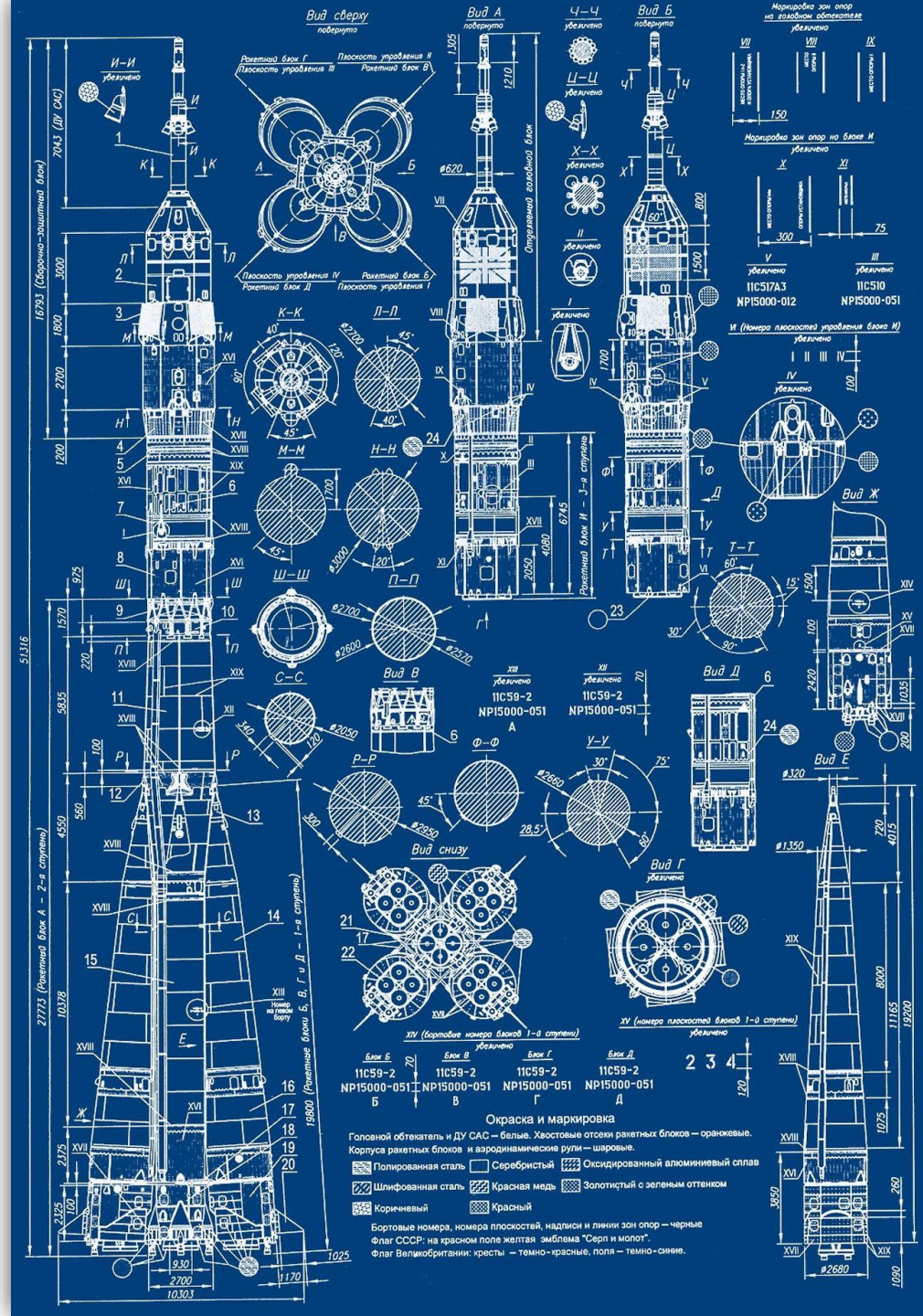
BCDV 1001
Intro to Blockchain
(prev. Blockchain Architecture BCDV 1003)

[WEEK 01 - LESSON 01]

Prof. Djordje (George) Petrovic
djordje.petrovic@georgebrown.ca

Summary

- Personal Introduction
- Course Evaluation
- Who should take this course
- Assignment & Use Cases
- What is covered vs. no covered in this course
- Myth vs. Reality
- Idea of Blockchain and 3rd party
- Problem Solved
- Byzantine General's Problem and PoW
- Centralized vs. Distributed vs. Decentralized
- Blockchain 1.0 2.0 3.0
- Transaction process explained from 100,000 ft – 10,000 ft – 1,000ft
- Block - Hash, Merkel Root, Difficulty Target, Nonce, Transactions, Coinbase…
- Consensus Mechanisms /PoW
- Smart Contracts
- Use Case Sample
- Further Readings and Resources

