Blockchain architectures

An introduction

Utrecht University

Claudio Di Ciccio

c.diciccio@uu.nl
https://www.uu.nl/staff/CdiCiccio

Agenda for today

09:00 - 10:00:
Transactions, ledgers, DLTs and blockchains

10:15 - 11:15:
Double spending, cryptocurrencies, smart contracts

11:30 - 12:00:
Tokens vs cryptocurrencies, public/private and permissionless/permissioned blockchain systems

12:00 - 12:45:
Lab and homework assignment

Kudos to Jan Martijn for the picture

What is a Blockchain?

- "Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World"
  - (title of a book)

Blockchain: The Invisible Technology That's Changing the World

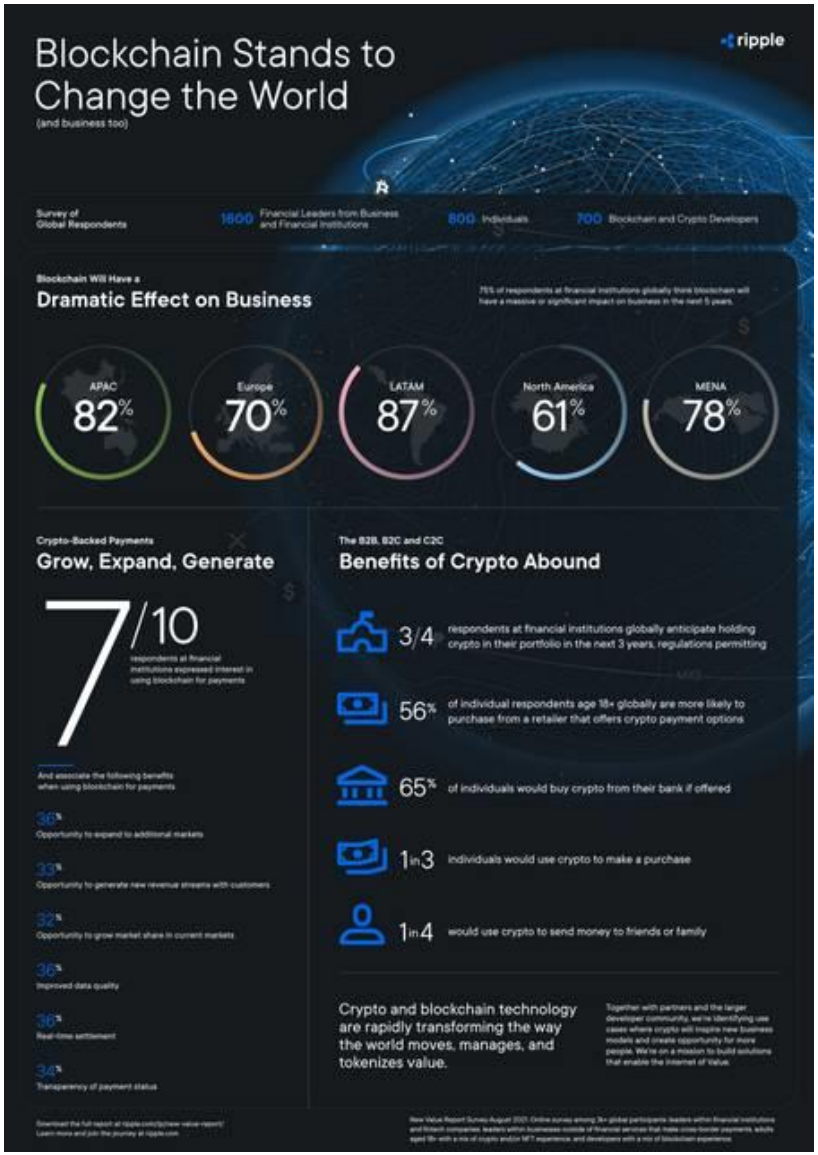
Blockchain-based networks, decentralized apps (DApps), and distributed ledgers are becoming the foundation of much of your digital life. There's a new immutable digital fabric remaking the internet beneath us, and you probably don't even realize it.

By Rob Marvin August 29, 2017 1:38PM EST

4.4K SHARES

https://www.pcmag.com/article/351486/blockchain-the-invisible-technology-thats-changing-the-wor

The fuzz is not over!



Blockchain: The Invisible Technology That's Changing the World

Blockchain-based networks, decentralized apps (DApps), and distributed ledgers are becoming the foundation of much of your digital life. There's a new immutable digital fabric remaking the internet beneath us, and you probably don't even realize it.

By Rob Marvin August 29, 2017 1:38PM EST

4.4K SHARES

https://ripple.com/insights/blockchain-stands-to-change-the-world/ (June 2022)

OK OK… what is a Blockchain?

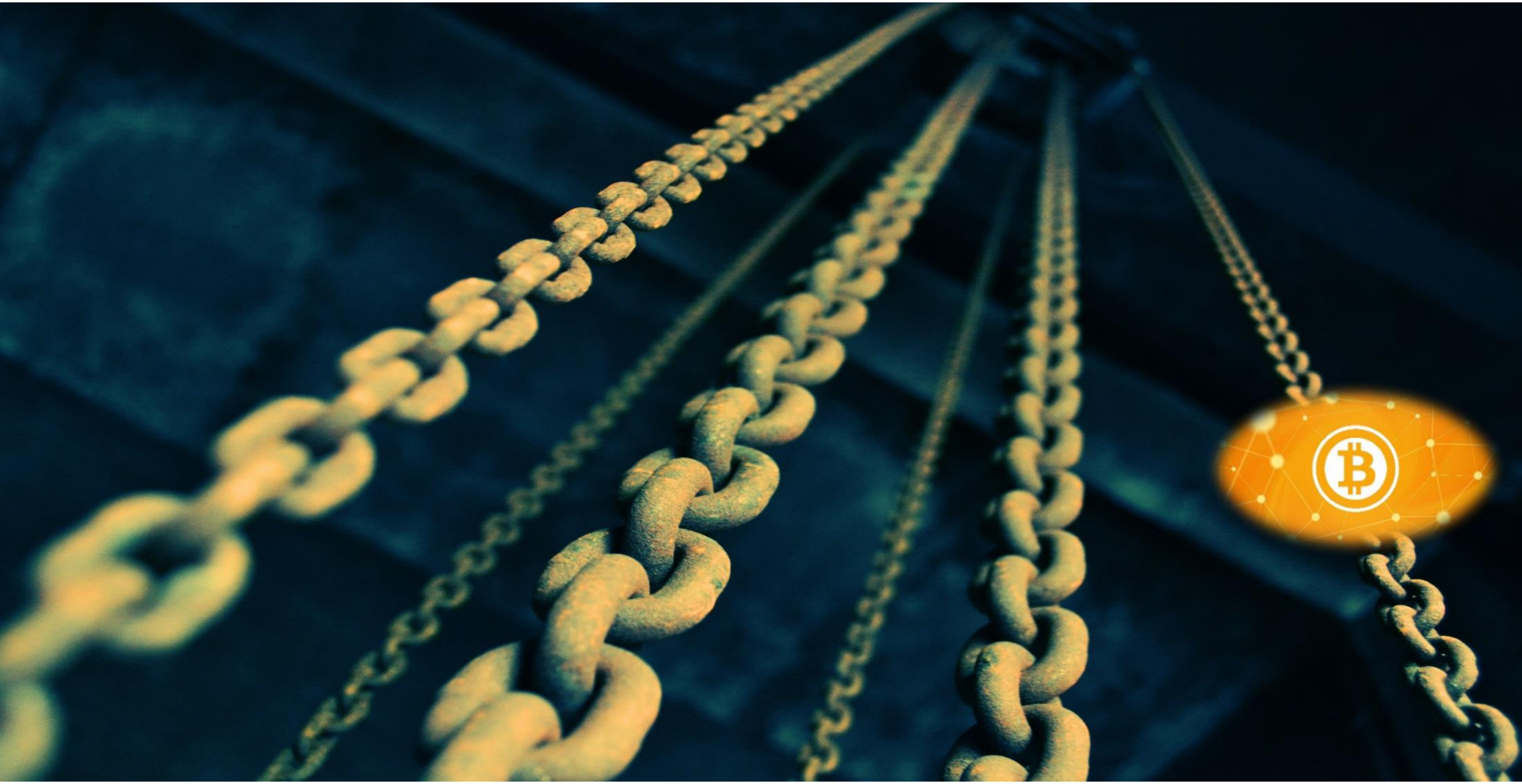
- *"Blockchain is an open, distributed ledger that can record transactions between two parties efficiently* and in a verifiable and permanent* way"*

[M. Iansiti, K. R. Lakhani: *The Truth about Blockchain*. Harvard Business Review 95, no. 1. 2017]

- **Transactions are immutable***
- A **copy** of the blockchain is accessible to **every node** on the network
  - It offers access to the history of all previous states
- **Consensus** is achieved through dedicated algorithms
  - Economic disincentive to history rewriting
- Offers the possibility of executing user-defined scripts (**smart contracts**)
  - Smart contracts are unstoppable from the outside

- * Now and in the rest of the course: asterisks mark words/sentences that are valid in most of the cases, but have exceptions

