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 Cyrptocurrency” 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.

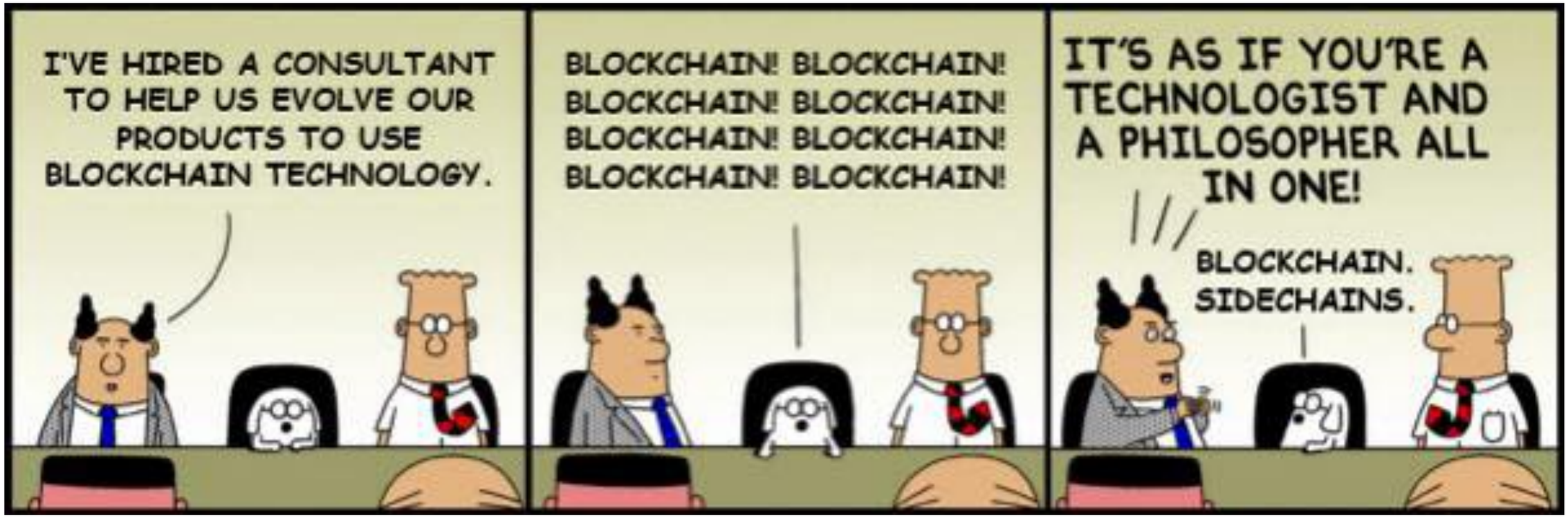
- **2nd part** (14:00 — 15:30): Hands-on practices in the lab with Smart Contracts.

- 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


I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
S. Adams E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.

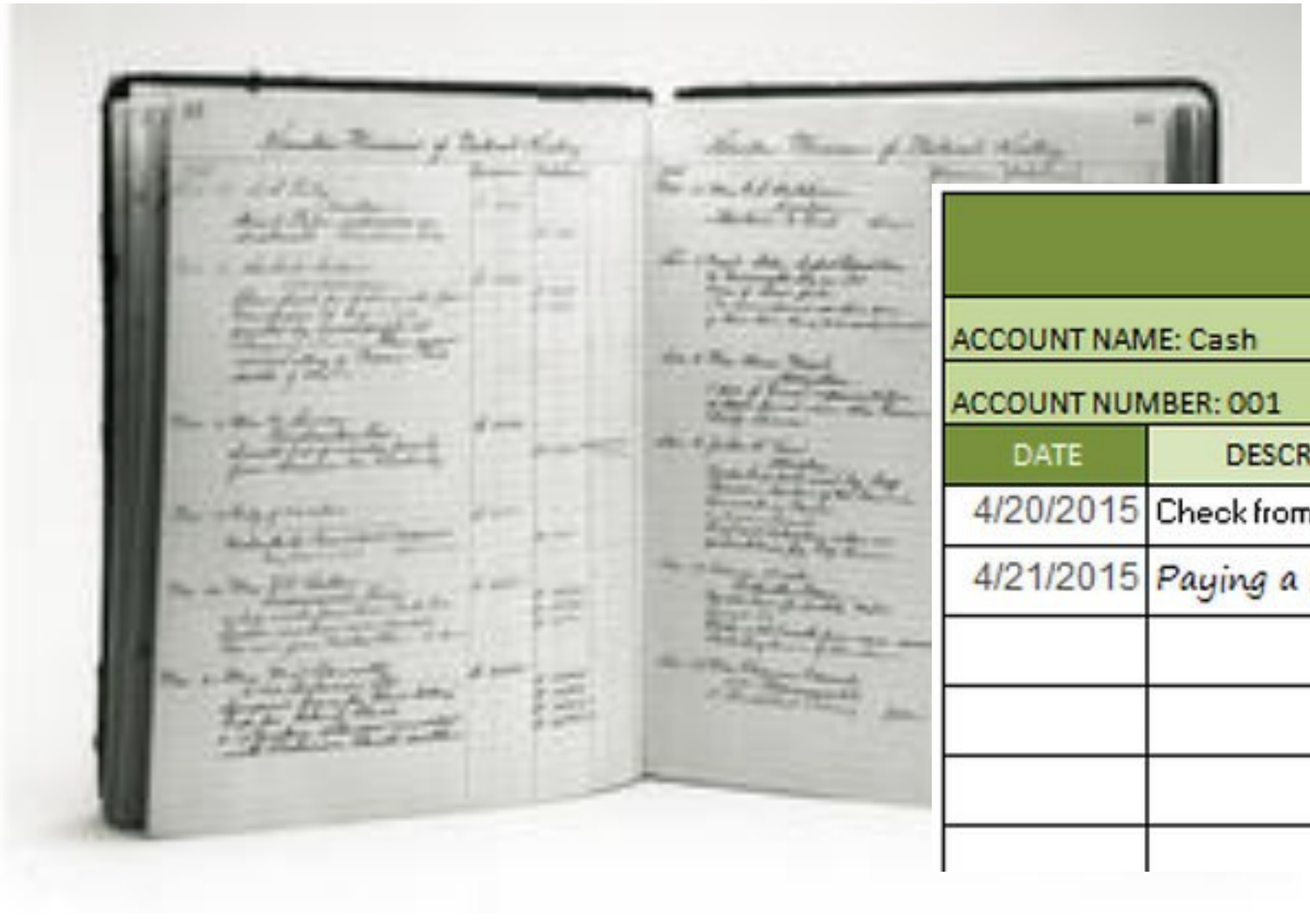

I'VE HIRED A CONSULTANT TO HELP US EVOLVE OUR PRODUCTS TO USE BLOCKCHAIN TECHNOLOGY.
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
BLOCKCHAIN! BLOCKCHAIN!
IT'S AS IF YOU'RE A TECHNOLOGIST AND A PHILOSOPHER ALL IN ONE!
BLOCKCHAIN. SIDECHAINS.

