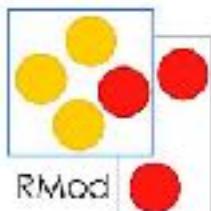


Blockchain & Smart Contracts Crash Course

CBSOFT 2018 Tutorial

Henrique Rocha (henrique.rocha@gmail.com)



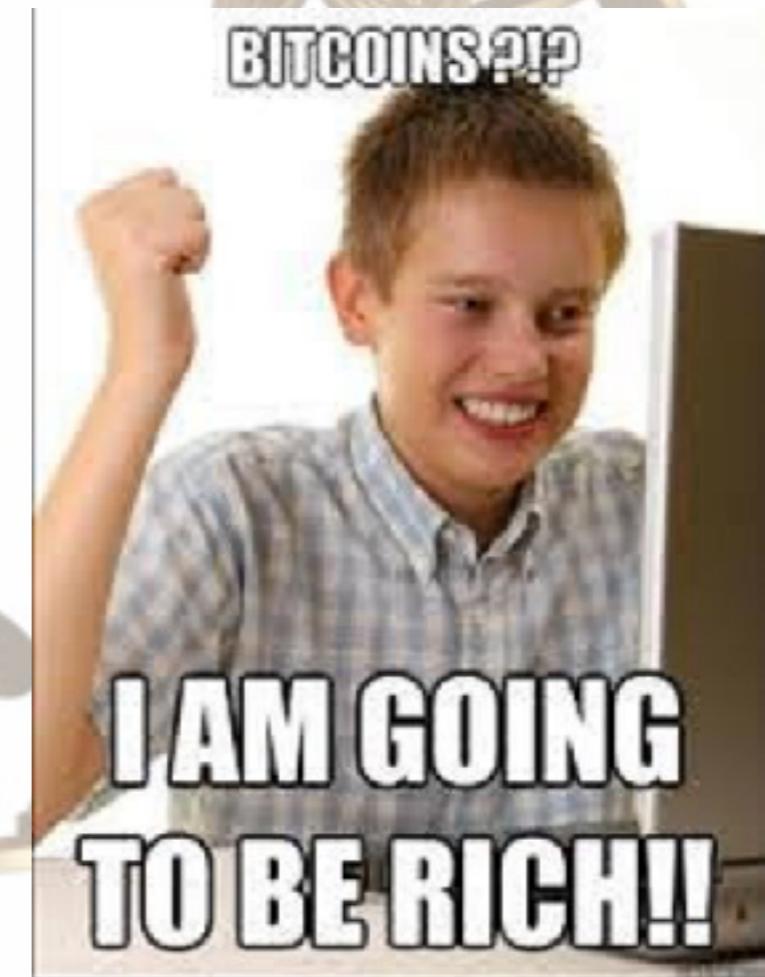
About Me

- Henrique Rocha (henrique.rocha@gmail.com)
- Post-doc at Inria Lille (France, 2017 – 2019)
- Ph.D. at UFMG (Brazil, 2016)
- College lecturer (Brazil): Cotemig (2012 – 2017), Una (2009 – 2011), Unipac BD (2007 – 2012)



Blockchain

- Be millionaire in a week!
- Super fast transactions!
- Escape those terrible taxes!
- Washing money like going to the laundry shop!



No, this is not a “get rich on Cryptocurrency” type of talk.

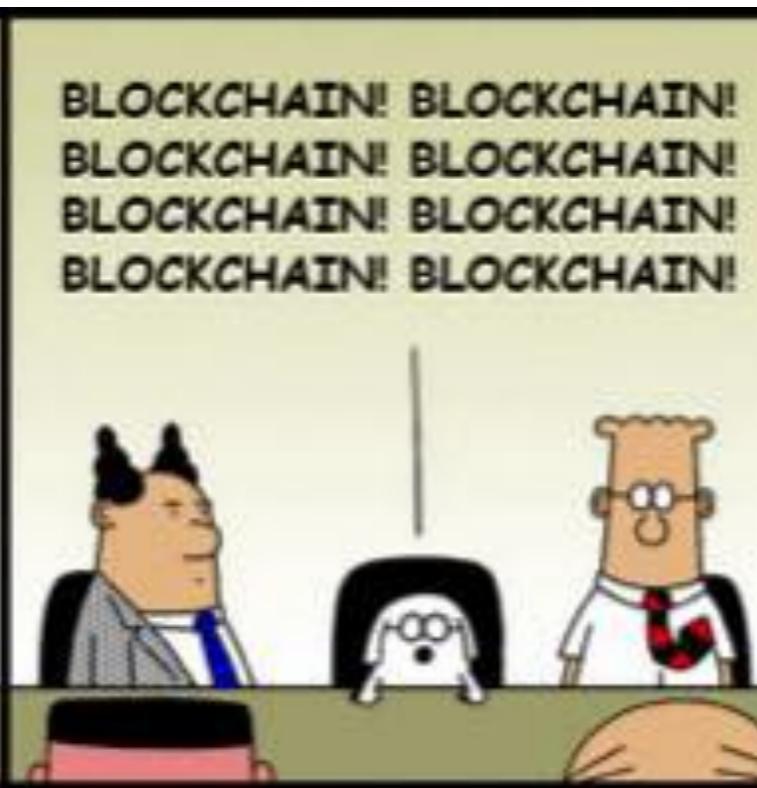
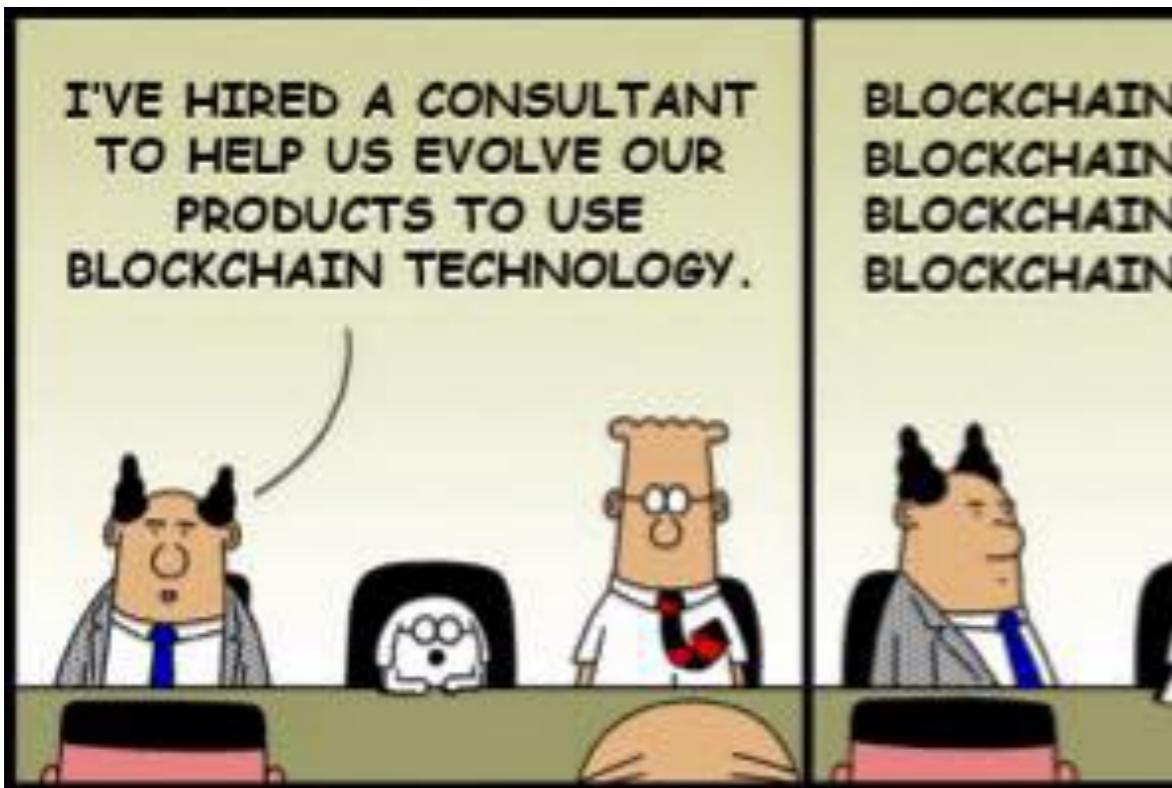
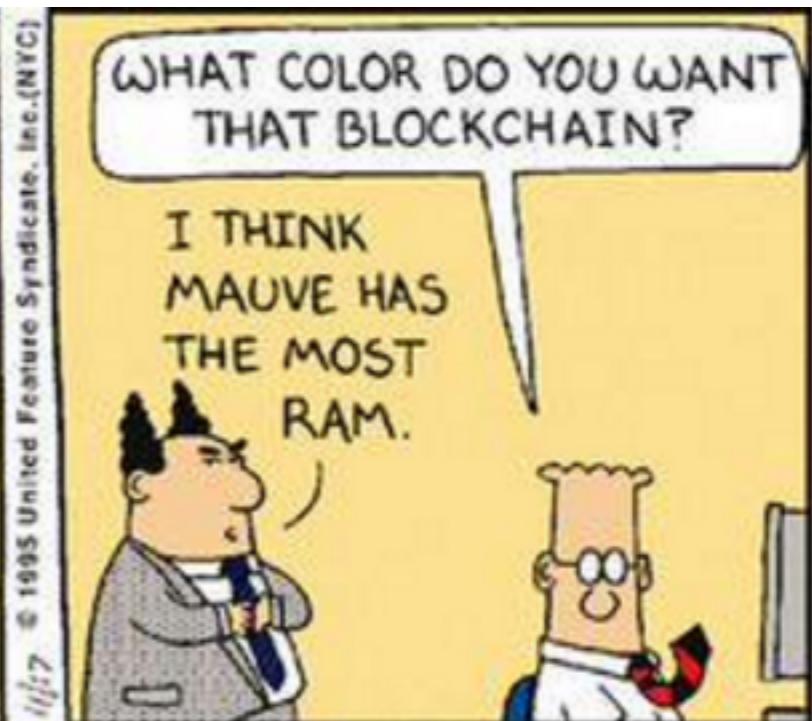
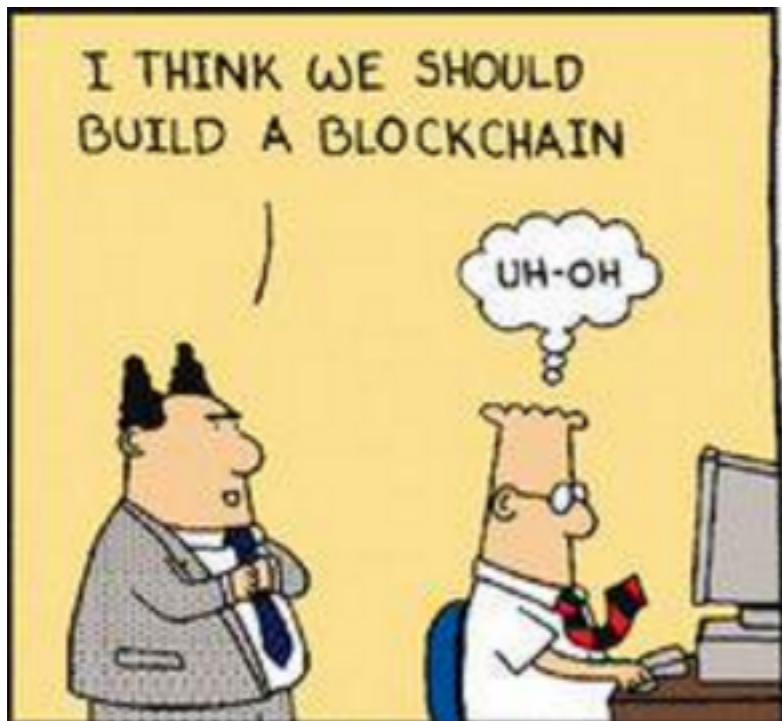
(you cannot leave, we already locked the door)