Blockchain is more than Bitcoin



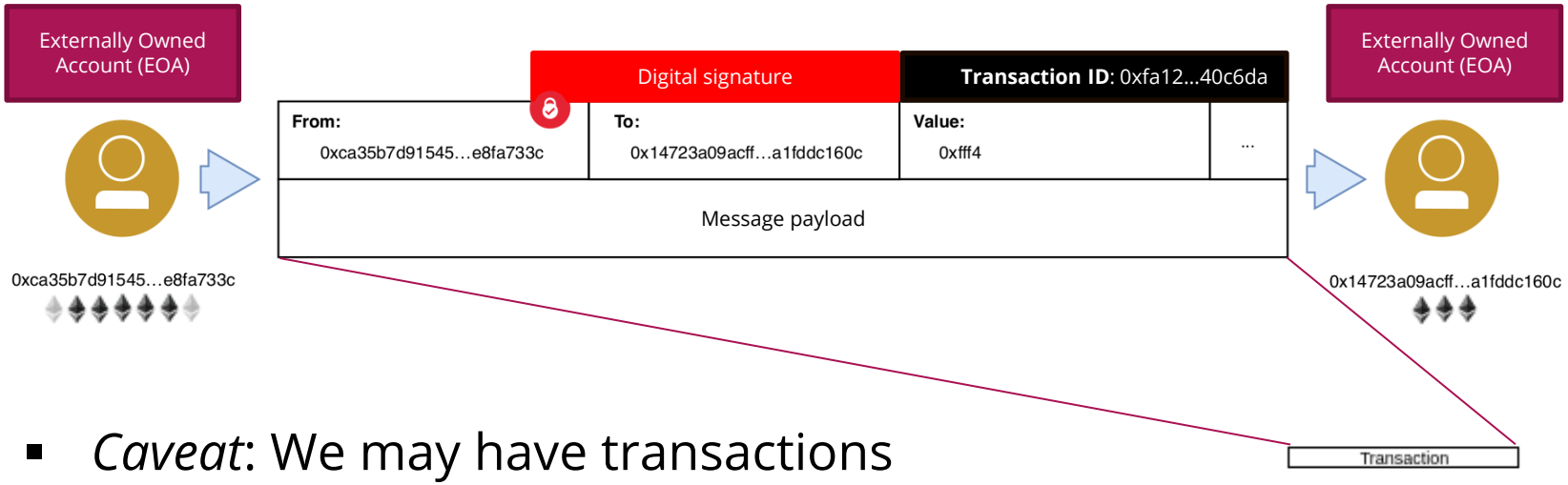
Utrecht University

The Blockchain in a few slides

[redacted]

Transaction

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



- *Caveat*: We may have transactions from account A to accounts B, C and A itself or from account A to an unspecified/non-existing/burning-bin accounts

Metaphor: the cheque

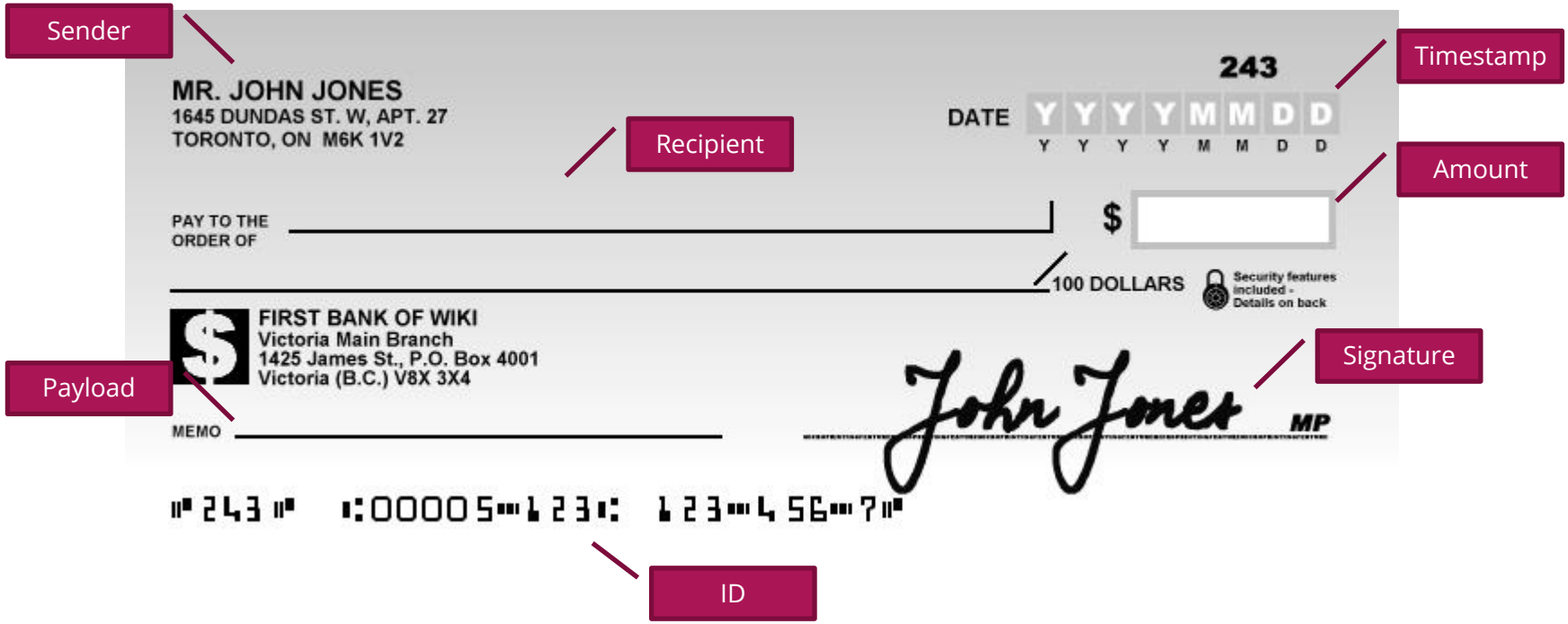
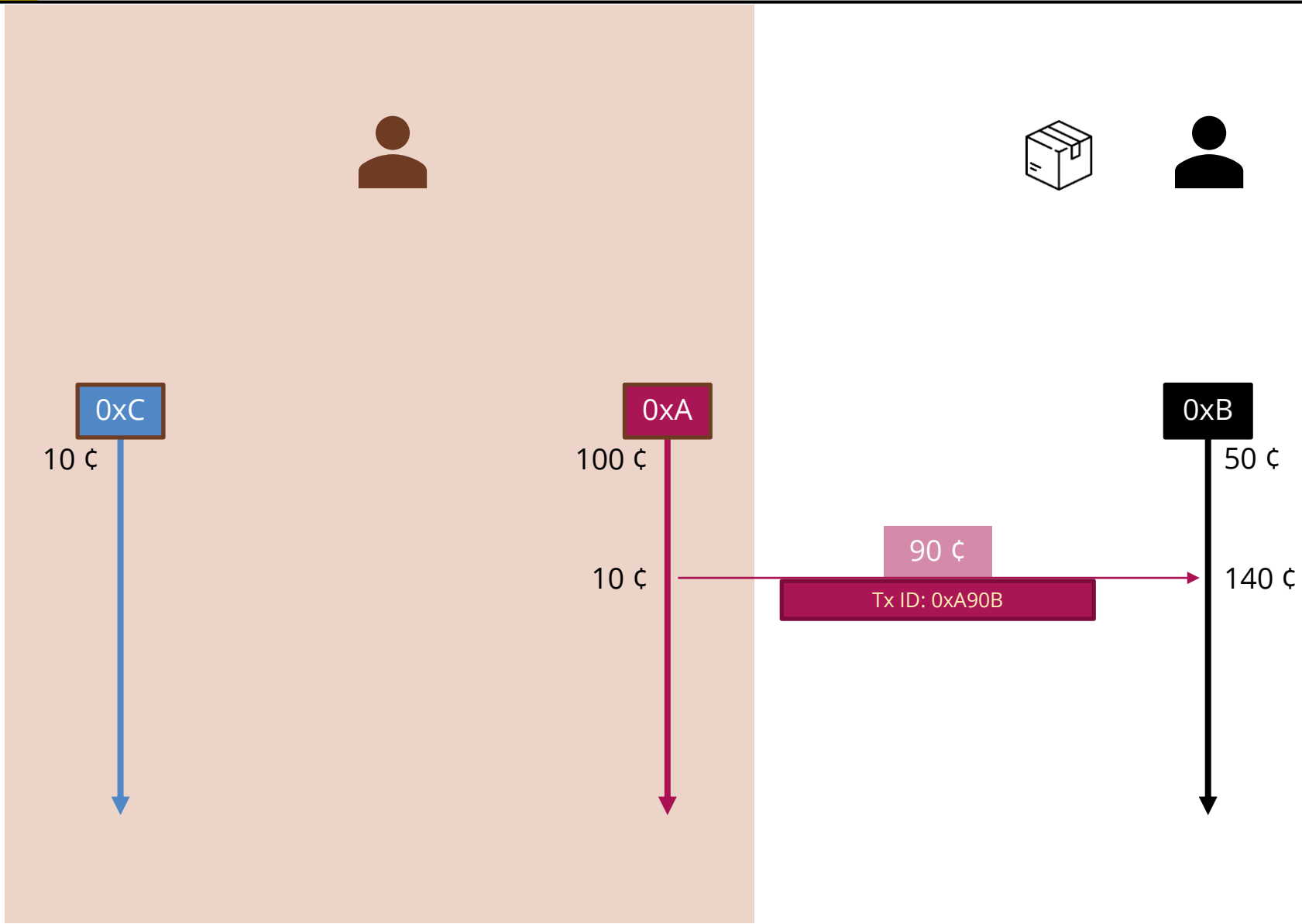