What is Blockchain?

Examples of Blockchain Technologies

What is Blockchain?
From an User's Perspective

- An open distributed Ledger that promotes privacy



GENERAL LEDGER

ACCOUNT NAME: Cash

ACCOUNT NUMBER: 001

DATE	DESCRIPTION	JOURNAL #	DEBIT	CREDIT	BALANCE
4/20/2015	Check from friend	J1	$ 500.00		$500.00
4/21/2015	*Paying a friend*	J1		$ 200.00	$300.00

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

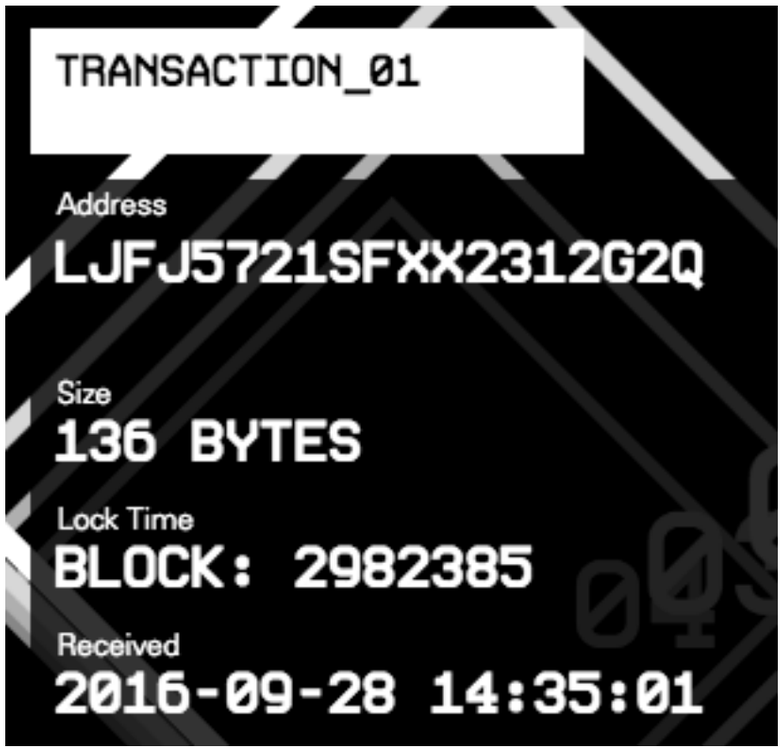
  - Distributed - the ledger is shared and synchronized among several "people"

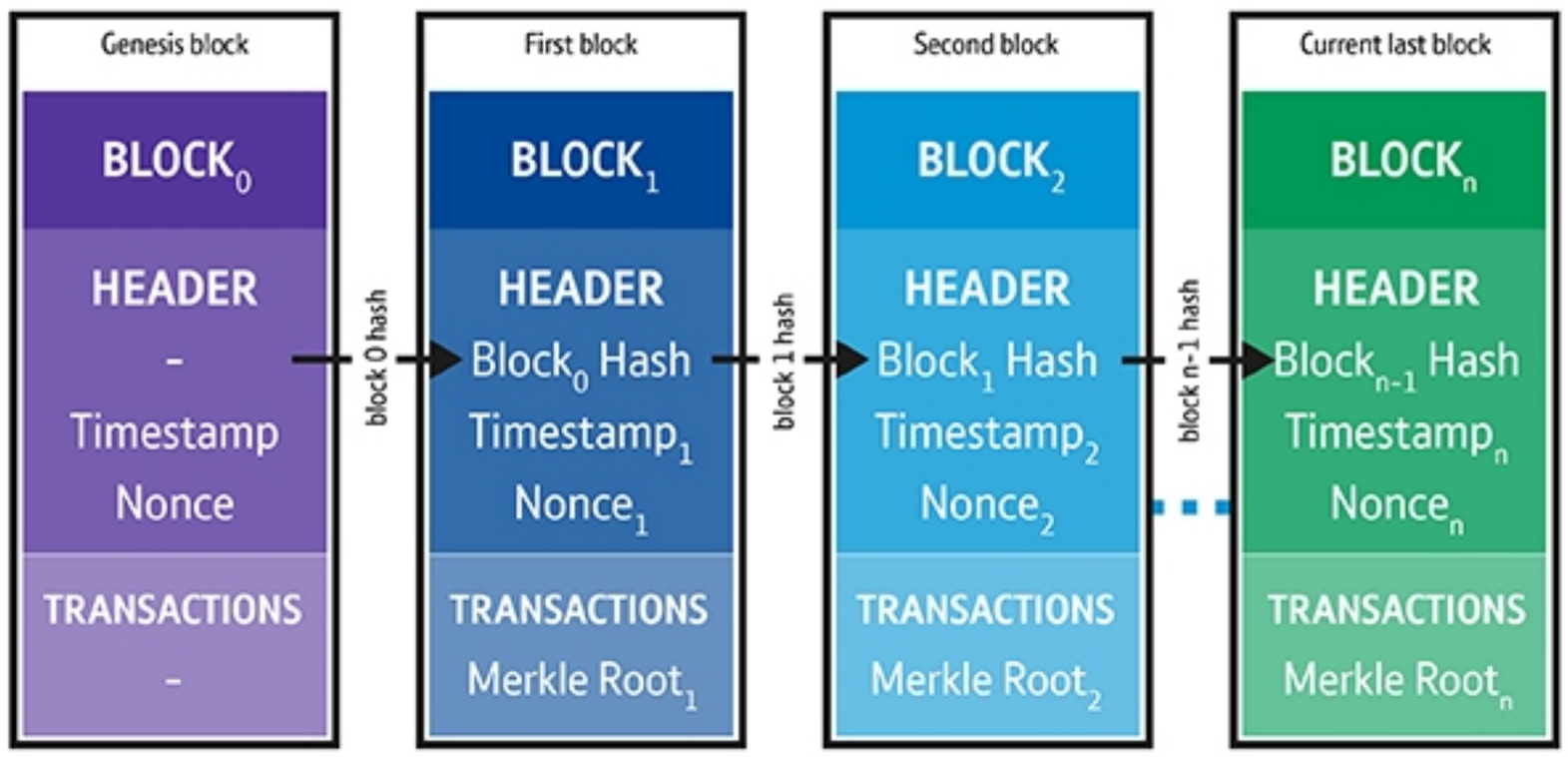
  - Privacy - the ledger transactions promote anonymity

