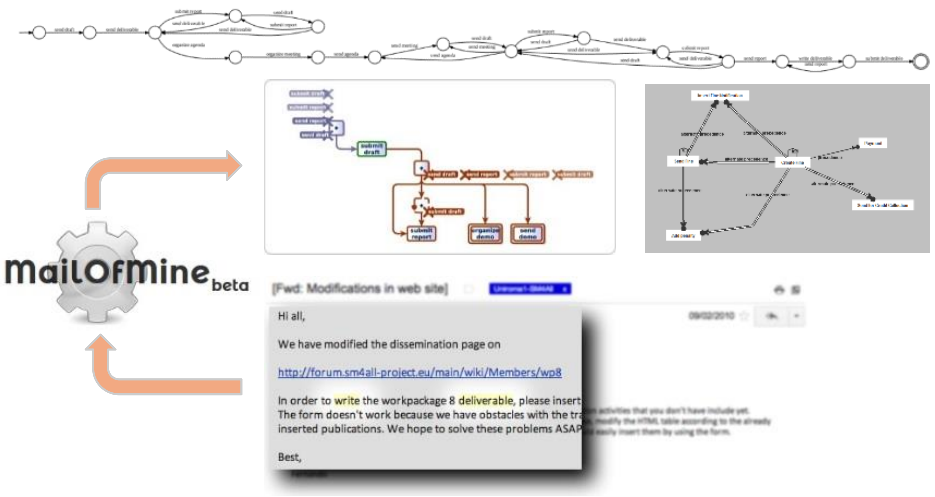
Cyber 4.0 Seminar, 2021, March the 3rd

Claudio Di Ciccio

Assistant professor
Ph.D. in Computer Science and Engineering

Main research interests:
process mining,
blockchains,
declarative process modelling,
service-oriented architectures





[Fwd: Modifications in web site]

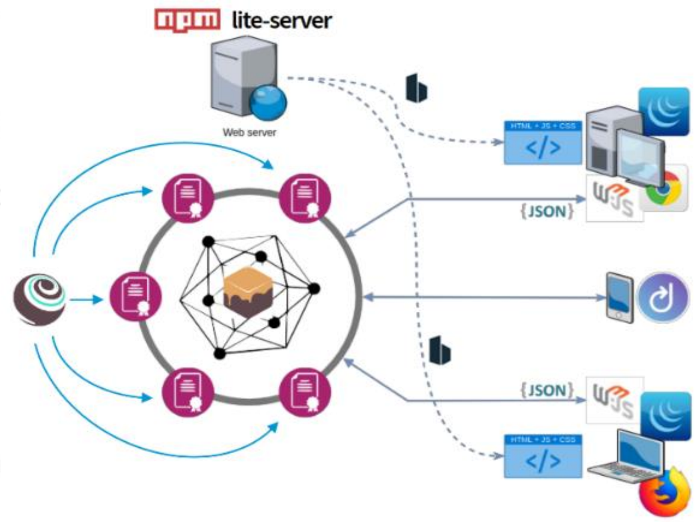
Hi all,

We have modified the dissemination page on

http://forum.sm4all-project.eu/main/wiki/Members/wp8

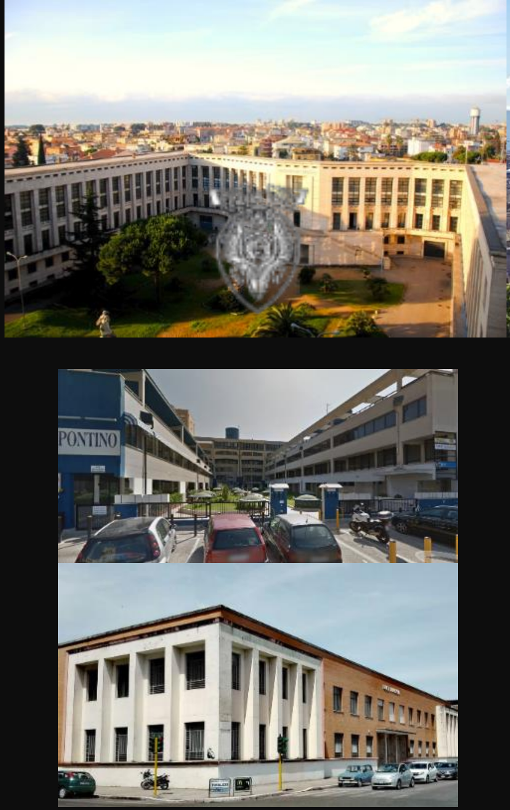
In order to write the workpackage 8 deliverable, please insert
The form doesn't work because we have obstacles with the tra
inserted publications. We hope to solve these problems ASAP

Best,

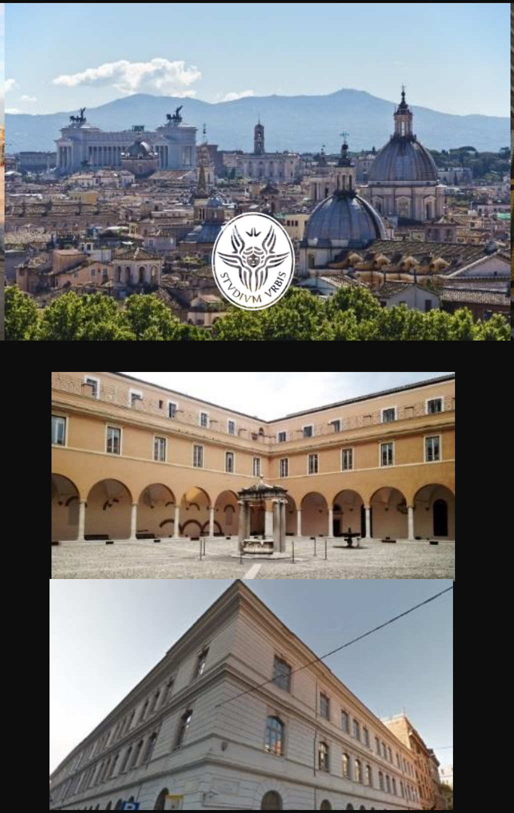


My experience so far

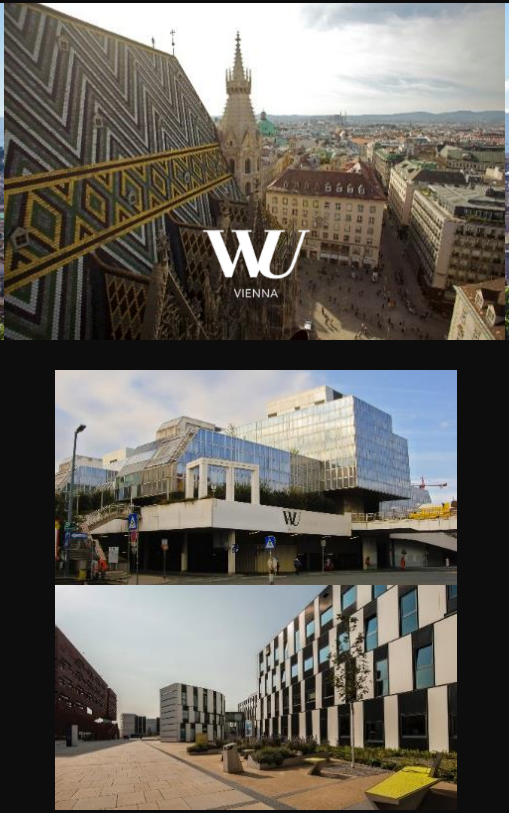
Latina, Italy (B.Sc)



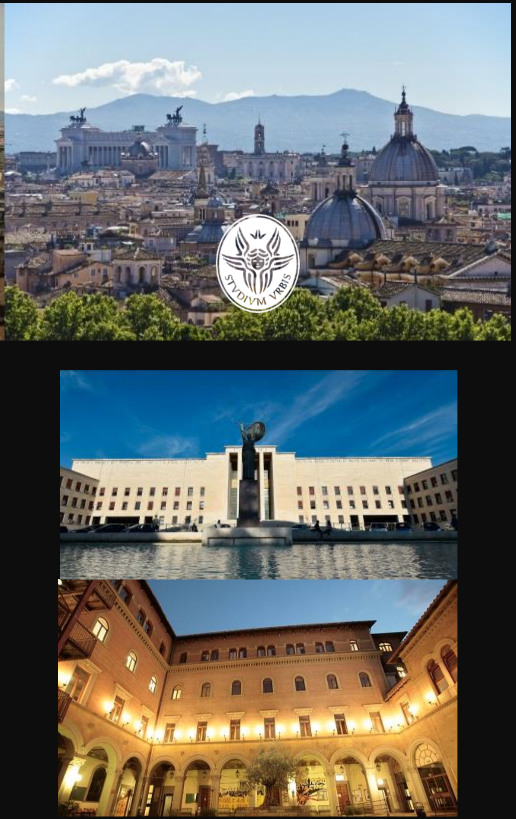
Rome, Italy (M.Sc, Ph.D)



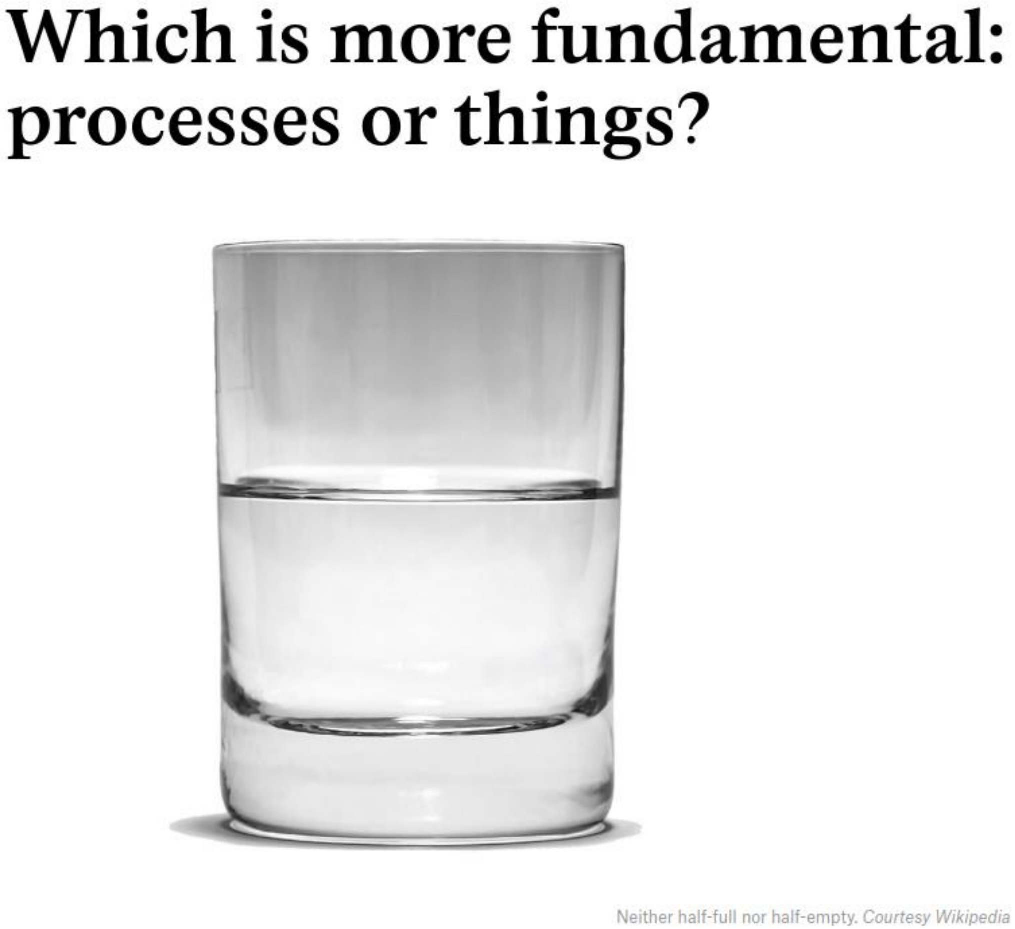
Vienna, Austria (Post-doc, Assistant Prof.)



Rome, Italy (Assistant Prof.)



Half empty or half full?

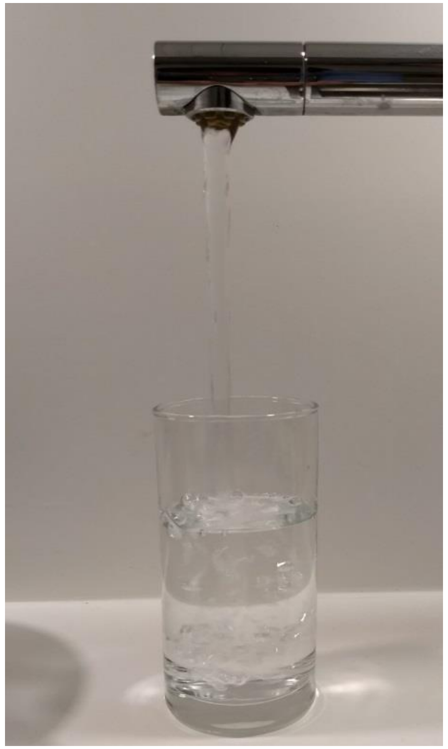


Which is more fundamental: processes or things?

Neither half-full nor half-empty. *Courtesy Wikipedia*

http://aeon.co/ideas/which-is-more-fundamental-processes-or-things

Processes are into dynamics

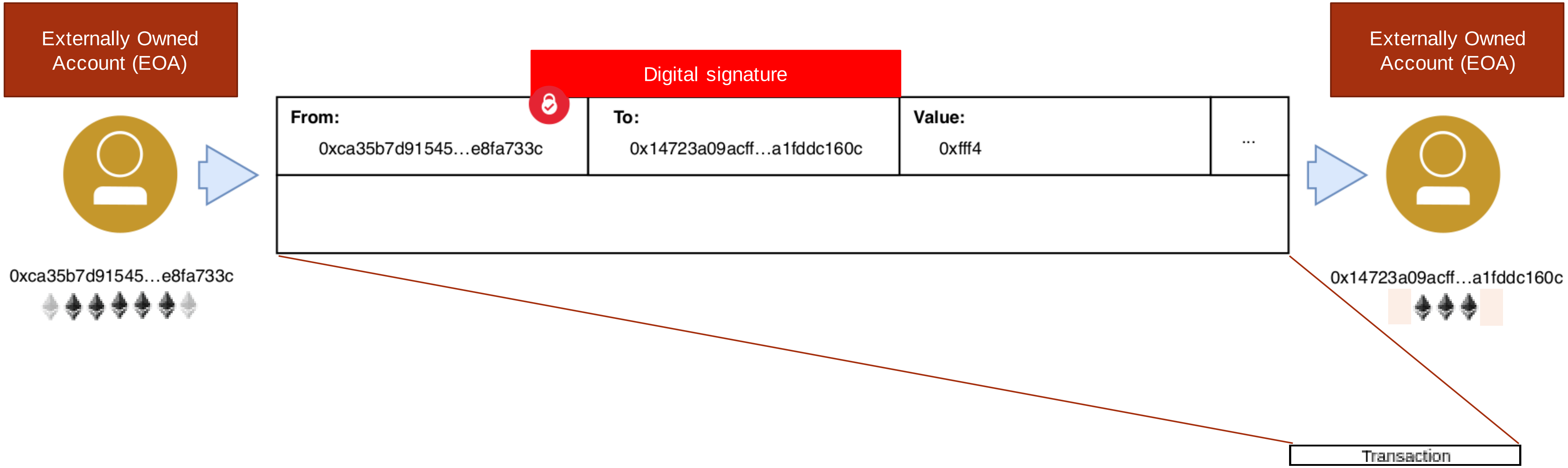


Thanks Dr. Mieke Jans for offering her hand

Blockchain as an infrastructure

Transaction

- Transfer of **(crypto)assets** (Ether, Bitcoin, Litecoin, EOS, …) from **account** A to **account** B



Externally Owned Account (EOA)

0xca35b7d91545…e8fa733c

Digital signature

From: 0xca35b7d91545…e8fa733c

To: 0x14723a09acff…a1fddc160c

Value: 0xfff4

…

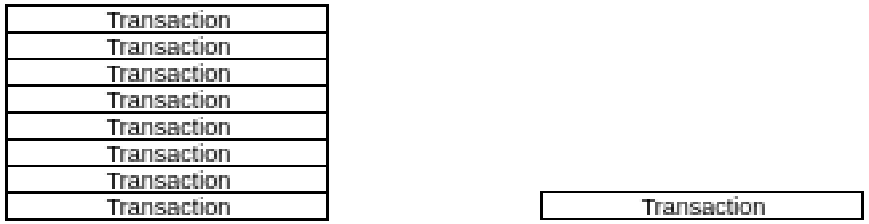
Externally Owned Account (EOA)

0x14723a09acff…a1fddc160c

Transaction

Ledger

- Ordered collection of transactions
- The order matters!

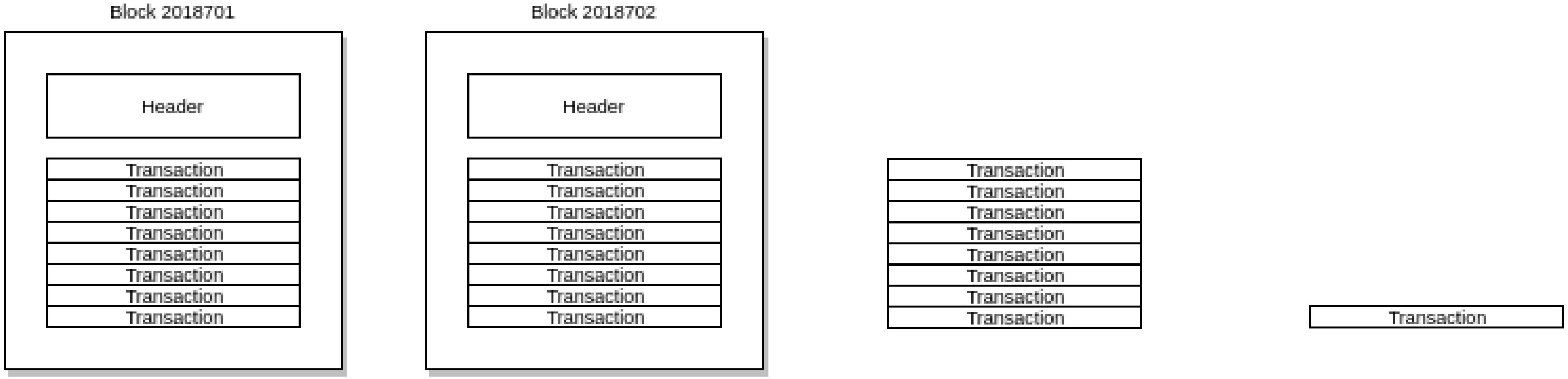


Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction
Transaction

Transaction

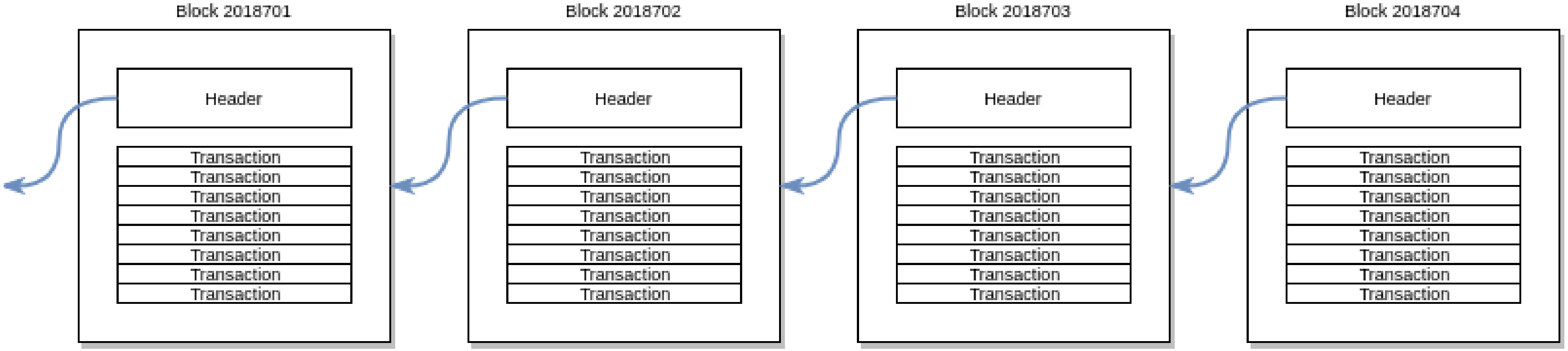
Block

- Blocks group and collate transactions
- The order matters!