Image by Airodyssey, https://en.wikipedia.org/wiki/File:BlankCheque.png

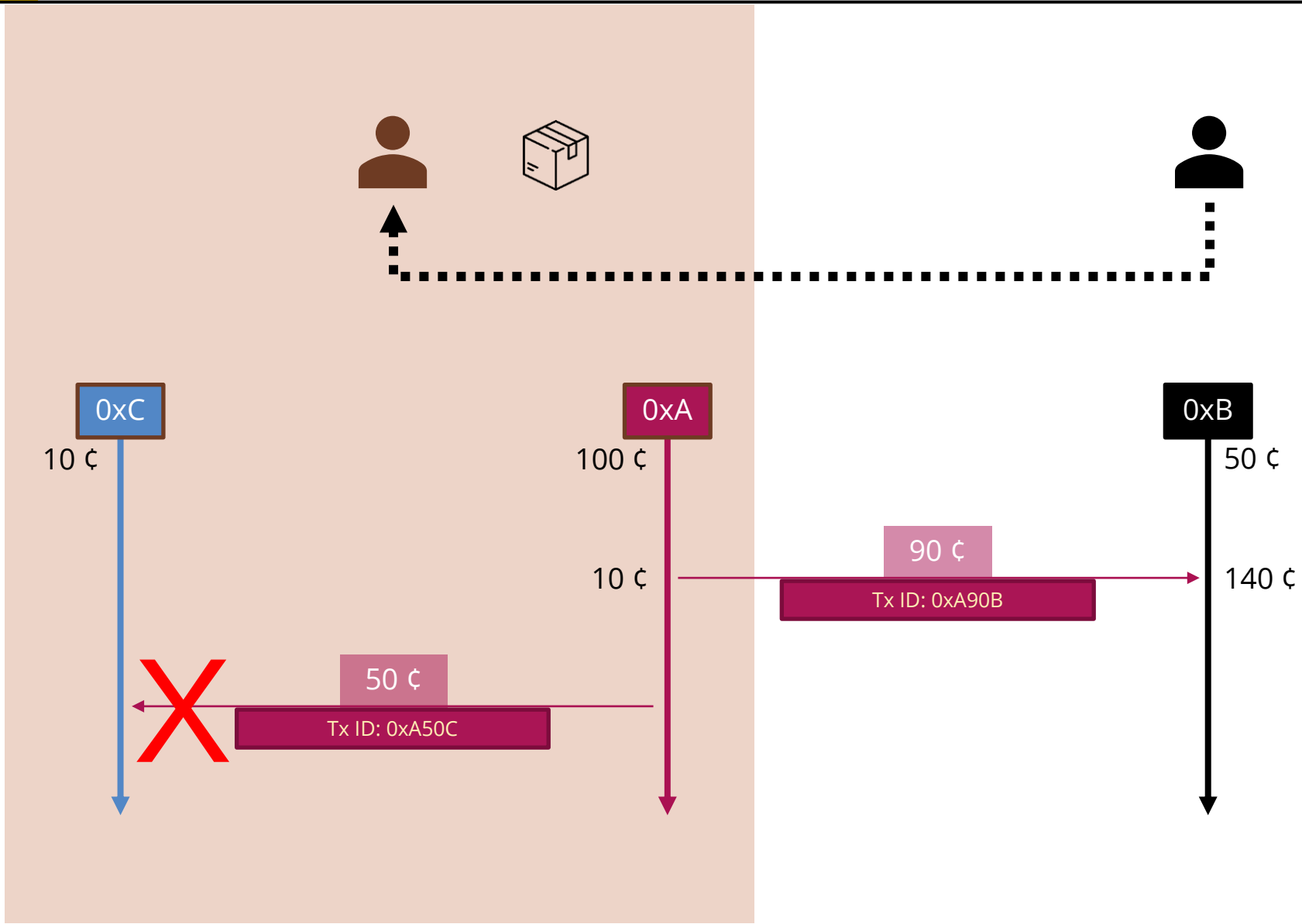
Ledger

- Ordered collection of transactions
- The order matters!

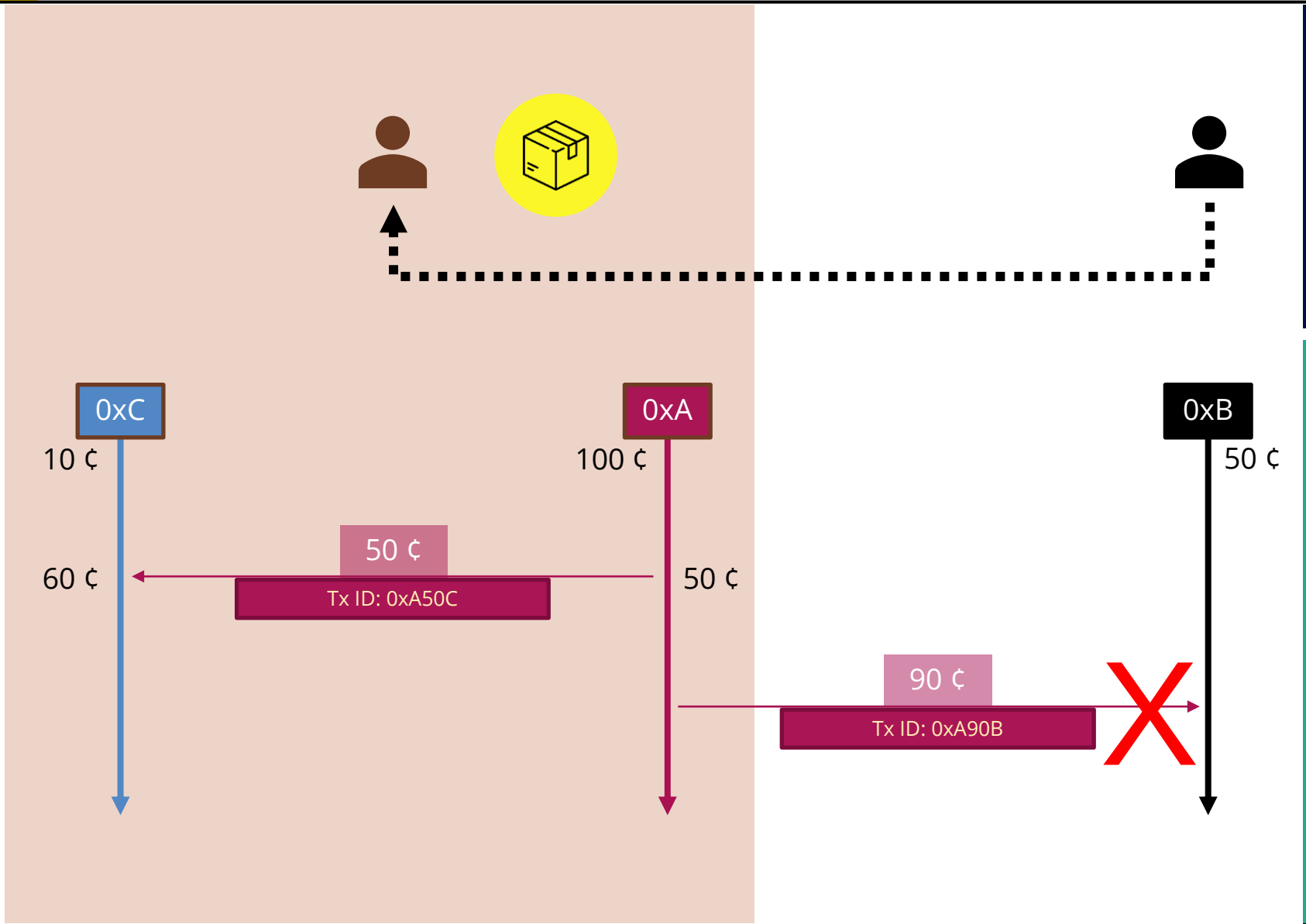
Double spending



Double spending

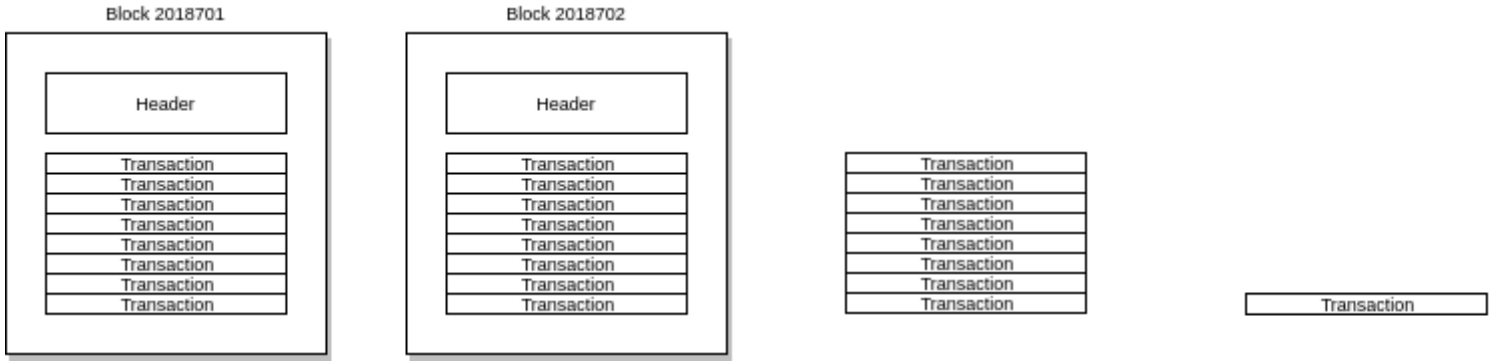


Double spending



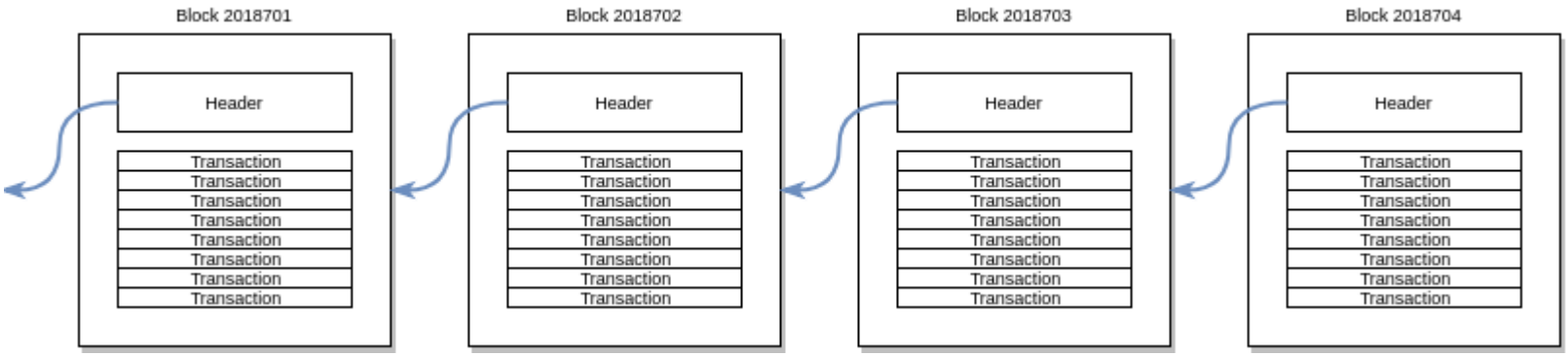
Block

- Blocks group and collate transactions
- The order matters!