This Tutorial at CBSoft 2018

- **1st part** (11:00 — 12:30): Presentation on Blockchain, Smart Contracts, Research, etc.
- **2nd part** (14:00 — 15:30): Hands-on practices in the lab with Smart Contracts.
- This tutorial is supposed to be understandable even if a person has almost no previous knowledge on this topic.

Summary (1st part)

- Introduction to Blockchain
- Blocks and the general Structure
- Mining and PoW
- Smart Contracts
- Research in Blockchain Oriented Software Engineering



What is Blockchain?

 *bitcoin*

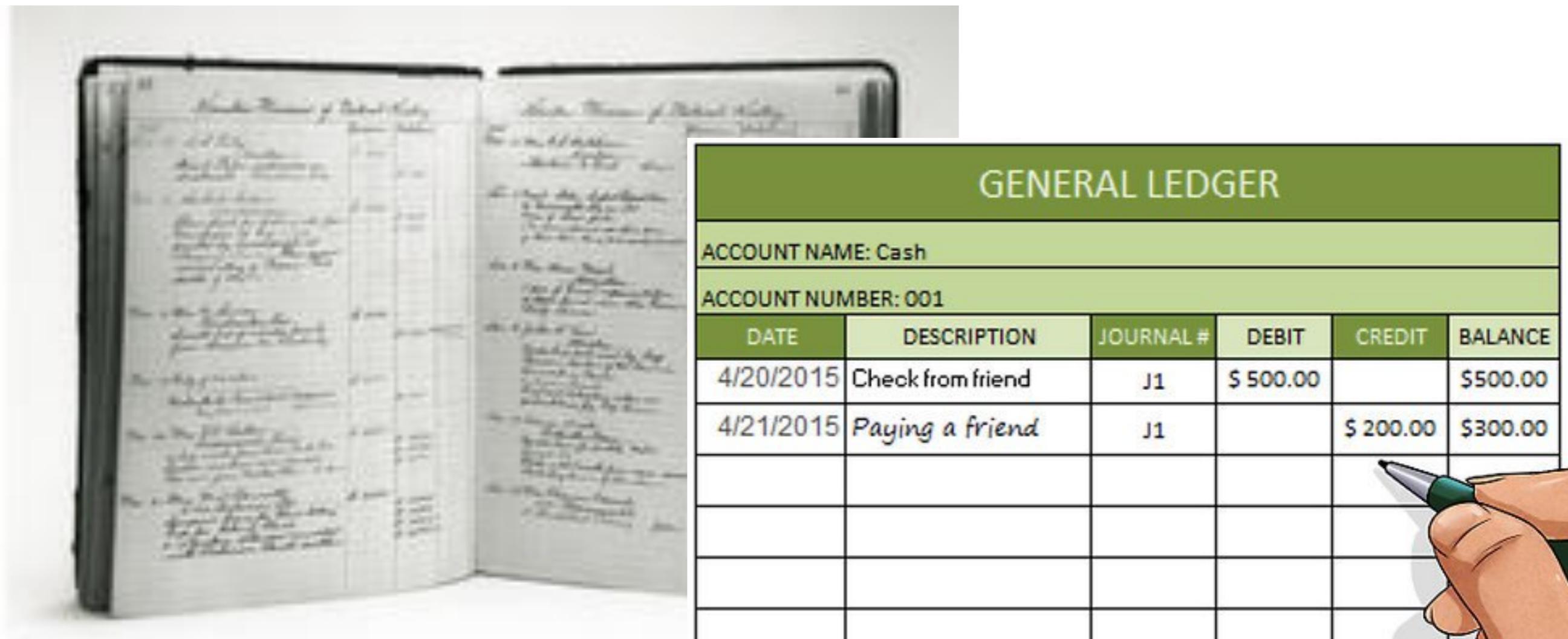
 ETHEREUM

Examples of Blockchain Technologies

What is Blockchain?

From an User's Perspective

- An open distributed Ledger that promotes privacy



What is Blockchain?

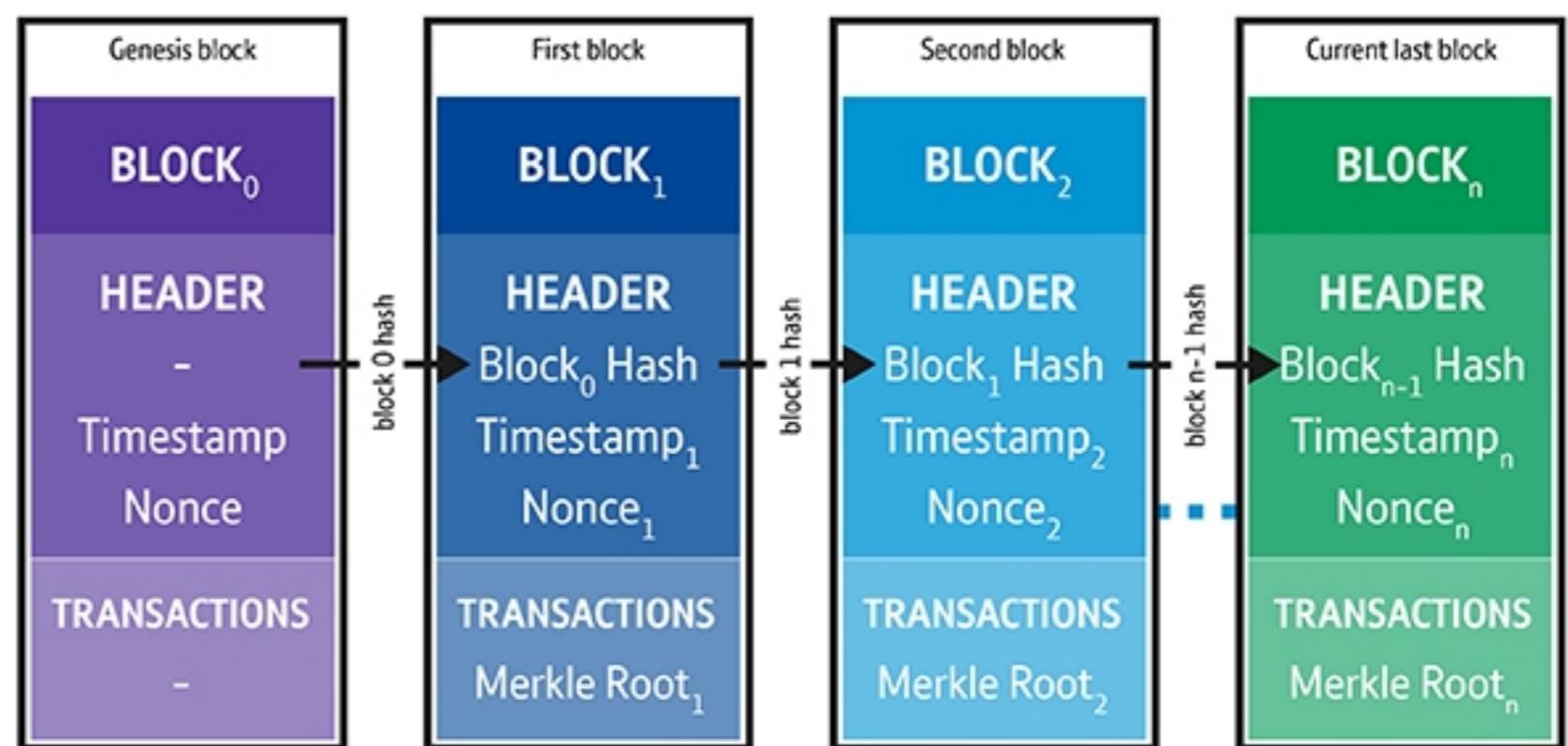
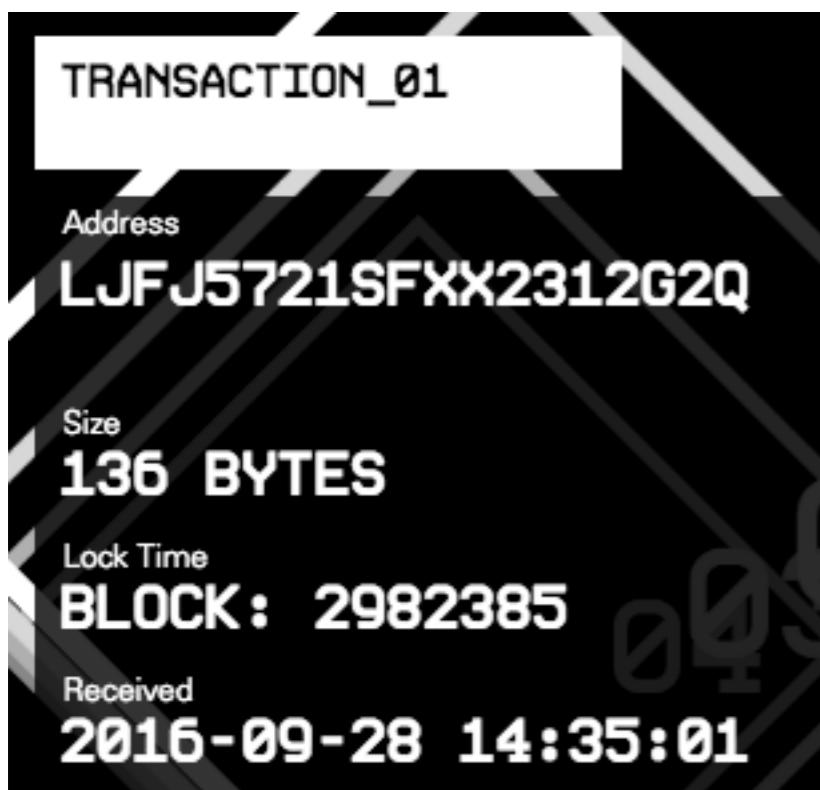
From an User's Perspective