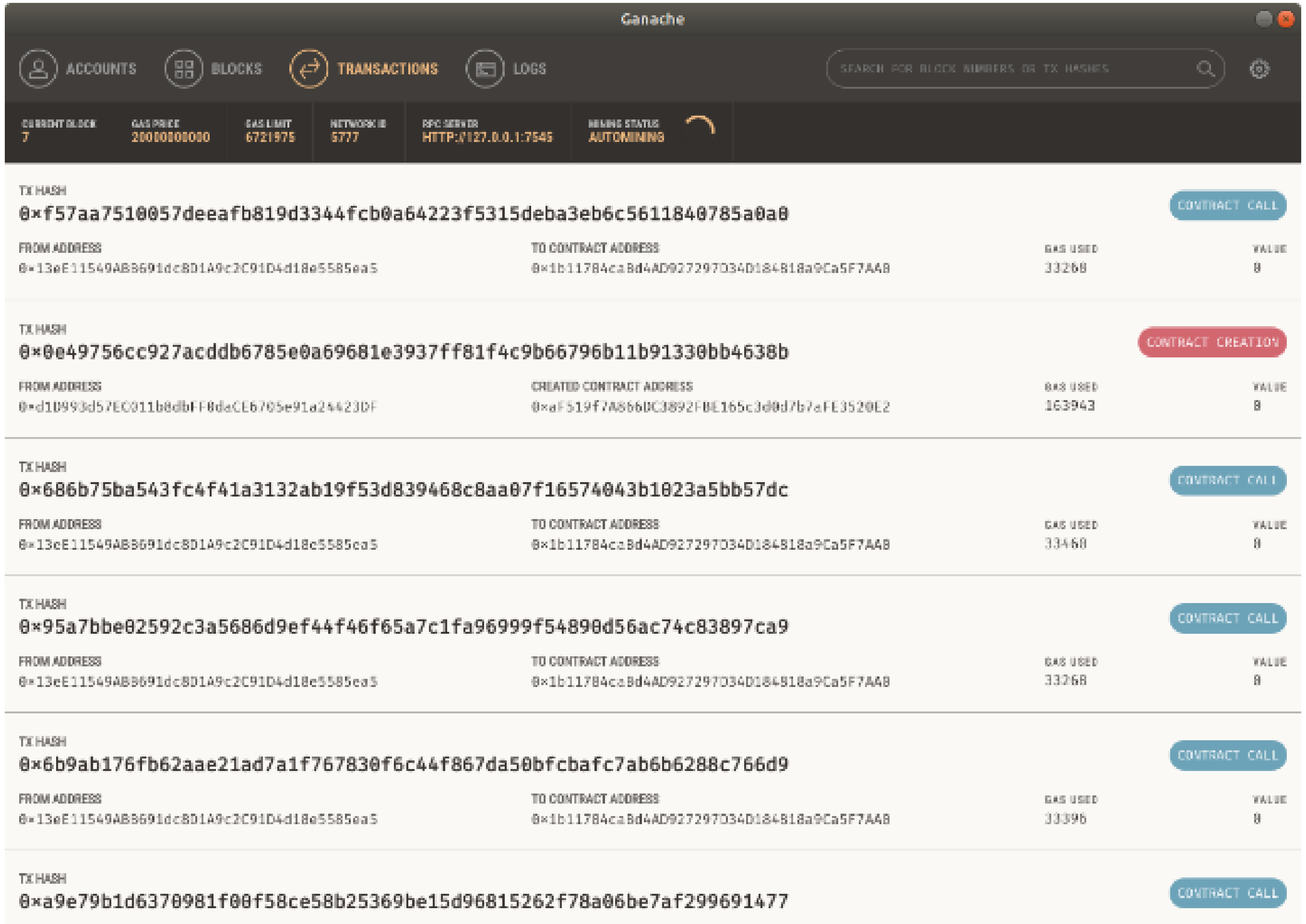


Hashing the previous block for immutability

- Blocks refer back to direct predecessors
- The order matters!



The Blockchain remembers



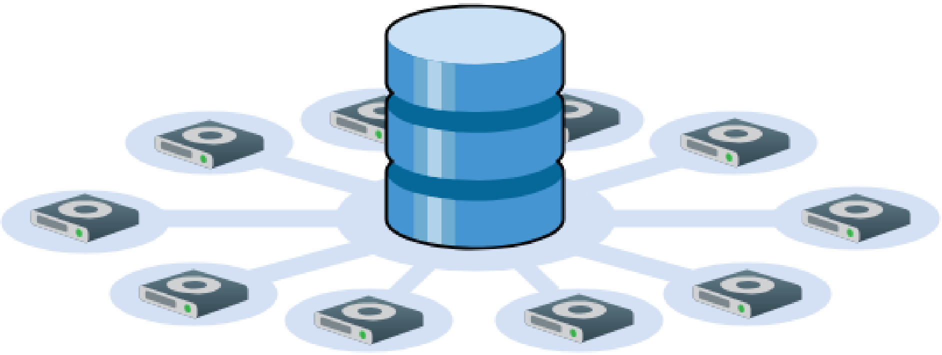
```
CURRENT BLOCK   GAS PRICE     GAS LIMIT   NETWORK ID   RPC SERVER              MINING STATUS
7               20000000000   6721975     5777         HTTP://127.0.0.1:7545   AUTOMINING

TX HASH
0×f57aa7510057deeafb819d3344fcb0a64223f5315deba3eb6c5611840785a0a0                        CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS                             GAS USED   VALUE
0×13eE11549AB3691dc8D1A9c2C91D4d18e5585ea5    0×1b11784caBd4AD927297D34D184818a9Ca5F7AA8      33268      0

TX HASH
0×0e49756cc927acddb6785e0a69681e3937ff81f4c9b66796b11b91330bb4638b                        CONTRACT CREATION
FROM ADDRESS                                  CREATED CONTRACT ADDRESS                        GAS USED   VALUE
0×d10993d57EC011b0dbFF0daCE6705e91a24423DF    0×aF519f7A866DC3892FBE165c3d0d7b7aFE3520E2      163943     0

TX HASH
0×686b75ba543fc4f41a3132ab19f53d839468c8aa07f16574043b1023a5bb57dc                        CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS                             GAS USED   VALUE
0×13eE11549AB3691dc8D1A9c2C91D4d18e5585ea5    0×1b11784caBd4AD927297D34D184818a9Ca5F7AA8      33460      0

TX HASH
0×95a7bbe02592c3a5686d9ef44f46f65a7c1fa96999f54890d56ac74c83897ca9                        CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS                             GAS USED   VALUE
0×13eE11549AB3691dc8D1A9c2C91D4d18e5585ea5    0×1b11784caBd4AD927297D34D184818a9Ca5F7AA8      33268      0

TX HASH
0×6b9ab176fb62aae21ad7a1f767830f6c44f867da50bfcbafc7ab6b6288c766d9                        CONTRACT CALL
FROM ADDRESS                                  TO CONTRACT ADDRESS                             GAS USED   VALUE
0×13eE11549AB3691dc8D1A9c2C91D4d18e5585ea5    0×1b11784caBd4AD927297D34D184818a9Ca5F7AA8      33396      0

TX HASH
0×a9e79b1d6370981f00f58ce58b25369be15d96815262f78a06be7af299691477                        CONTRACT CALL
```

Ledgers

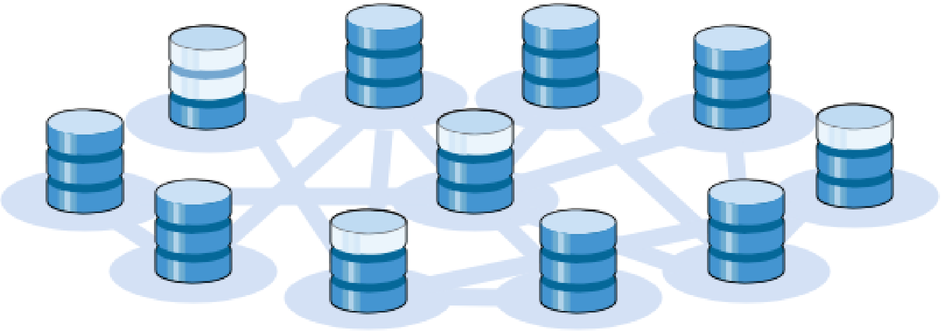
- A **ledger** is a collection of **transactions**.
  - Throughout history, on paper; recently, stored digitally
- Shortcomings of centralised ledgers:
  - They may be lost or **destroyed:**
    a user must *trust* that the owner is properly backing up the system
  - Transactions may **not** be **valid:**
    a user must *trust* that the owner is validating each received transaction
  - The transaction list may **not** be **complete:**
    a user must *trust* that the owner is including all valid transactions that have been received
  - The transaction data may have been **altered:**
    a user must *trust* that the owner is not altering past transactions

Decentralisation for persistence

Centralisation

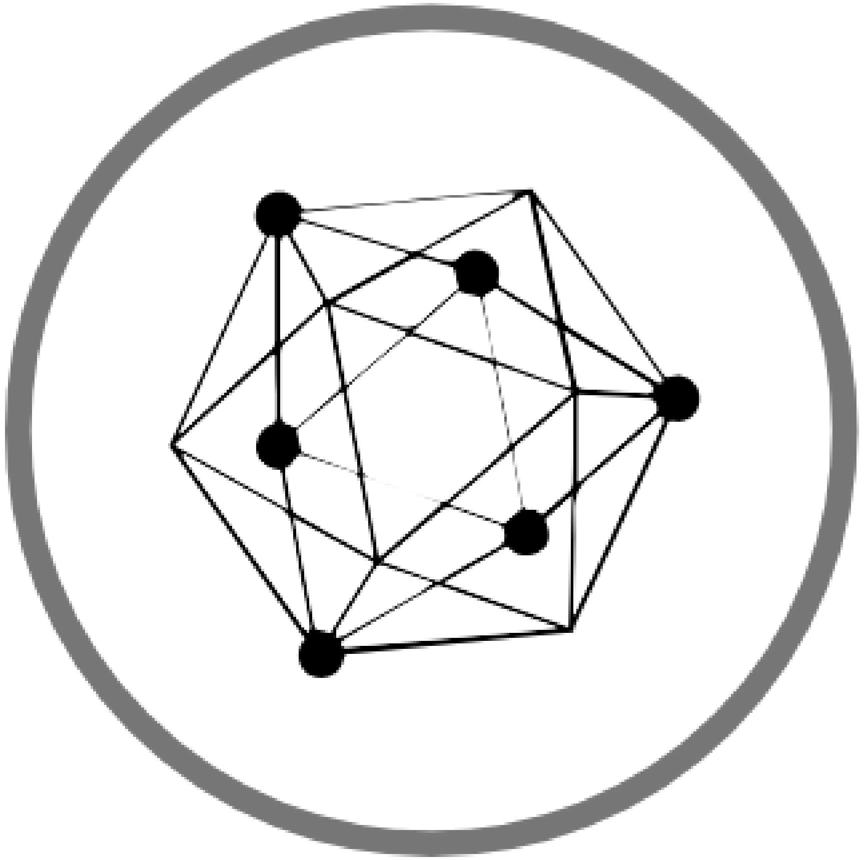


Decentralisation

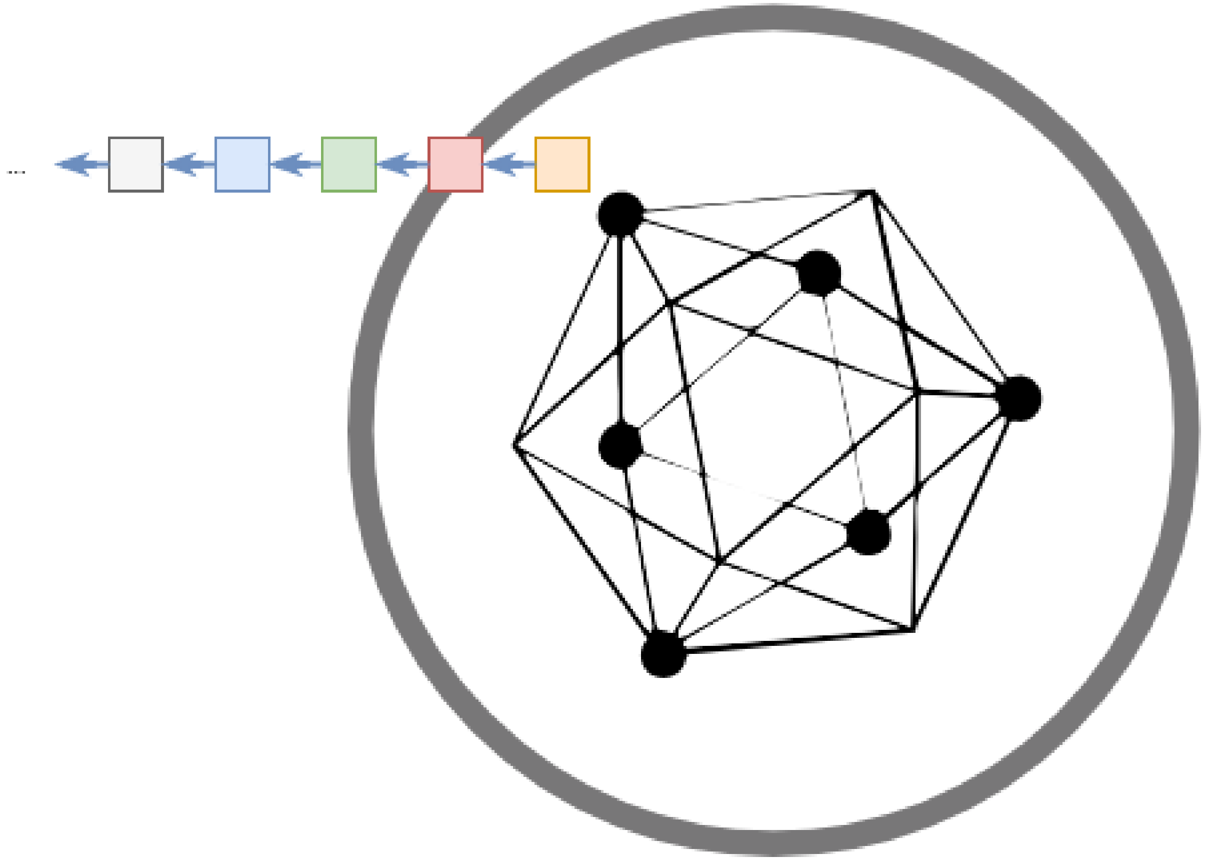


Distributing the ledger makes for permanence
BUT
entails no notion of unique distributed clock

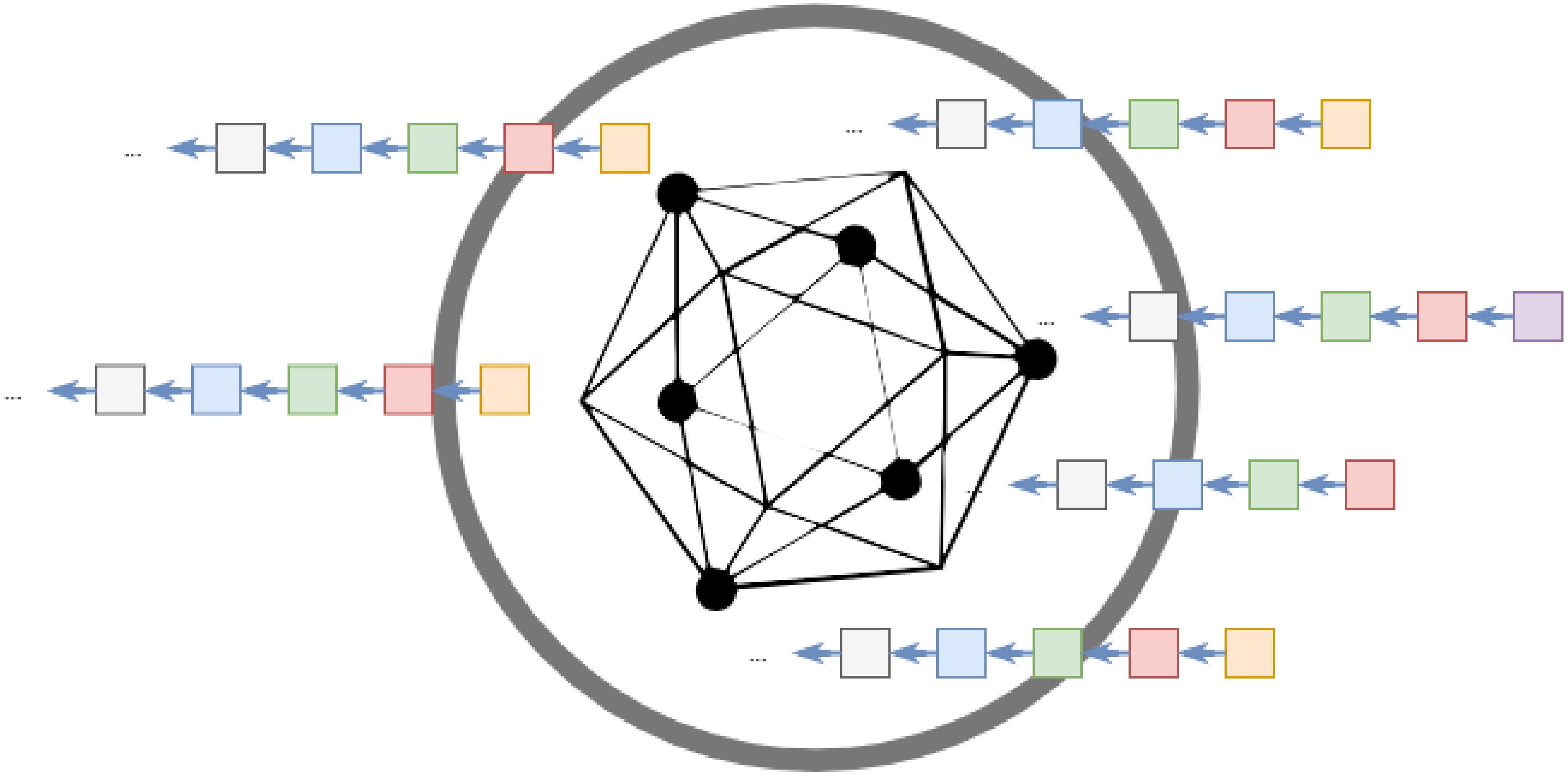
Distributed nature



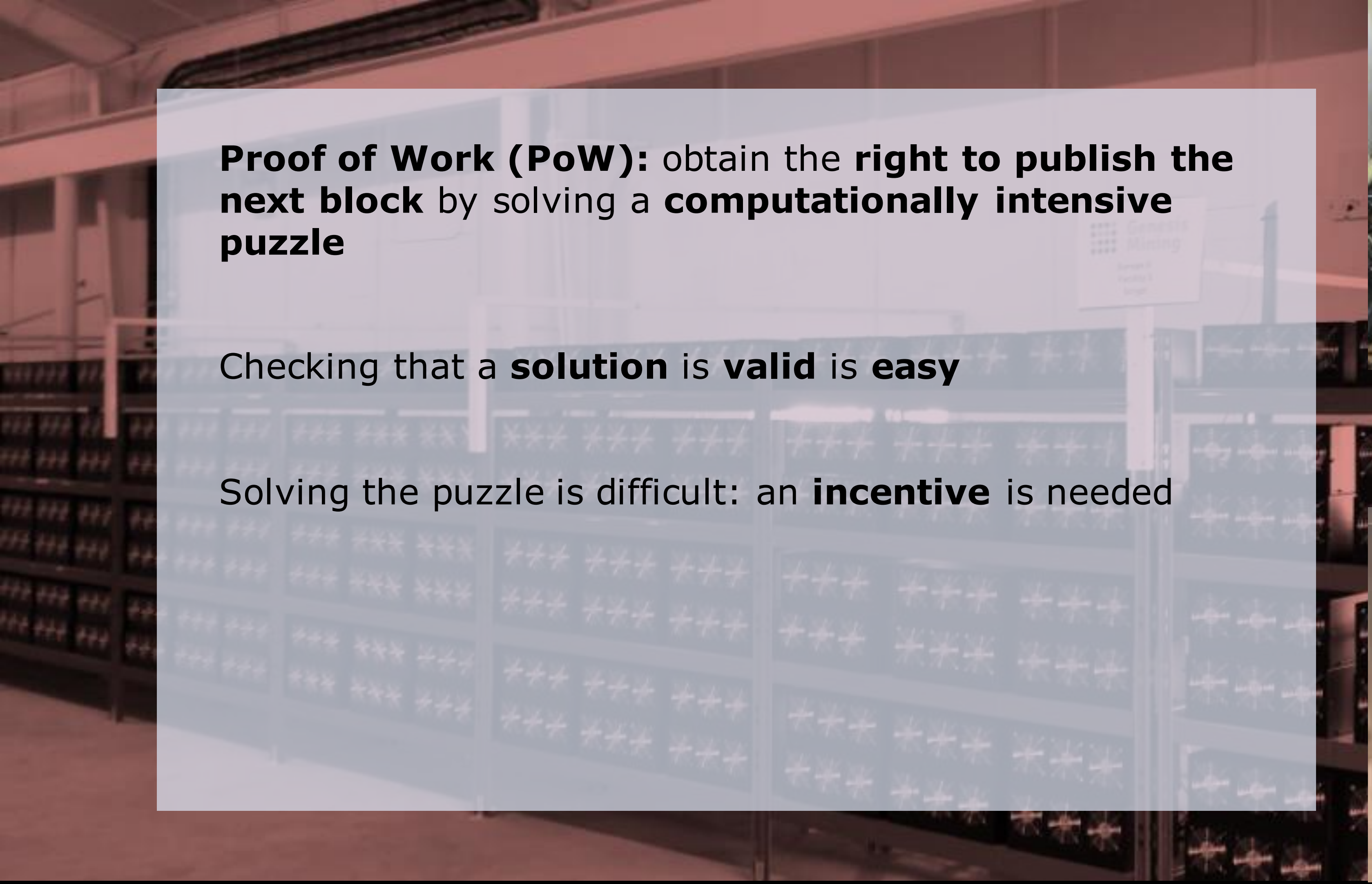
Distributed nature



Distributed nature



Mining for a blockchain

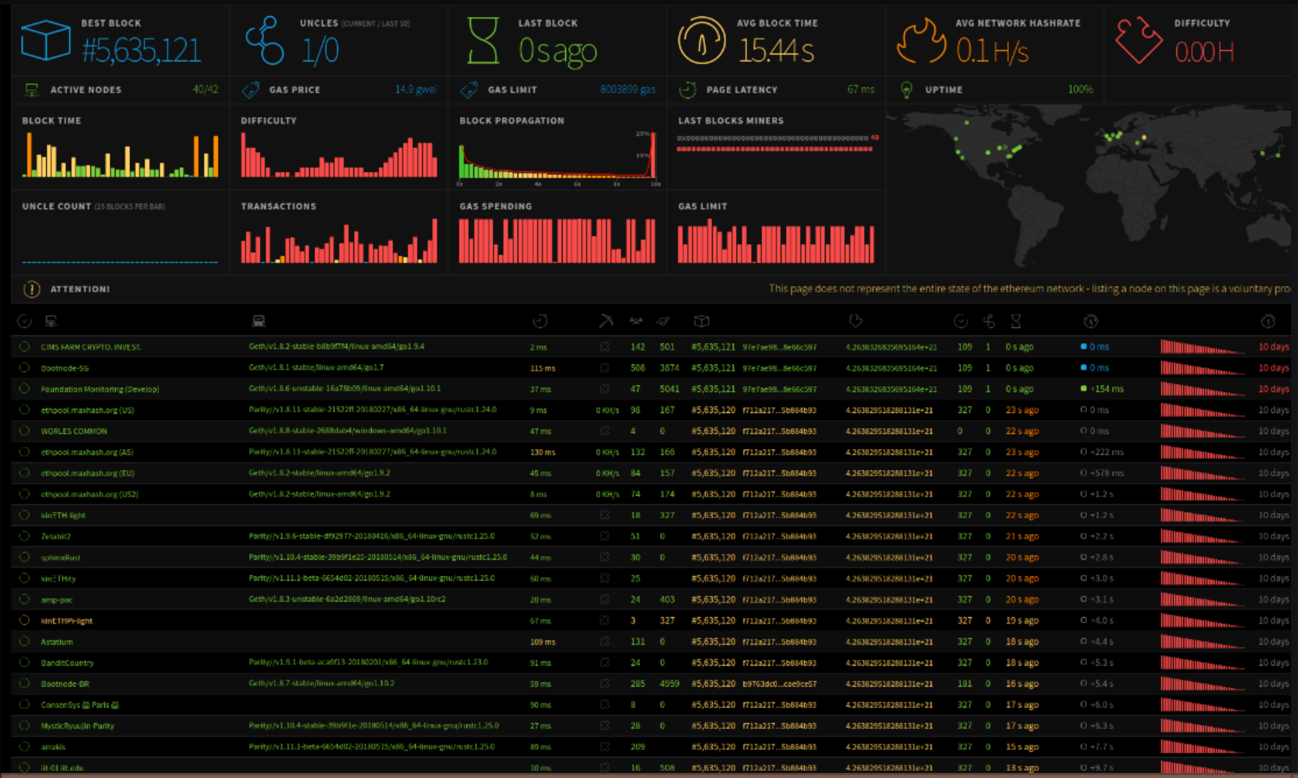


Proof of Work (PoW): obtain the **right to publish the next block** by solving a **computationally intensive puzzle**