Blockchain

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



The blockchain remembers

Ganache

ACCOUNTS | BLOCKS | TRANSACTIONS | LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

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	FROM ADDRESS	TO CONTRACT ADDRESS / CREATED CONTRACT ADDRESS	GAS USED	VALUE	
0×f57aa7510057deeafb819d3344fcb0a64223f5315deba3eb6c5611840785a0a0	0×13eE11549ABB691dc8D1A9c2C91D4d18e5585ea5	0×1b11784caBd4AD927297D34D184818a9Ca5F7AA0	33268	0	CONTRACT CALL
0×0e49756cc927acddb6785e0a69681e3937ff81f4c9b66796b11b91330bb4638b	0×d1D993d57EC011b8dbFF0daCE6705e91a24423DF	0×aF519f7A866DC3892FBE165c3d0d7b7aFE3520E2	163943	0	CONTRACT CREATION
0×686b75ba543fc4f41a3132ab19f53d839468c8aa07f16574043b1023a5bb57dc	0×13eE11549ABB691dc8D1A9c2C91D4d18e5585ea5	0×1b11784caBd4AD927297D34D184818a9Ca5F7AA0	33460	0	CONTRACT CALL
0×95a7bbe02592c3a5686d9ef44f46f65a7c1fa96999f54890d56ac74c83897ca9	0×13eE11549ABB691dc8D1A9c2C91D4d18e5585ea5	0×1b11784caBd4AD927297D34D184818a9Ca5F7AA0	33268	0	CONTRACT CALL
0×6b9ab176fb62aae21ad7a1f767830f6c44f867da50bfcbafc7ab6b6288c766d9	0×13eE11549ABB691dc8D1A9c2C91D4d18e5585ea5	0×1b11784caBd4AD927297D34D184818a9Ca5F7AA0	33396	0	CONTRACT CALL
0×a9e79b1d6370981f00f58ce58b25369be15d96815262f78a06be7af299691477					CONTRACT CALL

Shortcomings of centralised ledgers

- Potentially
  - lost or destroyed
  - containing invalid transactions
  - incomplete
  - altered

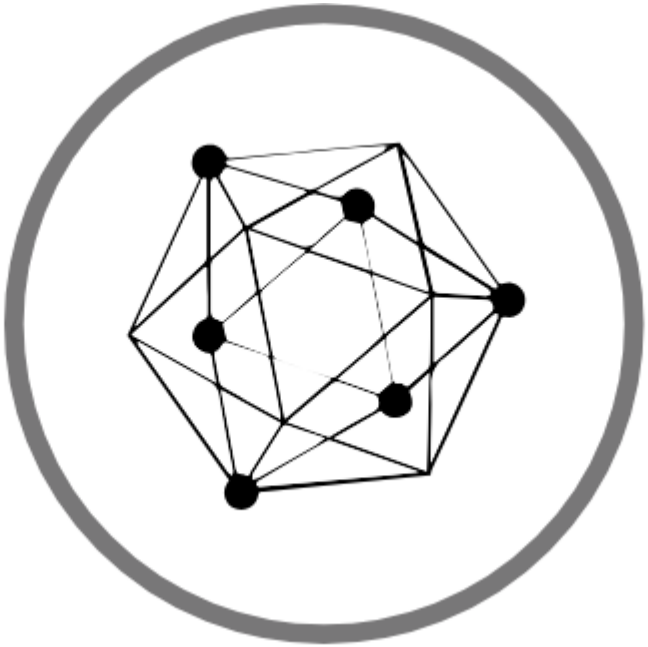
About decentralisation

Centralisation	Decentralisation

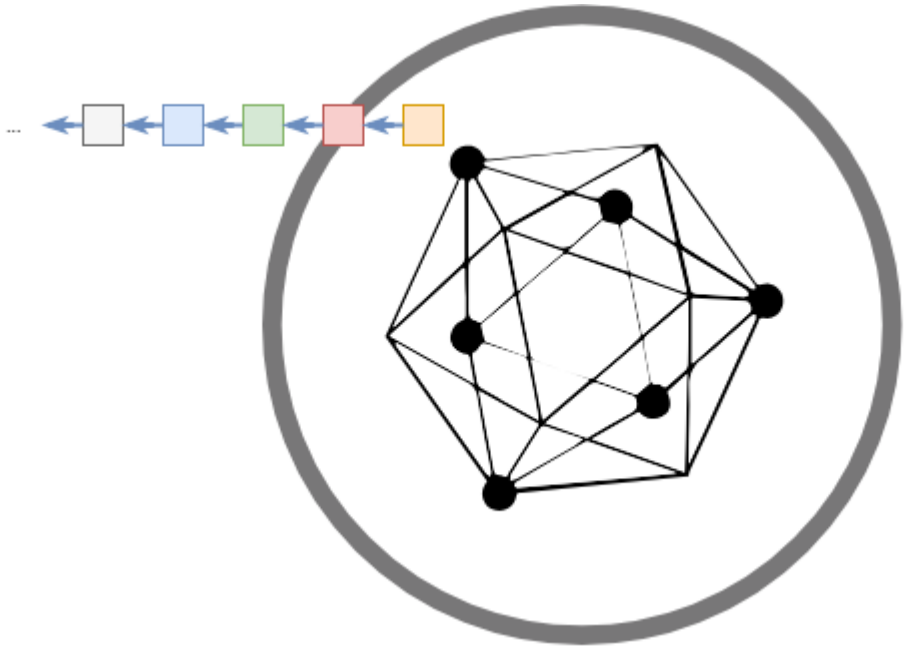
Distributing the ledger makes for permanence BUT entails no notion of unique distributed clock

Warning: possible information inconsistency → proof-of-* and consensus

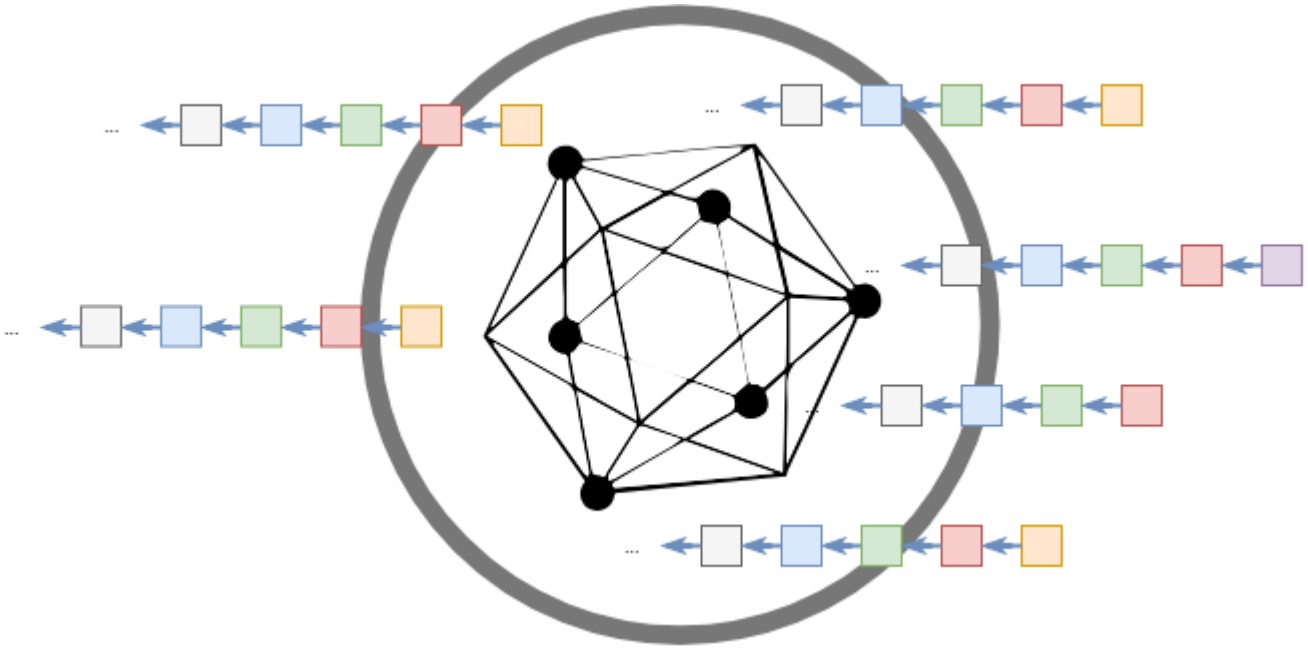
Distributed nature



Distributed nature



Distributed nature



Who can read what is stored on chain?

- In principle: everyone!
  - Mind what you write on transaction payloads!

What about confidentiality?

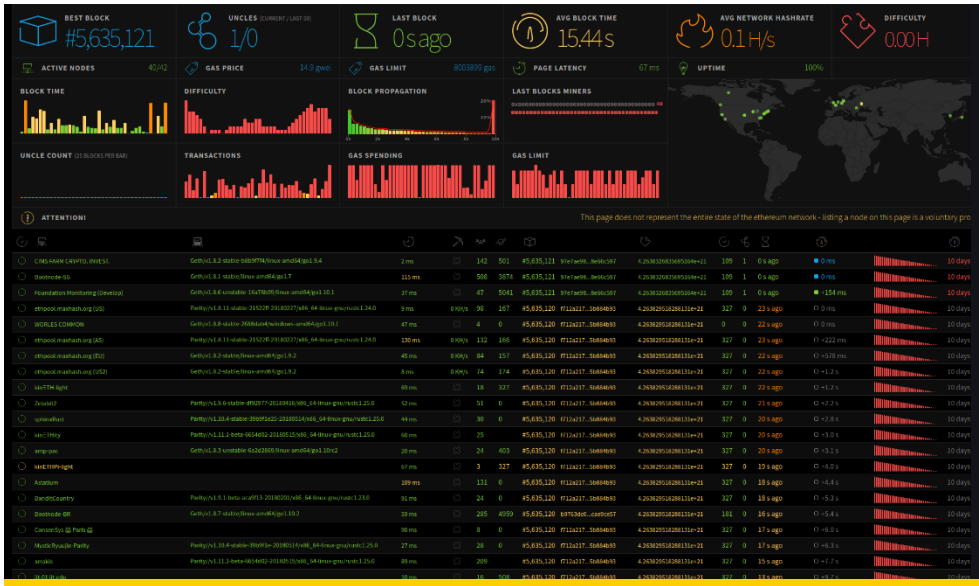
Scene from The Truman Show (1998). Image source: https://redeemingculture.com/film/drama/4106-the-truman-show-empathy-and-reality

Mind the difference between a node, an account, and a user!