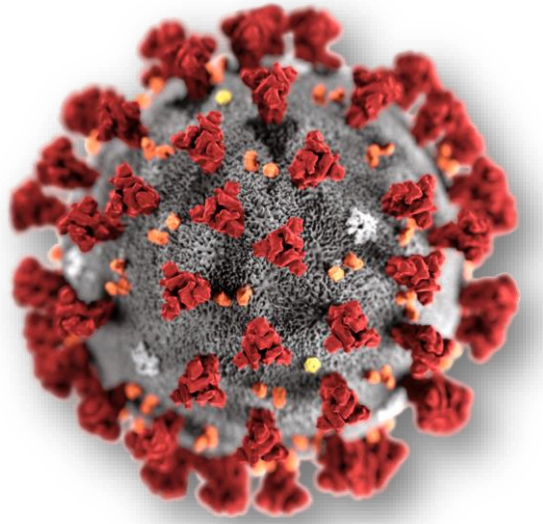


EVALUATION SYSTEM

- Participation: (class & updates) **10%**
- Lab Exercises: 5 @ 3% each >> total of **15%**
- Lab Tests: 5 @ 3% each >> total of **15%**
- Assignment: (groups of 2, 3 up to 4): **30%**
- Final Exam: **30%**

- Important to attend all classes as big chunk of your mark is the assignment and the final exam, which we work on and prepare each class.
- 4-week course consists of six 4-hour sessions (last two classes reserved for your assignment presentation and final exam).

UPDATE to the course



- With COVID-19 our course has moved online;
- This course is the foundation for the rest of your courses;
- The content of the course is related to your assignment and thus important to attend all classes, labs, test, follow links, etc.
- Students will pick a real life problem (in any industry) and the course will help you develop a solution incorporating blockchain technology;
- Students are encourage to research on topic covered in class as much as possible.
- 10,000 feet vs. 10 feet

Who has completed this course…

- Programmers | Engineers | Human Resources | Criminology | Teachers | Computer Scientists | Government employees | Banking and Financial Industry | Architects | Construction | Entrepreneurs | +more

- From:

  Canada | USA | Russia | United Kingdom | France | Italy | Germany | China | Japan | South Korea | Brazil | Ukraine | Serbia | Singapore | Saudi Arabia | Pakistan | Turkey | Iran | Palestine | India | Mexico | Ecuador | Trinidad and Tobago | Philippines | Bangladesh | Zambia | Barbados | Armenia | +more

- ***Point to be made*** *– blockchain will impact every profession everywhere around the world, thus people that take this course come from diverse professional and cultural background. Getting ready to what is to come!*

Assignment

1/2

- Pick on of the real world problems and design a solution for it using blockchain technology.
- Evaluate the requirements and challenges of the business network and participating entities that your solution will integrate with, and show the platform and consensus algorithm that are best suited to fit the overall architecture of your design.
- All of the use cases provided are legitimate problems that people are looking to solve as we speak, so this assignment can potentially be the starting point for a larger project that you continue to build on and refine as part of your assignment for the courses that a follow – and could even be something to carry on and develop as a personal project beyond the scope of the course should you feel passionate about it.