Checking that a **solution** is **valid** is **easy**

Solving the puzzle is difficult: an **incentive** is needed

Ledgers are distributed and maintained by a network

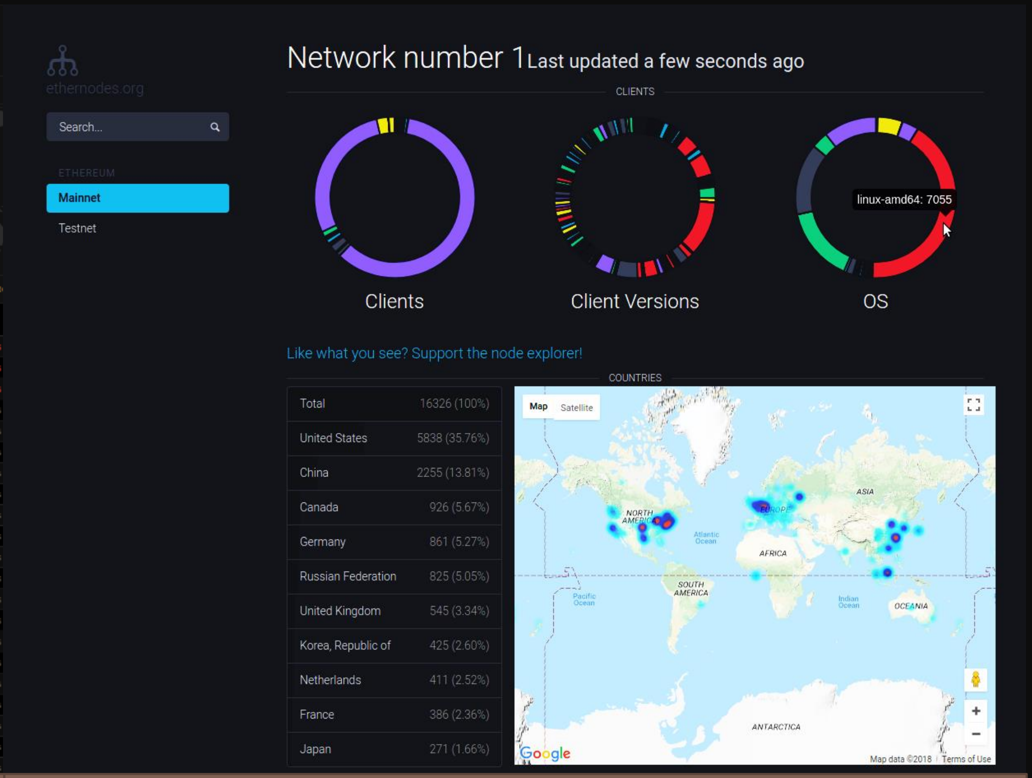


ATTENTION!

This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary pro

CIMS FARM CRYPTO. INVEST.	Geth/v1.8.2-stable-b8b9f7f4/linux-amd64/go1.9.4	2 ms		142	501	#5,635,121	97e7ae98...8e66c597	4.2638326835695164e+21	109	1	0 s ago	0 ms	10 days
Bootnode-SG	Geth/v1.8.1-stable/linux-amd64/go1.7	115 ms		508	3874	#5,635,121	97e7ae98...8e66c597	4.2638326835695164e+21	109	1	0 s ago	0 ms	10 days
Foundation Monitoring (Develop)	Geth/v1.8.6-unstable-16a78b09/linux-amd64/go1.10.1	37 ms		47	5041	#5,635,121	97e7ae98...8e66c597	4.2638326835695164e+21	109	1	0 s ago	+154 ms	10 days
ethpool.maxhash.org (US)	Parity//v1.8.11-stable-21522ff-20180227/x86_64-linux-gnu/rustc1.24.0	9 ms	0 KH/s	98	167	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	23 s ago	0 ms	10 days
WORLES COMMON	Geth/v1.8.8-stable-2688dab4/windows-amd64/go1.10.1	47 ms		4	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	0	0	22 s ago	0 ms	10 days
ethpool.maxhash.org (AS)	Parity//v1.8.11-stable-21522ff-20180227/x86_64-linux-gnu/rustc1.24.0	130 ms	0 KH/s	132	166	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	23 s ago	+222 ms	10 days
ethpool.maxhash.org (EU)	Geth/v1.8.2-stable/linux-amd64/go1.9.2	45 ms	0 KH/s	84	157	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	22 s ago	+578 ms	10 days
ethpool.maxhash.org (US2)	Geth/v1.8.2-stable/linux-amd64/go1.9.2	8 ms	0 KH/s	74	174	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	22 s ago	+1.2 s	10 days
kinETH-light		69 ms		18	327	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	22 s ago	+1.2 s	10 days
Zetabit2	Parity//v1.9.6-stable-df92977-20180416/x86_64-linux-gnu/rustc1.25.0	52 ms		51	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	21 s ago	+2.2 s	10 days
sphinxRust	Parity//v1.10.4-stable-39b9f1e25-20180514/x86_64-linux-gnu/rustc1.25.0	44 ms		30	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	20 s ago	+2.8 s	10 days
kinETHity	Parity//v1.11.1-beta-6654d02-20180515/x86_64-linux-gnu/rustc1.25.0	60 ms		25		#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	20 s ago	+3.0 s	10 days
amp-pac	Geth/v1.8.3-unstable-6a2d2869/linux-amd64/go1.10rc2	20 ms		24	403	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	20 s ago	+3.1 s	10 days
kinETHPi-light		67 ms		3	327	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	19 s ago	+4.0 s	10 days
Astatium		109 ms		131	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	18 s ago	+4.4 s	10 days
BanditCountry	Parity//v1.9.1-beta-aca9f13-20180201/x86_64-linux-gnu/rustc1.23.0	91 ms		24	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	18 s ago	+5.3 s	10 days
Bootnode-BR	Geth/v1.8.7-stable/linux-amd64/go1.10.2	59 ms		285	4959	#5,635,120	b9763dc0...cae9ce57	4.263829518288131e+21	181	0	16 s ago	+5.4 s	10 days
ConsenSys 🤖 Paris 🤖		90 ms		8	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	17 s ago	+6.0 s	10 days
MysticRyuujin-Parity	Parity//v1.10.4-stable-39b9f1e-20180514/x86_64-linux-gnu/rustc1.25.0	27 ms		28	0	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	17 s ago	+6.3 s	10 days
arrakis	Parity//v1.11.1-beta-6654d02-20180515/x86_64-linux-gnu/rustc1.25.0	89 ms		209		#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	15 s ago	+7.7 s	10 days
iit-01.iit.edu		10 ms		16	508	#5,635,120	f712a217...5b884b93	4.263829518288131e+21	327	0	13 s ago	+9.7 s	10 days

https://ehtstats.net



Network number 1Last updated a few seconds ago

Like what you see? Support the node explorer!

COUNTRIES

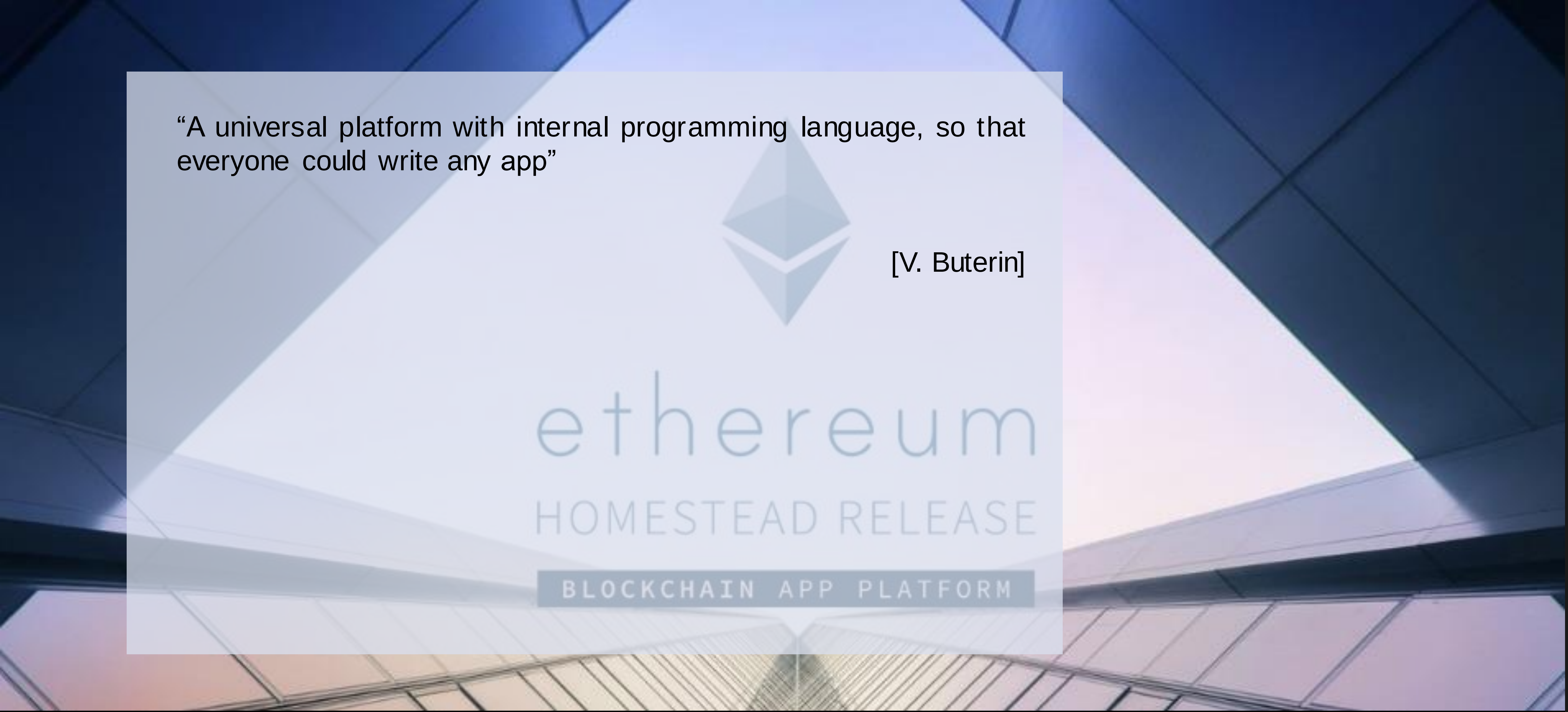
Total	16326 (100%)
United States	5838 (35.76%)
China	2255 (13.81%)
Canada	926 (5.67%)
Germany	861 (5.27%)
Russian Federation	825 (5.05%)
United Kingdom	545 (3.34%)
Korea, Republic of	425 (2.60%)
Netherlands	411 (2.52%)
France	386 (2.36%)
Japan	271 (1.66%)

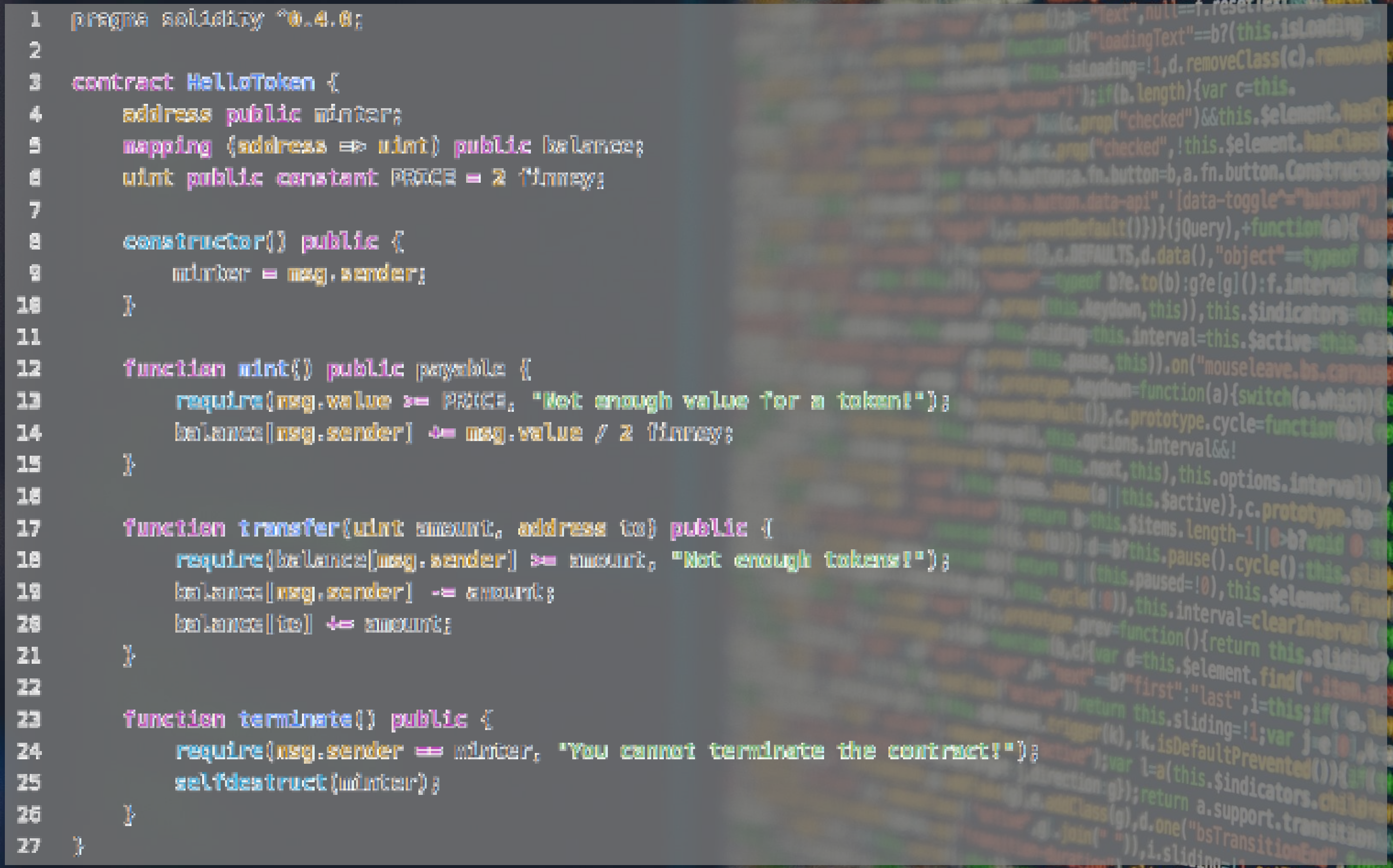
https://ehternodes.org

Crypto-fuel needed!

From peer-to-peer electronic cash system to programmable distributed environment

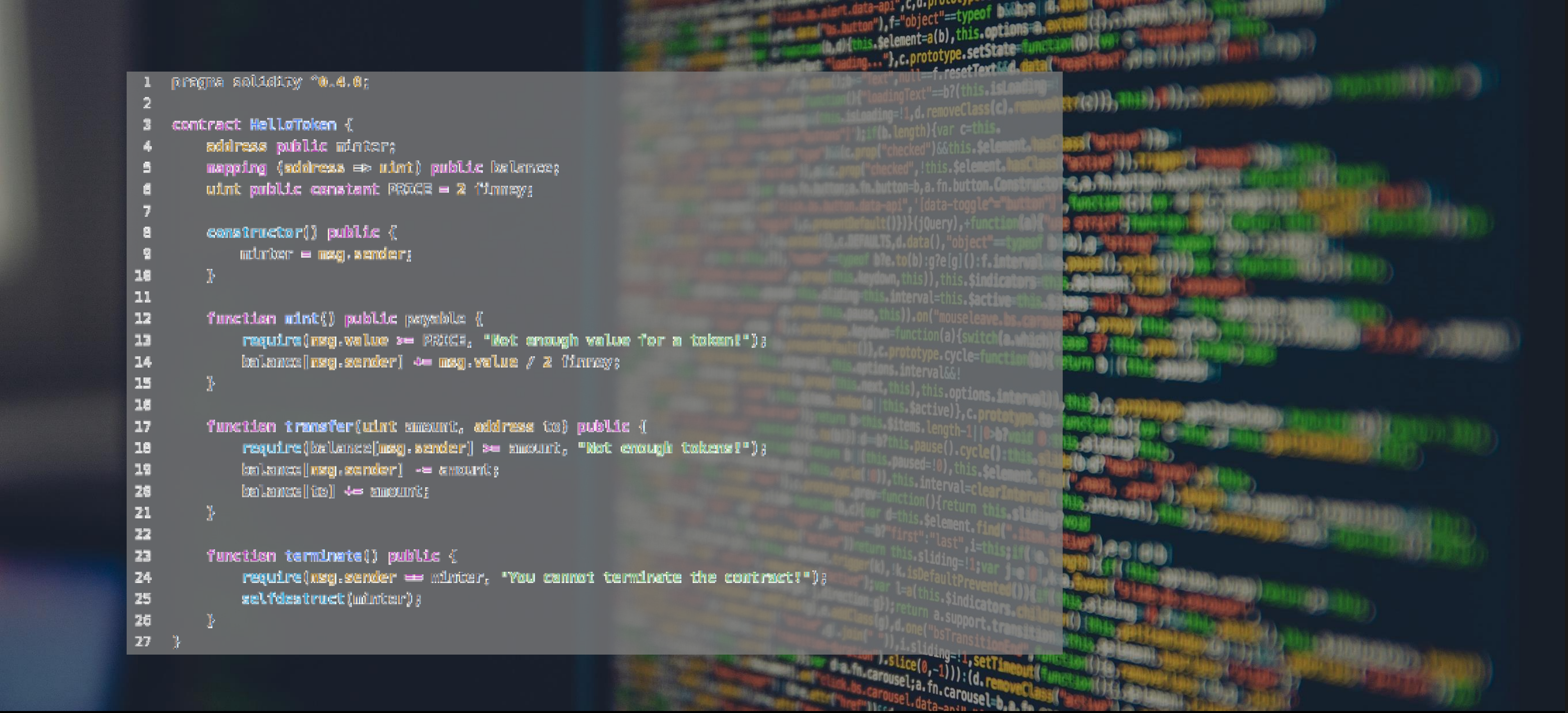
> “A universal platform with internal programming language, so that everyone could write any app”
>
> [V. Buterin]





```
pragma solidity ^0.4.0;

contract HelloToken {
    address public minter;
    mapping (address => uint) public balance;
    uint public constant PRICE = 2 finney;

    constructor() public {
        minter = msg.sender;
    }

    function mint() public payable {
        require(msg.value >= PRICE, "Not enough value for a token!");
        balance[msg.sender] += msg.value / 2 finney;
    }

    function transfer(uint amount, address to) public {
        require(balance[msg.sender] >= amount, "Not enough tokens!");
        balance[msg.sender] -= amount;
        balance[to] += amount;
    }

    function terminate() public {
        require(msg.sender == minter, "You cannot terminate the contract!");
        selfdestruct(minter);
    }
}
```