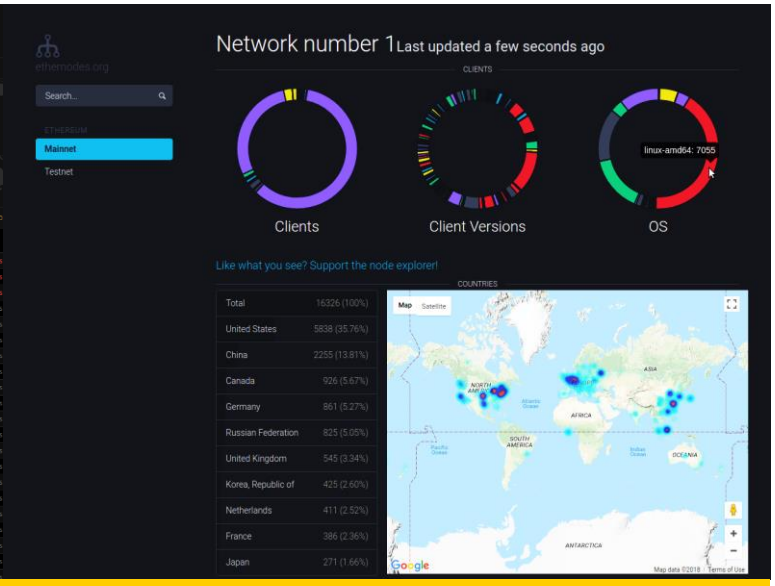
Node	Account	User
Keeps the infrastructure, executes the protocol	Has a balance, issues and receives transactions	Owns account(s), signs transactions

Keep this distinction in mind when designing your software architecture!

Ledgers are distributed and maintained by a network



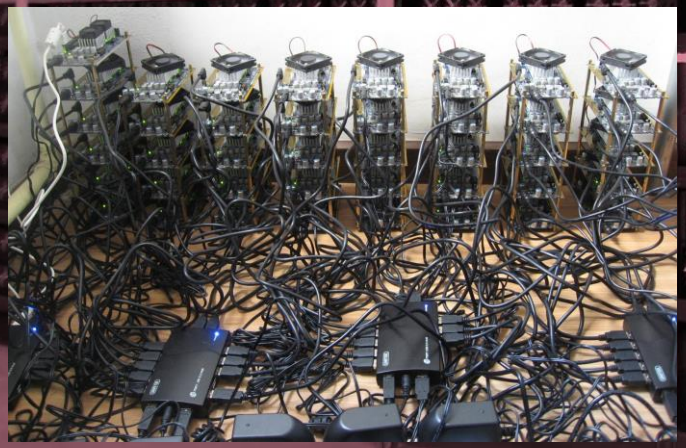
https://ehtstats.net



https://ehternodes.org

Maintaining the infrastructure has a price

- **Proof of Work** (PoW): obtain 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**.
- Some sort of incentive must be provided!



Crypto-fuel needed!

Market capitalisation of cryptocurrencies

Cryptocurrencies | Categories | Telegram Bot | Base Ecosystem | FTX Bankruptcy Estate | Real World Assets | Show rows 100 | Filters | Customize

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$26,210.08	-0.01%	0.11%	-3.21%	$511,002,576,069	$10,187,930,150 388,511 BTC	19,496,412 BTC	
2	Ethereum ETH	$1,585.73	-0.11%	0.58%	-3.45%	$190,655,666,415	$3,754,936,868 2,365,939 ETH	120,232,366 ETH	
3	Tether USDt USDT	$1.00	-0.00%	0.04%	-0.04%	$83,219,064,445	$17,113,469,523 17,114,401,096 USDT	83,207,883,381 USDT	
4	BNB BNB	$211.92	-0.13%	1.51%	-2.61%	$32,603,361,687	$602,689,523 2,841,922 BNB	153,847,152 BNB	
5	XRP XRP	$0.5017	0.25%	0.87%	-1.48%	$26,713,127,252	$774,759,332 1,544,414,676 XRP	53,245,240,268 XRP	
6	USDC USDC	$1.00	0.02%	0.03%	-0.00%	$25,646,475,609	$2,625,643,138 2,624,892,271 USDC	25,637,513,324 USDC	
7	Cardano ADA	$0.2458	0.03%	0.65%	-3.83%	$8,632,174,909	$112,908,596 459,404,416 ADA	35,124,390,151 ADA	
8	Dogecoin DOGE	$0.06068	-0.11%	-0.21%	-3.20%	$8,565,328,813	$100,194,848 1,650,154,540 DOGE	141,164,916,384 DOGE	
9	Solana SOL	$19.29	-0.10%	-1.27%	-3.45%	$7,966,359,212	$155,247,953 8,039,295 SOL	412,877,419 SOL	
10	TRON TRX	$0.08468	-0.20%	0.56%	0.47%	$7,545,610,040	$145,864,939 1,721,446,774 TRX	89,109,993,499 TRX	
11	Toncoin TON	$2.17	-0.27%	-0.49%	-12.60%	$7,441,203,779	$28,882,024 13,289,182 TON	3,431,892,088 TON	
12	Dai DAI	$0.9999	0.01%	-0.03%	0.05%	$5,347,466,014	$96,301,749 96,302,194 DAI	5,347,888,596 DAI	

Source: https://coinmarketcap.com/ (accessed: 2023-09-26)

Smart Contracts are ~~codified autonomous agents~~ pieces of code[1]

```
// SPDX-License-Identifier: CC-BY-SA-4.0
pragma solidity >=0.8.0 <0.9.0;

contract HelloToken {
    address public minter;  // The creator of the contract instance
    mapping (address => uint) public balances;  // The balances in Hello-Tokens
    uint public constant PRICE = 2000000000;  // The price of a Hello Token (2 Gwei)

    constructor() {  // Deploys new instances of the smart contract
        minter = msg.sender;  // The sender is the creator
    }

    function mint() public payable {
        // Request the minimum amount for a Hello Token, or terminate
        require(msg.value >= PRICE, "Not enough value for a token!");
        // Add new Hello Tokens to the balance of the sender
        balances[msg.sender] += msg.value / PRICE;
        // The value of the transaction is acquired by the Smart Contract account
    }

    function transfer(uint amount, address to) public {
        require(balances[msg.sender] >= amount, "Not enough tokens!");
        // Decrese the amount from the sender
        balances[msg.sender] -= amount;
        // Increase the amount of Hello Tokens to a specified address
        balances[to] += amount;
    }

    function terminate() public {
        // Only the contract creator can terminate this instance
        require(msg.sender == minter, "You cannot terminate the contract!");
        // Terminate the contract instance and transfer the balance amount to the creator
        selfdestruct(payable(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**

[1] Thanks to Prof Alexander Norta for the hint

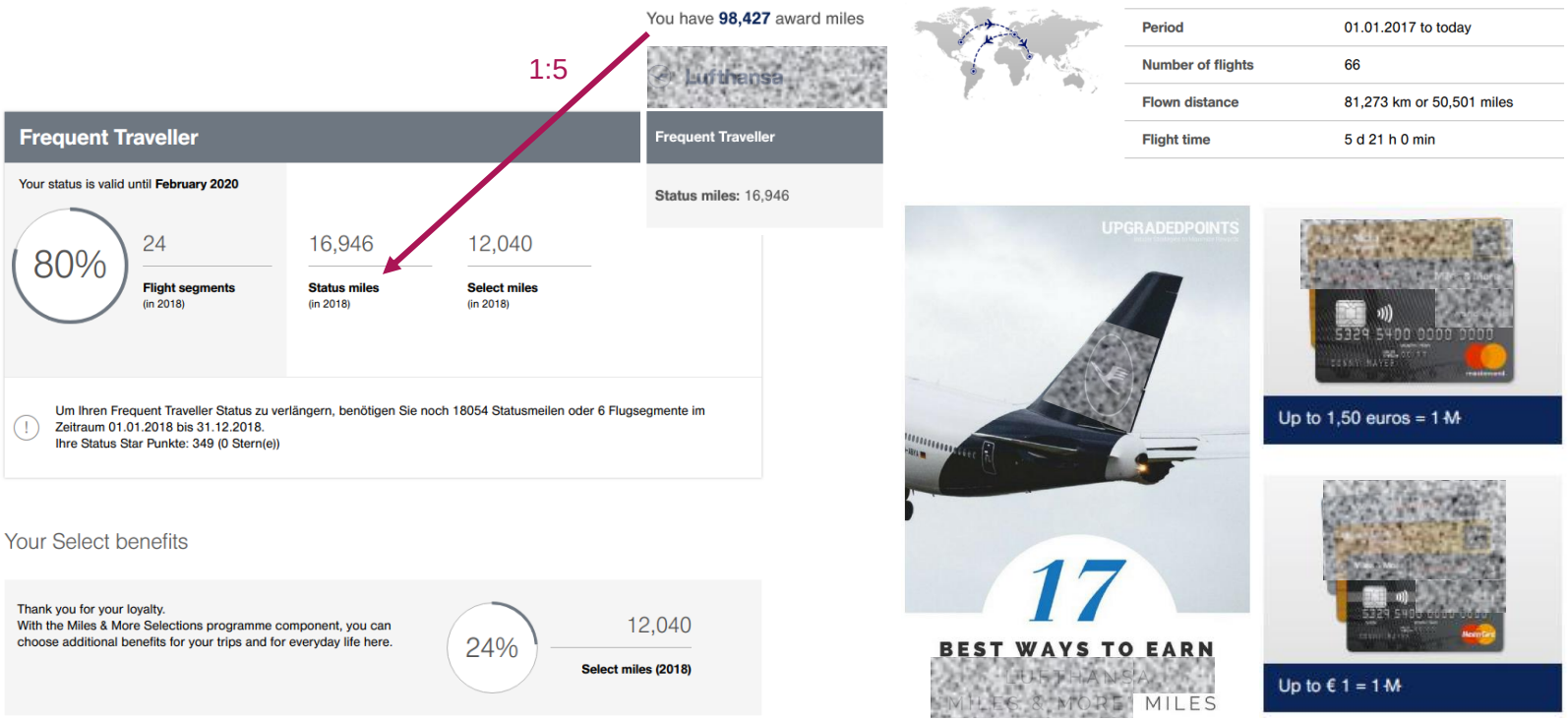
From high-level code to bytecode to bits and bytes