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 possibilites
- "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

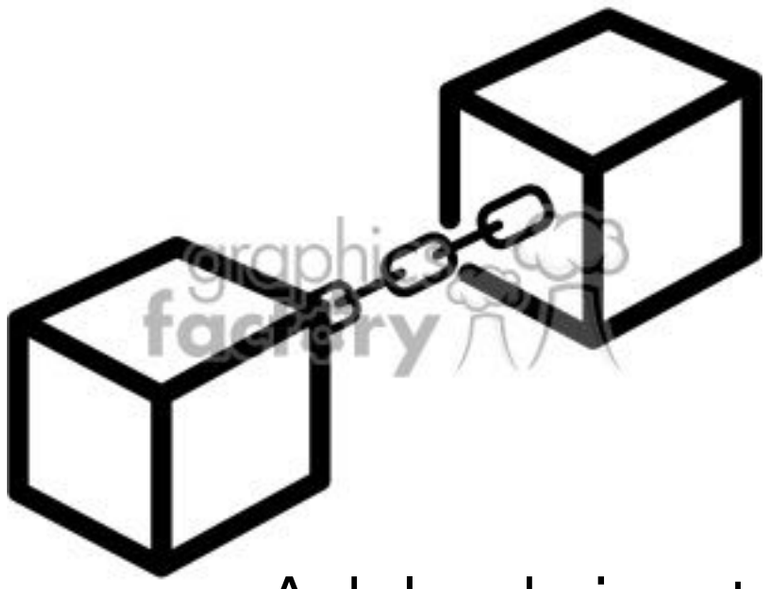
- We need an account to interact with the blockchain
- Roughly, an account's id/address is a public key and whoever holds the private key owns it.
- For example see: <https://etherscan.io/accounts>

Transactions

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

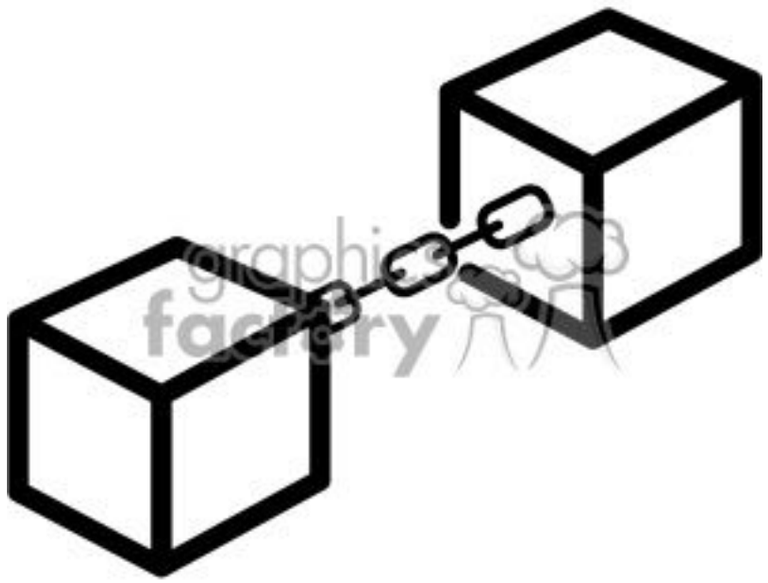
The information on transactions is public to everyone on the blockchain.

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



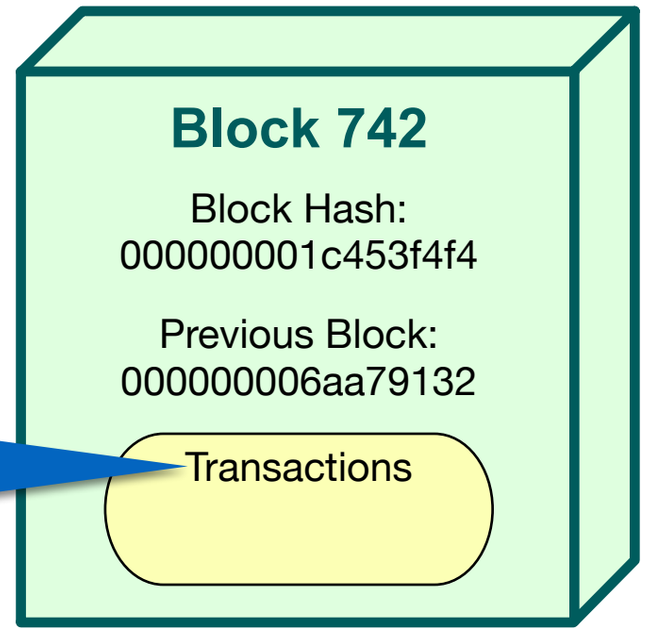
Blocks

- 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

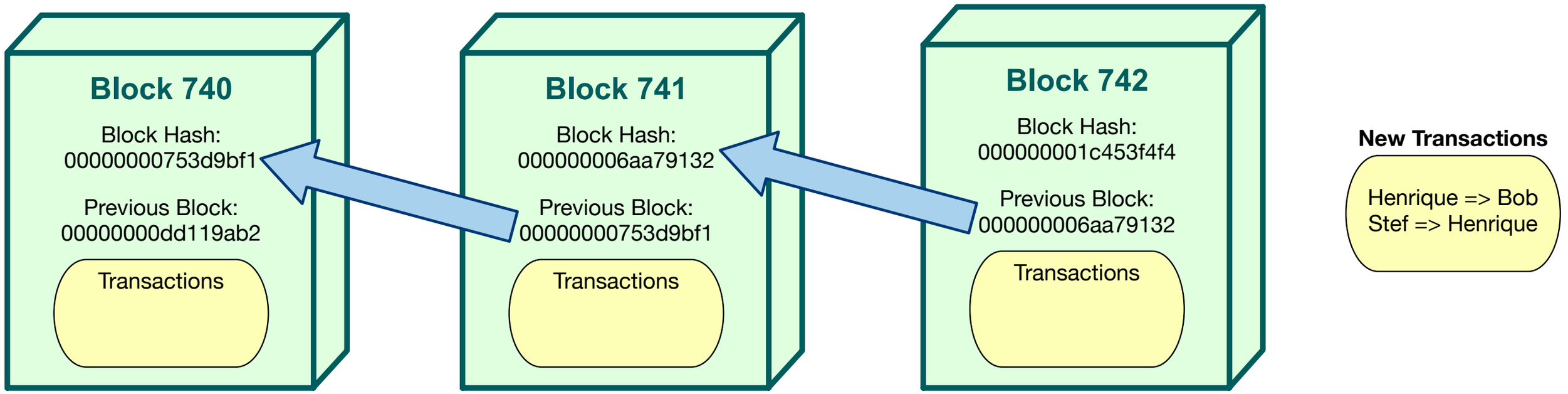
T.hash	From	To	Value
0x01…	0xFA…	0x9E…	25
0x22…	0x9E…	0x2F…	0
0xC3…	0x9E…	0x77…	7