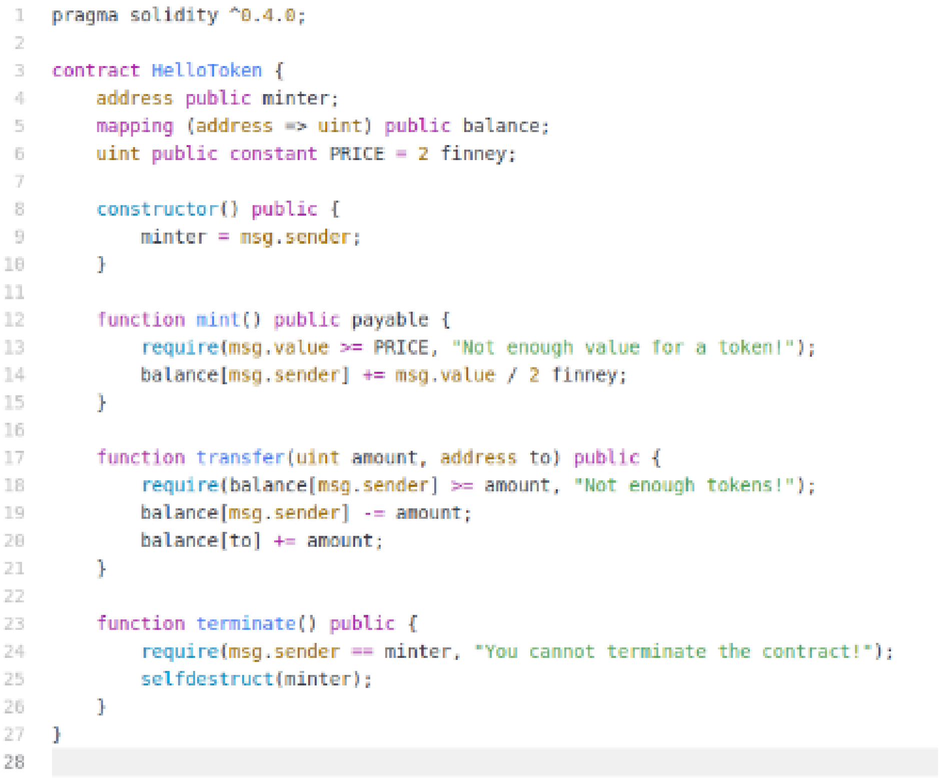
Smart Contracts are ~~codified autonomous agents~~



```
pragma solidity ^0.4.0;

contract HelloToken {
    address public minter;
    mapping (address => uint) public balance;
    uint public constant PRICE = 2 finney;

    constructor() public {
        minter = msg.sender;
    }

    function mint() public payable {
        require(msg.value >= PRICE, "Not enough value for a token!");
        balance[msg.sender] += msg.value / 2 finney;
    }

    function transfer(uint amount, address to) public {
        require(balance[msg.sender] >= amount, "Not enough tokens!");
        balance[msg.sender] -= amount;
        balance[to] += amount;
    }

    function terminate() public {
        require(msg.sender == minter, "You cannot terminate the contract!");
        selfdestruct(minter);
    }
}
```

Smart Contracts are pieces of code

Smart Contracts are pieces of code



```
pragma solidity ^0.4.0;

contract HelloToken {
    address public minter;
    mapping (address => uint) public balance;
    uint public constant PRICE = 2 finney;

    constructor() public {
        minter = msg.sender;
    }

    function mint() public payable {
        require(msg.value >= PRICE, "Not enough value for a token!");
        balance[msg.sender] += msg.value / 2 finney;
    }

    function transfer(uint amount, address to) public {
        require(balance[msg.sender] >= amount, "Not enough tokens!");
        balance[msg.sender] -= amount;
        balance[to] += amount;
    }

    function terminate() public {
        require(msg.sender == minter, "You cannot terminate the contract!");
        selfdestruct(minter);
    }
}

```

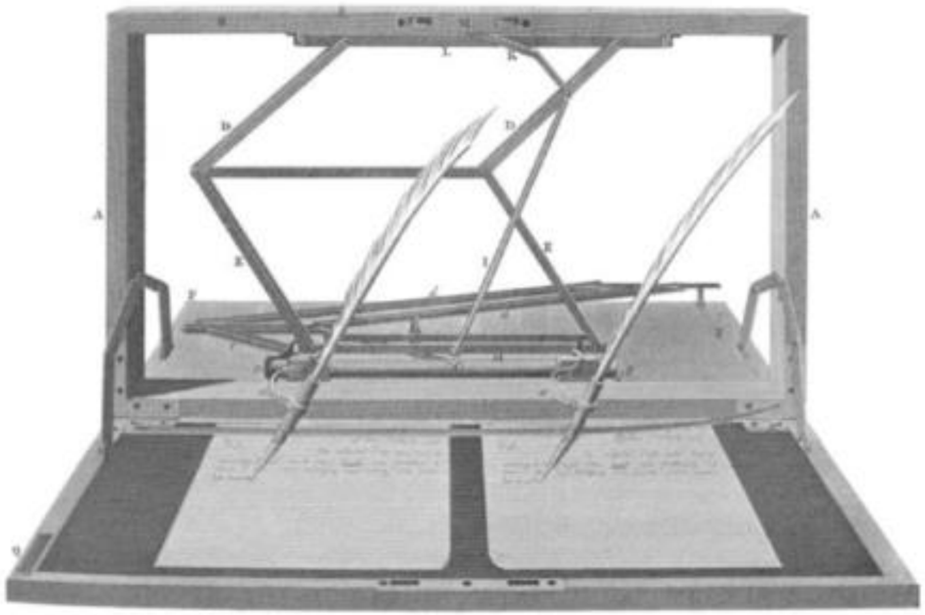
- Smart Contracts in Ethereum
  - live in the Ethereum environment
  - execute a function when called
  - have direct control over their own balance and key/value storage
  - have their behaviour fully specified by their **code**

The polygraph machine

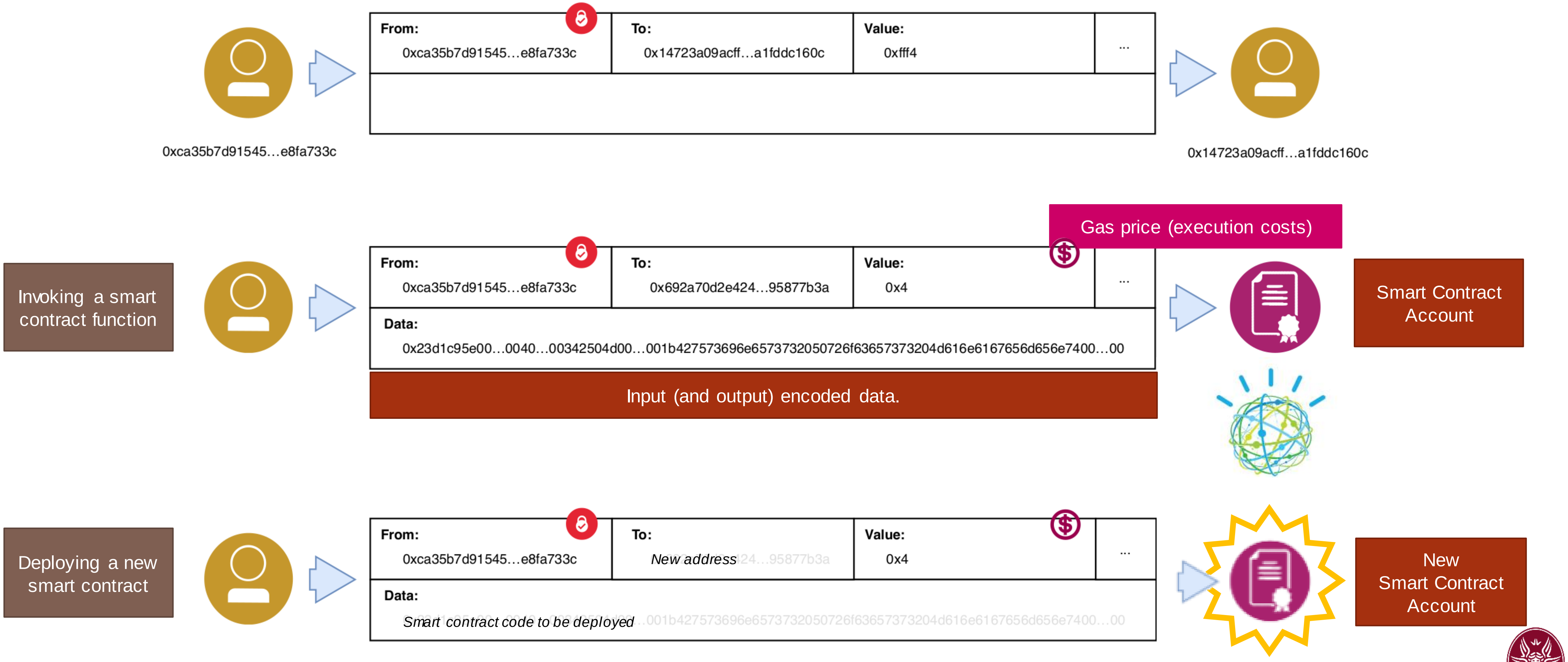
Where are Smart Contracts executed?

First on the mining nodes.
Then, potentially, on every node!

Only absolutely needed instructions should be put in code!



A programmable distributed environment



0xca35b7d91545…e8fa733c

From:	To:	Value:	…
0xca35b7d91545…e8fa733c	0x14723a09acff…a1fddc160c	0xfff4	

0x14723a09acff…a1fddc160c

Invoking a smart contract function

From:	To:	Value:	…
0xca35b7d91545…e8fa733c	0x692a70d2e424…95877b3a	0x4	

Data:
0x23d1c95e00…0040…00342504d00…001b427573696e6573732050726f63657373204d616e6167656d656e7400…00

Input (and output) encoded data.

Gas price (execution costs)

Smart Contract Account

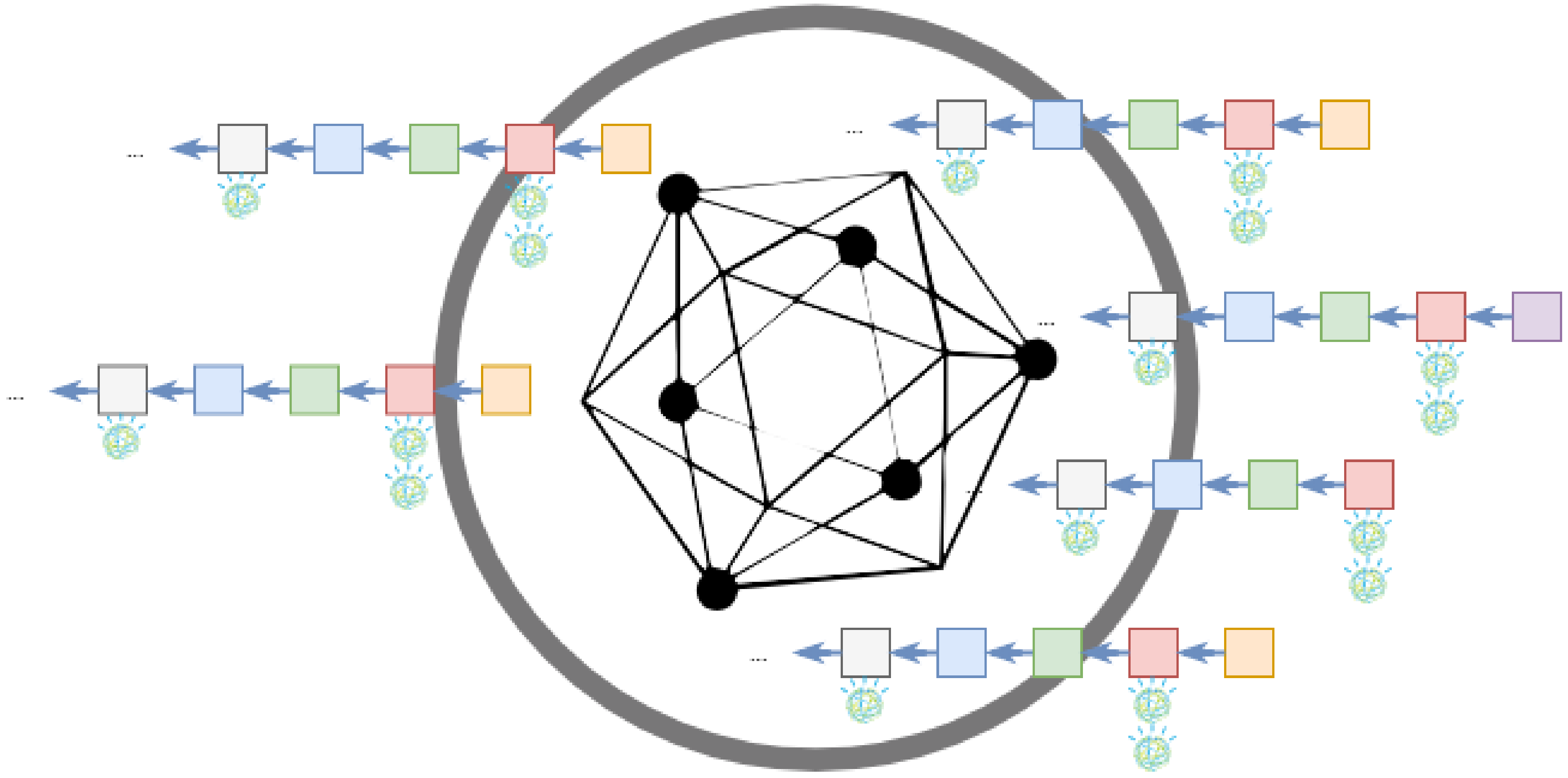
Deploying a new smart contract

From:	To:	Value:	…
0xca35b7d91545…e8fa733c	*New address* …424…95877b3a	0x4	

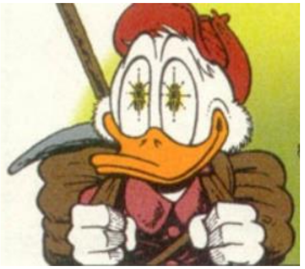
Data:
Smart contract code to be deployed …001b427573696e6573732050726f63657373204d616e6167656d656e7400…00

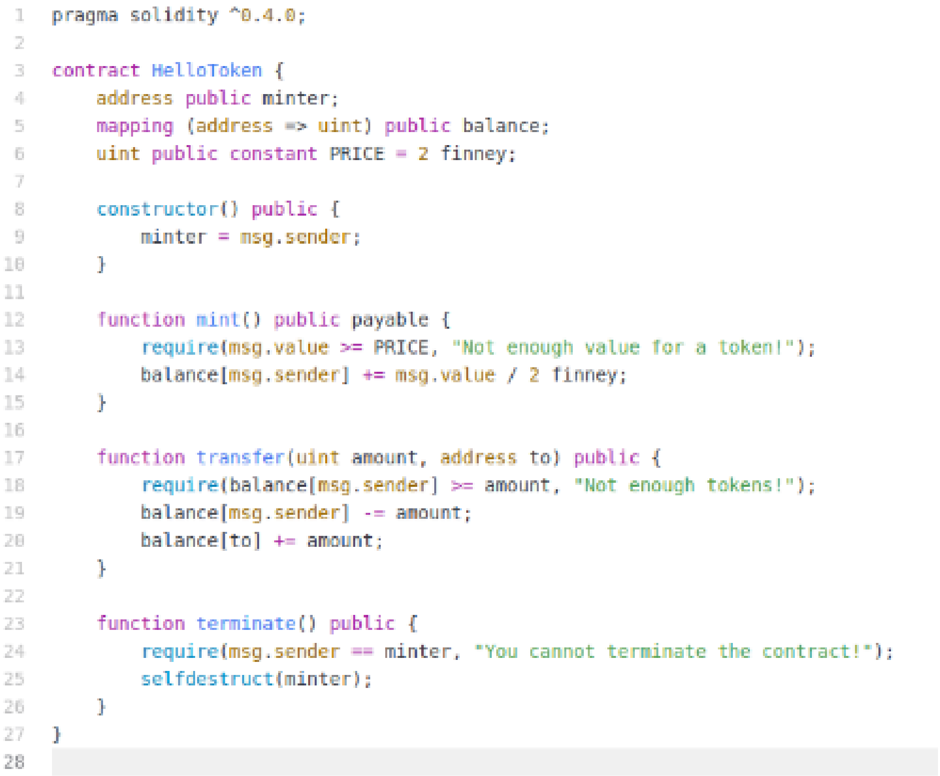
New Smart Contract Account

Distributed nature

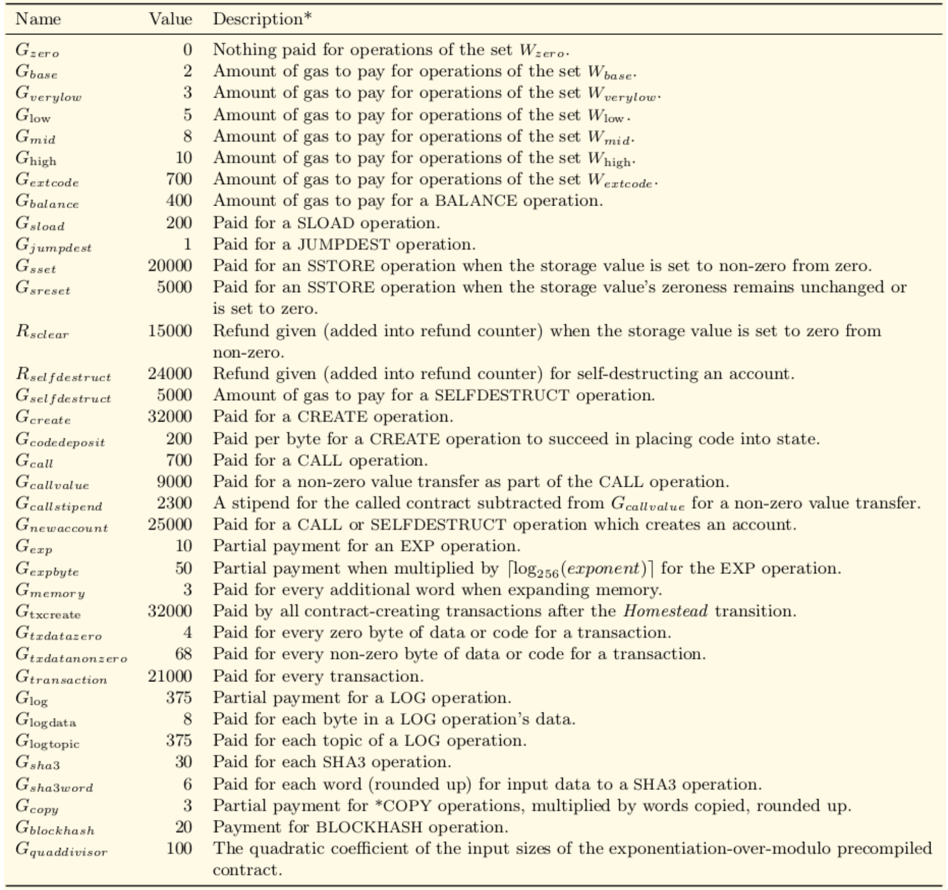


Smart Contracts are pieces of code (not for free)





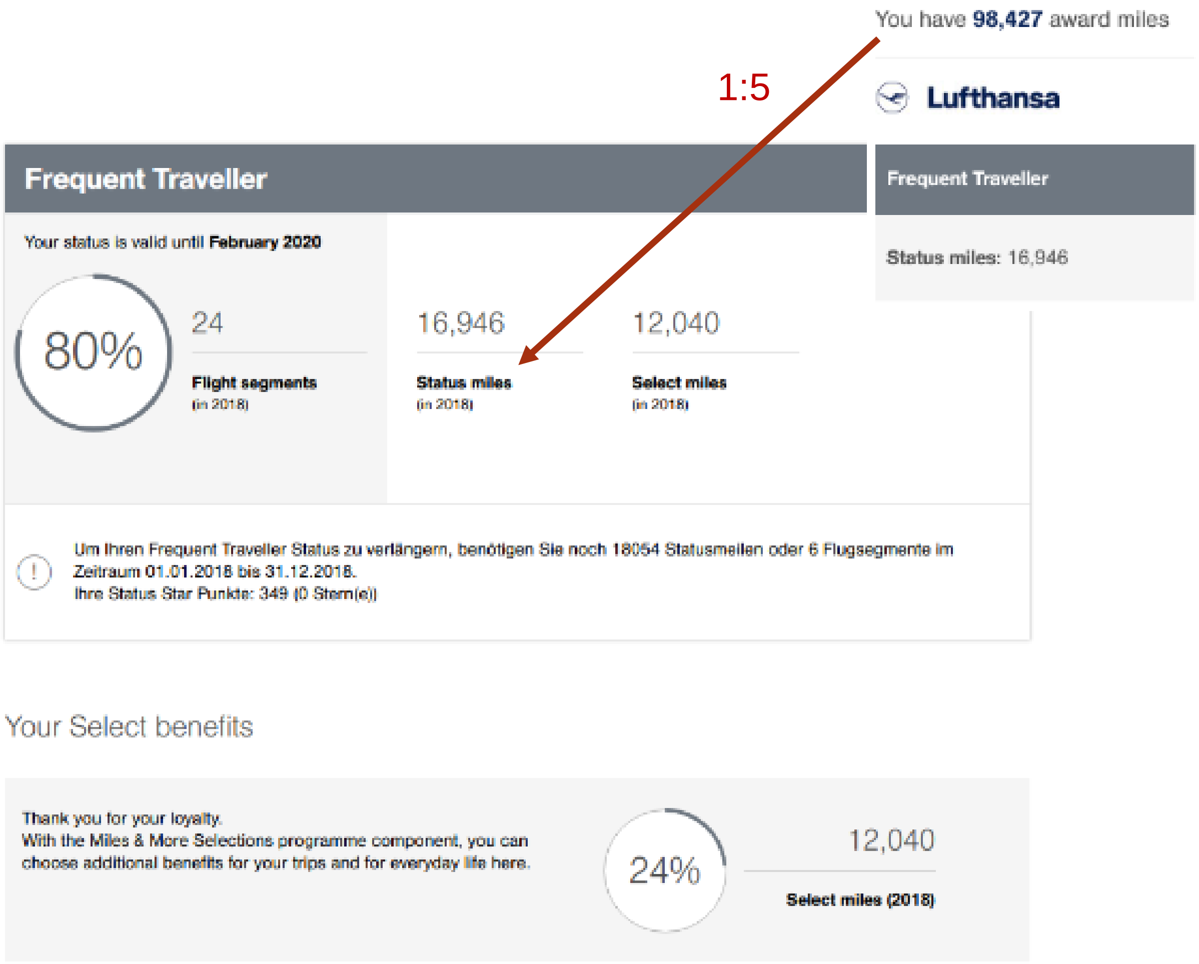
```
pragma solidity ^0.4.0;

contract HelloToken {
    address public minter;
    mapping (address => uint) public balance;
    uint public constant PRICE = 2 finney;

    constructor() public {
        minter = msg.sender;
    }

    function mint() public payable {
        require(msg.value >= PRICE, "Not enough value for a token!");
        balance[msg.sender] += msg.value / 2 finney;
    }

    function transfer(uint amount, address to) public {
        require(balance[msg.sender] >= amount, "Not enough tokens!");
        balance[msg.sender] -= amount;
        balance[to] += amount;
    }

    function terminate() public {
        require(msg.sender == minter, "You cannot terminate the contract!");
        selfdestruct(minter);
    }
}