```solidity
// SPDX-License-Identifier: CC-BY-SA-4.0
pragma solidity >=0.8.0 <0.9.0;

contract HelloToken {
    address public minter;  // The creator of the contract instance
    mapping (address => uint) public balances;  // The balances in Hello-Tokens
    uint public constant PRICE = 2000000000;  // The price of a Hello Token (2 Gwei)

    constructor() {  // Deploys new instances of the smart contract
        minter = msg.sender;  // The sender is the creator
    }

    function mint() public payable {
        // Request the minimum amount for a Hello Token, or terminate
        require(msg.value >= PRICE, "Not enough value for a token!");
        // Add new Hello Tokens to the balance of the sender
        balances[msg.sender] += msg.value / PRICE;
        // The value of the transaction is acquired by the Smart Contract account
    }

    function transfer(uint amount, address to) public {
        require(balances[msg.sender] >= amount, "Not enough tokens!");
        // Decrease the amount from the sender
        balances[msg.sender] -= amount;
        // Increase the amount of Hello Tokens to a specified address
        balances[to] += amount;
    }

    function terminate() public {
        // Only the contract creator can terminate this instance
        require(msg.sender == minter, "You cannot terminate the contract!");
        // Terminate the contract instance and transfer the balance amount to the creator
        selfdestruct(payable(minter));
    }
}
```

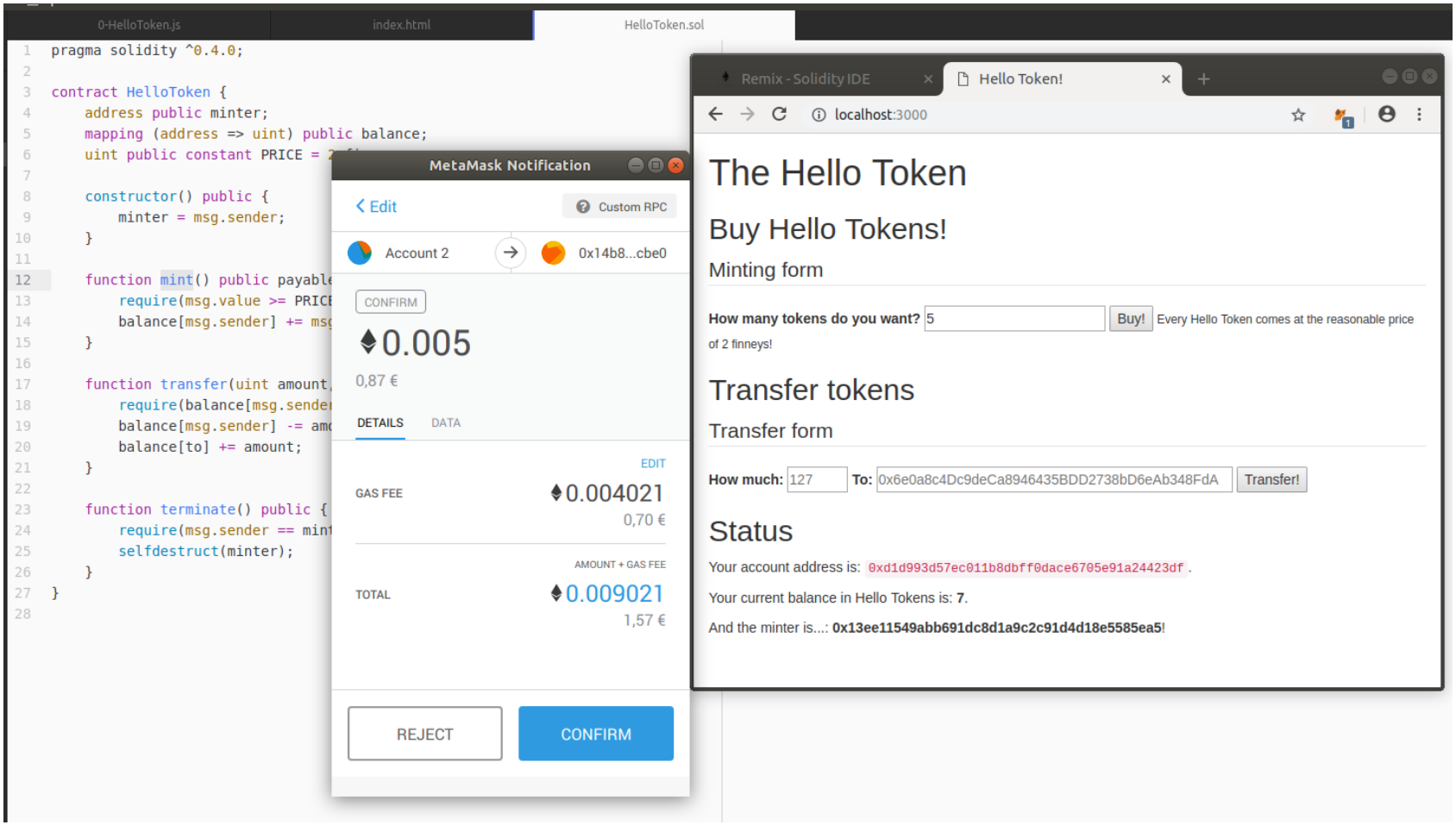
```
tag 33        function transfer(uint amount,...
  JUMPDEST        function transfer(uint amount,...
  DUP2      amount
  PUSH 1      balances
  PUSH 0      balances[msg.sender]
  CALLER      msg.sender
  PUSH FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  AND       balances[msg.sender]
  PUSH FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  AND       balances[msg.sender]
  DUP2      balances[msg.sender]
  MSTORE      balances[msg.sender]
  PUSH 20      balances[msg.sender]
  ADD       balances[msg.sender]
  SWAP1      balances[msg.sender]
  DUP2      balances[msg.sender]
  MSTORE      balances[msg.sender]
  PUSH 20      balances[msg.sender]
  ADD       balances[msg.sender]
  PUSH 0      balances[msg.sender]
  KECCAK256       balances[msg.sender]
  SLOAD      balances[msg.sender]
  LT     balances[msg.sender] >= amount
  ISZERO      balances[msg.sender] >= amount
  PUSH [tag] 47     require(balances[msg.sender] >.
  JUMPI      require(balances[msg.sender] >...
  PUSH 40      require(balances[msg.sender] >...
  MLOAD      require(balances[msg.sender] >...
  PUSH 8C379A000000000000000000000000000000000000000
  DUP2      require(balances[msg.sender] >...
  MSTORE      require(balances[msg.sender] >...
  PUSH 4      require(balances[msg.sender] >...
  ADD       require(balances[msg.sender] >...
  PUSH [tag] 48     require(balances[msg.sender] >..
  SWAP1      require(balances[msg.sender] >...
  PUSH [tag] 49     require(balances[msg.sender] >..
  JUMP [in]     require(balances[msg.sender] >...
```