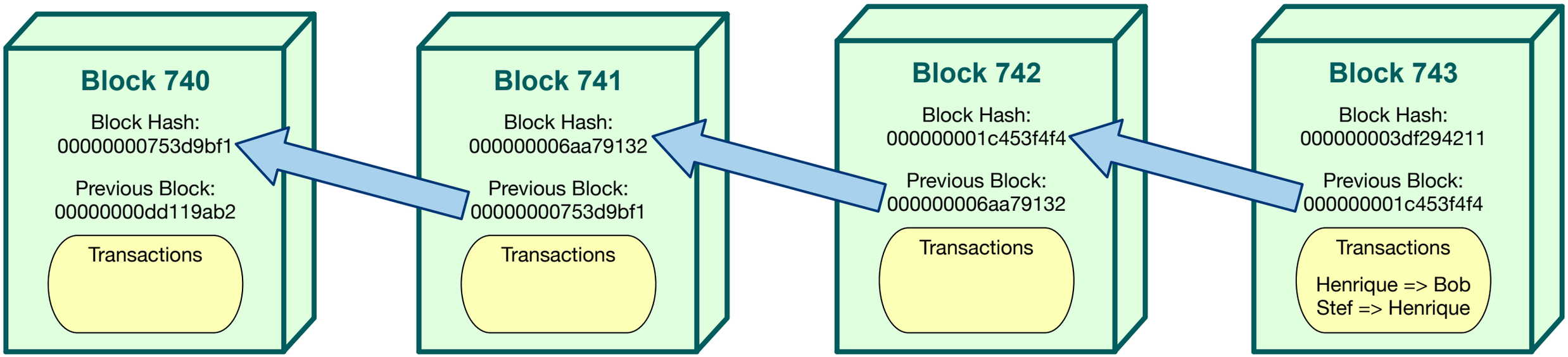
How are the Blocks Linked?

- The blocks are linked by a **Hash** number
    - When a new block arrieves, 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/>

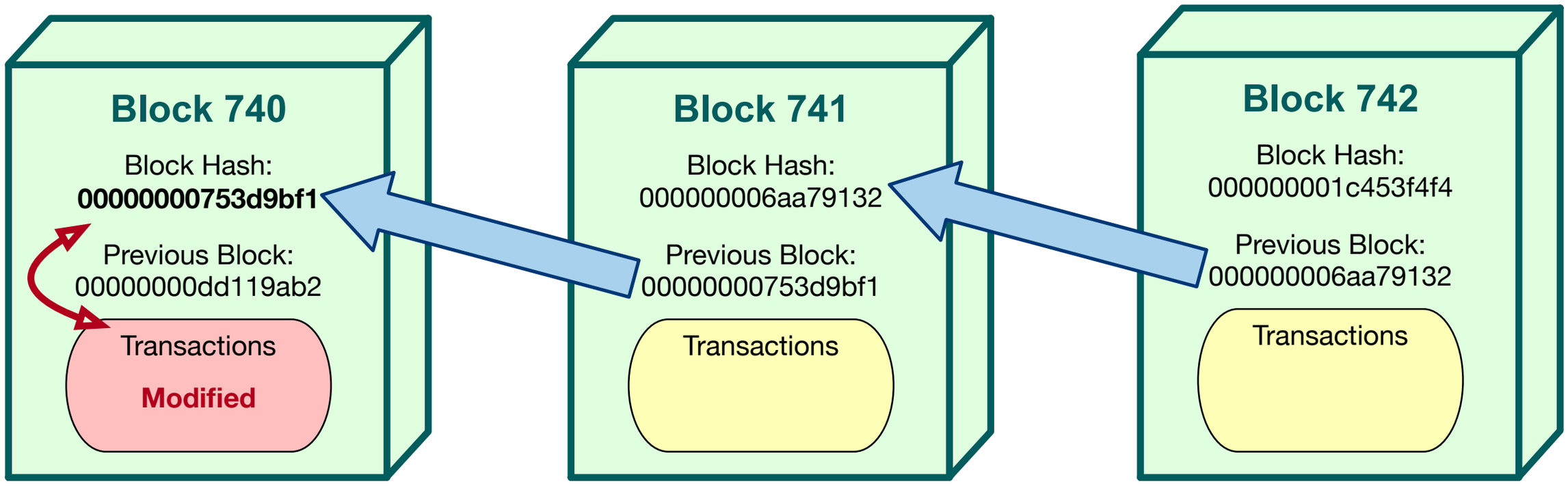
Ethereum varies according to the gas price, but the average time is ~0.24 min