- An open distributed Ledger that promotes privacy
 - Ledger - Records economic transactions of cryptocurrency (BitCoin, Ether).
 - Open - anyone can participate on and inspect the transactions
 - Distributed - the ledger is shared and synchronized among several “people”
 - Privacy - the ledger transactions promote anonymity

What is Blockchain?

From a Developer's Perspective

- Roughly, an append-only globally shared transactional database



What is Blockchain?

From a Developer's Perspective

- Roughly, an append-only globally shared transactional database
 - Database — stores and manages digital resources
 - Transaction — ACID properties
 - Append-only — immutable data (cannot delete or alter), just append new information.
 - Globally Shared — managed by a P2P network, all peers store a complete copy of the database.

What is Blockchain?

From an Academic Perspective

- Blockchain is a hyped topic with many research possibilities
- "Bitcoin is a rare case where practice seems to be ahead of theory." — Joseph Bonneau et al., Research perspectives and challenges for bitcoin and cryptocurrencies, 2015.
 - But we are catching on =)

Account

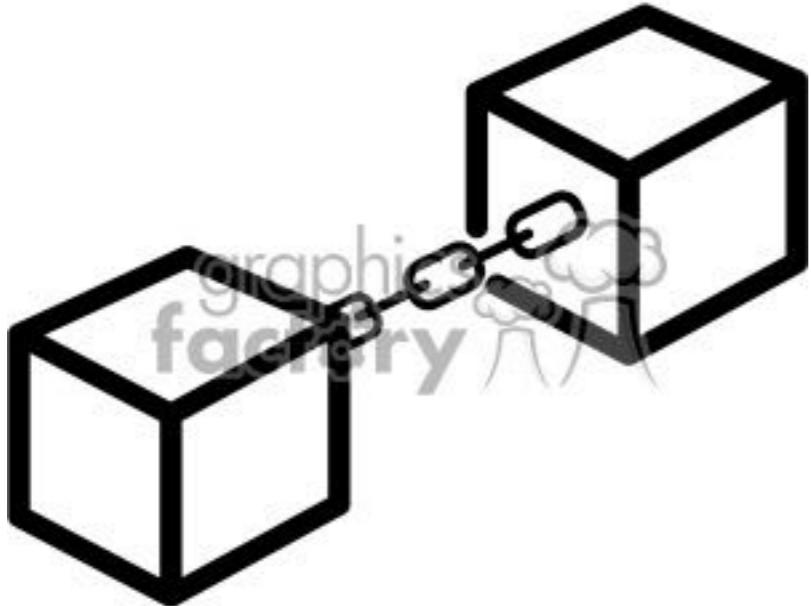
- We need an account to interact with the blockchain
- Roughly, an account's id/address is a public key and whoever holds the private key owns it.
- For example see: <<https://etherscan.io/accounts>>

Transactions

A transaction is an operation that changes something on the blockchain.

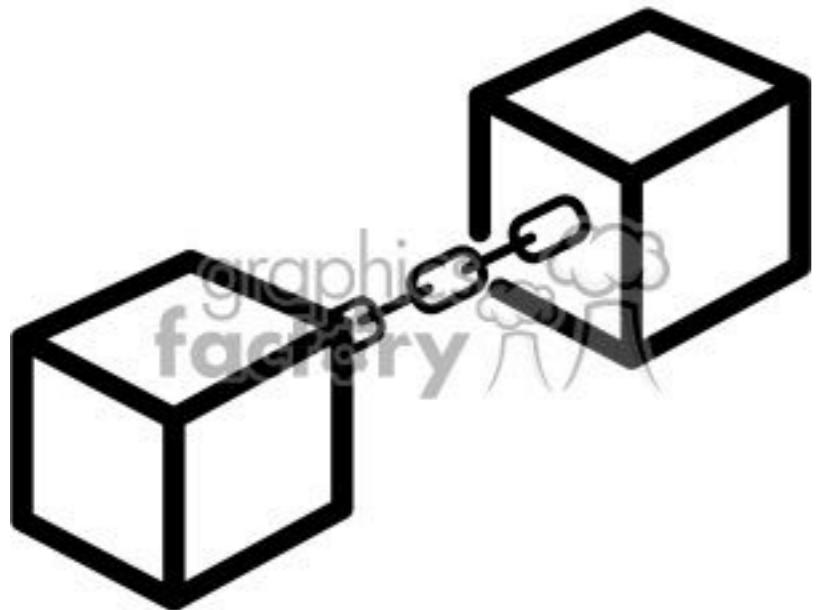
The information on transactions is public to everyone on the blockchain.

T.hash	From	To	Value
0x01...	0xFA...	0x9E...	25
0x22...	0x9E...	0x2F...	0
0xC3...	0x9E...	0x77...	7



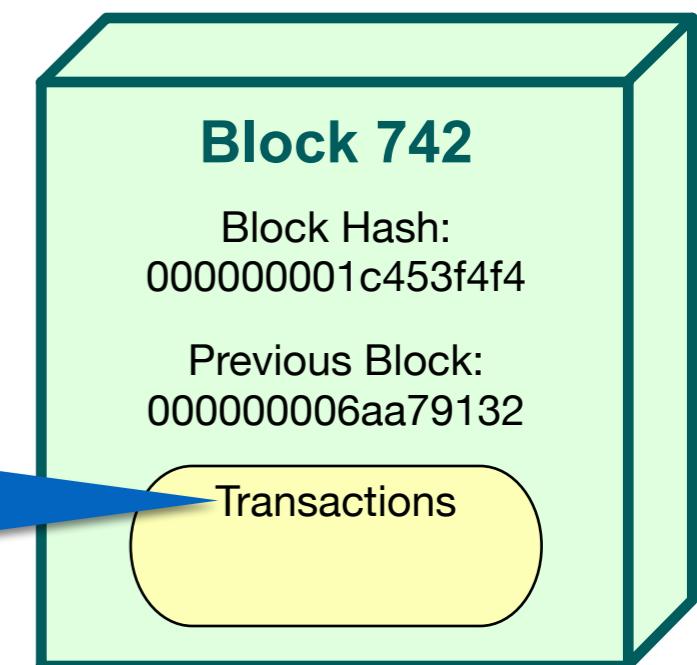
Blocks

- A block is storage unit in the blockchain database.
- Transactions are bundled into a block and distributed among all peers.
- A Block is linked to the previous one forming a linear sequence in time.
- Blocks are immutable (read-only data).