```
tag 48      require(balances[msg.sender] >...
  JUMPDEST      require(balances[msg.sender] >...
  PUSH 40      require(balances[msg.sender] >...
  MLOAD      require(balances[msg.sender] >...
  DUP1      require(balances[msg.sender] >...
  SWAP2      require(balances[msg.sender] >...
  SUB       require(balances[msg.sender] >...
  SWAP1      require(balances[msg.sender] >...
  REVERT      require(balances[msg.sender] >...
tag 47      require(balances[msg.sender] >...
  JUMPDEST      require(balances[msg.sender] >...
  DUP2      amount
  PUSH 1      balances
  PUSH 0      balances[msg.sender]
  CALLER      msg.sender
  PUSH FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  AND       balances[msg.sender]
  PUSH FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  AND       balances[msg.sender]
  DUP2      balances[msg.sender]
  MSTORE      balances[msg.sender]
  PUSH 20      balances[msg.sender]
  ADD       balances[msg.sender]
  SWAP1      balances[msg.sender]
  DUP2      balances[msg.sender]
  MSTORE      balances[msg.sender]
  PUSH 20      balances[msg.sender]
  ADD       balances[msg.sender]
  PUSH 0      balances[msg.sender]
  KECCAK256       balances[msg.sender]
  PUSH 0      balances[msg.sender]
  DUP3      balances[msg.sender] -= amount
  DUP3      balances[msg.sender] -= amount
  SLOAD      balances[msg.sender] -= amount
  PUSH [tag] 50     balances[msg.sender] -= amount
  SWAP2      balances[msg.sender] -= amount
  SWAP1      balances[msg.sender] -= amount
```

Tokens are neither cryptofuel nor anything conceptually new, after all!



Your brand new token in 5 minutes or less



Tokens tokens tokens tokens

Private|public / Permissioned|permissionless

Transactability / visibility

Consensus

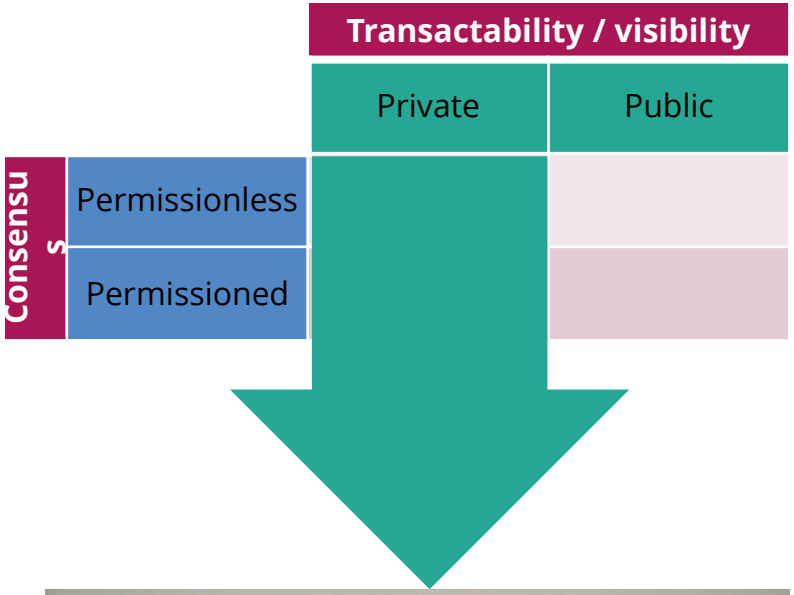
Anderberg et al. “Blockchain Now And Tomorrow” (2019) http://dx.doi.org/10.2760/901029;
Image sources (top-left to bottom-left, clockwise): https://www.ltonetwork.com/; https://ethereum.org/; https://eos.io/; https://www.hyperledger.org/projects/fabric

Private|public / Permissioned|permissionless

		Transactability / visibility	
		Private	Public
Consensus	Permissionless	**Selected** nodes can transact and view, **all** nodes can participate in consensus	**Every** node can transact and view, participate in consensus
	Permissioned	**Selected** nodes can transact and view, or participate in consensus	**Every** node can transact and view, **selected** nodes participate in consensus

Anderberg et al. "Blockchain Now And Tomorrow" (2019) http://dx.doi.org/10.2760/901029;
Image sources (top-left to bottom-left, clockwise): https://www.ltonetwork.com/; https://ethereum.org/; https://eos.io/; https://www.hyperledger.org/projects/fabric

Does every crypto an exchange value in fiat currencies?



Fees and gas expenditure have a market quotation in fiat money if we consider public platforms

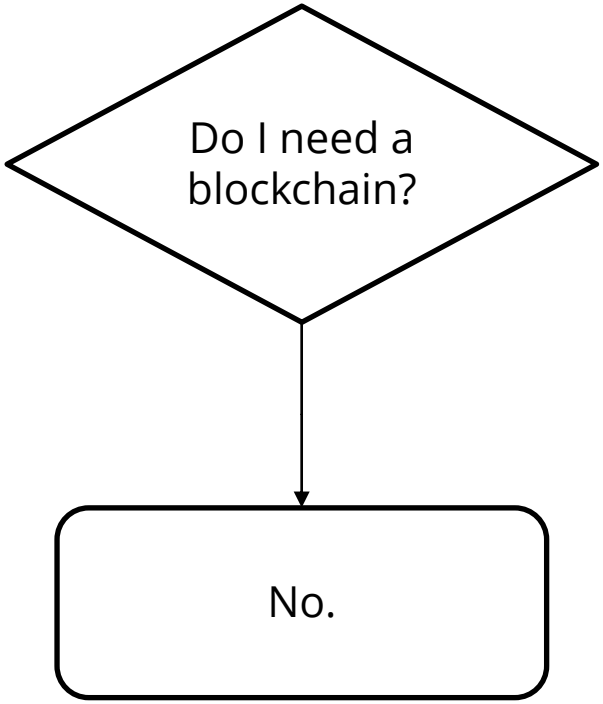
Photo: Monopoly | Close up photo of Monopoly money by Steve Berry CC BY-NC-SA (https://www.flickr.com/photos/unloveable/2400877902)

Utrecht University

Do I need a blockchain?

I mean, really

Do I need a blockchain? (Birch model)