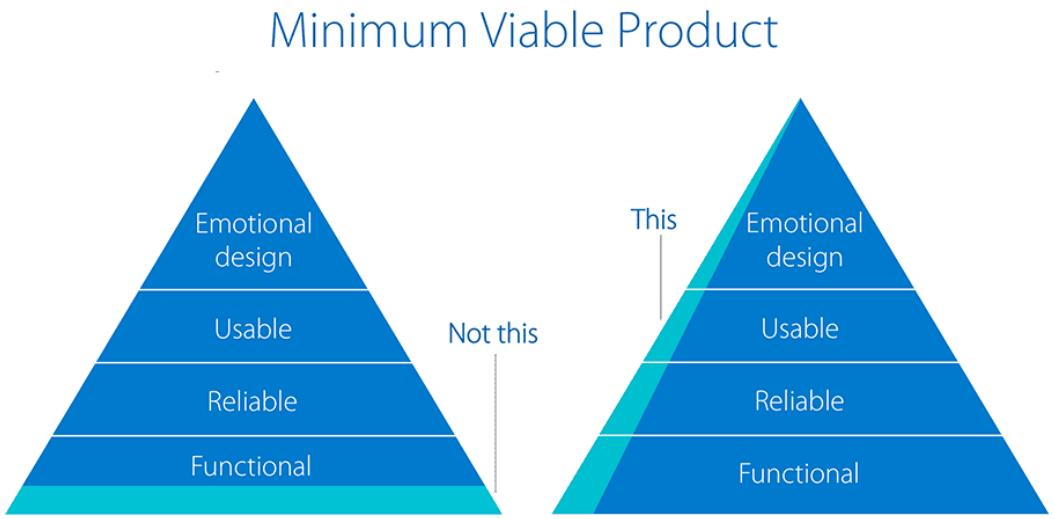
Assignment

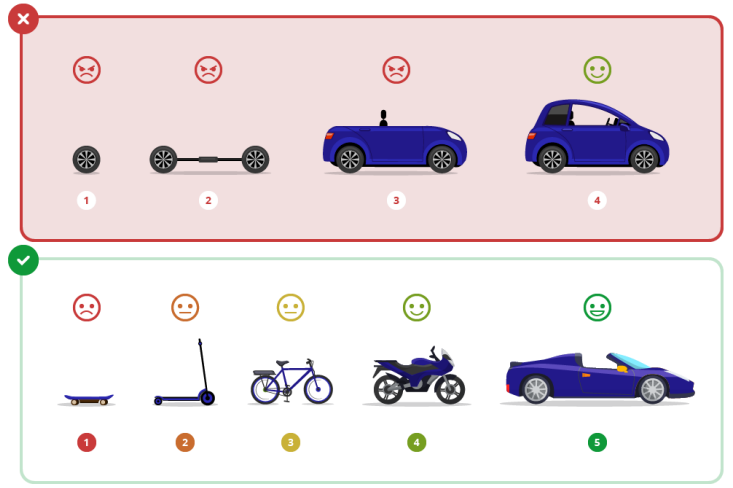
2/2

- There won’t be any development involved in this stage of the project, you’ll simply be thinking about the components parts of the overall solution, engaging in some creative problem solving, and design a **very high-level** architectural outline.
- You can think of this as a non-technical hackathon of sorts, and structure your project as though it was a startup.
- Your assignment should include a name for your platform, a brief write-up detailing the problem that you’re attempting to solve and why you chose to tackle this particular issue, and a wireframe diagram and description of the component parts and how they interact.
- **Presenting /Pitching your solution to the rest of the class on the final day!**

Your Vision? Your Path?

- Quiz / Labs / Assignments & Presentation / Final Exam – all connected
- What you do here for the assignment you can continue in the next courses… create a MVP – have a start-up idea and complete it.
- But, have in mind its better to work on multiple problems during your studying period at George Brown





Use Cases

[pick one per group]

SUPPLY CHAIN	Organic foods ◆ Clothing Industry – combating sweat shops and child labor ◆ Sustainable/eco friendly products and ingredients
IDENTITY	Solution for refugees ◆ Solution for combating sex slave trade ◆ Solution for individual to retain control of personal data
GAMING	Tradable tokenized assets ◆ Character achievements ◆ Upgradable digital content ◆ A “multiverse” of cross-platform content, characters, and worlds
DRM/DECENTRALIZED MARKETPLACES	Art ◆ Music ◆ Publishing
DIRECT DEMOCRACY PLATFORM	Voting on community issues ◆ Transparency for government spending
LAND REGISTRY	Transparent record of deed and land patent ownership
FINANCIAL	Social impact investment platform
HEALTH	Patient data ◆ Prescriptions
LOCATION and AUTOMATION	Tracking and Logistics
other	Please see the instructor for advice and consultation

INTRODUCTIONS

Be prepared to answer following questions:

- Where were you in 2009… when did you first time hear about it and by whom?
- **Past life** >> Educational and Professional experience…
- **Current life** >> Why am I involved now with blockchain?

Blockchain Terms

[start creating your slide with all the terms being used in the course]

Permissioned | Permission-less | Private | Public | Consortium/Hybrid | Consensus Mechanisms| PoW | PoS | PoET | BFT | Centralized | Distributed | Decentralized | Hyperledger | Ethereum | Bitcoin | Hash | Merkel Tree/Root | P2P | 51% Attack | Blockchain 1.0-2.0-3.0 | Sidechains | Oracle | Smart contract | Data storage |nonce | Coinbase transaction | on-chain vs off-chain | Immutable | DeFi | CBDC | Scalability | Forking | Open vs. Closed | Blockchain as a Service – BaaS | **+ more**

Not Covered in course but could be mentioned

- Regulatory & Legal advice
- Financial and Investment advice
- Political and social-economic views

*This program is tailored for **developers** but many have completed the programme and went on to have successful carriers in the blockchain industry as non-developers – this being said we will cover as much as possible beside already mentioned blockchain development.*