Blocks

T.hash	From	To	Value
0x01...	0xFA...	0x9E...	25
0x22...	0x9E...	0x2F...	0
0xC3...	0x9E...	0x77...	7

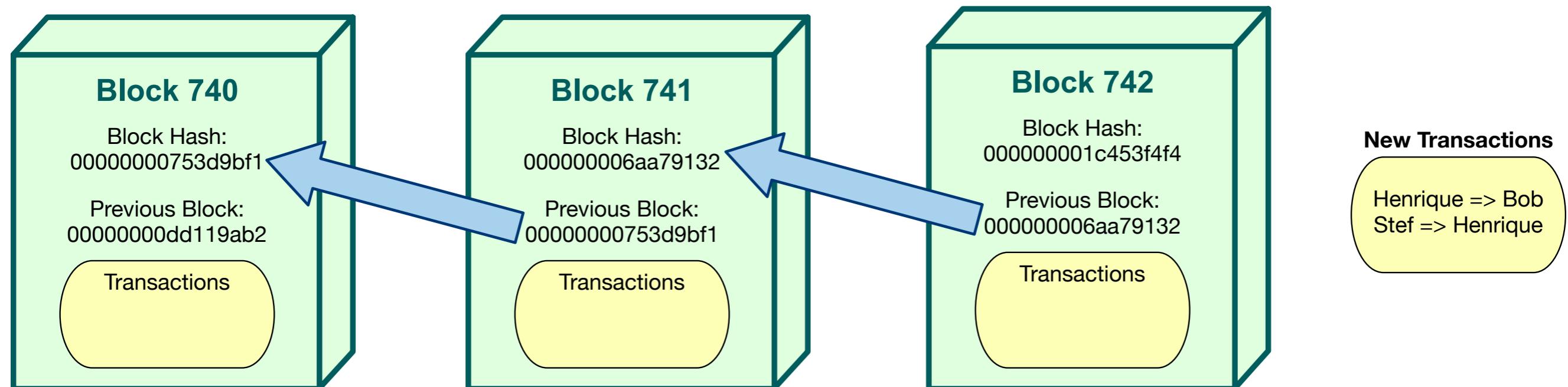


How are the Blocks Linked?

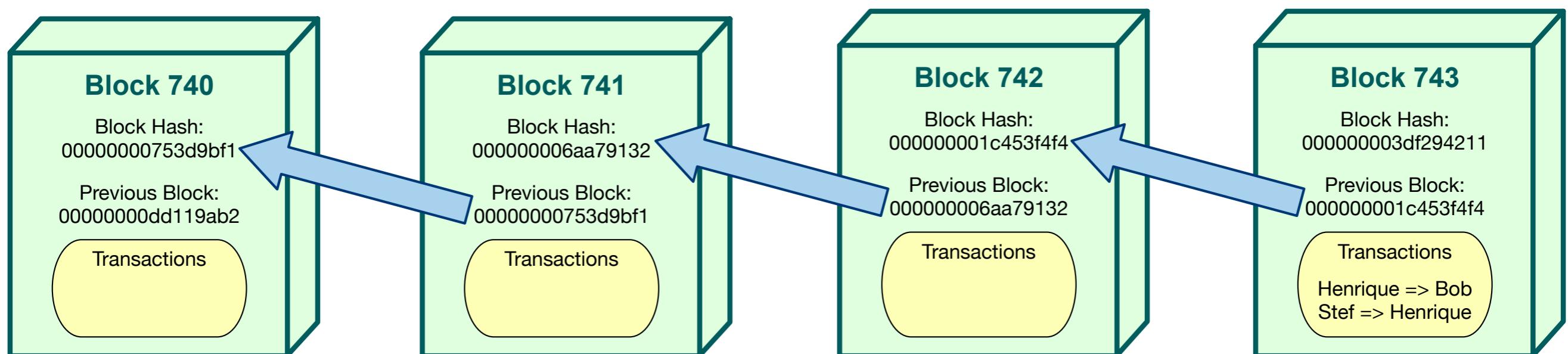
- The blocks are linked by a **Hash** number
 - When a new block arrives, someone in the blockchain computes the Hash using the new block and the most current block.
 - A timestamp is also used in the Hash calculation.
- Each block also carries the previous block hash for quick reference (and linking).
- Therefore, the blocks are linked in a time sequence manner.



Linking Blocks Example



Linking Blocks Example



more secure

less secure

Blocks are “more secure” as you go further back in the chain

How long does it take... to create a block?

The average time for a new block to be added in BitCoin is ~9.4 min https://data.bitcoinity.org/bitcoin/block_time/

Ethereum varies according to the gas price, but the average time is ~0.24 min

<https://bitinfocharts.com/comparison/ethereum-confirmationtime.html>

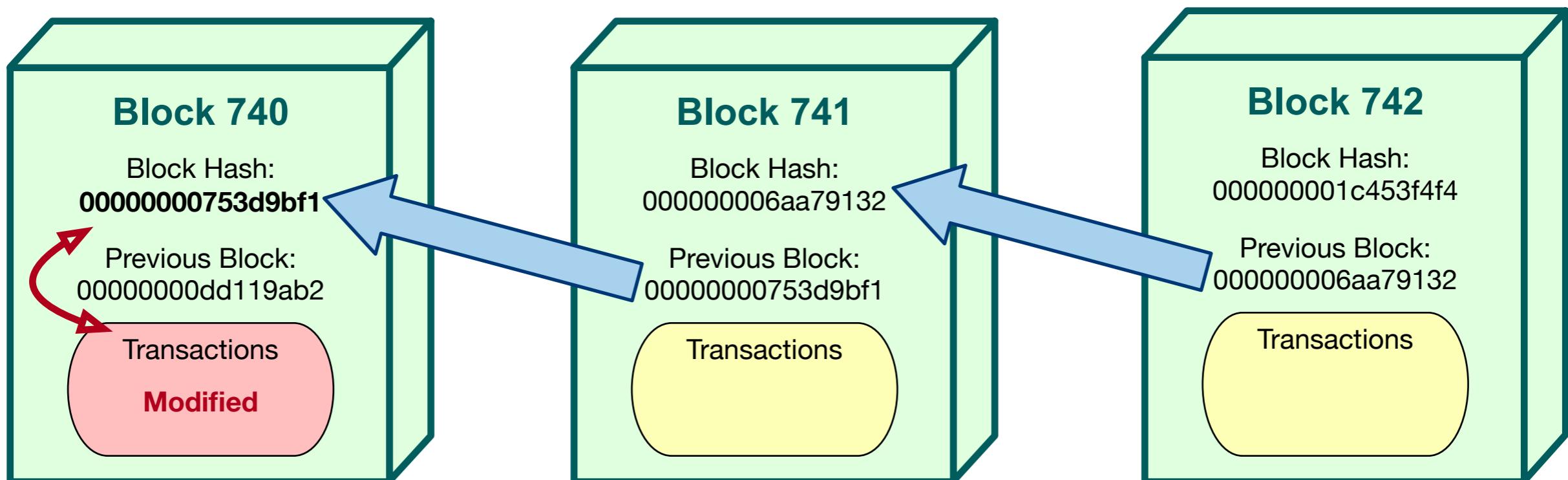
What if...



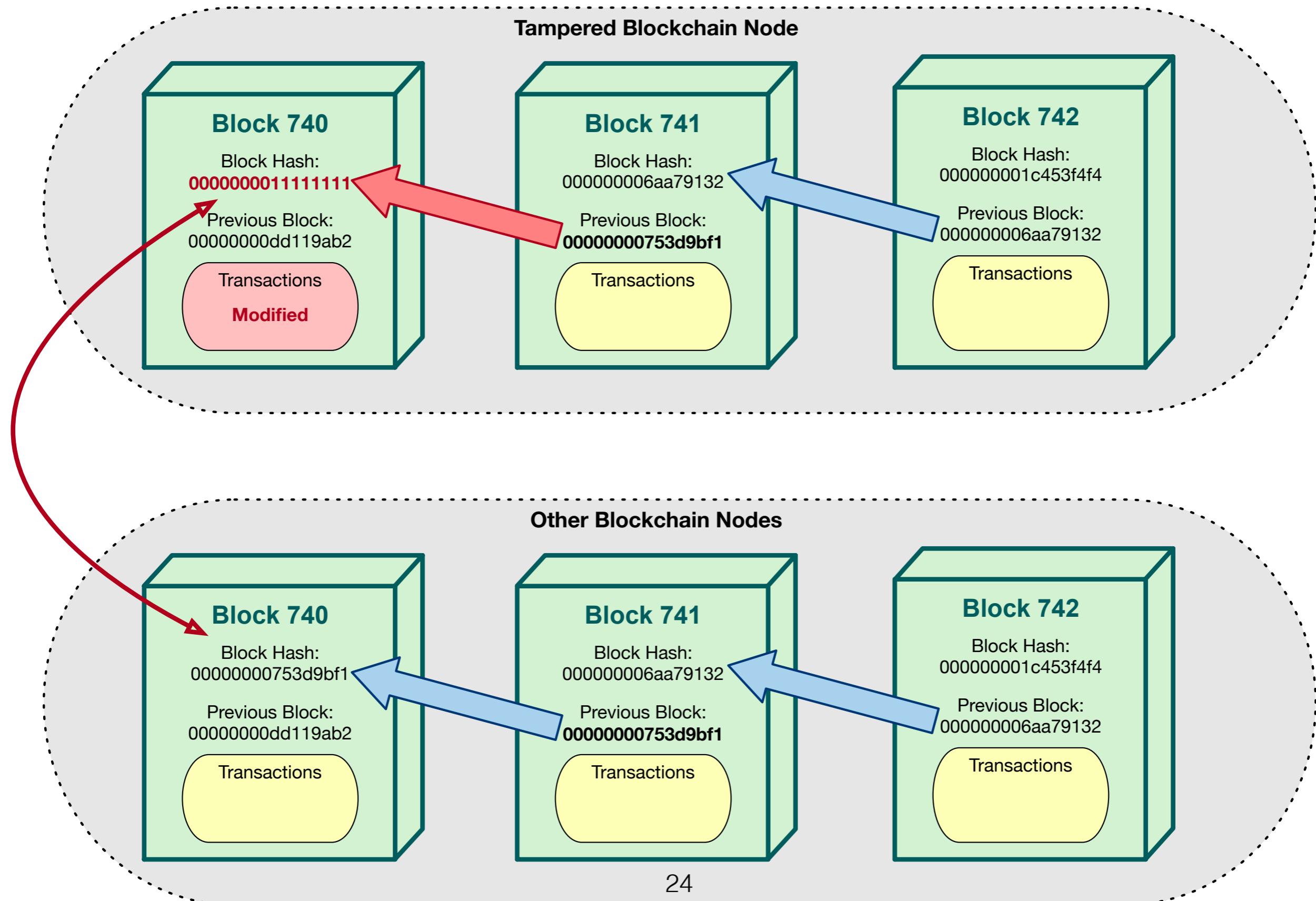
Someone Tampers the Blocks?