```



Name	Value	Description*
G_{zero}	0	Nothing paid for operations of the set W_{zero}.
G_{base}	2	Amount of gas to pay for operations of the set W_{base}.
$G_{verylow}$	3	Amount of gas to pay for operations of the set $W_{verylow}$.
G_{low}	5	Amount of gas to pay for operations of the set W_{low}.
G_{mid}	8	Amount of gas to pay for operations of the set W_{mid}.
G_{high}	10	Amount of gas to pay for operations of the set W_{high}.
$G_{extcode}$	700	Amount of gas to pay for operations of the set $W_{extcode}$.
$G_{balance}$	400	Amount of gas to pay for a BALANCE operation.
G_{sload}	200	Paid for a SLOAD operation.
$G_{jumpdest}$	1	Paid for a JUMPDEST operation.
G_{sset}	20000	Paid for an SSTORE operation when the storage value is set to non-zero from zero.
G_{sreset}	5000	Paid for an SSTORE operation when the storage value's zeroness remains unchanged or is set to zero.
R_{sclear}	15000	Refund given (added into refund counter) when the storage value is set to zero from non-zero.
$R_{selfdestruct}$	24000	Refund given (added into refund counter) for self-destructing an account.
$G_{selfdestruct}$	5000	Amount of gas to pay for a SELFDESTRUCT operation.
G_{create}	32000	Paid for a CREATE operation.
$G_{codedeposit}$	200	Paid per byte for a CREATE operation to succeed in placing code into state.
G_{call}	700	Paid for a CALL operation.
$G_{callvalue}$	9000	Paid for a non-zero value transfer as part of the CALL operation.
$G_{callstipend}$	2300	A stipend for the called contract subtracted from $G_{callvalue}$ for a non-zero value transfer.
$G_{newaccount}$	25000	Paid for a CALL or SELFDESTRUCT operation which creates an account.
G_{exp}	10	Partial payment for an EXP operation.
$G_{expbyte}$	50	Partial payment when multiplied by $\lceil \log_{256}(exponent) \rceil$ for the EXP operation.
G_{memory}	3	Paid for every additional word when expanding memory.
G_{txcreate}	32000	Paid by all contract-creating transactions after the *Homestead* transition.
$G_{txdatazero}$	4	Paid for every zero byte of data or code for a transaction.
$G_{txdatanonzero}$	68	Paid for every non-zero byte of data or code for a transaction.
$G_{transaction}$	21000	Paid for every transaction.
G_{log}	375	Partial payment for a LOG operation.
G_{logdata}	8	Paid for each byte in a LOG operation's data.
G_{logtopic}	375	Paid for each topic of a LOG operation.
G_{sha3}	30	Paid for each SHA3 operation.
$G_{sha3word}$	6	Paid for each word (rounded up) for input data to a SHA3 operation.
G_{copy}	3	Partial payment for *COPY operations, multiplied by words copied, rounded up.
$G_{blockhash}$	20	Payment for BLOCKHASH operation.
$G_{quaddivisor}$	100	The quadratic coefficient of the input sizes of the exponentiation-over-modulo precompiled contract.

Wood 2014

Tokens are not cryptofuel
Nothing specific of blockchains, after all!



You have **98,427** award miles

1:5

Lufthansa

Frequent Traveller

Status miles: 16,946

Frequent Traveller

Your status is valid until **February 2020**

80%

24	16,946	12,040
Flight segments (in 2018)	**Status miles** (in 2018)	**Select miles** (in 2018)

Um Ihren Frequent Traveller Status zu verlängern, benötigen Sie noch 18054 Statusmeilen oder 6 Flugsegmente im Zeitraum 01.01.2018 bis 31.12.2018.
Ihre Status Star Punkte: 349 (0 Stern(e))

Your Select benefits

Thank you for your loyalty.
With the Miles & More Selections programme component, you can choose additional benefits for your trips and for everyday life here.

24%

12,040

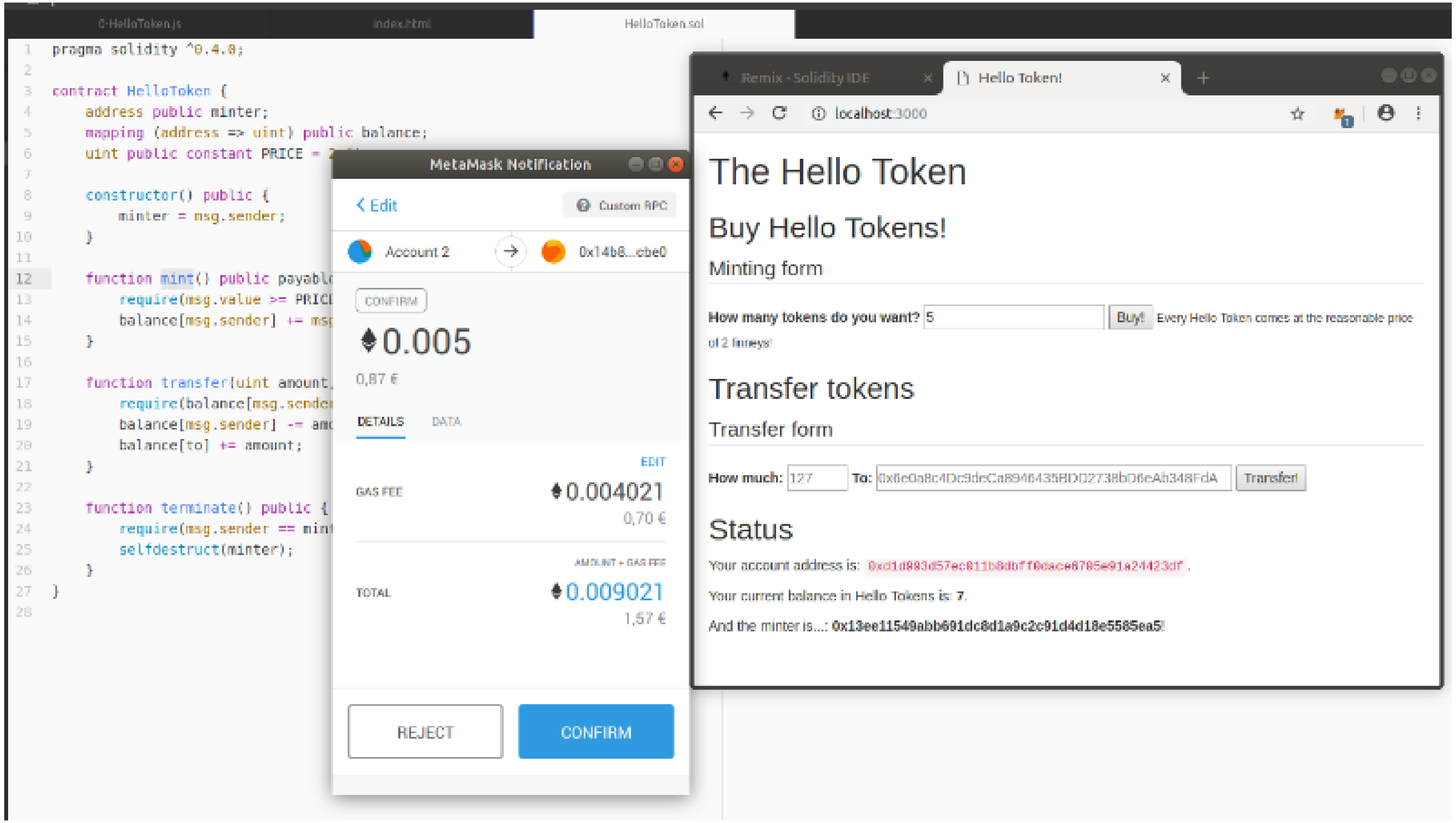
Select miles (2018)

Period	01.01.2017 to today
Number of flights	66
Flown distance	81,273 km or 50,501 miles
Flight time	5 d 21 h 0 min

Up to 1,50 euros = 1 M

Up to € 1 = 1 M

Your brand new token in 5 minutes or less



```
pragma solidity ^0.4.0;

contract HelloToken {
    address public minter;
    mapping (address => uint) public balance;
    uint public constant PRICE = 2

    constructor() public {
        minter = msg.sender;
    }

    function mint() public payabl
        require(msg.value >= PRICE
        balance[msg.sender] += msg
    }

    function transfer(uint amount,
        require(balance[msg.sender
        balance[msg.sender] -= amo
        balance[to] += amount;
    }

    function terminate() public {
        require(msg.sender == mint
        selfdestruct(minter);
    }
}
```

0.005
0,87 €

GAS FEE 0.004021
0,70 €

AMOUNT + GAS FEE
TOTAL 0.009021
1,57 €

The Hello Token

Buy Hello Tokens!

Minting form

How many tokens do you want? 5 Buy! Every Hello Token comes at the reasonable price of 2 finneys!

Transfer tokens

Transfer form

How much: 127 To: 0x6e0a8c4Dc9deCa8946435BDD2738bD6eAb348FdA Transfer!

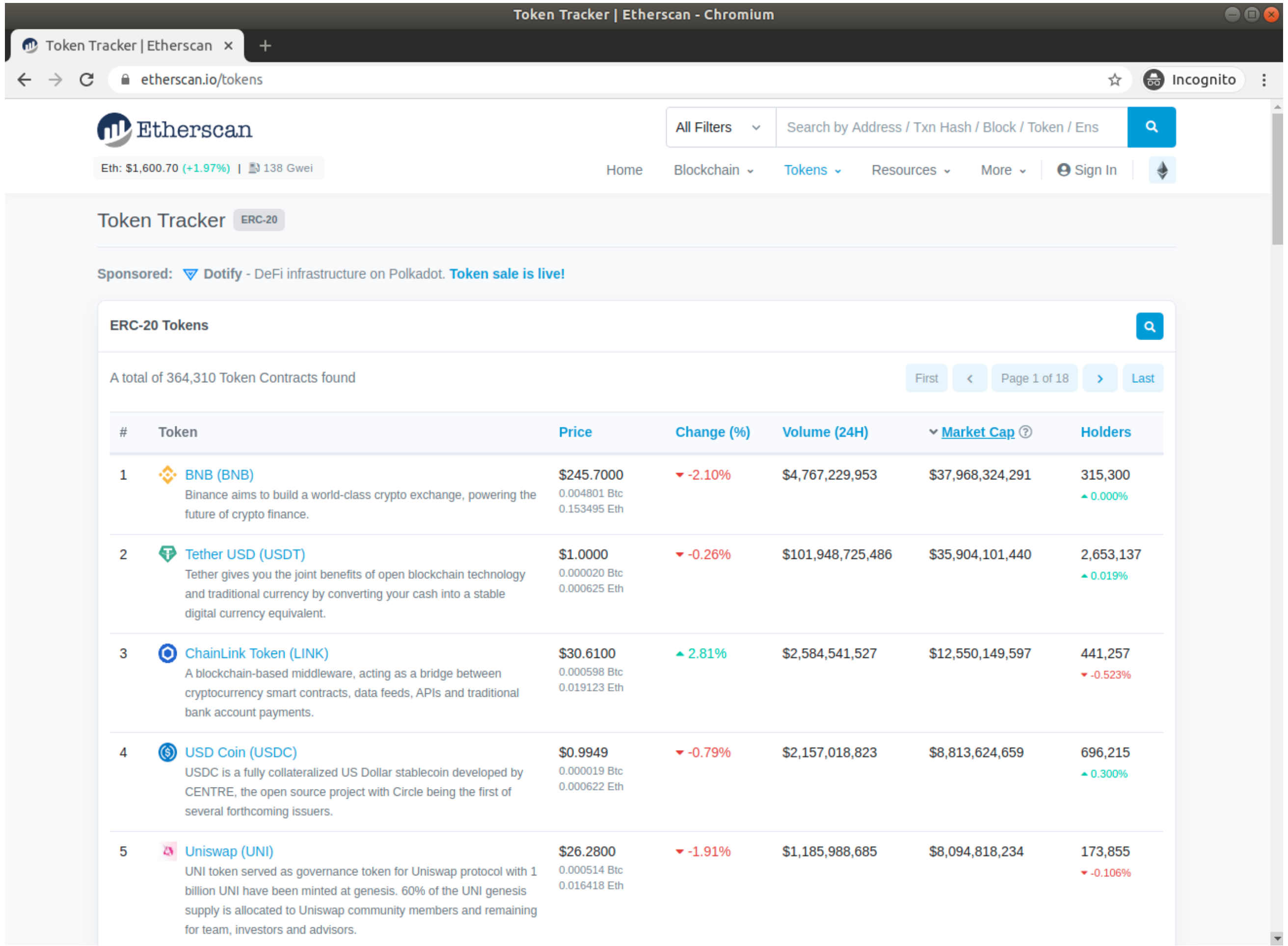
Status

Your account address is: 0xd1d893d57ec811b8dbff0dace8785e91a24423df .

Your current balance in Hello Tokens is: **7**.

And the minter is...: **0x13ee11549abb691dc8d1a9c2c91d4d18e5585ea5**!

Tokens



Token Tracker | Etherscan - Chromium
Token Tracker | Etherscan
etherscan.io/tokens
Incognito
Etherscan
Eth: $1,600.70 (+1.97%) | 138 Gwei
All Filters
Search by Address / Txn Hash / Block / Token / Ens
Home
Blockchain
Tokens
Resources
More
Sign In

Token Tracker ERC-20

Sponsored: Dotify - DeFi infrastructure on Polkadot. Token sale is live!

ERC-20 Tokens

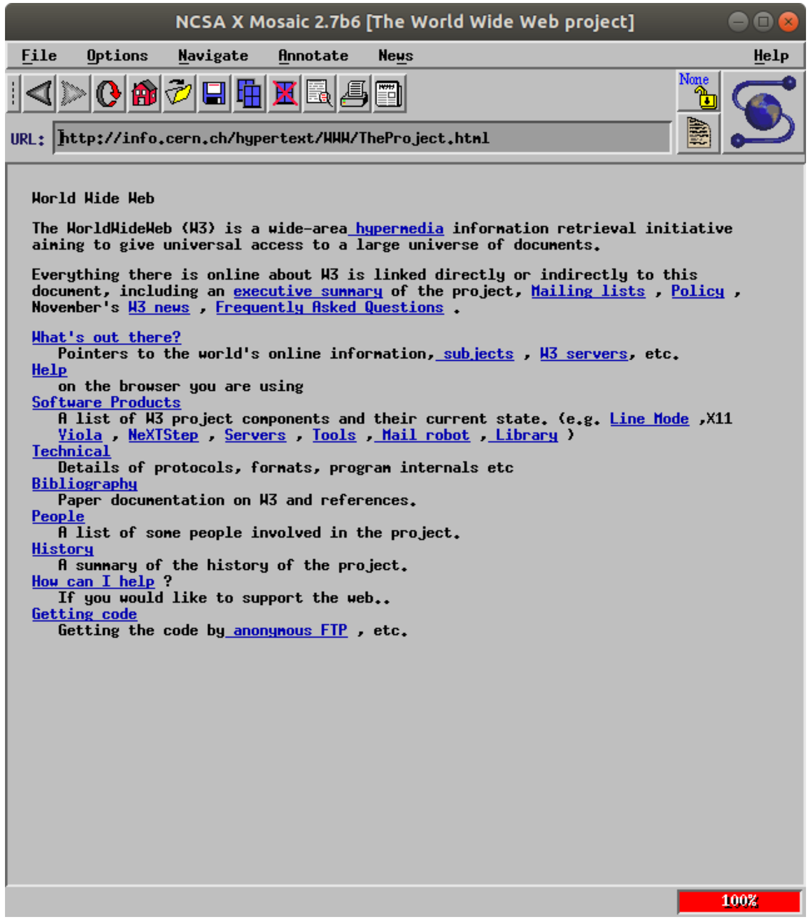
A total of 364,310 Token Contracts found

#	Token	Price	Change (%)	Volume (24H)	Market Cap	Holders
1	BNB (BNB) Binance aims to build a world-class crypto exchange, powering the future of crypto finance.	$245.7000 0.004801 Btc 0.153495 Eth	▼ -2.10%	$4,767,229,953	$37,968,324,291	315,300 ▲ 0.000%
2	Tether USD (USDT) Tether gives you the joint benefits of open blockchain technology and traditional currency by converting your cash into a stable digital currency equivalent.	$1.0000 0.000020 Btc 0.000625 Eth	▼ -0.26%	$101,948,725,486	$35,904,101,440	2,653,137 ▲ 0.019%
3	ChainLink Token (LINK) A blockchain-based middleware, acting as a bridge between cryptocurrency smart contracts, data feeds, APIs and traditional bank account payments.	$30.6100 0.000598 Btc 0.019123 Eth	▲ 2.81%	$2,584,541,527	$12,550,149,597	441,257 ▼ -0.523%
4	USD Coin (USDC) USDC is a fully collateralized US Dollar stablecoin developed by CENTRE, the open source project with Circle being the first of several forthcoming issuers.	$0.9949 0.000019 Btc 0.000622 Eth	▼ -0.79%	$2,157,018,823	$8,813,624,659	696,215 ▲ 0.300%
5	Uniswap (UNI) UNI token served as governance token for Uniswap protocol with 1 billion UNI have been minted at genesis. 60% of the UNI genesis supply is allocated to Uniswap community members and remaining for team, investors and advisors.	$26.2800 0.000514 Btc 0.016418 Eth	▼ -1.91%	$1,185,988,685	$8,094,818,234	173,855 ▼ -0.106%

Tokens

reddcoin
Nautiluscoin
IN PINK WE TRUST
Un
Syscoin
THE CURRENCY OF THE FUTURE
reddcoin

The Blockchain and the Internet

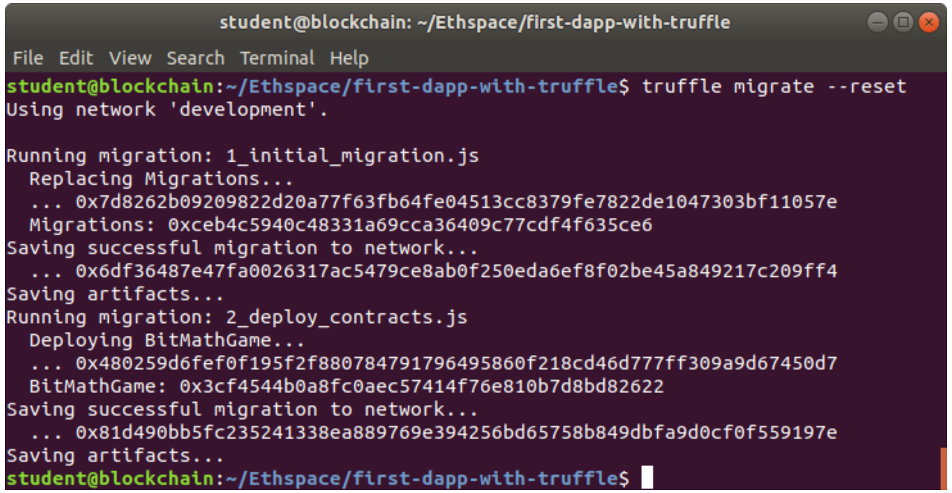

NCSA X Mosaic 2.7b6 [The World Wide Web project]
File Options Navigate Annotate News Help
None
URL: http://info.cern.ch/hypertext/WWW/TheProject.html
100%