Myth vs. Reality

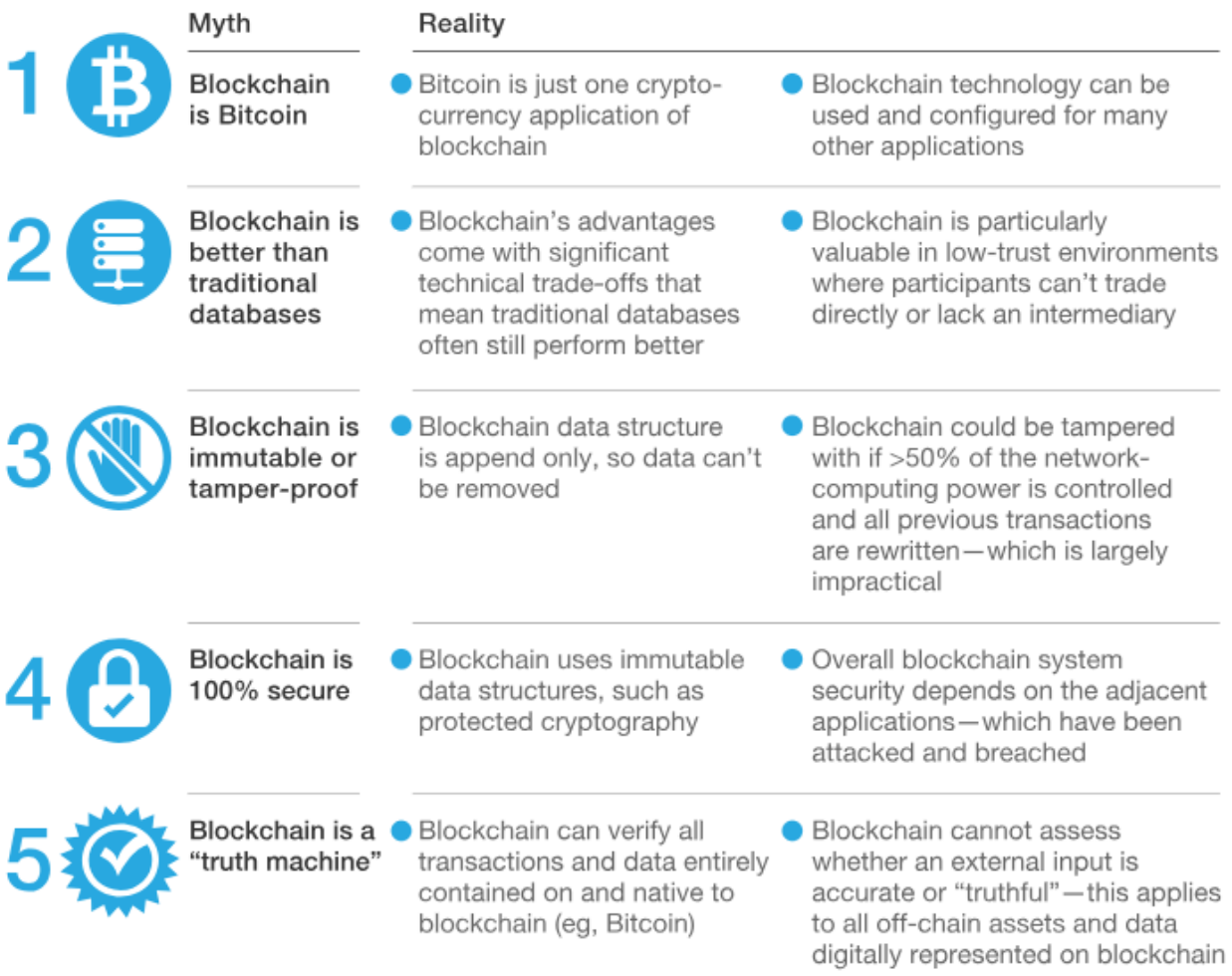
- Will Governments will disappear…
- Will Banks bankrupt…
- No more need for lawyers…
- Satoshi Nakamoto…

Blockchain

[Quick Recap]

- Five common blockchain myths create misconceptions about the advantages and limitations of the technology