- If you change the data inside a block, the hash for that block would **not** match anymore.
 - Even if you tried to tamper the block hash as well, all other peers in the blockchain would have a copy of the original showing a mismatch.
- Since the next block also used that information in their hash, it also will **not** match.

Tampering with Blocks



Tampering with Blocks



Cool but...
what is it good for?

One word... trust.

Trustless Trust



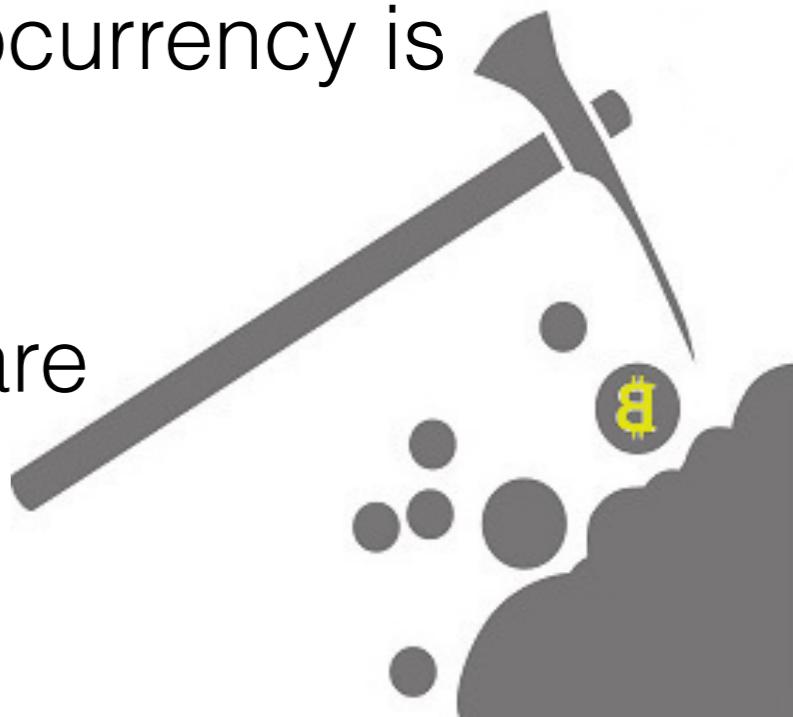
The transactions/blocks are verified by every node (trustless).

This ensures the approved transactions/block are legit (promoting trust).

And allows entities to interact without a trusted 3rd party.

Mining

- Mining is the process of creating a block and adding it to the blockchain (using the PoW consensus algorithm)
 - The goal is to solve cryptographic puzzles to validate the transaction and create a block.
 - Since this process consumes computation resources (CPU, energy, time), a reward in cryptocurrency is given to cover the cost.
- A Miner is someone who uses his hardware to mine the blockchain.





BitCoin Proof of Work (PoW)

- The goal is to find an acceptable Hash number
 - Use SHA-256 on the new block, the previous block hash, and a seed number (called nonce)
 - If SHA-256 outputs a hash with a required number of leading zeroes you solved the puzzle.
 - Otherwise, increment the seed and try again.
 - The faster you can compute these operations (measured in Hashes per second), the more successful your mining is.

Is it worth Mining?

- Short Answer: No (for BitCoin)!
 - The time for casual Miners has passed.
 - The mining reward might not even cover its energy costs.
 - Specialized hardware need for efficiency mining
 - “Unfair” competition with Mining Farms





Mining Example

- USA BitCoin Miner
 - Hardware Antminer S9i
14 TH/s (\$600 Amazon)
 - Average power cost
for US (0.12\$/kWh)
 - “Profit” p/year: -\$205.97
 - And that's not counting the
hardware cost.

Day	Profit per day \$ -0.6 Pool Fee \$ 0	Mined/day B 0.0005015
Week	Profit per week \$ -3.95 Pool Fee \$ 0	Mined/week B 0.003511
Month	Profit per month \$ -16.93 Pool Fee \$ 0	Mined/month B 0.01505
Year	Profit per year \$ -205.97 Pool Fee \$ 0	Mined/year B 0.1831

<https://www.cryptocompare.com/mining/calculator/>

Mining Pool vs Farms

- Mining pool is like a workers cooperative. The rewards are split among the participants.



- Mining Farms are data centers focused on mining.



Ethereum PoW

<https://github.com/ethereum/wiki/wiki/Ethash>



- Ethereum uses a different PoW, called Ethash.
 - Ethereum PoW discourages specific hardware by focusing on Memory Hardness instead of processing power.
 - It uses slices of a large dataset (stored in memory) as a part of the hash.
 - So the vast majority of a miner's effort is reading the dataset, and not performing operations.
- Ethereum is migrating to a Proof-of-Stake (PoS) algorithm

Can We Trust Miners?

Can We Trust Miners?

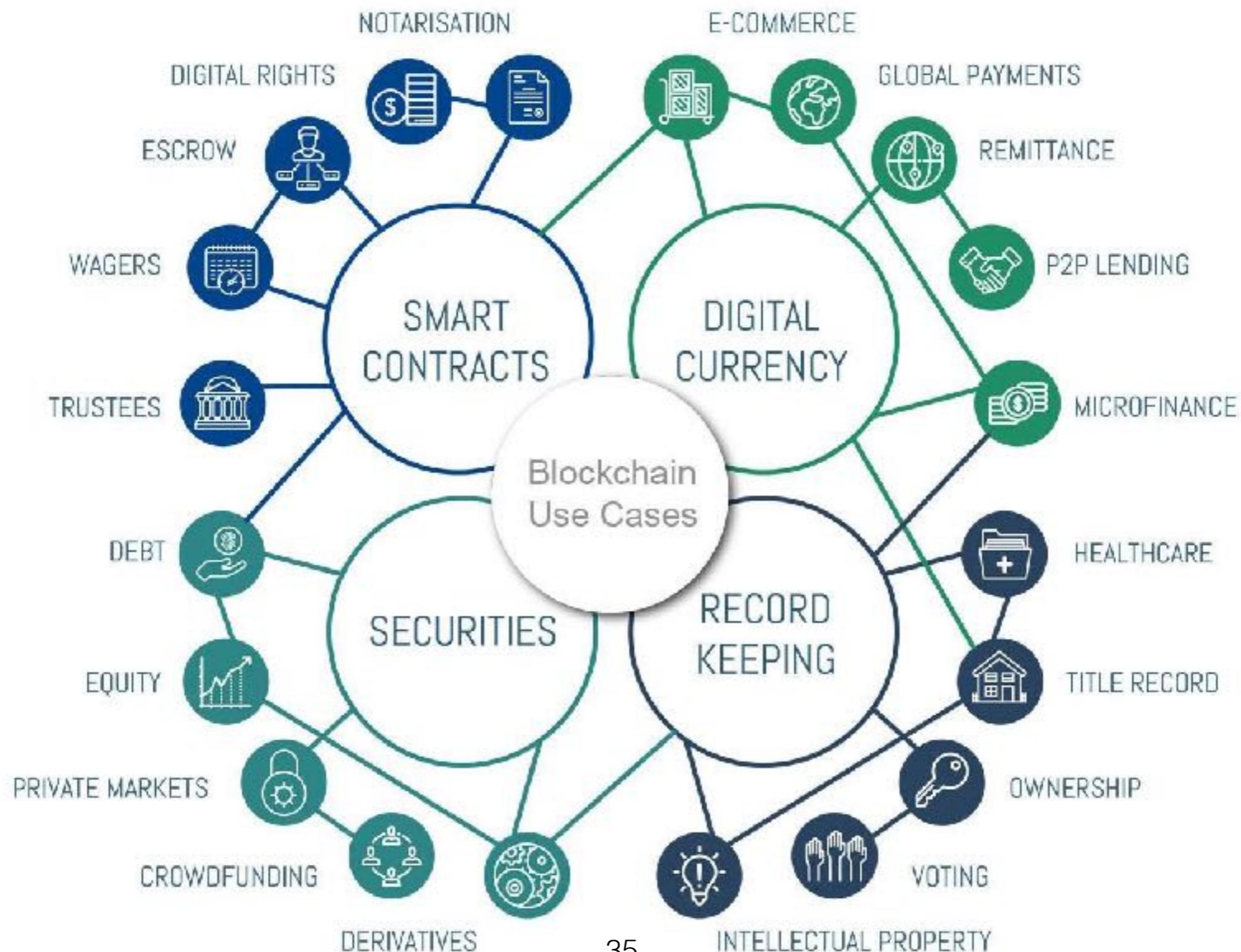
No, we can't!

Miners also don't trust each other, so they will check blocks from another.