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

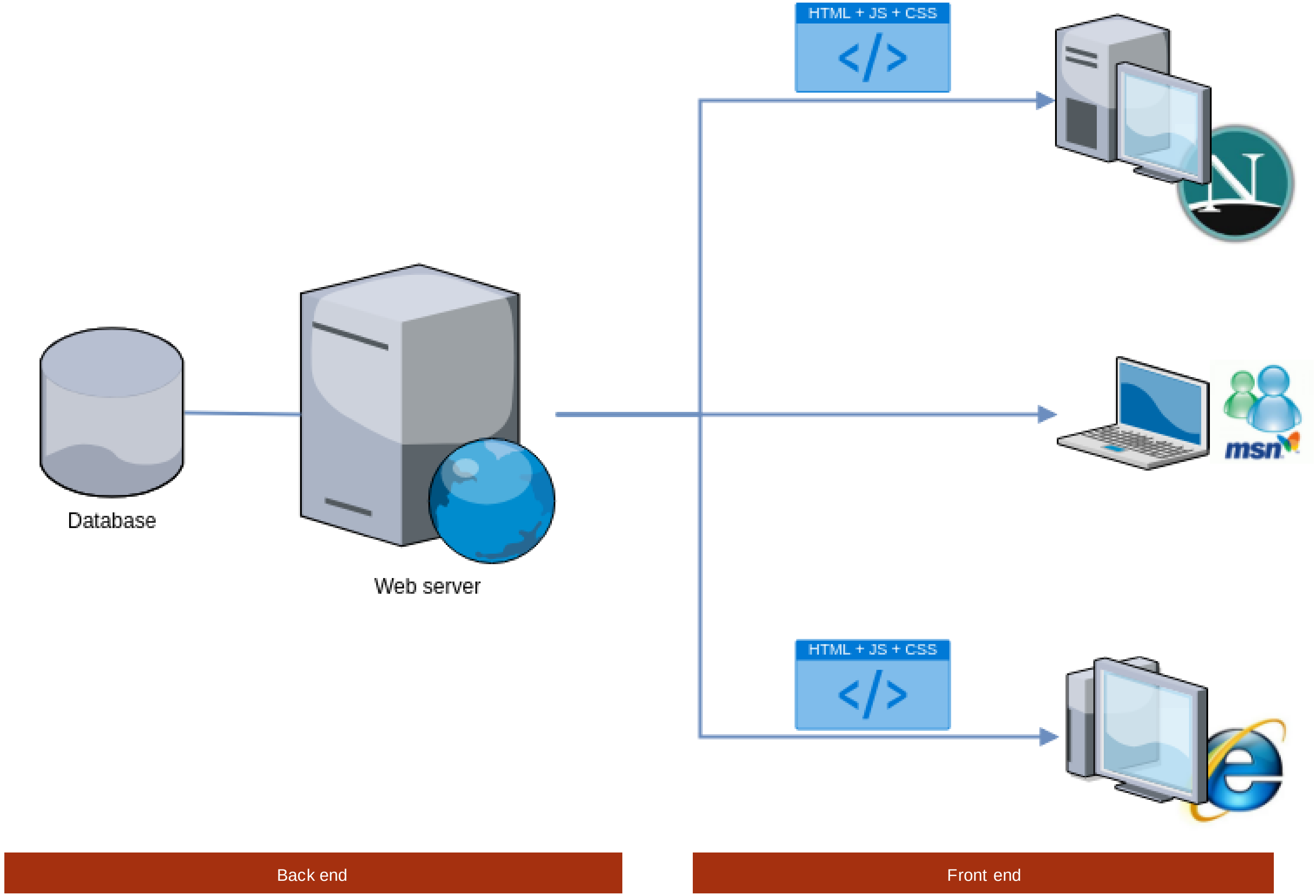
Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
 Pointers to the world's online information, subjects , W3 servers, etc.
Help
 on the browser you are using
Software Products
 A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
 Details of protocols, formats, program internals etc
Bibliography
 Paper documentation on W3 and references.
People
 A list of some people involved in the project.
History
 A summary of the history of the project.
How can I help ?
 If you would like to support the web..
Getting code
 Getting the code by anonymous FTP , etc.

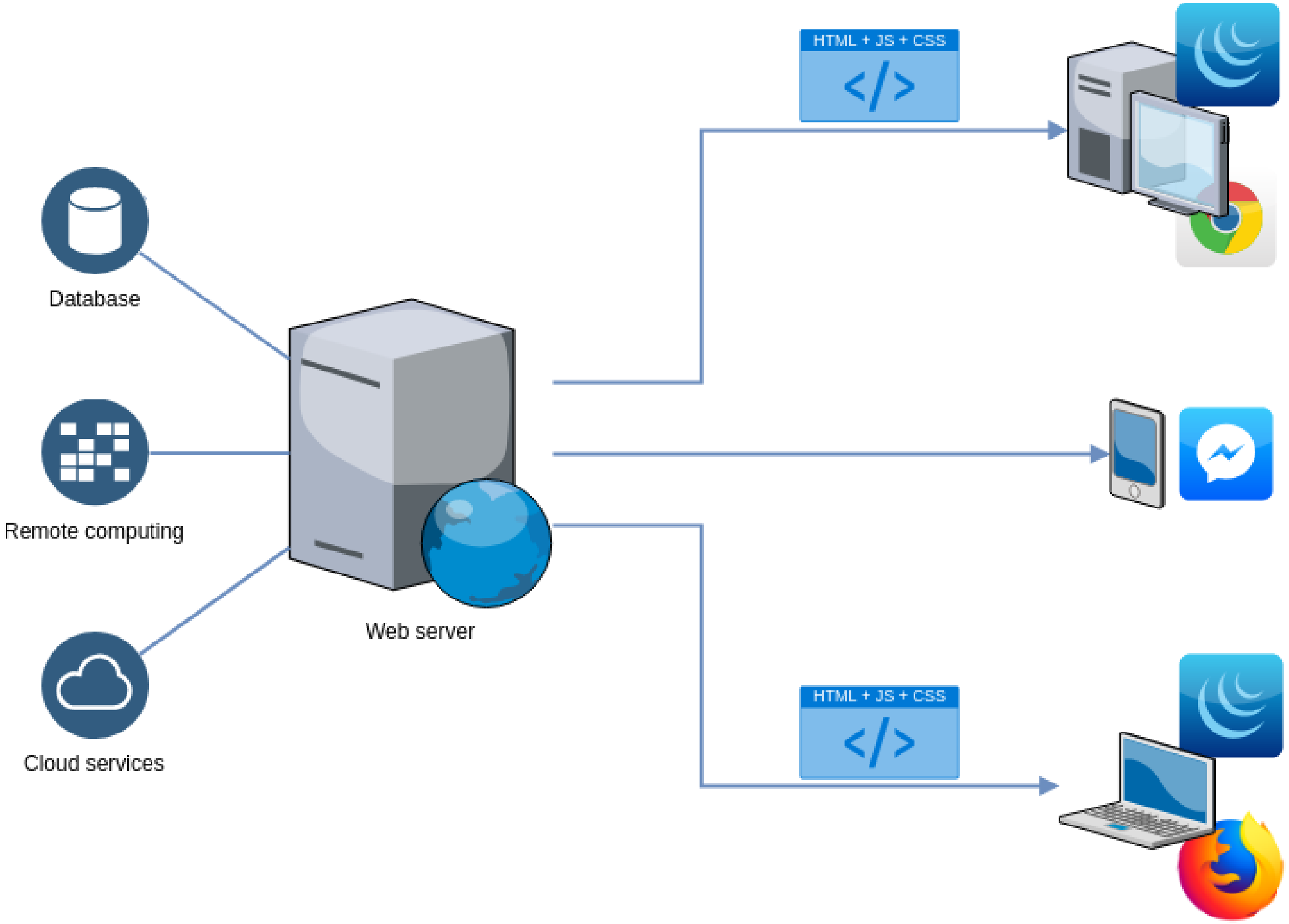

student@blockchain: ~/Ethspace/first-dapp-with-truffle
File Edit View Search Terminal Help

```
student@blockchain:~/Ethspace/first-dapp-with-truffle$ truffle migrate --reset
Using network 'development'.

Running migration: 1_initial_migration.js
  Replacing Migrations...
  ... 0x7d8262b09209822d20a77f63fb64fe04513cc8379fe7822de1047303bf11057e
  Migrations: 0xceb4c5940c48331a69cca36409c77cdf4f635ce6
Saving successful migration to network...
  ... 0x6df36487e47fa0026317ac5479ce8ab0f250eda6ef8f02be45a849217c209ff4
Saving artifacts...
Running migration: 2_deploy_contracts.js
  Deploying BitMathGame...
  ... 0x480259d6fef0f195f2f880784791796495860f218cd46d777ff309a9d67450d7
  BitMathGame: 0x3cf4544b0a8fc0aec57414f76e810b7d8bd82622
Saving successful migration to network...
  ... 0x81d490bb5fc235241338ea889769e394256bd65758b849dbfa9d0cf0f559197e
Saving artifacts...
student@blockchain:~/Ethspace/first-dapp-with-truffle$
```

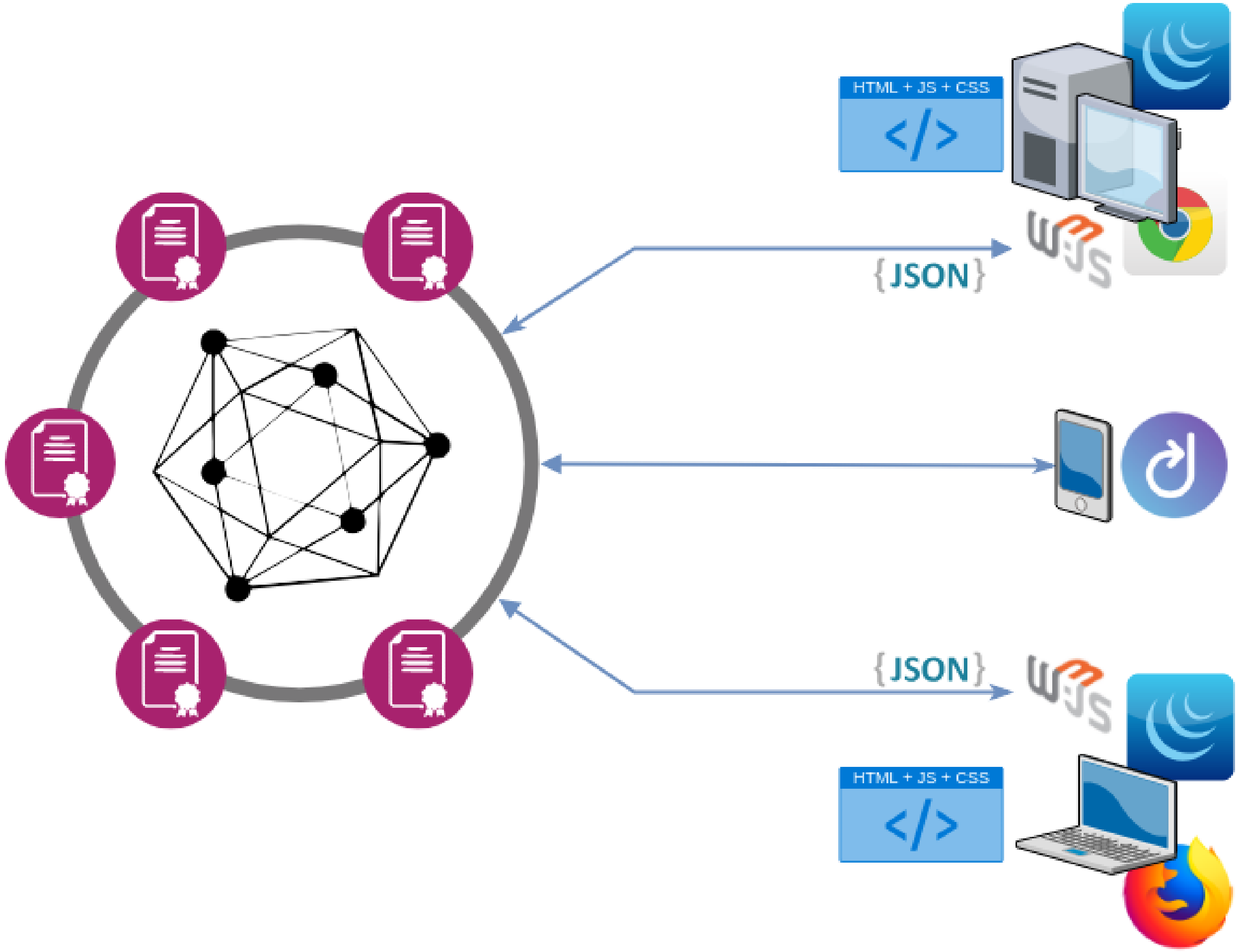
Web 1.0


HTML + JS + CSS
</>
Database
Web server
msn
HTML + JS + CSS
</>
Back end
Front end

Web 2.0

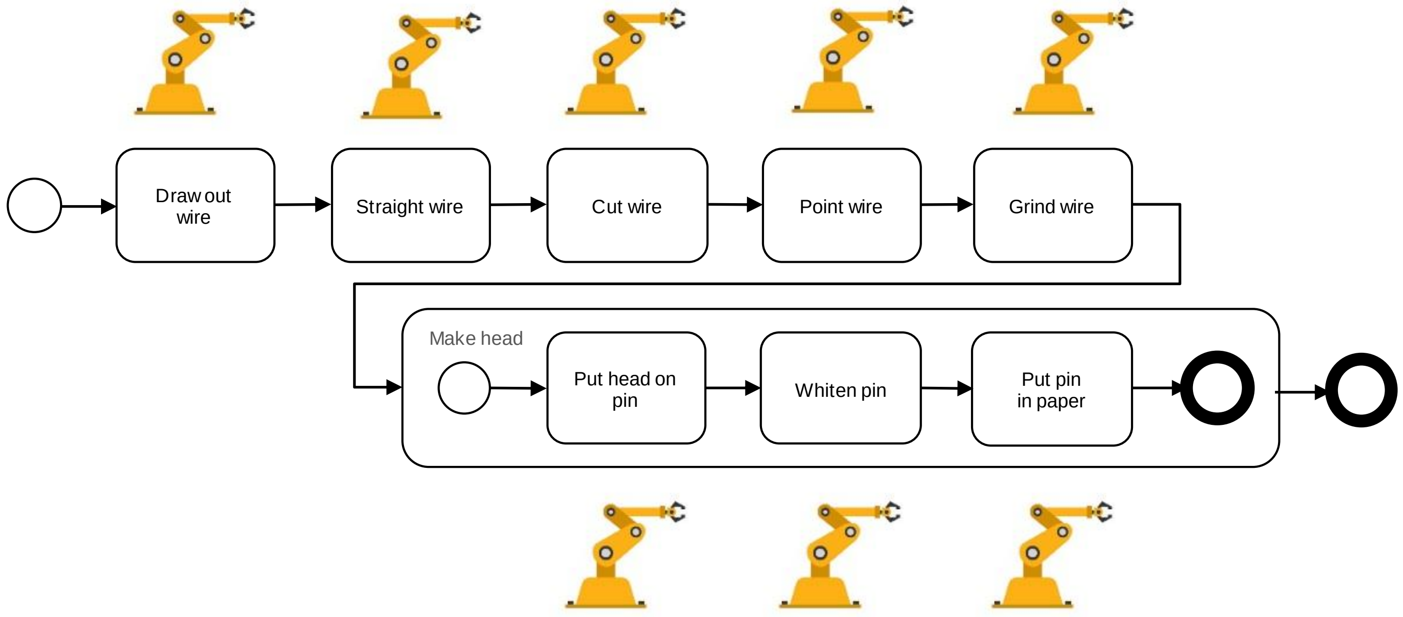

HTML + JS + CSS
</>
Database
Remote computing
Cloud services
Web server
HTML + JS + CSS
</>

Web 3.0



Blockchain as a process execution infrastructure

Division of labour → Automation



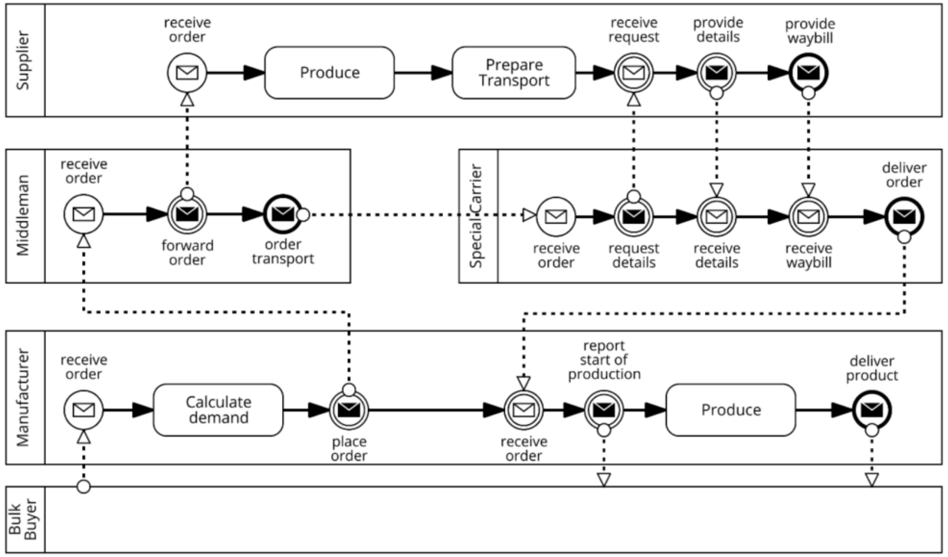
Icons © freepik.com

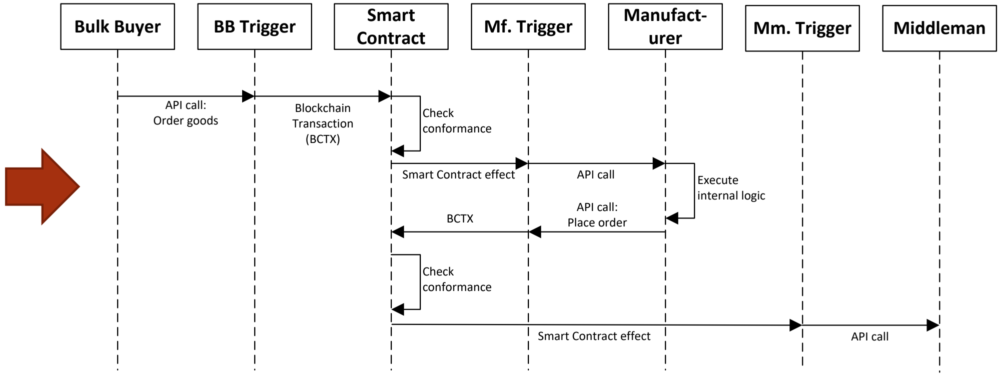
Systems like to report on their job (logging)

- [2019-02-18T12:30:00-02:00] 0xACDC0801 executes Draw Out Wire on Item 0xAA01
- [2019-02-18T12:30:10-02:00] 0xACDC0802 executes Straight Wire on Item 0xAA01
- [2019-02-18T12:30:20-02:00] 0xACDC0803 executes Cut Wire on Item 0xAA01
- [2019-02-18T12:30:30-02:00] 0xACDC0801 executes Draw Out Wire on Item 0xAA02
- [2019-02-18T12:30:40-02:00] 0xACDC0802 executes Straight Wire on Item 0xAA02
- [2019-02-18T12:30:50-02:00] 0xACDC0804 executes Point Wire on Item 0xAA01
- [2019-02-18T12:31:00-02:00] 0xACDC0801 executes Draw Out Wire on Item 0xAA03
- …

Icons © freepik.com

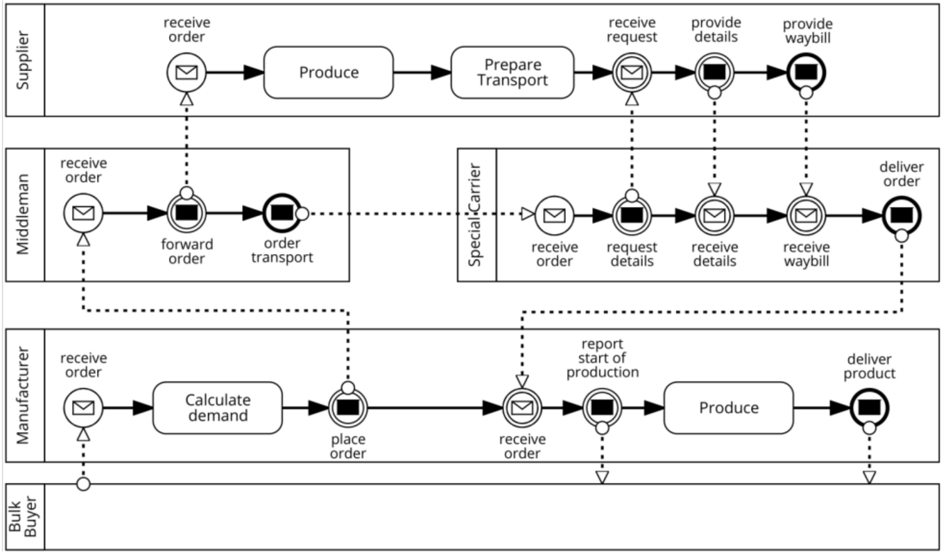
Smart contracts can execute processes

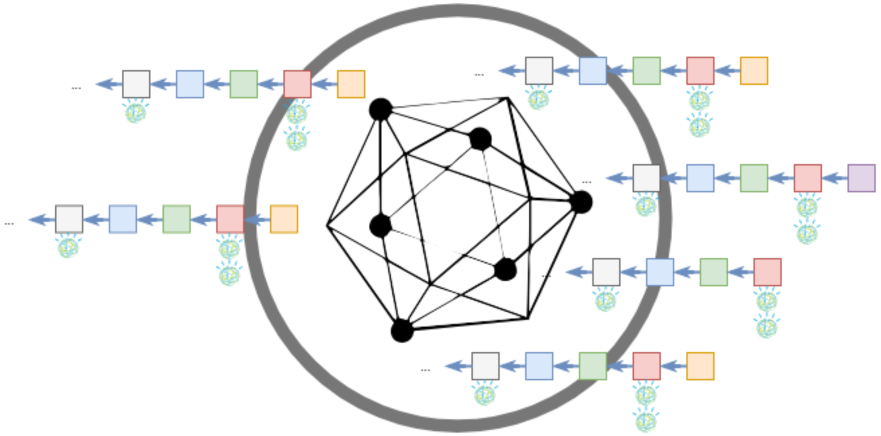


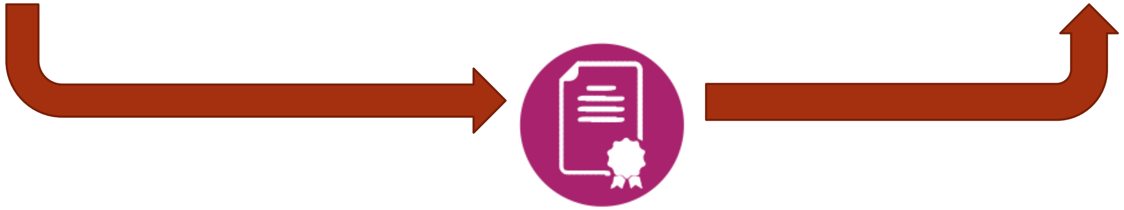


Weber et al.: Untrusted business process monitoring and execution using blockchain. In: Proc. of BPM. Springer, 2016.