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

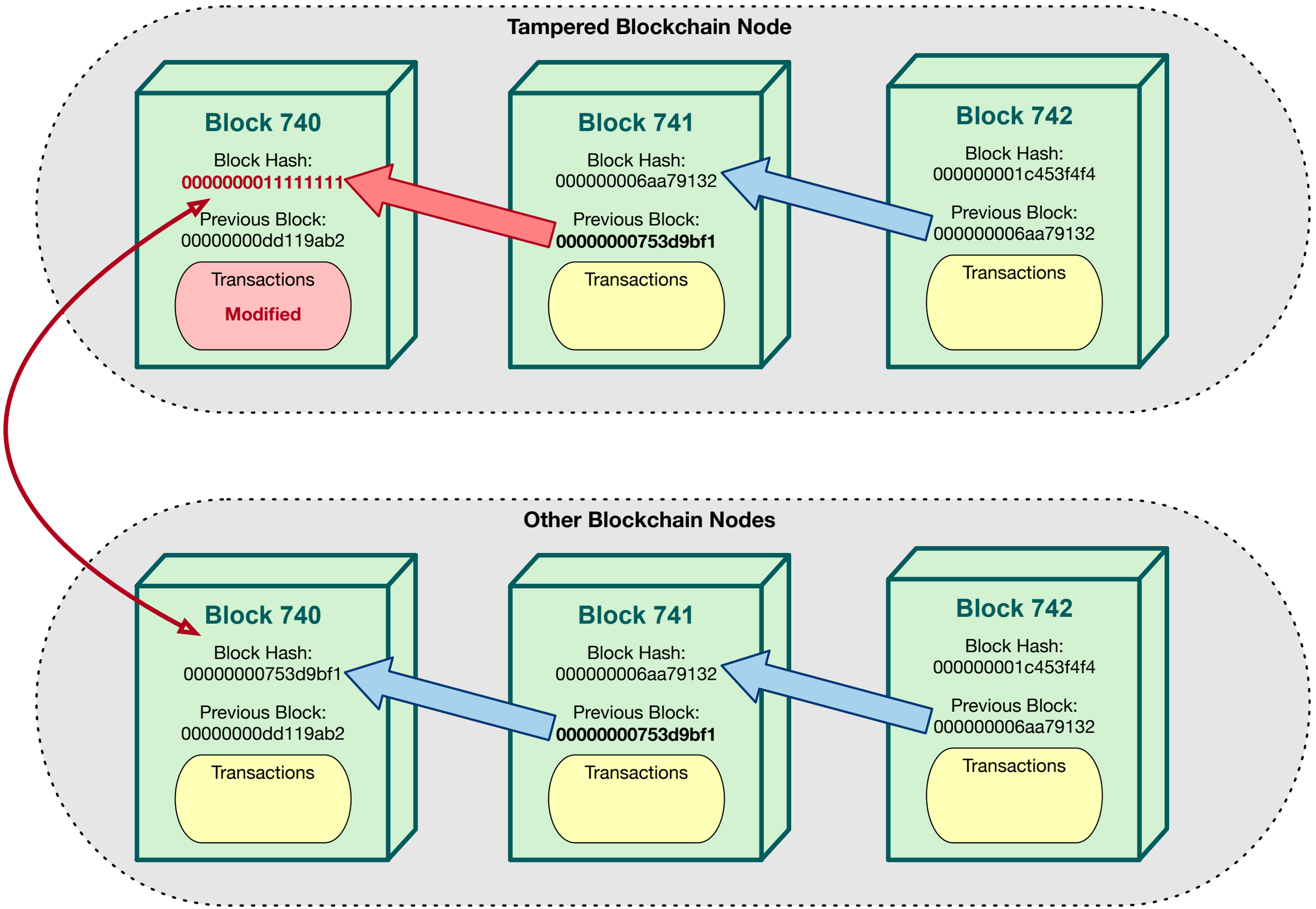
What if…  Someone Tampers the Blocks?

- 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 in Blockchain

- 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)

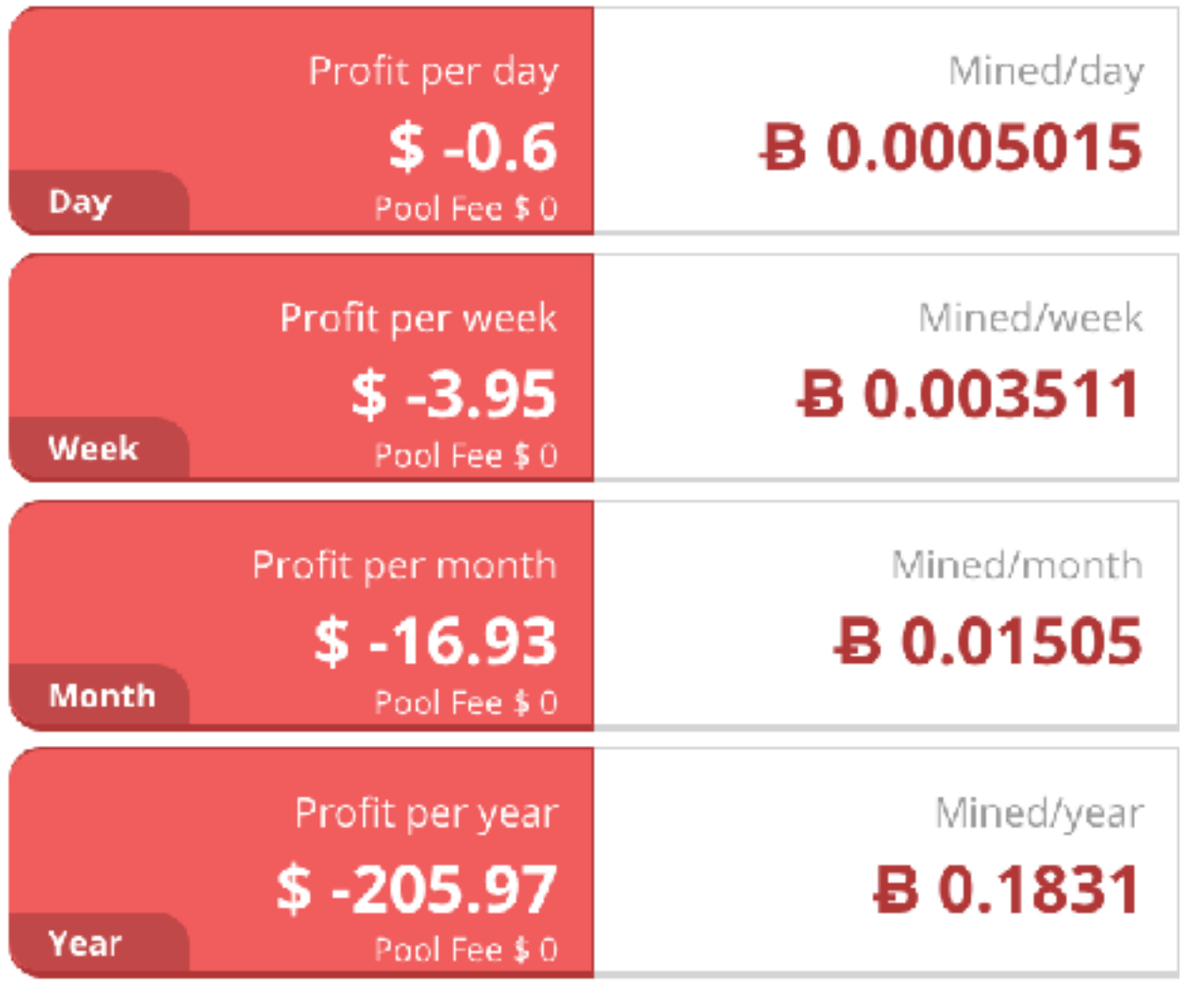
- The goal is to find an acceptable Hash number
  - Use SHA-256 on the new block, the previous block hash, and a seed number (called nonce)
  - If SHA-256 outputs a hash with a required number of leading zeroes you solved the puzzle.
  - Otherwise, increment the seed and try again.
  - The faster you 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 evergy 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 thats not counting the hardware cost.