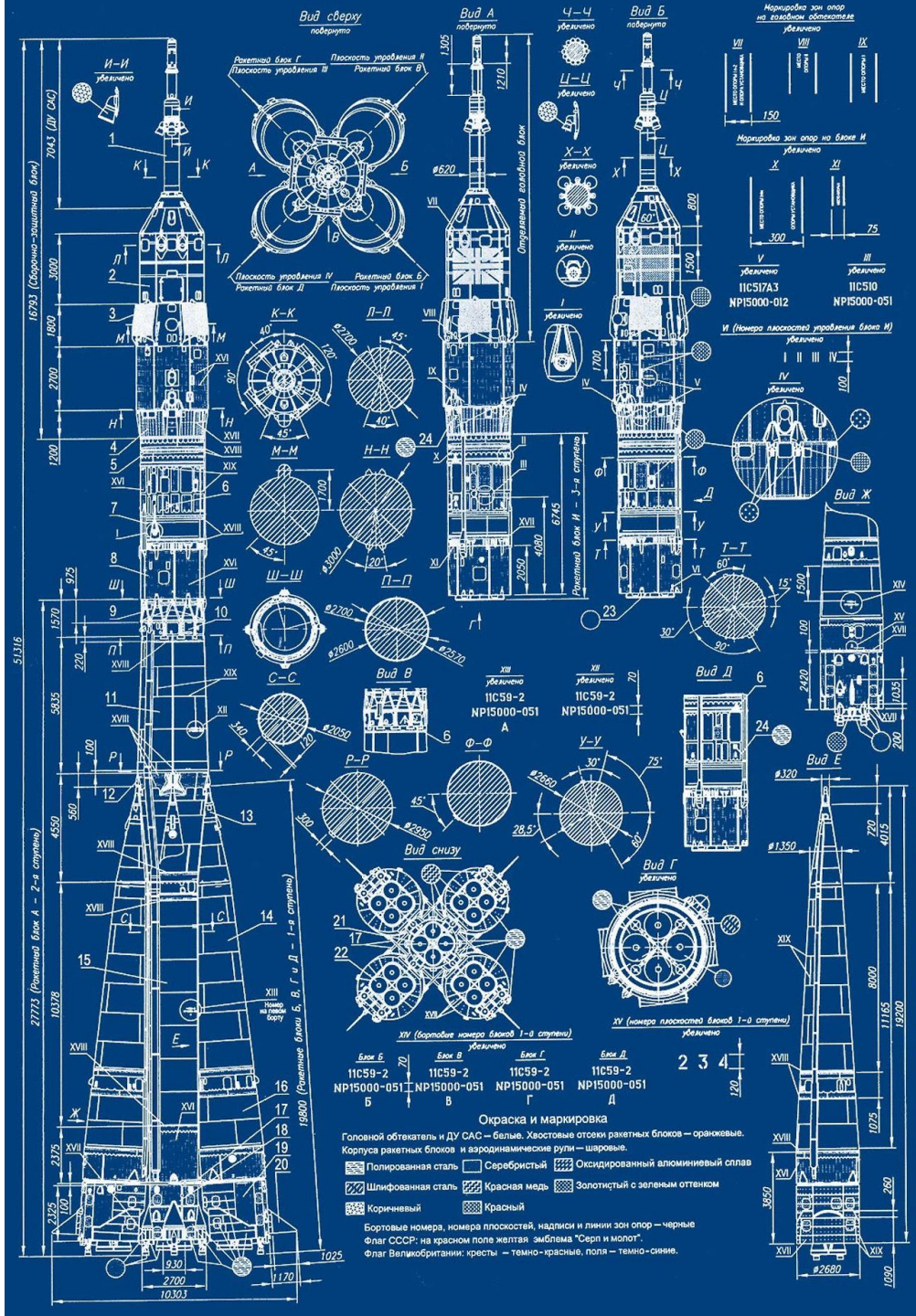
- bitcoin is not blockchain…
- **B**itcoin vs. **b**itcoin ???
- Blockchain is like hot sauce…
- Is it legal?




WELCOME
to the
BLOCKCHAIN
ENTERING A NEW ECONOMY

What will do is…

- Explain Blockchain…
- Find a problem and build a solution….
- Break blockchain into building blocks…
- Work on Blockchain Architecture…
- Look under the hood, and take things apart



One Step Back – 99 Forward…

- What is disruptive? Which tech is disruptive now or in the past?
- Is Distributed Ledger technology (DLT) same as Blockchain…
- Why blockchain?
- What is bitcoin, isn't it blockchain or blockchain is bitcoin?

The New Idea? Not really…

[economic point of view]

- Magazine - The Economist, publishes a paper in Jan 9, 1988; "**Get Ready for the New World Economy**";
  - *"THIRTY years from now, Americans, Japanese, Europeans, and people in many other rich countries, and some relatively poor ones will probably be paying for their shopping with the same currency."*
  - *"In time … its value against national currencies would cease to matter, because people would choose it for its convenience and the stability of its purchasing power."*
  - *"As telecommunications technology continues to advance, these transactions will be cheaper and faster still."*

- Friedrich Hayek (Nobel Prize in Economics), 1984 [link]
- Milton Friedman (Nobel Prize in Economics), 1999 [link]
- David Chaum (DigiCash), Wei Dai (B-money), Nick Szabo (Bit Gold)
- Last 25+ years there have been multiple attempts to solve what bitcoin did