Executing inter-organisational processes on the Blockchain: A model-driven approach







HAUPTBEITRAG / **BLOCKCHAIN SUPPORT FOR BUSINESS PROCESSES** }

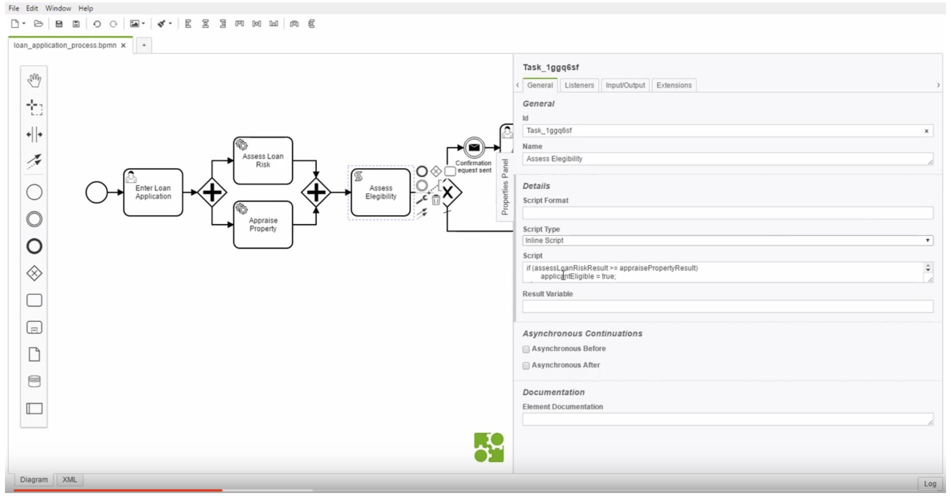
Blockchain Support for Collaborative Business Processes

Claudio Di Ciccio · Alessio Cecconi
Marlon Dumas
Luciano García-Bañuelos
Orlenys López-Pintado · Qinghua Lu
Jan Mendling · Alexander Ponomarev
An Binh Tran · Ingo Weber

D.C, Cecconi, Dumas et al. Blockchain support for collaborative business processes. Informatik Spektrum pp. 1–9 (May 2019)

Executing inter-organisational processes on the Blockchain: A model-driven approach

Caterpillar



Task_1ggq6sf

General | Listeners | Input/Output | Extensions

General

Id: Task_1ggq6sf

Name: Assess Elegibility

Details

Script Format:

Script Type: Inline Script

Script:

```
if (assessLoanRiskResult >= appraisePropertyResult)
    applicantEligible = true;
```

Result Variable:

Asynchronous Continuations

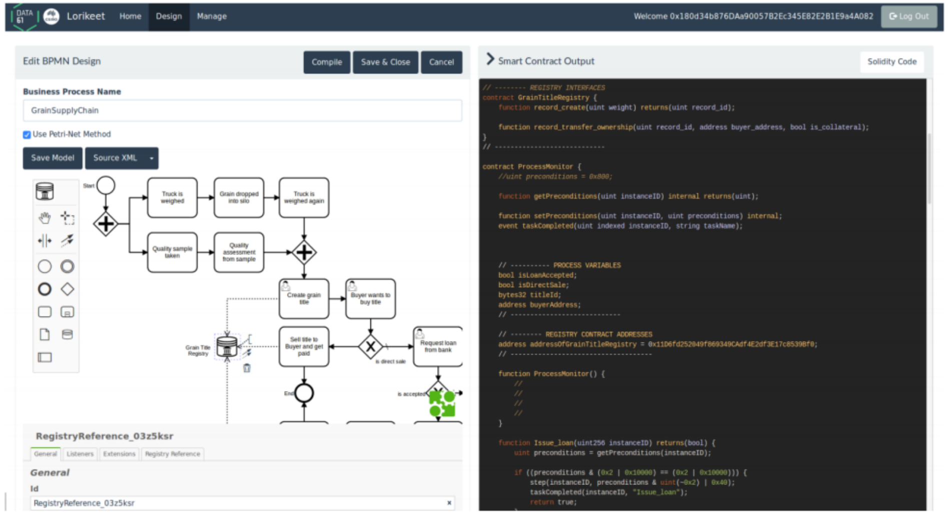
□ Asynchronous Before

□ Asynchronous After

Documentation

Element Documentation:

Lorikeet



Welcome 0x180d34b876DAa90057B2Ec345E82E2B1E9a4A082

Edit BPMN Design

Business Process Name: GrainSupplyChain

☑ Use Petri-Net Method

RegistryReference_03z5ksr

General | Listeners | Extensions | Registry Reference

General

Id: RegistryReference_03z5ksr

Smart Contract Output

```
// -------- REGISTRY INTERFACES
contract GrainTitleRegistry {
    function record_create(uint weight) returns(uint record_id);

    function record_transfer_ownership(uint record_id, address buyer_address, bool is_collateral);
}
// --------------------------

contract ProcessMonitor {
    //uint preconditions = 0x800;

    function getPreconditions(uint instanceID) internal returns(uint);

    function setPreconditions(uint instanceID, uint preconditions) internal;
    event taskCompleted(uint indexed instanceID, string taskName);



    // ---------- PROCESS VARIABLES
    bool isLoanAccepted;
    bool isDirectSale;
    bytes32 titleId;
    address buyerAddress;
    // --------------------------

    // -------- REGISTRY CONTRACT ADDRESSES
    address addressOfGrainTitleRegistry = 0x11D6fd252049f869349CAdf4E2df3E17c8539Bf0;
    // --------------------------------

    function ProcessMonitor() {
        //
        //
        //
        //
    }

    function Issue_loan(uint256 instanceID) returns(bool) {
        uint preconditions = getPreconditions(instanceID);

        if ((preconditions & (0x2 | 0x10000) == (0x2 | 0x10000))) {
            step(instanceID, preconditions & uint(~0x2) | 0x40);
            taskCompleted(instanceID, "Issue_loan");
            return true;
```

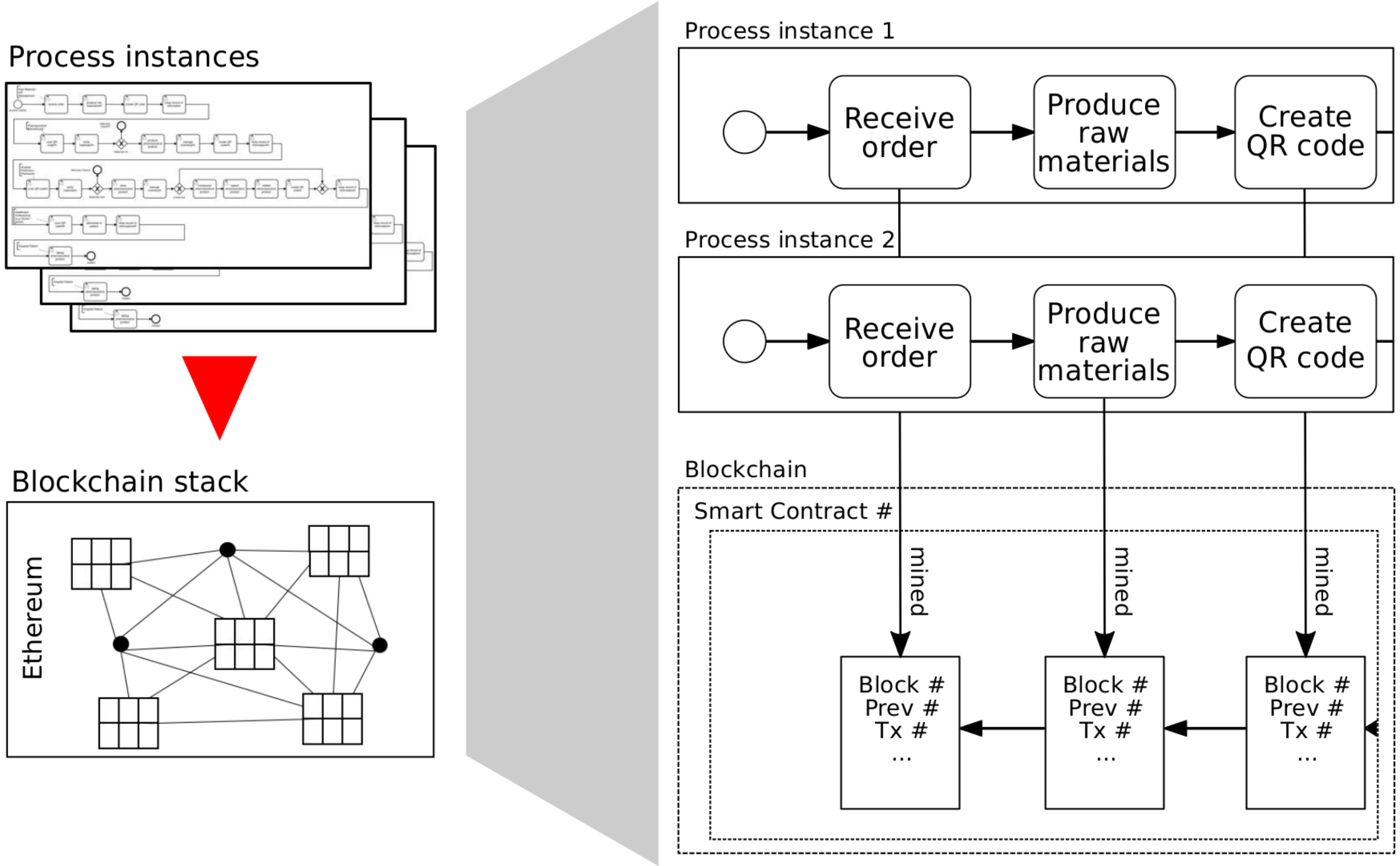
López-Pintado, García-Bañuelos, Dumas, Weber. **Caterpillar**: A blockchain-based business process management system. In: BPM Demos. CEUR.ws, 2017.
Tran, Lu, Weber. **Lorikeet**: A Model-Driven Engineering Tool for Blockchain-Based Business Process Execution and Asset. In: BPM Demos. CEUR.ws, 2018.

D.C, Cecconi, Dumas et al. Blockchain support for collaborative business processes. Informatik Spektrum pp. 1–9 (May 2019)

Rationale

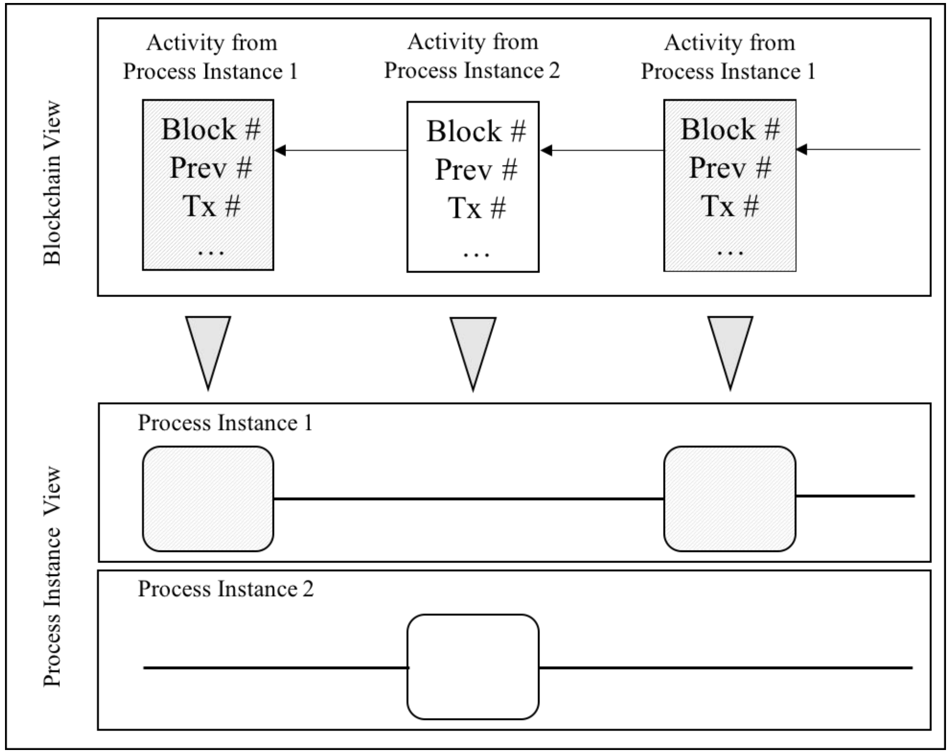
Blockchain-Based Traceability of Inter-organisational Business Processes

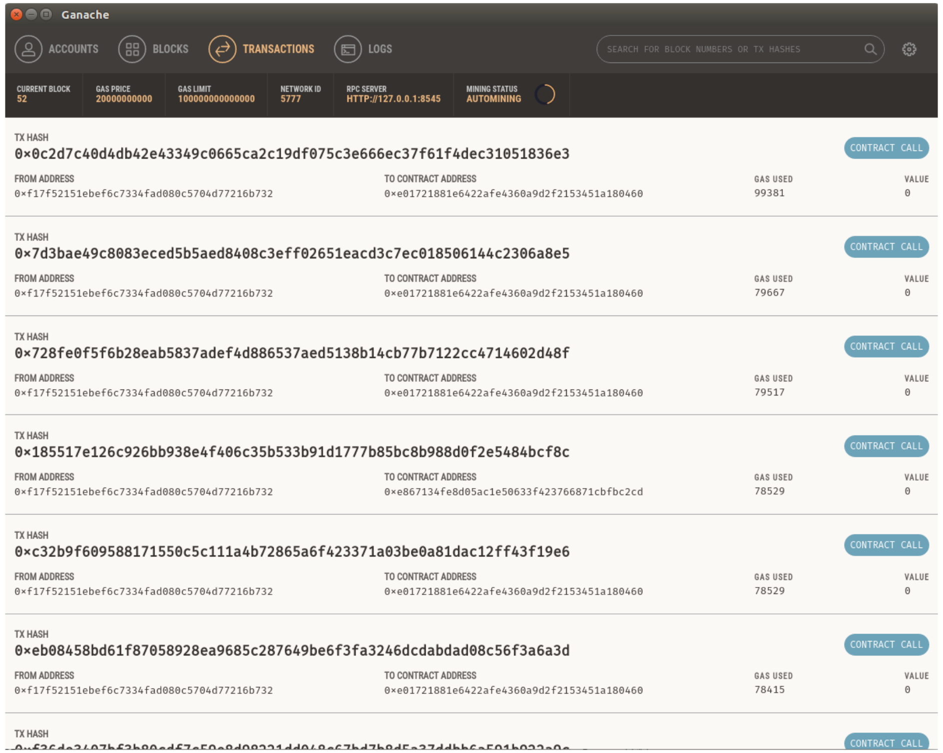
Claudio Di Ciccio(✉), Alessio Cecconi, Jan Mendling, Dominik Felix, Dominik Haas, Daniel Lilek, Florian Riel, Andreas Rumpl, and Philipp Uhlig



D.C. et al. Blockchain-Based Traceability of Inter-organisational Business Processes. In: BMSD. Springer, 2018.

Rationale





```
CURRENT BLOCK  GAS PRICE    GAS LIMIT        NETWORK ID  RPC SERVER              MINING STATUS
52             20000000000  100000000000000  5777        HTTP://127.0.0.1:8545   AUTOMINING

TX HASH                                                                                    CONTRACT CALL
0×0c2d7c40d4db42e43349c0665ca2c19df075c3e666ec37f61f4dec31051836e3
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×f17f52151ebef6c7334fad080c5704d77216b732   0×e01721881e6422afe4360a9d2f2153451a180460   99381     0

TX HASH                                                                                    CONTRACT CALL
0×7d3bae49c8083eced5b5aed8408c3eff02651eacd3c7ec018506144c2306a8e5
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×f17f52151ebef6c7334fad080c5704d77216b732   0×e01721881e6422afe4360a9d2f2153451a180460   79667     0

TX HASH                                                                                    CONTRACT CALL
0×728fe0f5f6b28eab5837adef4d886537aed5138b14cb77b7122cc4714602d48f
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×f17f52151ebef6c7334fad080c5704d77216b732   0×e01721881e6422afe4360a9d2f2153451a180460   79517     0

TX HASH                                                                                    CONTRACT CALL
0×185517e126c926bb938e4f406c35b533b91d1777b85bc8b988d0f2e5484bcf8c
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×f17f52151ebef6c7334fad080c5704d77216b732   0×e867134fe8d05ac1e50633f423766871cbfbc2cd   78529     0

TX HASH                                                                                    CONTRACT CALL
0×c32b9f609588171550c5c111a4b72865a6f423371a03be0a81dac12ff43f19e6
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×f17f52151ebef6c7334fad080c5704d77216b732   0×e01721881e6422afe4360a9d2f2153451a180460   78529     0

TX HASH                                                                                    CONTRACT CALL
0×eb08458bd61f87058928ea9685c287649be6f3fa3246dcdabdad08c56f3a6a3d
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED  VALUE
0×f17f52151ebef6c7334fad080c5704d77216b732   0×e01721881e6422afe4360a9d2f2153451a180460   78415     0

TX HASH                                                                                    CONTRACT CALL
[illegible]
```

D.C. et al. Blockchain-Based Traceability of Inter-organisational Business Processes. In: BMSD. Springer, 2018.

Coming next: Smart contracts × supply chain (demo)

Claudio Di Ciccio | http://diciccio.net | claudio.diciccio@uniroma1.it

Sapienza, University of Rome, Italy

Blockchain Tech course 2020-21 at Sapienza:
https://sites.google.com/uniroma1.it/cfa-msc-blockchaintech/

Blockchain and smart contracts: infrastructure and platforms

Claudio Di Ciccio | http://diciccio.net | claudio.diciccio@uniroma1.it

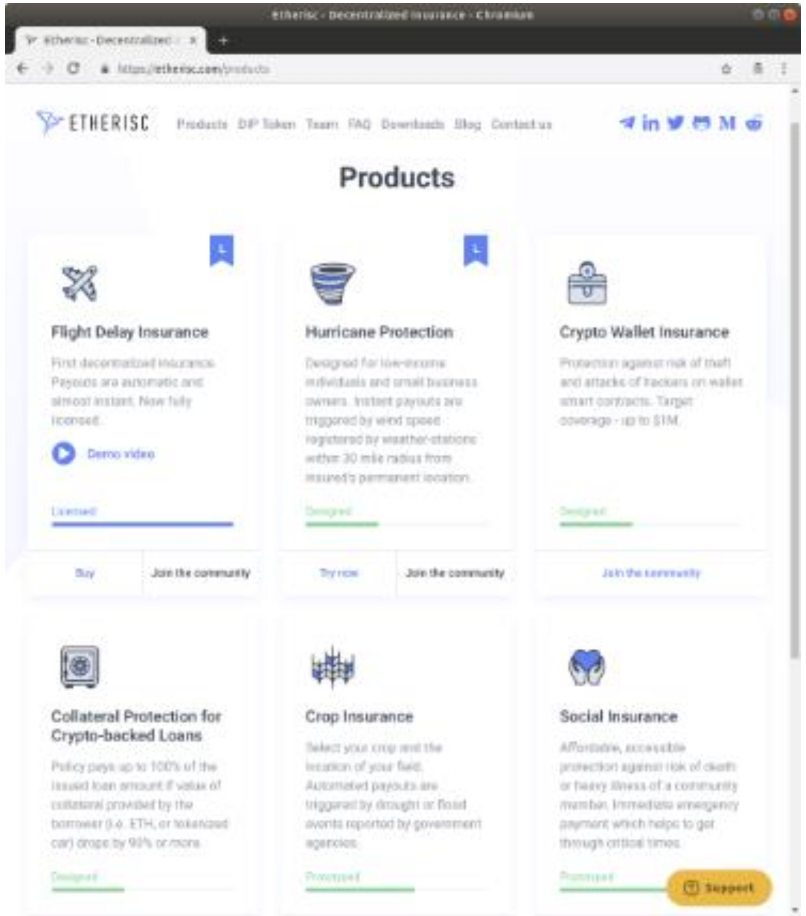
Sapienza, University of Rome, Italy

Blockchain Tech course 2020-21 at Sapienza:
https://sites.google.com/uniroma1.it/cfa-msc-blockchaintech/

How about the real world?