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

Ethereum PoW

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

- Ethereum uses a different PoW, called Ethash.
  - Ethereum PoW discourages “Mining Farms” 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?

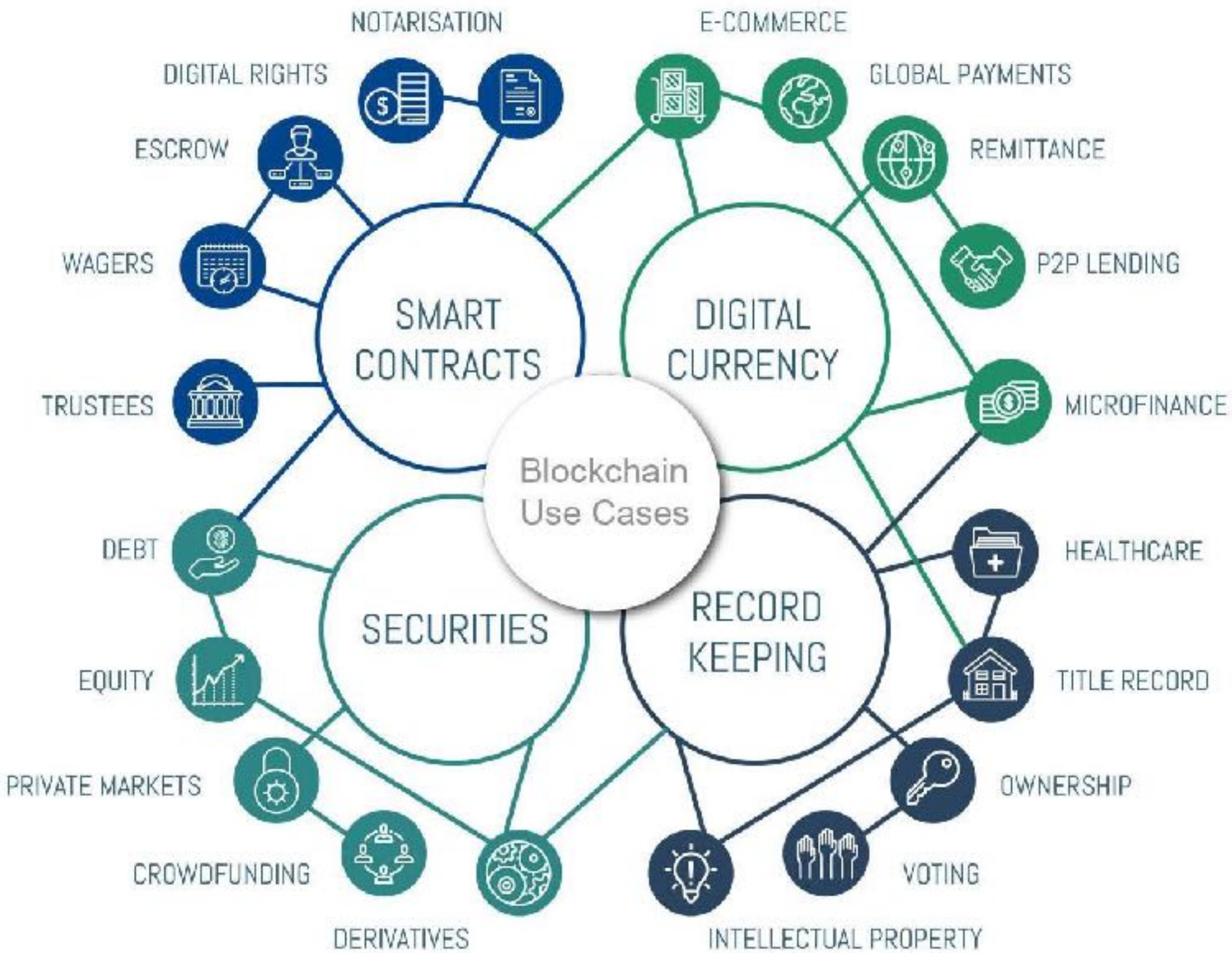
Can We Trust Miners?

Short answer: No!

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

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE

A smart contract-based blockchain is being used by insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM

HYPERLEDGER

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM

Walmart

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy.**

PROPY

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY OF PUBLIC REGISTRY

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING

New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT

Waltonchain is using RFID technology to store waste management data on the blockchain in China.

ENERGY

Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC.

DIAMONDS

The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers

FINE ART

By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY

For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM

In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network.**

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE

COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS

Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

HOBOTPAHC

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google

Alphabet

MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

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”

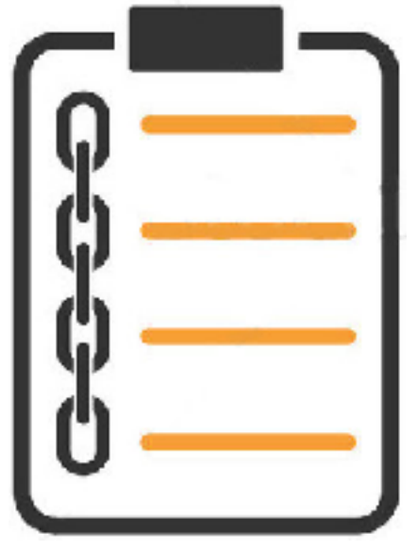
- They are more like “autonomous agents” that live inside the blockchain

- 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.