BLOCKCHAIN

- Is it a new idea, a new tech? Bitcoin combines 3 distinct technologies:
  - **Game theory** (incentive to secure a network)
  - **P2P** (file sharing of a common ledger)
  - **Encryption**/Cryptography
- Blockchain 1.0 – the **killer app** called **bitcoin** – electronic money, also known as **crypto**.
- What is the problem that bitcoin solves and what did Satoshi Nakamoto succeed in? **bitcoin solves a mathematical problem**; the **double spend problem (reversibility of electronic payments) in a electronic network without a 3rd party (created decentralized system). It secures ownership of an digital asset via a distributed computation.**
- Why is it important? **Eliminates 3rd party**.

source: 'Mastering Bitcoin – programming the Open Blockchain' by Andreas M. Antonopoulos

Problems solved – the big solution

- A practical novel solution to a Distributed Computing Problem – known as "**The Byzantine Generals' Problem**" (PoW) – a mathematical problem solved;
- Uses **concept of Proof-of-Work to achieve a consensus without a central trusted authority**, represents a breakthrough in distributed computing and has wide applicability beyond currency;
- It can be used to achieve consensus on decentralized networks **to prove the fairness** of elections, lotteries, asset registries, digital notarization, and more.

BYZANTINE GENERALS PROBLEM

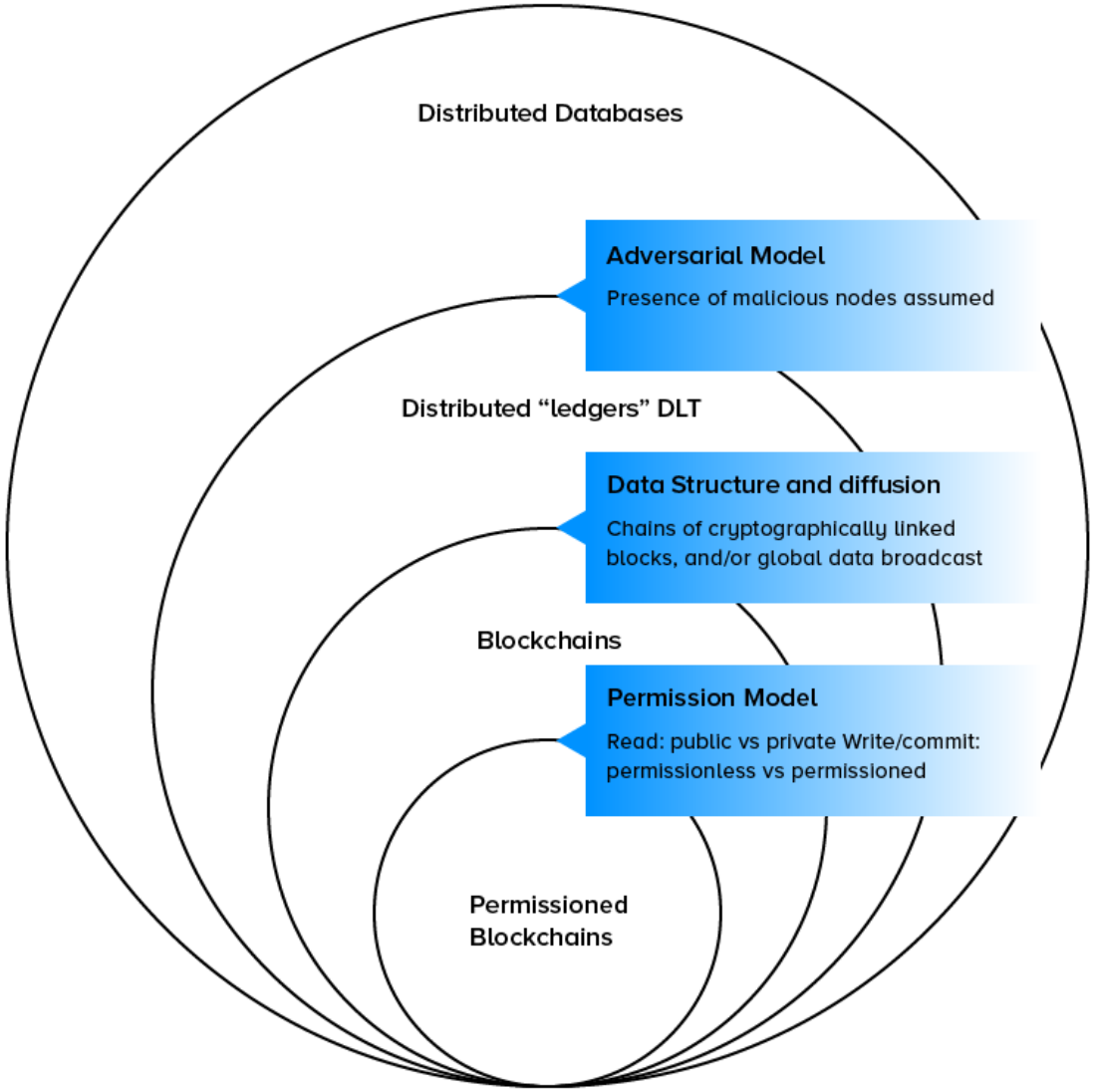
[BYZANTINE FAULT TOLERANCE / BFT]