Oracles: From on-chain to off-chain and vice versa

Etherisc



Etherisc - Decentralized insurance - Chromium

https://etherisc.com/products

Products

Flight Delay Insurance

First decentralized insurance. Payouts are automatic and almost instant. Now fully licensed.

Demo video

Licensed

Buy | Join the community

Hurricane Protection

Designed for low-income individuals and small business owners. Instant payouts are triggered by wind speed registered by weather-stations within 30 mile radius from insured's permanent location.

Designed

Try now | Join the community

Crypto Wallet Insurance

Protection against risk of theft and attacks of hackers on wallet smart contracts. Target coverage - up to $1M.

Designed

Join the community

Collateral Protection for Crypto-backed Loans

Policy pays up to 100% of the issued loan amount if value of collateral provided by the borrower (i.e. ETH, or tokenized car) drops by 90% or more.

Designed

Crop Insurance

Select your crop and the location of your field. Automated payouts are triggered by drought or flood events reported by government agencies.

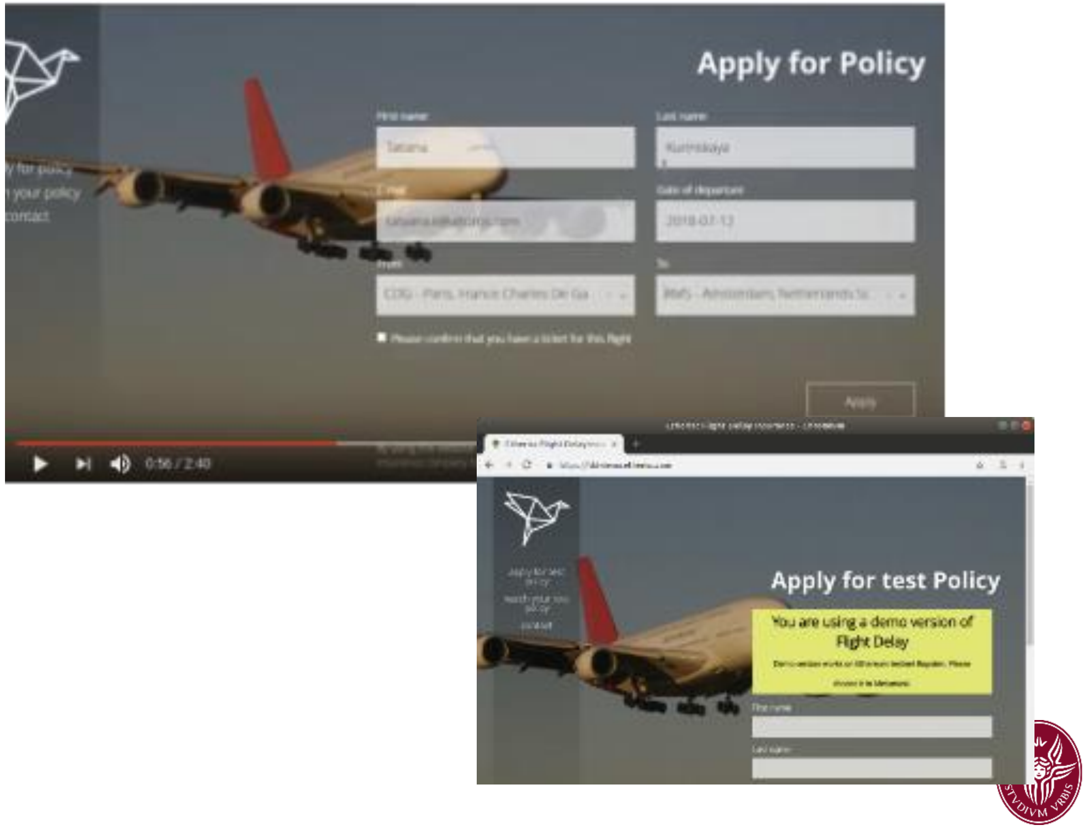
Prototyped

Social Insurance

Affordable, accessible protection against risk of death or heavy illness of a community member. Immediate emergency payment which helps to get through critical times.

Prototyped

Support



Apply for Policy

First name: Tatiana

Last name: Kurnitskaya

Email: [illegible]

Date of departure: 2018-07-13

From: CDG - Paris, France Charles De Ga...

To: AMS - Amsterdam, Netherlands Sc...

□ Please confirm that you have a ticket for this flight

Apply

Apply for test Policy

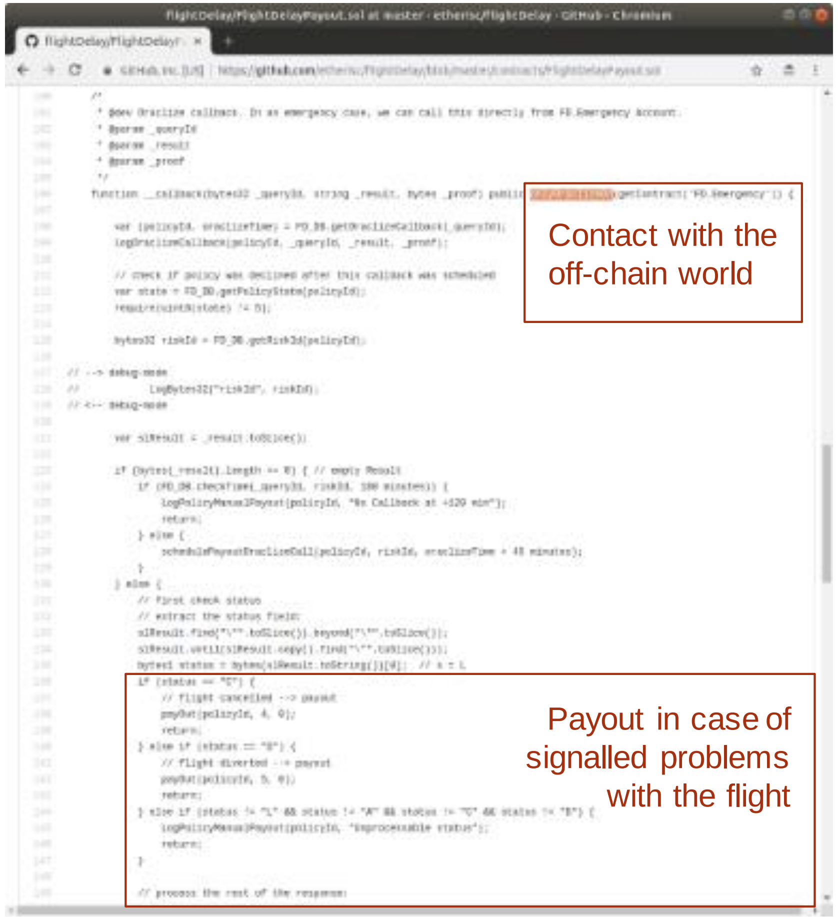
You are using a demo version of Flight Delay

Demo version works on Ethereum testnet Ropsten. Please choose it in Metamask.

First name

Last name

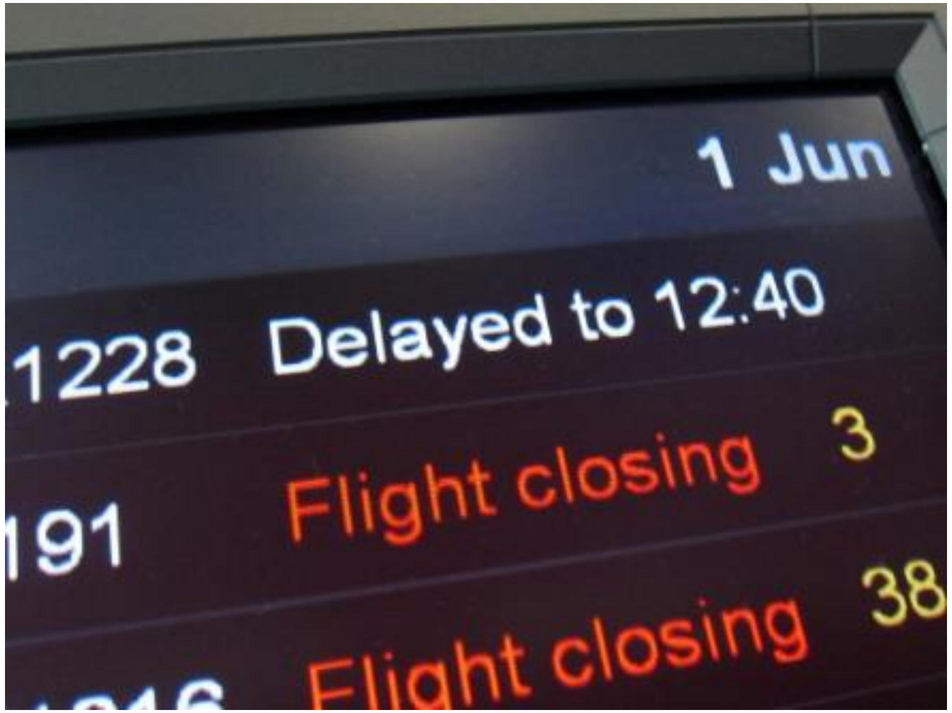
Flight delay insurance:
the FlightDelayPayout contract


FlightDelay/FlightDelayPayout.sol at master · etherisc/flightDelay · GitHub - Chromium
FlightDelay/FlightDelayP ×
GitHub, Inc. [US] | https://github.com/etherisc/flightDelay/blob/master/contracts/FlightDelayPayout.sol

```
    /*
     * @dev Oraclize callback. In an emergency case, we can call this directly from FD.Emergency Account.
     * @param _queryId
     * @param _result
     * @param _proof
     */
    function __callback(bytes32 _queryId, string _result, bytes _proof) public onlyOraclizeOr(getContract('FD.Emergency')) {

        var (policyId, oraclizeTime) = FD_DB.getOraclizeCallback(_queryId);
        LogOraclizeCallback(policyId, _queryId, _result, _proof);

        // check if policy was declined after this callback was scheduled
        var state = FD_DB.getPolicyState(policyId);
        require(uint8(state) != 5);

        bytes32 riskId = FD_DB.getRiskId(policyId);

// --> debug-mode
//            LogBytes32("riskId", riskId);
// <-- debug-mode

        var slResult = _result.toSlice();

        if (bytes(_result).length == 0) { // empty Result
            if (FD_DB.checkTime(_queryId, riskId, 180 minutes)) {
                LogPolicyManualPayout(policyId, "No Callback at +120 min");
                return;
            } else {
                schedulePayoutOraclizeCall(policyId, riskId, oraclizeTime + 45 minutes);
            }
        } else {
            // first check status
            // extract the status field:
            slResult.find("\"".toSlice()).beyond("\"".toSlice());
            slResult.until(slResult.copy().find("\"".toSlice()));
            bytes1 status = bytes(slResult.toString())[0];  // s = L
            if (status == "C") {
                // flight cancelled --> payout
                payOut(policyId, 4, 0);
                return;
            } else if (status == "D") {
                // flight diverted --> payout
                payOut(policyId, 5, 0);
                return;
            } else if (status != "L" && status != "A" && status != "C" && status != "D") {
                LogPolicyManualPayout(policyId, "Unprocessable status");
                return;
            }

            // process the rest of the response:
```

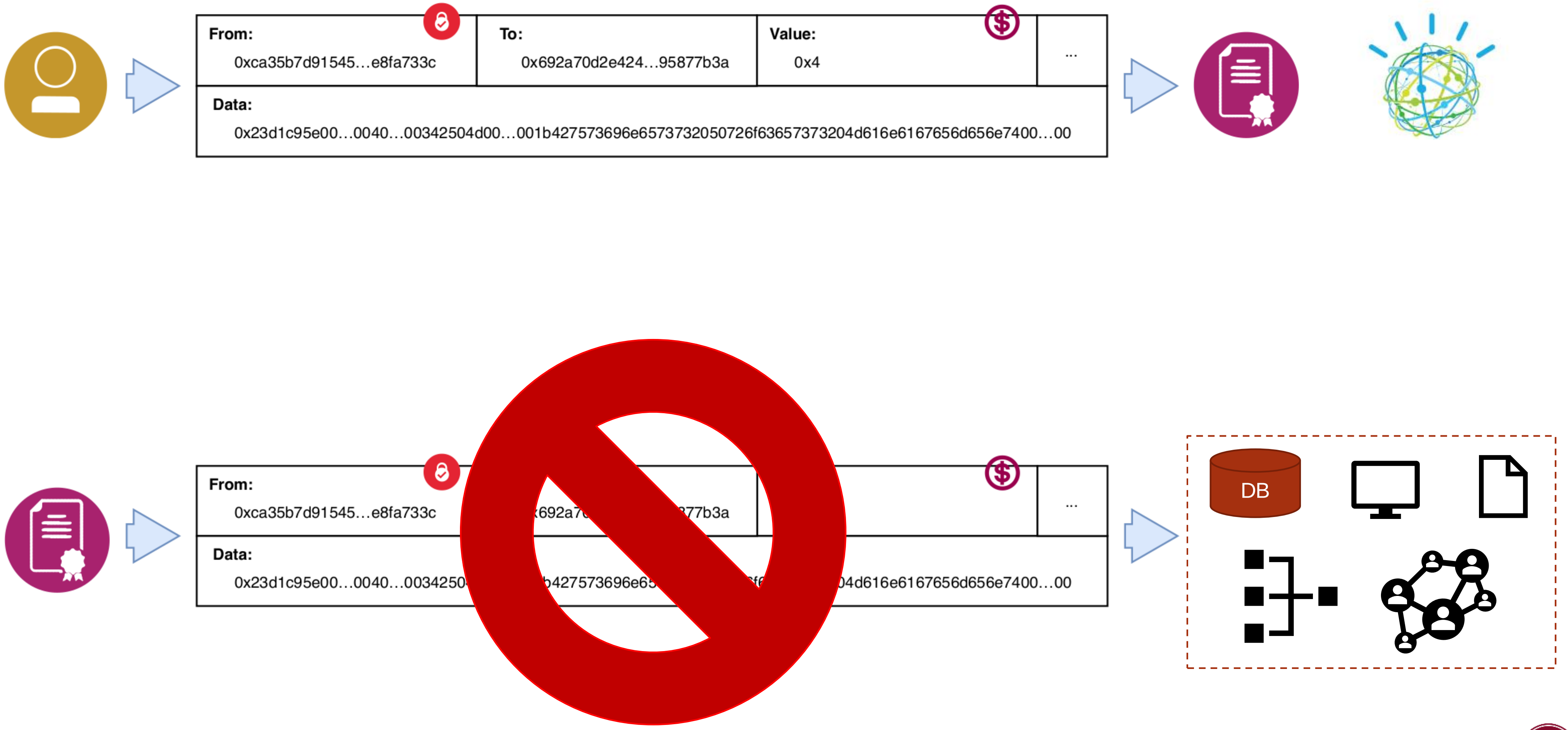
Contact with the off-chain world

Payout in case of signalled problems with the flight



Source: https://www.flickr.com/photos/michaelduxbury/5824469025

The problem



From: 0xca35b7d91545…e8fa733c

To: 0x692a70d2e424…95877b3a

Value: 0x4

…

Data: 0x23d1c95e00…0040…00342504d00…001b427573696e6573732050726f63657373204d616e6167656d656e7400…00

From: 0xca35b7d91545…e8fa733c

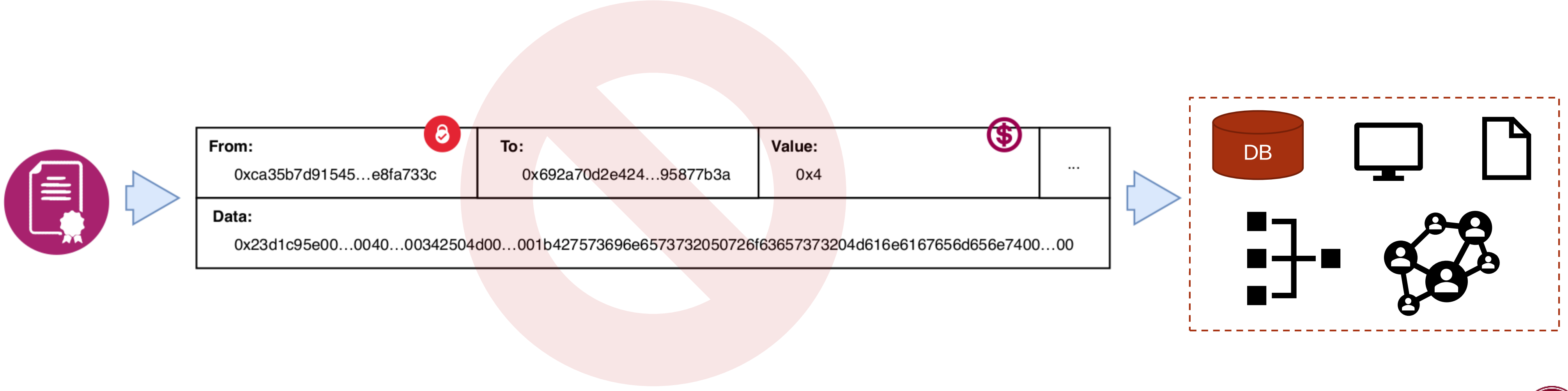
692a7 77b3a

…

Data: 0x23d1c95e00…0040…0034250 b427573696e65 f6 04d616e6167656d656e7400…00

The Oracle

Source: http://matrix.wikia.com/wiki/File:The_Oracle_Making_Cookies.jpg



From:	To:	Value:	...
0xca35b7d91545…e8fa733c	0x692a70d2e424…95877b3a	0x4	

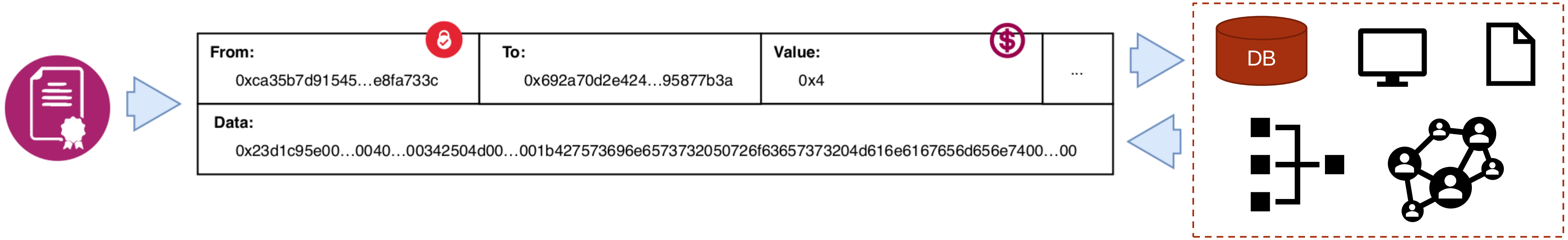
Data:
0x23d1c95e00…0040…00342504d00…001b427573696e657373205072 6f63657373204d616e6167656d656e7400…00

The Oracle

ISO/TC 307, ISO/TR 2345: “[A] **DLT Oracle** [is a] **service** that updates a distributed ledger using **data from outside** the distributed ledger system”. (2019)

Previous literature: oracles as off-chain information providers.

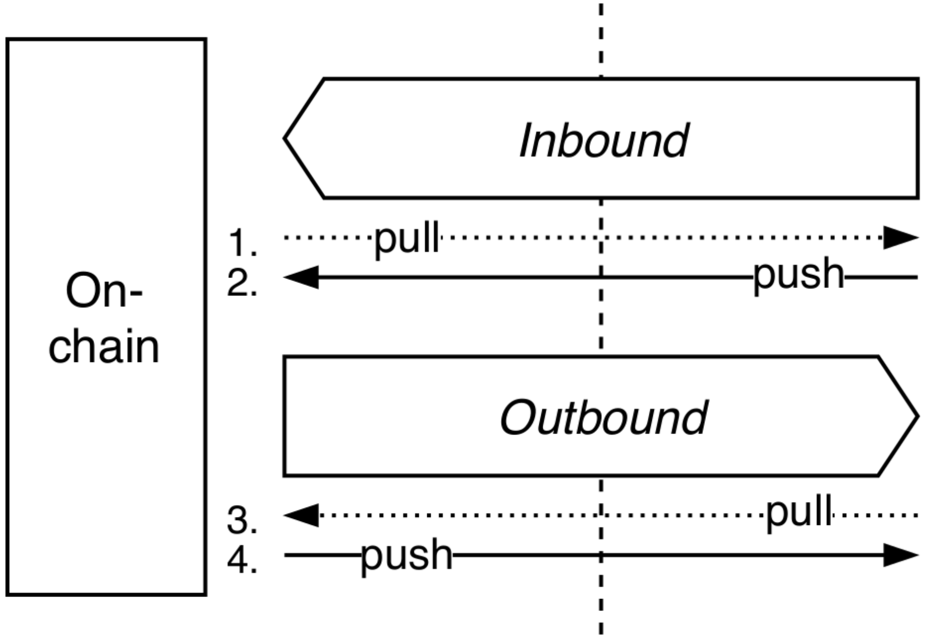
We see **oracles** as a **bridge**
between the on-chain and off-chain worlds.



From: 0xca35b7d91545…e8fa733c	**To:** 0x692a70d2e424…95877b3a	**Value:** 0x4	…
Data: 0x23d1c95e00…0040…00342504d00…001b427573696e657373205072 6f63657373204d616e6167656d656e7400…00			

Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World. BPM (Blockchain and RPA Forum) 2020: 35-51

Oracle patterns: Overview



1. Pull-based Inbound
2. Push-based Inbound
3. Pull-based Outbound
4. Push-based Outbound

⇨ Data flow
┈► Pull strategy
─► Push strategy

Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World. BPM (Blockchain and RPA Forum) 2020: 35-51