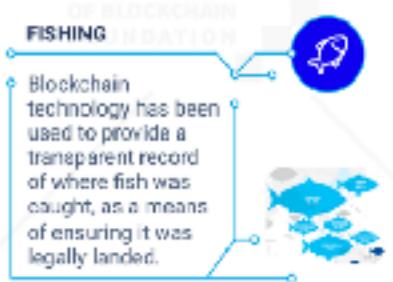
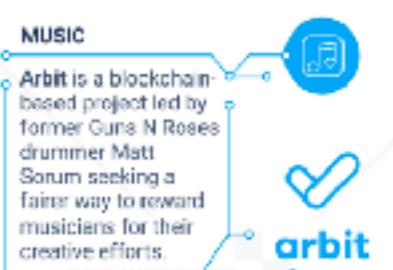
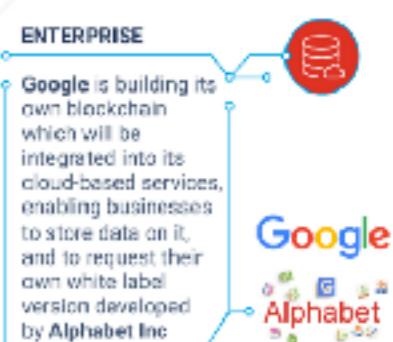
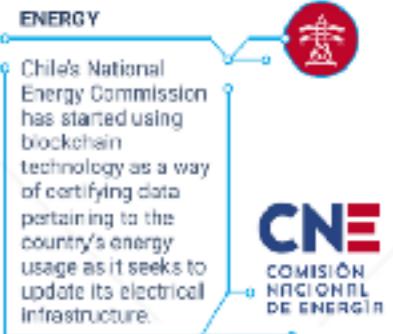
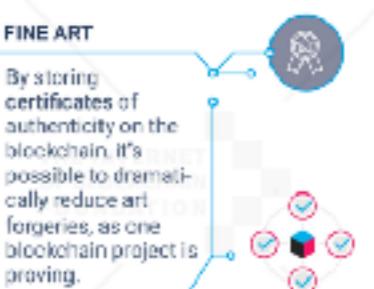
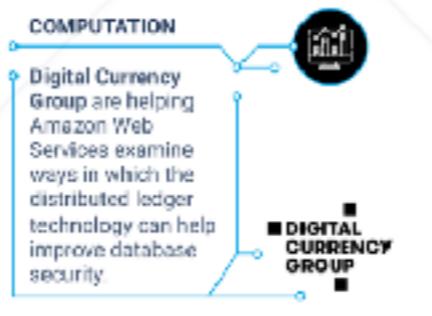
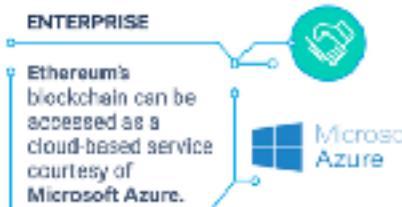
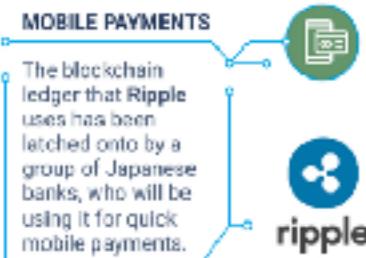
This competition assures that Miners can't cheat and promotes trust on the platform.



Blockchain Use Cases



50+ BLOCKCHAIN REAL WORLD USES CASES



Smart Contracts

[Fritz Henglein, Smart Contracts..., 2017]

- “Smart Contracts are neither Smart nor Contracts”
 - Smart Contracts are self-executing programs coded in complex Turing-complete language.
 - Rules & Actions intermixed (not a contract)
 - Low-level programs hard to analyze (not smart)





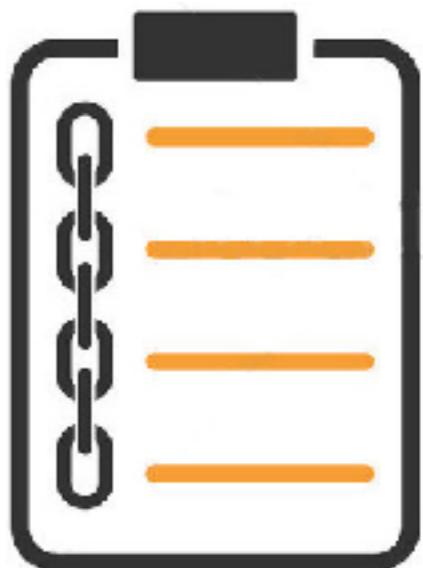
Smart Contracts

[Ethereum Doc, 2018]

- Contracts should not be seen as something that should be “fulfilled” or “complied with”
- They are more like “autonomous agents” that live inside the blockchain
 - Executing a specific piece of code when “poked” by a message or transaction
 - Have direct control over their cryptocurrency and attributes to store their permanent state.

Smart Contracts

[Henrique Rocha, CBSoft, 2018]

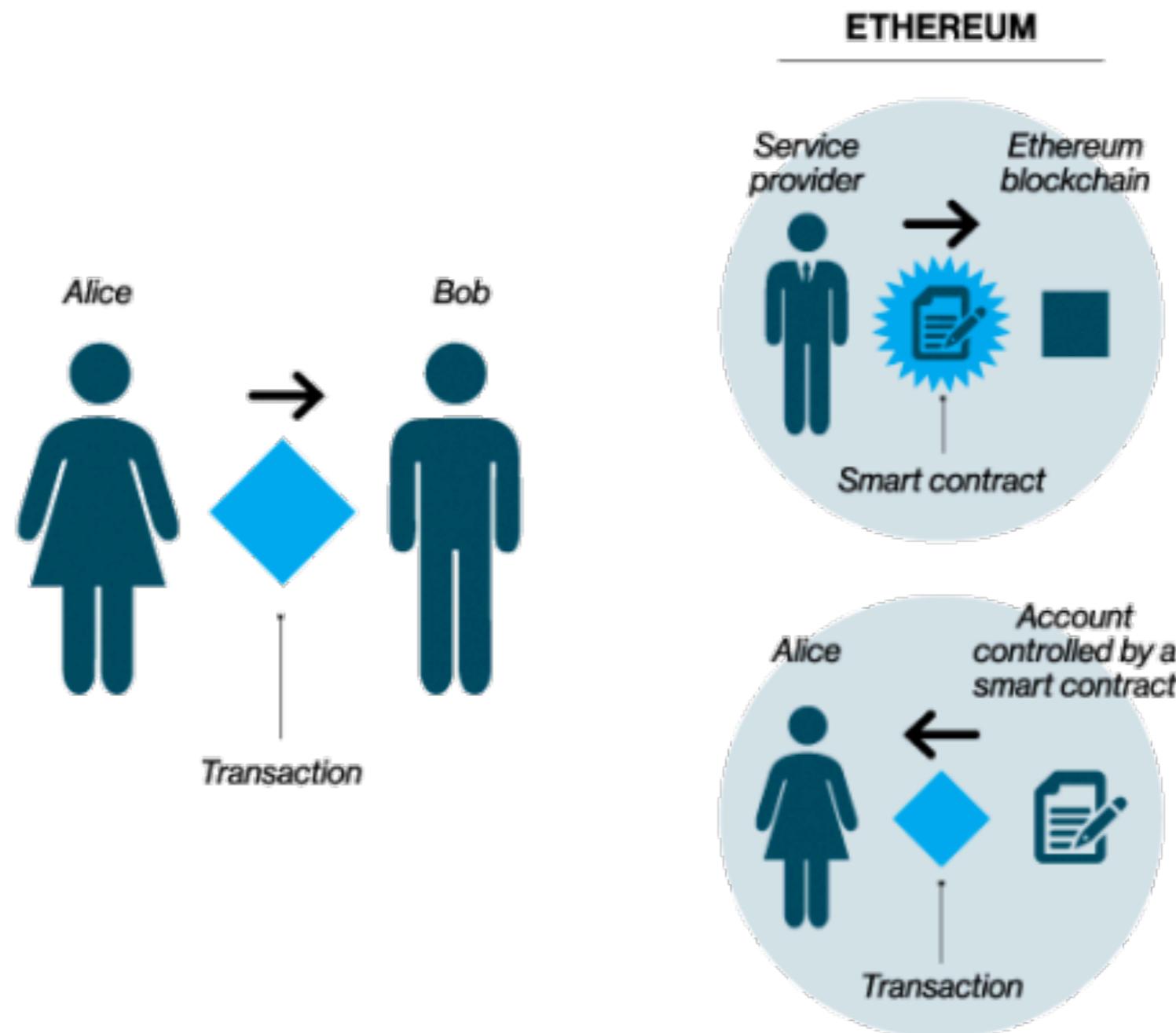


- Smart Contracts are objects deployed in the blockchain.
 - More specifically, code and data (like a class) residing at a Blockchain address.
 - Transactions created by function execution.
 - Contracts are sandboxed in the Blockchain.

Contract Ex: Pair Storage

```
1 pragma solidity^0.4.24;
2 /**
3  * @title Simple Pair Storage contract
4  * @author Henrique
5  */
6 contract SimplePairStorage{
7     int private data1;
8     uint data2;
9
10    function setData(int _data1, uint _data2) public {
11        data1 = _data1;
12        data2 = _data2;
13    }
14
15    function getData() public view returns(int,uint){
16        return (data1,data2);
17    }
18 } //end of contract
```

Diagram Contract Interaction

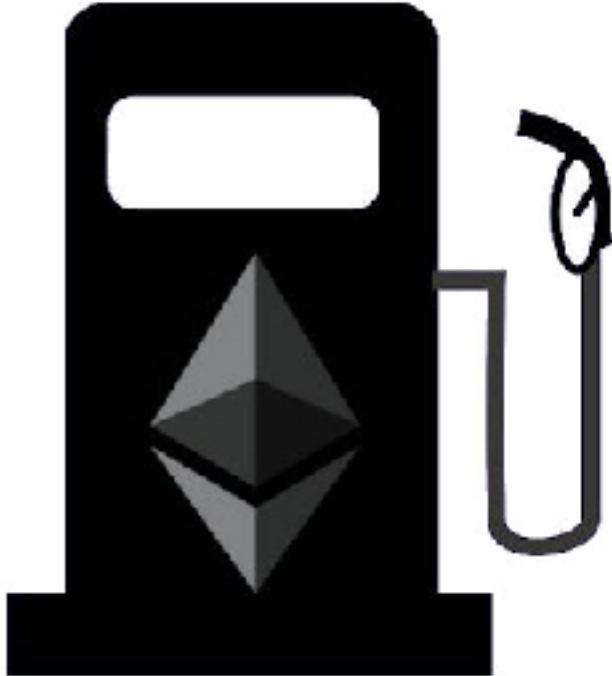


Security on Contracts

- Blockchain and Smart Contracts are very secure.
- Security issues are often the programmer's fault.
 - The same applies to other technologies (e.g. SQL Injection)
 - We need to aid the programmer into coding properly.