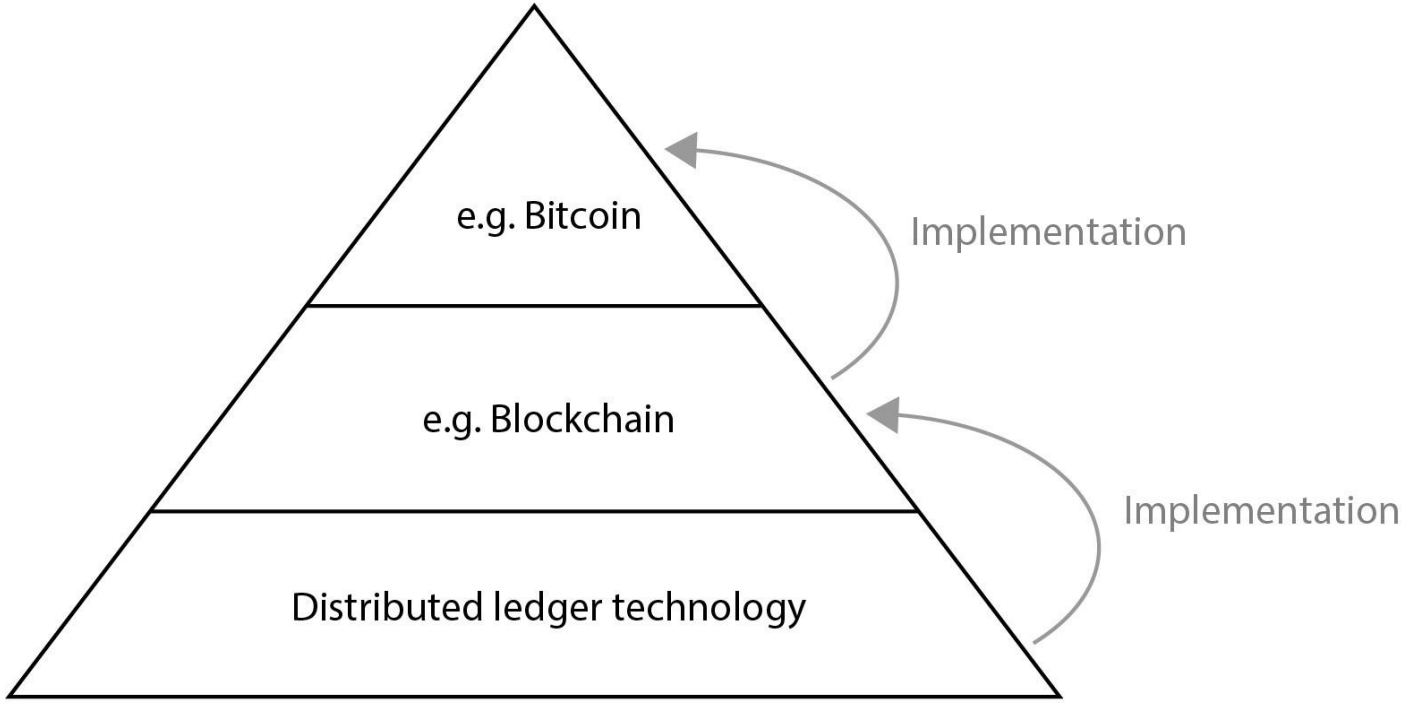
- Byzantine Fault Tolerance Explained [link]
- Marko Vukolic – PoW vs BFT [link]

- If *n* number of Byzantine generals are attacking an enemy city, then what is the maximum number of traitors that can be tolerated and the battle be won?

- If *n* number of nodes are misbehaving (fraudulent, hacked, etc.) towards a ledger, then what is the maximum number of different results and there is still a consensus on what is the true record on the ledger?