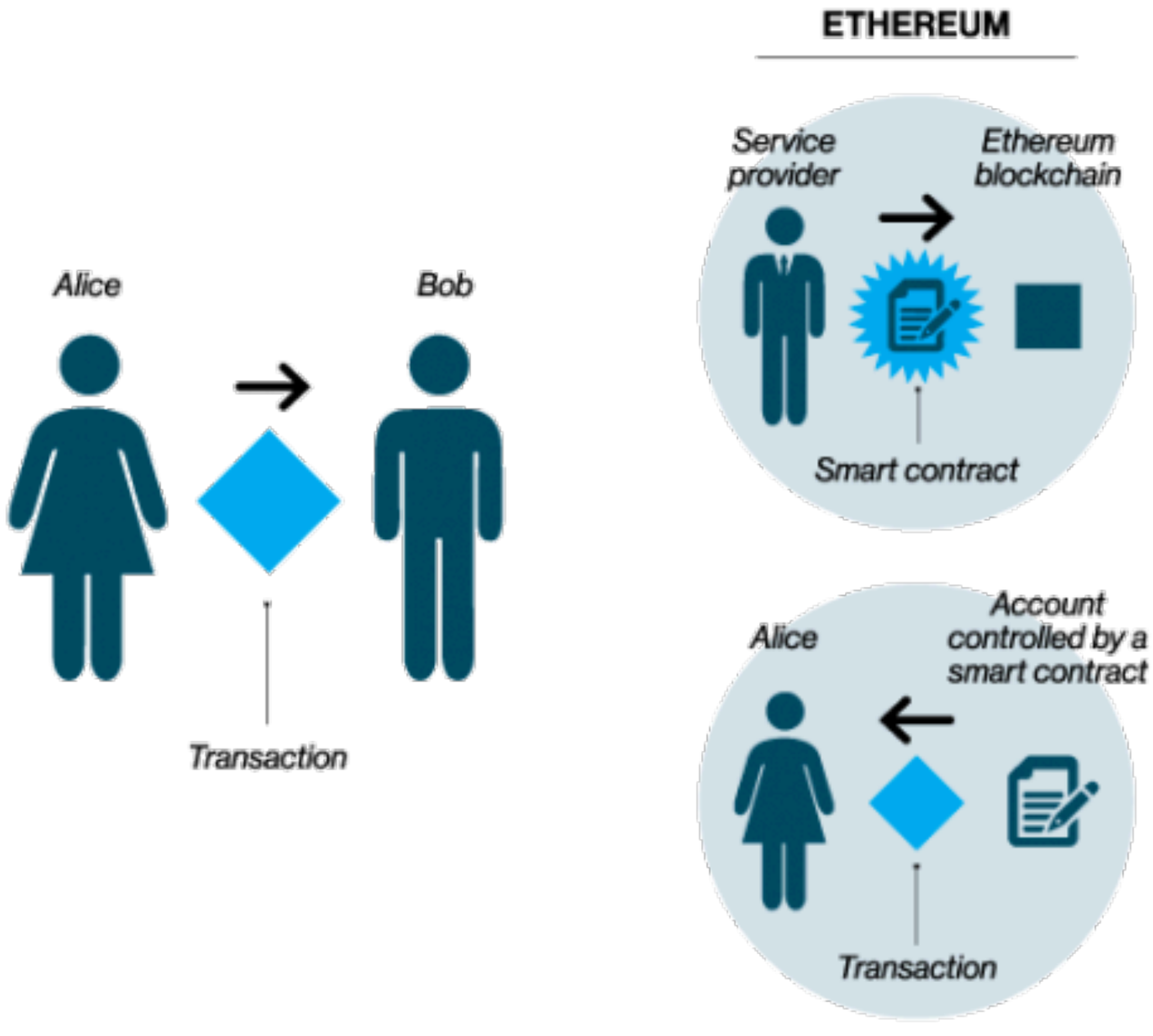
- Transactions created by function execution.

- 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

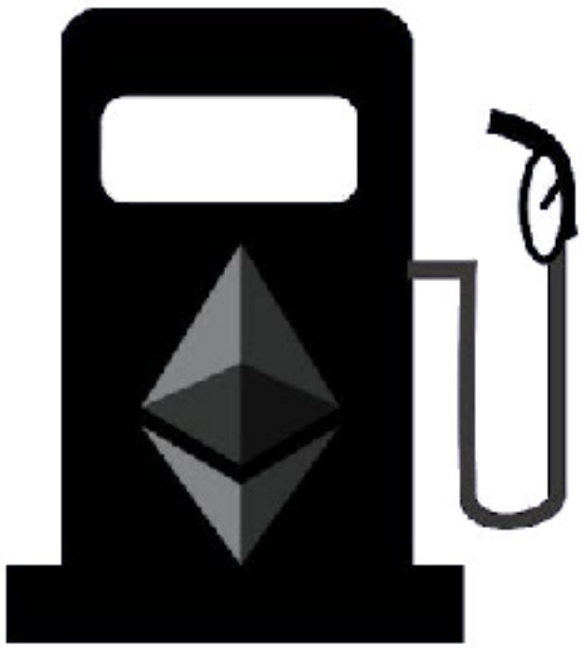


Security on Contracts

- 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.

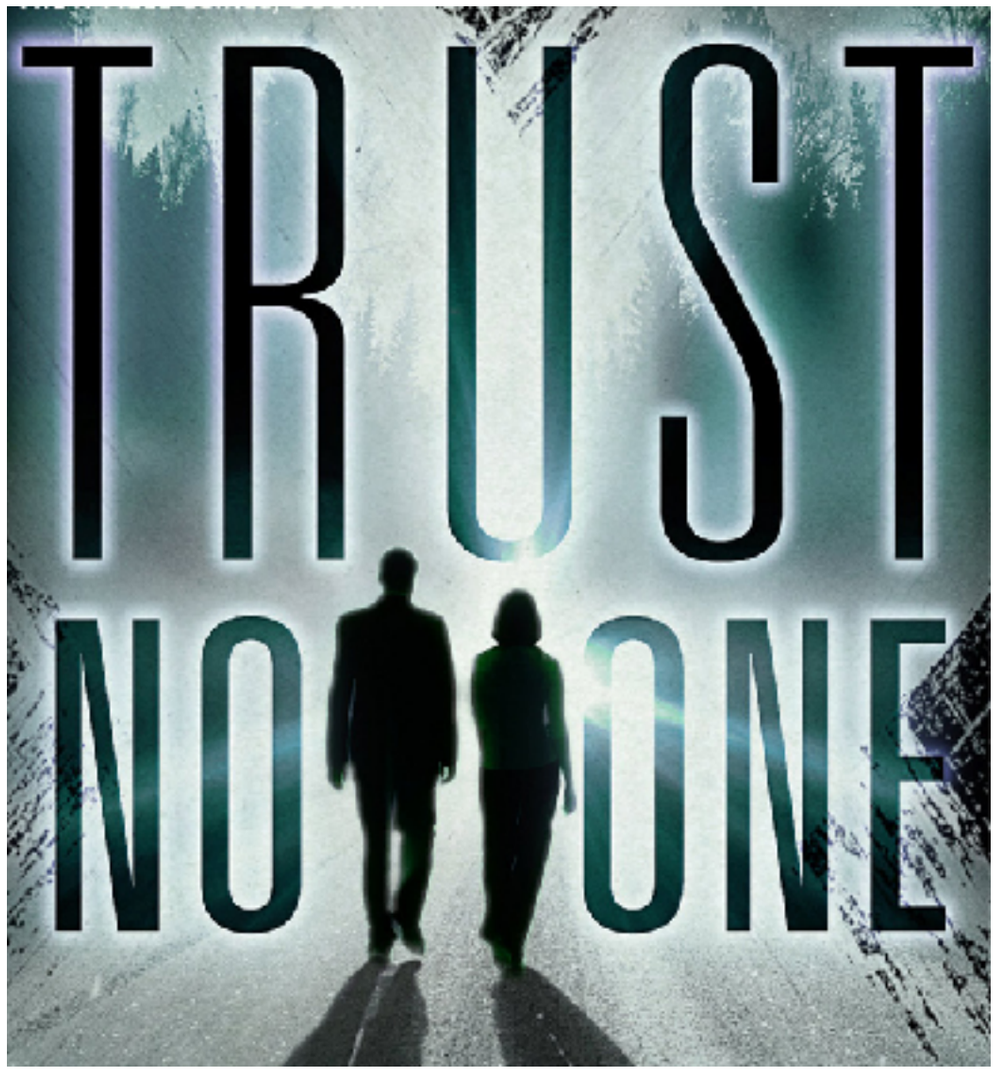
- Every transaction is charged an amount of Gas.
  The idea is to avoid infinite loops (and DoS attacks), encourage efficient code, and make users pay for the resources they use (bandwidth, CPU, storage).