Gas

<https://ethgasstation.info/>



- Gas is a resource to execute contracts in the Ethereum Blockchain.
- Every transaction is charged an amount of Gas. The idea is to avoid infinite loops (and DoS attacks), encourage efficient code, and make users pay for the resources they use (bandwidth, CPU, storage).
 - Gas has an Wei (Ether) cost adjusted by the user using the transaction. The Miner is awarded the gas price.
 - If gas is insufficient for an execution, an out-of-gas exception is thrown.

Can We Trust Contracts?

Can We Trust Contracts?



If you can't see the code...
Hell No!

There are ways to verify if the source code is the same deployed object.

Otherwise, you need to trust the contract's creator.

Where to start with Blockchain

- Remix is a browser IDE for Solidity Smart Contracts (Compiler, Debugger, Runtime Environments, etc.)
- Ganache is a runtime environment to create a personal Ethereum blockchain.
- Etherscan is an Ethereum explorer and analytics platform.



Blockchain Research

BOS

- **B**lockchain-**O**riented **S**oftware (BOS) is a software interacting with blockchain [Porru et al., 2017]
 - Usually, it uses a Smart Contract to perform tasks in the blockchain.
 - And off-chain programming for user interface and complex tasks.

BOS: MyEtherWallet

Open source web-app Wallet to store Ether.

The screenshot shows the MyEtherWallet web application interface. At the top, there is a navigation bar with the logo, version (3.10.4.3), language (English), gas price (21 Gwei), and network (ETH (MyEtherWallet)). Below the navigation bar, there are links for New Wallet, Send Ether & Tokens (which is underlined), Swap, Send Offline, Contracts, ENS, Check TX Status, View Wallet Info, and Help.

The main section is titled "Send Ether & Tokens". It contains fields for "To Address" (0x7cB57B5A97eAbe94205C07890BE4c1aD31E486A8), "Amount to Send" (with "Amount" and "ETH" dropdown), "Send Entire Balance" button, "Gas Limit" (21000), and an "Advanced: Add Data" link. A large blue button at the bottom says "Generate Transaction".

To the right, there is a sidebar with "Account Address" (0xaFFb8483F052791b9a6b5cFa25715b3234a10C37) represented by a purple circle icon, "Account Balance" (0 ETH), "Transaction History" (links to Etherscan.io and Ethplorer.io), and a "Buy ETH with USD" button with a coinbase logo. The coinbase button shows 1 ETH for 297.35 USD.

BOS: Catalizr

Digital manager for business investments.
<https://www.utocat.com/catalizr-en/>

The screenshot displays the Catalizr platform's user interface. At the top, there is a blue header bar with the Catalizr logo. Below the header, a navigation bar features four steps: "Accueil" (Home) with a house icon, "Ajoutez les documents de l'entreprise" (Add company documents) with a red circular icon containing a document, "Complétez les informations de l'investissement" (Complete investment information) with a blue circular icon containing a clipboard, and "Signez vos documents" (Sign your documents) with a purple circular icon containing a pen.

Below the navigation bar, three cards illustrate the process:

- IBAN de l'entreprise:** Shows two bank account statements from Crédit Agricole and Société Générale, both titled "Relevé d'Identité Bancaire".
- Projets de statuts de l'entreprise:** Shows a template for a company's articles of association (Statuts) for "SOCIÉTÉ COOPÉRATIVE D'ÉCONOMIE SOCIALE ET SOLIDAIRE L'ÉCOLE DES MÉTIERS". It includes sections for "ARTICLE 1. NOMMAGE", "ARTICLE 2. PERSONNEL", and "ARTICLE 3. FINANCES".
- Kbis de l'entreprise:** Shows a template for a commercial register extract (Kbis) for "SOCIÉTÉ COOPÉRATIVE D'ÉCONOMIE SOCIALE ET SOLIDAIRE L'ÉCOLE DES MÉTIERS". It includes sections for "ARTICLE 1. NOMMAGE", "ARTICLE 2. PERSONNEL", and "ARTICLE 3. FINANCES".

BOSE

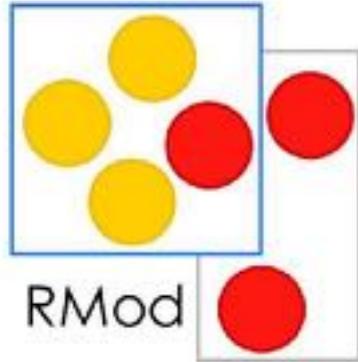
- **B**lockchain-**O**riented **S**oftware **E**ngineering (BOSE)
- New research field, applying software engineering techniques and practices to BOS.
- Porru et al. (2017) identify the most relevant BOSE challenges, and the issues which originate from them.

Opportunities for Improvement

- Resources Optimization (e.g., gas, storage)
- Coding Recommendations (e.g., prevent programming flaws)
- Visualization (e.g., represent the blockchain)
- Design (e.g., plan the architecture of a BOS)
- Inspection & debugging (e.g., asses contracts)
- Code Generation & Reengineering (e.g., auto-generate)
- Mining Alternatives (e.g., green computing)

Papers to start your Research

- Luu et al., 2016. **Making Smart Contracts Smarter.** In Conference on Computer and Communications Security (CCS '16). p.254-269.
- Juels et al., 2016. **The Ring of Gyges: Investigating the Future of Criminal Smart Contracts.** In Conference on Computer and Communications Security (CCS '16). p.283-295.
- Porru et al., 2017. **Blockchain-Oriented Software Engineering: Challenges and New Directions.** Short paper. In 39th International Conference on Software Engineering Companion (ICSE), p.169-171.
- Nakamoto, 2009. **Bitcoin: A peer-to-peer electronic cash system.** bitcoin.org.
- *Ethereum Foundation*, 2014. **Ethereum's white paper.** https://en.wikibooks.org/wiki/LaTeX/Bibliography_Management.



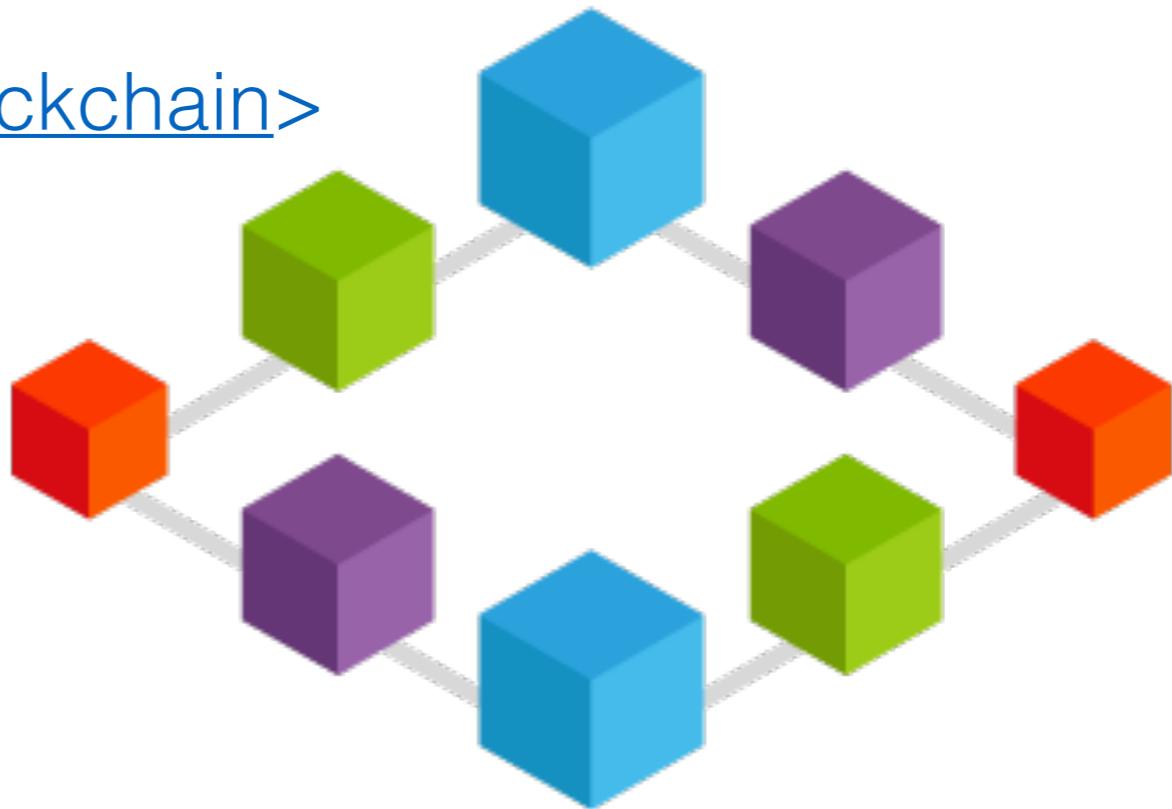
Rmod-Blockchain

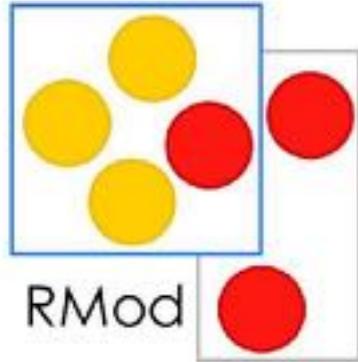
We welcome any research idea you may have for us.