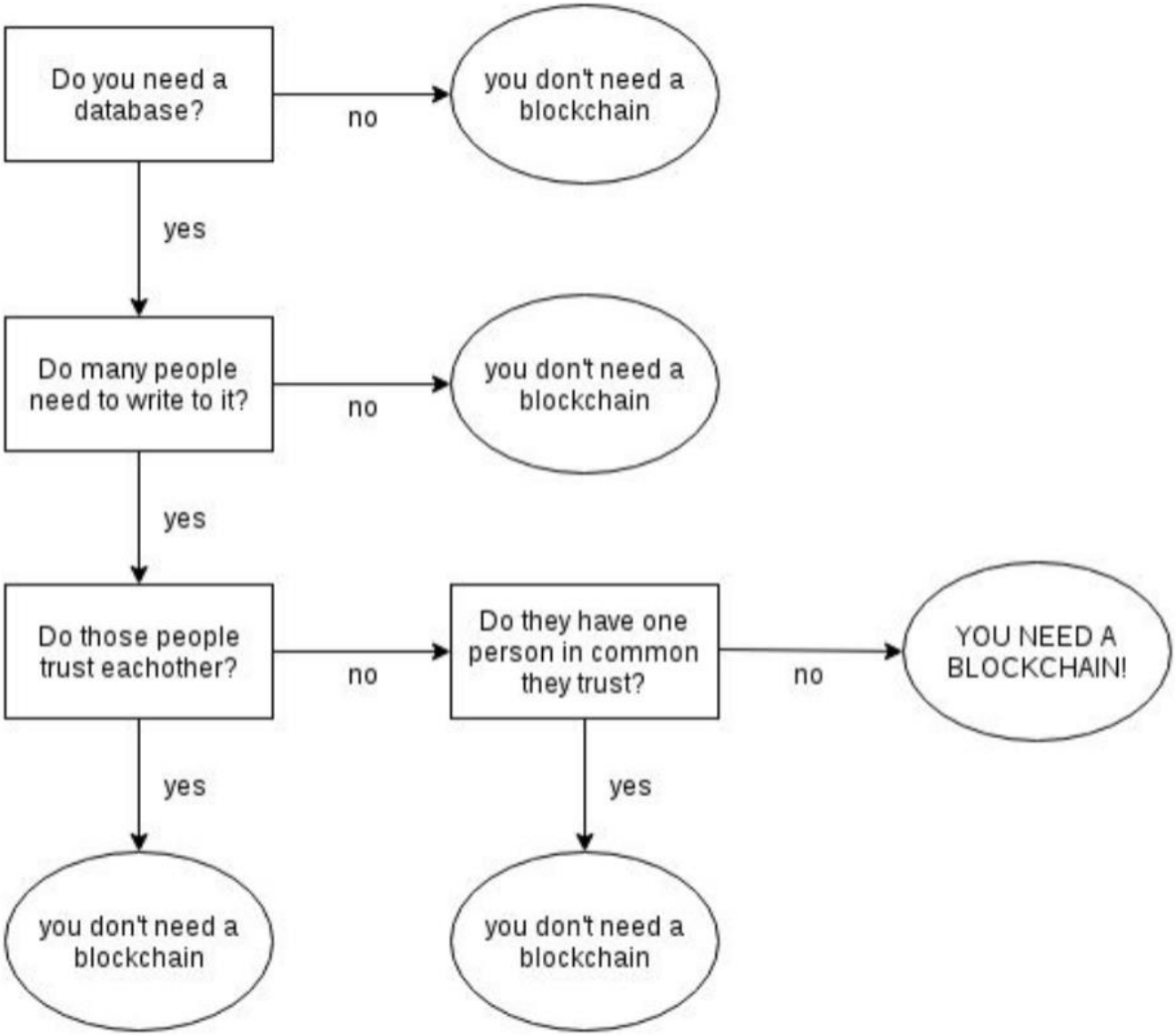


A few projects

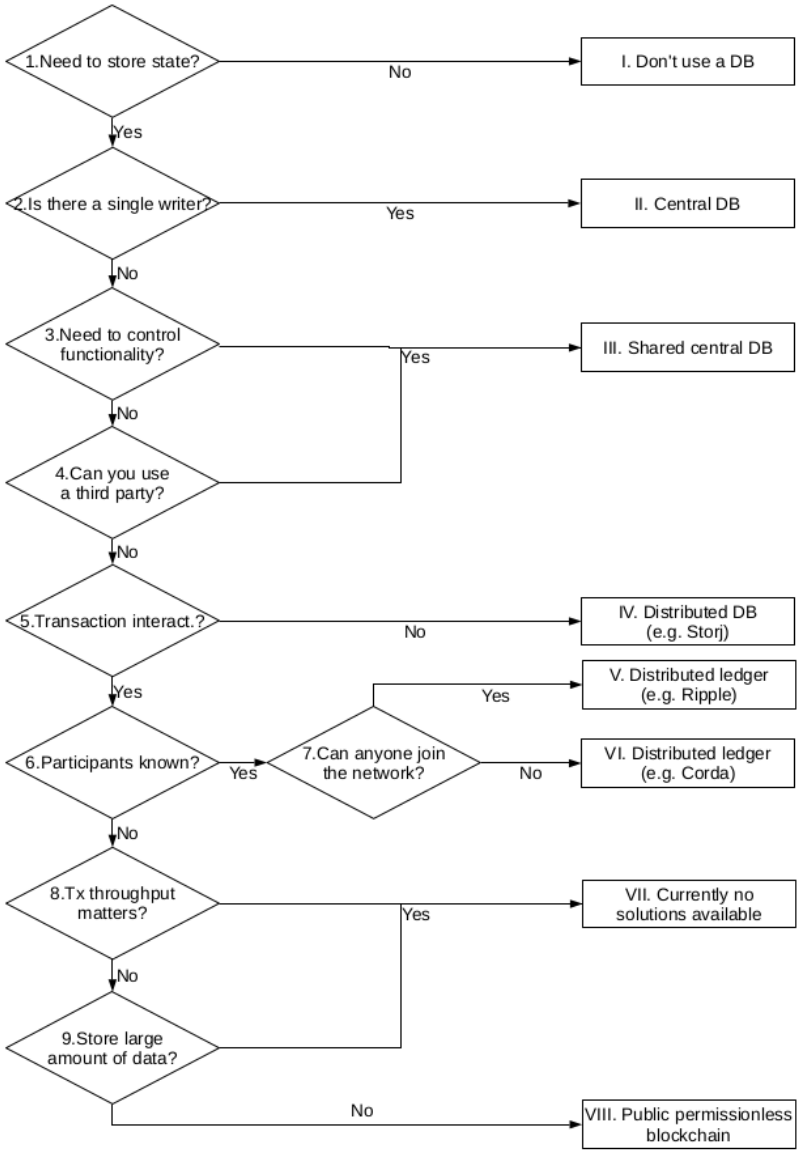
- Steem (social media)
- Open music initiative (copyright)
- MadHive (blockchain-based advertising)
- Voatz (voting)
- Tradelens (logistics)
- Patientory (healthcare)
- Propy (real estate)
- Algorand (finance)
- Forestcoin (green)
- …

Some resources from: https://builtin.com/blockchain/blockchain-applications. The list is not exhaustive and does not represent any form of recommendation or sponsorship

Do I need a blockchain?

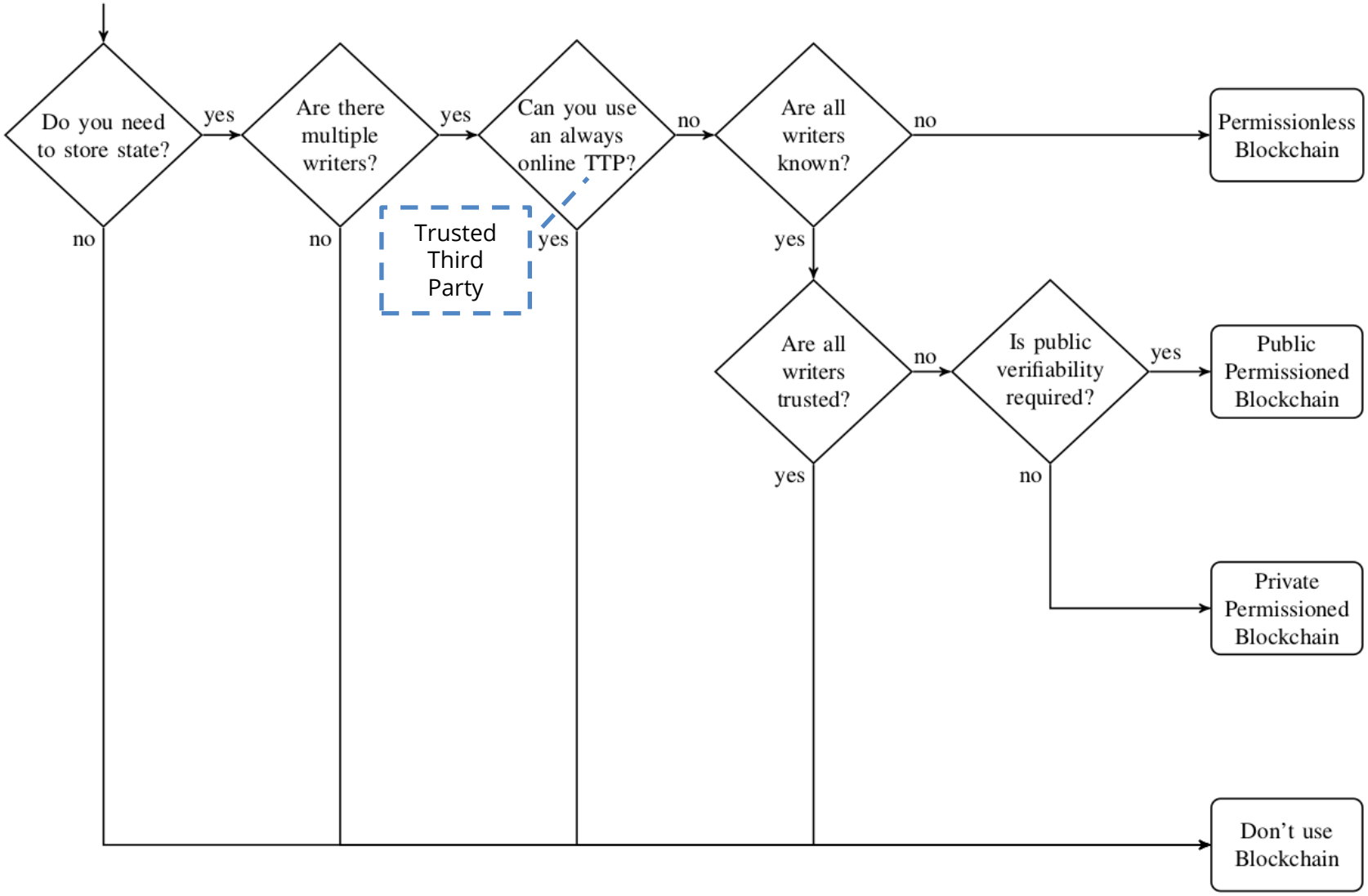


Do I need a blockchain? (Koens & Poll)



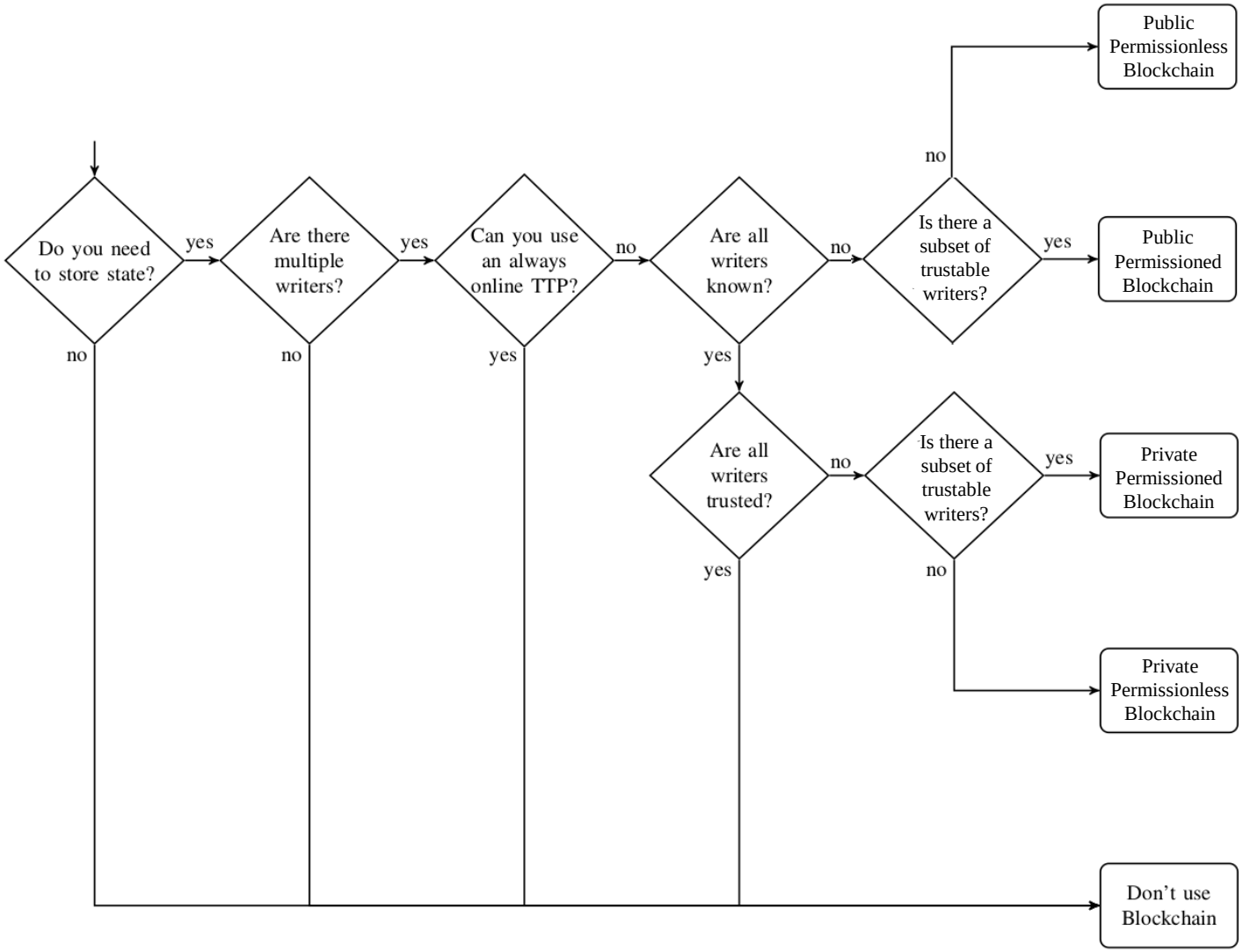
Koens, T. & Poll, E. What Blockchain Alternative Do You Need? ESORICS, Springer, 2018

Do I need a blockchain? (Wüst & Gervais)



Wüst, K. & Gervais, A. Do you Need a Blockchain? CVCBT, IEEE, 2018

Do I need a blockchain? (Wüst & Gervais, revised)



Wüst, K. & Gervais, A. Do you Need a Blockchain? CVCBT, IEEE, 2018 (revised to be compatible with the Private|public / Permissioned|permissionless categories)

Bibliography

- Acronyms in square brackets indicate the reference

  - [**NISTIR**] Yaga, D., Mell, P., Roby, N., Scarfone, K. *Blockchain Technology Overview*. NISTIR 8202. https://doi.org/10.6028/NIST.IR.8202
  - [**ABA**] Xiwei Xu, Ingo Weber, Mark Staples: Architecture for Blockchain Applications. Springer 2019, ISBN 978-3-030-03034-6, pp. 1-307
  - [**MB**] Antonopoulos, A. M. Mastering Bitcoin: Programming the open blockchain. O'Reilly 2017. ISBN: 978-1-491-95438-6
  - [**ME**] Antonopoulos, A. M., Wood, G. Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly 2017. ISBN: 978-1-491-97194-9
  - [**btc**] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf
  - [**wp**] Buterin, V. *A Next-Generation Smart Contract and Decentralized Application Platform.* https://github.com/ethereum/wiki/wiki/White-Paper
  - [**yp**] Wood, G. *Ethereum: A secure decentralised generalised transaction ledger*. https://ethereum.github.io/yellowpaper/paper.pdf
  - [**IES**] Dannen, C. *Introducing Ethereum and Solidity. Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress. ISBN: 978-1-4842-2535-6
  - [**e**] Diedrich, H. *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*. Wildfire Publishing. ISBN: 978-1523930470
  - [**BDLT**] Di Ciccio, C. Blockchain and Distributed Ledger Technologies. In: Leo, S., Panetta, I.C., The Role of Distributed Ledger Technology in Banking. Cambridge (in print)

Contents are mainly based on these publications. They are not expected to be all studied. Paying attention during the class is PARAMOUNT. Don't read me, I am just a chatty slide. listen to the instructor now!

Agenda for today

09:00 - 10:00:
Transactions, ledgers, DLTs and blockchains

10:15 - 11:15:
Double spending, cryptocurrencies, smart contracts

11:30 - 12:00:
Tokens vs cryptocurrencies, public/private and permissionless/permissioned blockchain systems

12:00 - 12:45:
Lab and homework assignment

Kudos to Jan Martijn for the picture

DISCLAIMER

The information in this presentation has been compiled with the utmost care,
but no rights can be derived from its contents.