- Gas has an Wei (Ether) cost adjusted by the user using the transaction. The Miner is awarded the gas price.

- If gas is insuficient 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?

- Remix is a browser IDE for Solidity (Compiler, Debugger, Runtime Enviroments, etc.)

- Ganache is a runtime enviroment to create a personal Ethereum blockchain.

- Etherscan is an Ethereum explorer and analytics platform.

Blockchain Research

BOS

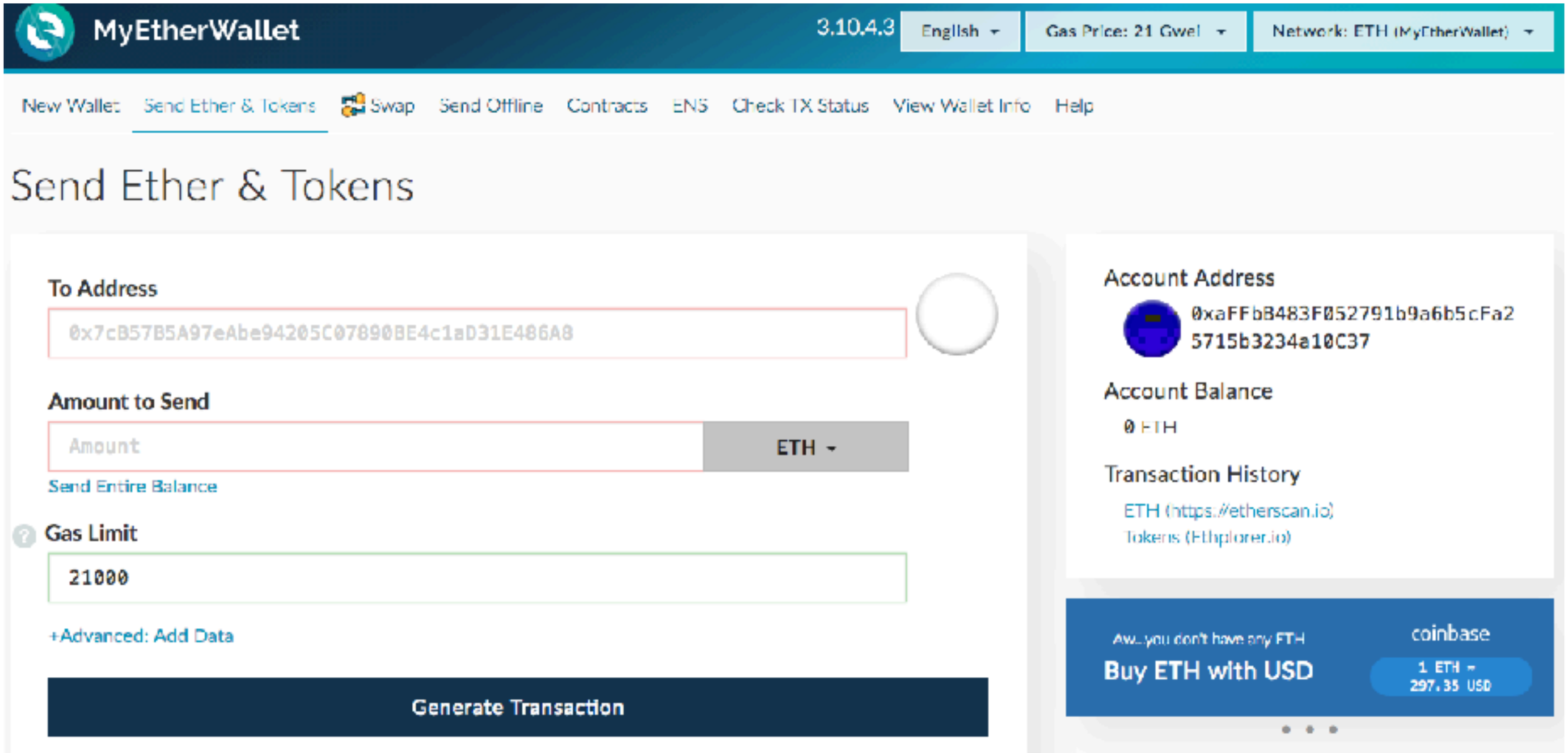
- **B**lockchain-**O**riented **S**oftware (BOS) is a software interacting with blockchain [Porru et al., 2017]

  - Usually, it is 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.



BOS: Catalizr

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

BOSE

- **B**lockchain-**O**riented **S**oftware **E**ngineering (BOSE)
- New research field, appling software engineering techniques and practices to BOS.

Opportunities for Improvement

- Resources Optimization (e.g., gas, storage)
- Coding Recommendations (e.g., prevent programming flaws)
- Vizualization (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)

Issues & Pitfalls

- Blockchain still is a new technology therefore be prepared when doing research that:
  - Few and sparse papers
  - Lack of specific venues to publish
  - Lack of experience/knowledge from general users

Papers to start your Research

- Luu et al., 2016. **Making Smart Contracts Smarter.** In 2016 ACM SIGSAC 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 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). p.283-295.

- Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, [online] Available: bitcoin.org.

- "Ethereum's white paper", *Ethereum Foundation*, 2014, [online] Available: 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.

Thank you!
Questions?