We are also open to industrial and academic partnerships to advance blockchain research.

[<https://github.com/RMODINRIA-Blockchain>](https://github.com/RMODINRIA-Blockchain)

[<https://rmod.inria.fr/web>](https://rmod.inria.fr/web)



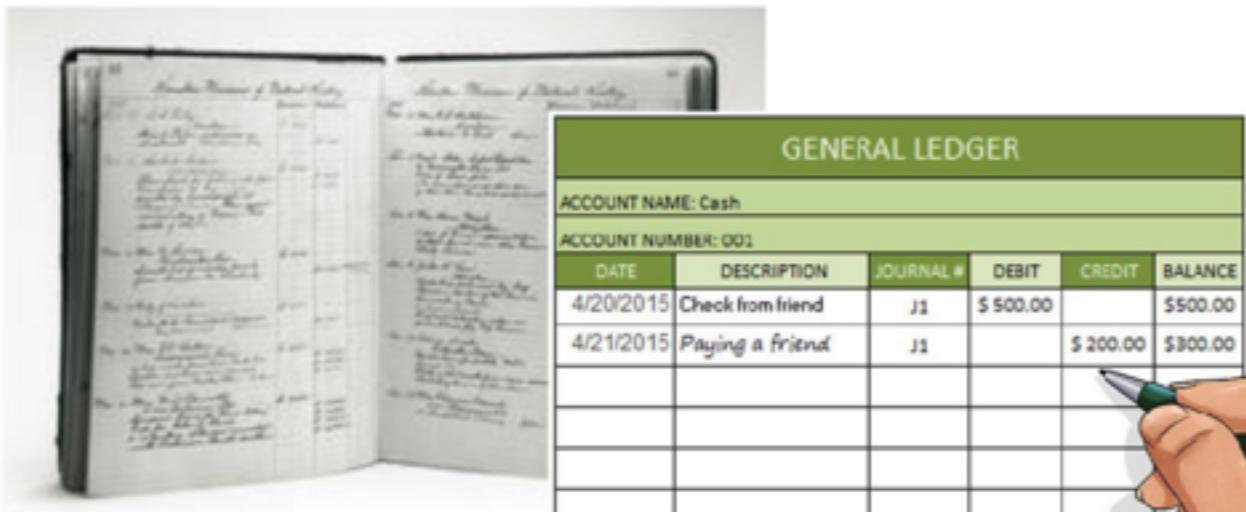


Rmod-Blockchain

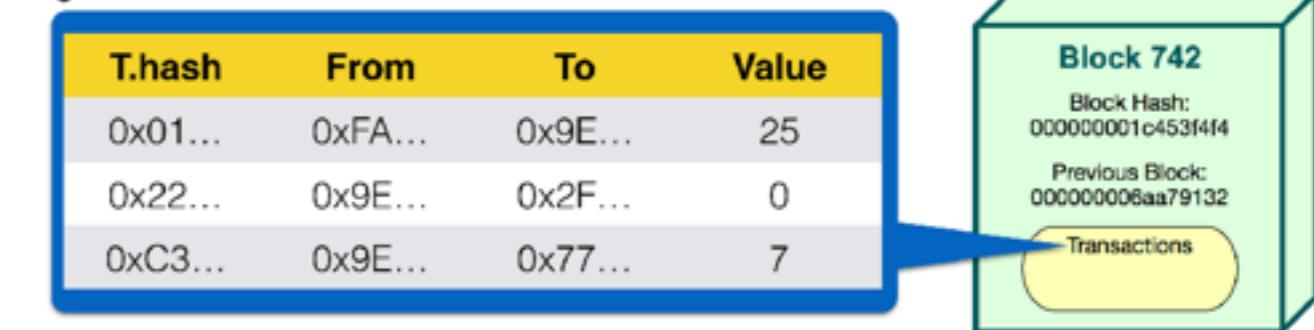
- SmartInspect: Contract internal state inspector
- EQL: query language for Ethereum blockchain
- SmartMetrics: Metric suite for contracts
- SolVis: Visualization tool for Solidity contracts
- BcModel: Modeling tools & practices for BOS

What is Blockchain? From an User's Perspective

- An open distributed Ledger that promotes privacy



Blocks



Blockchain Use Cases

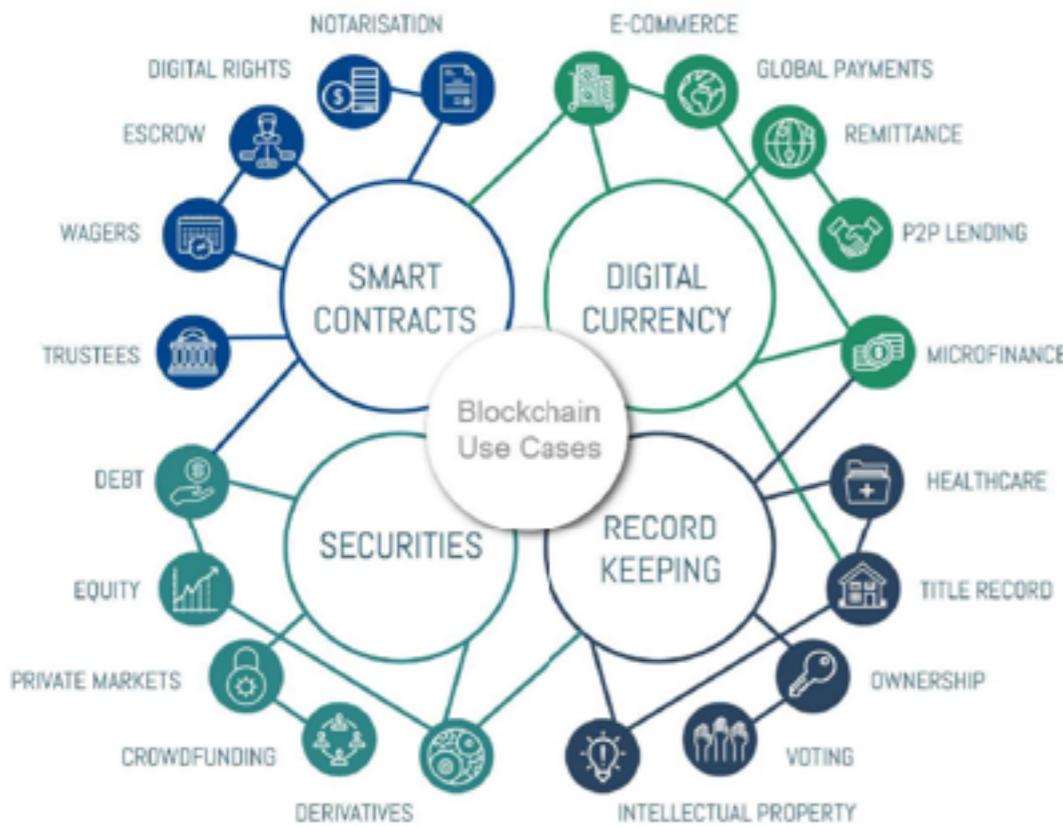
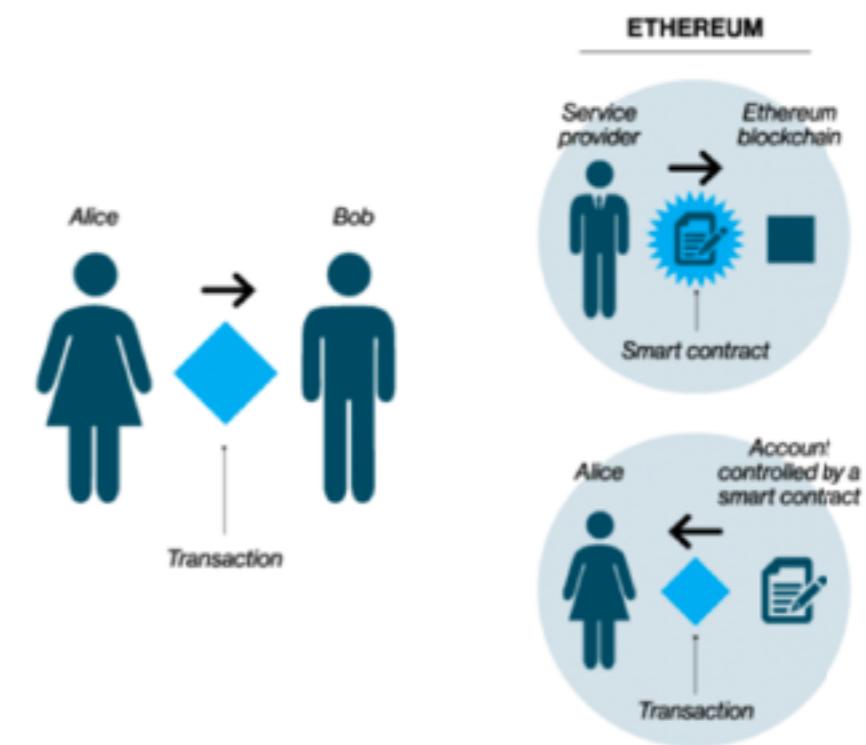


Diagram Contract Interaction



Thanks... questions?