DLT vs. Blockchain



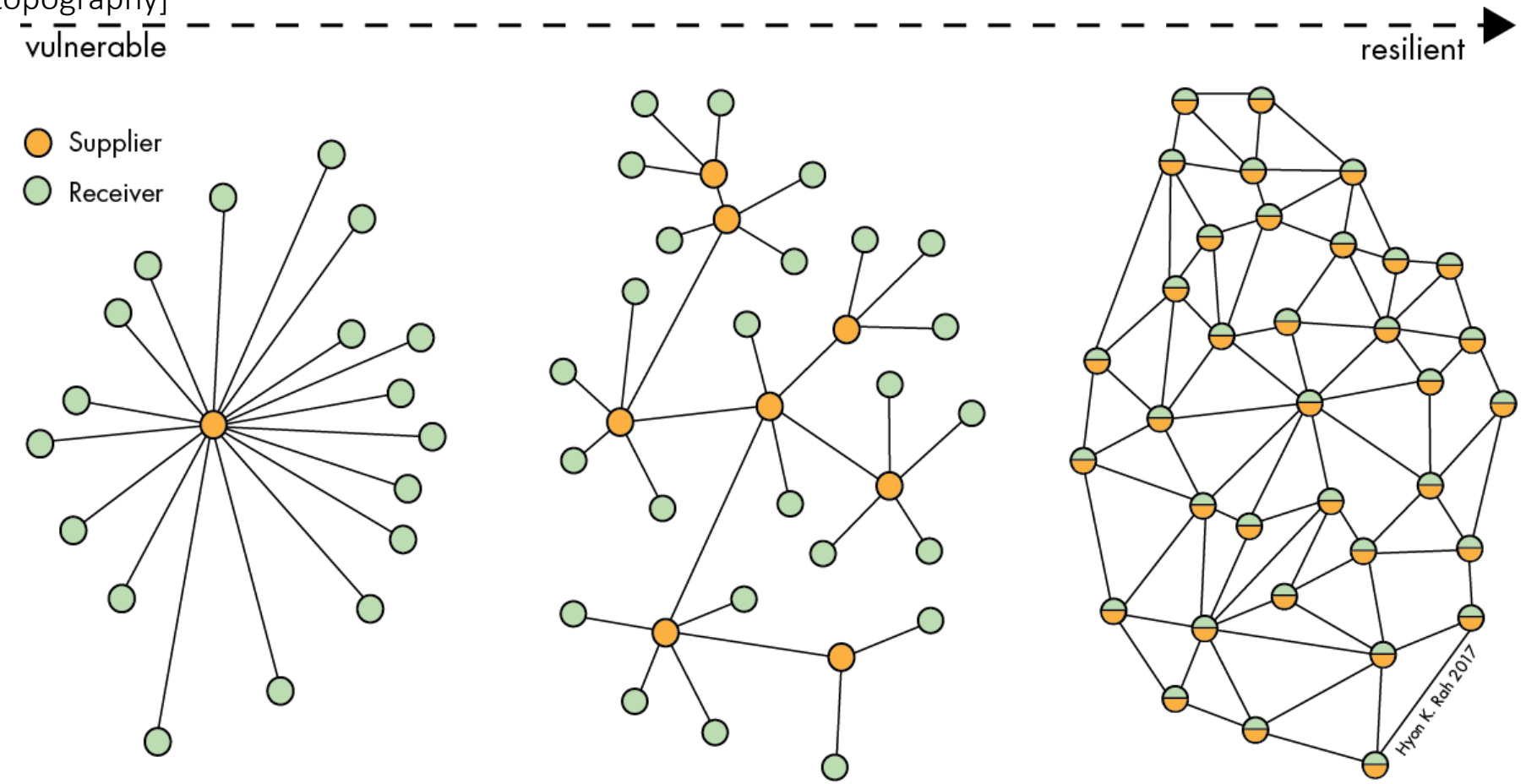


*Blockchain is implementation of DLT, just as email is implementation of internet.

If email was the killer app of internet, what is the killer app of blockchain, and does it exist yet?

Centralized vs Distributed vs Decentralized

[network topography]



A. Centralized System

Failure of the single supplier leads to the failure of the entire system

B. Decentralized System

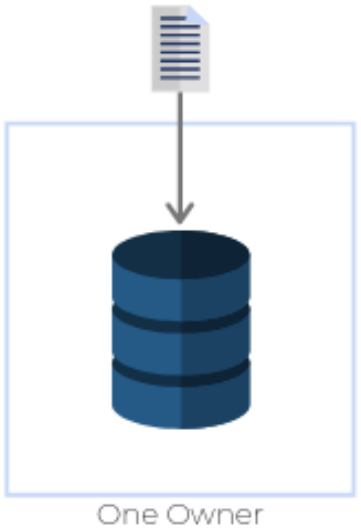
Failure of one supplier leads to localized failure; failure of all suppliers leads to system failure

C. Distributed System

Every node can supply to and receive from the other nodes; system failure cannot occur unless all nodes fail

Centralized vs Distributed vs Decentralized

[ledger]

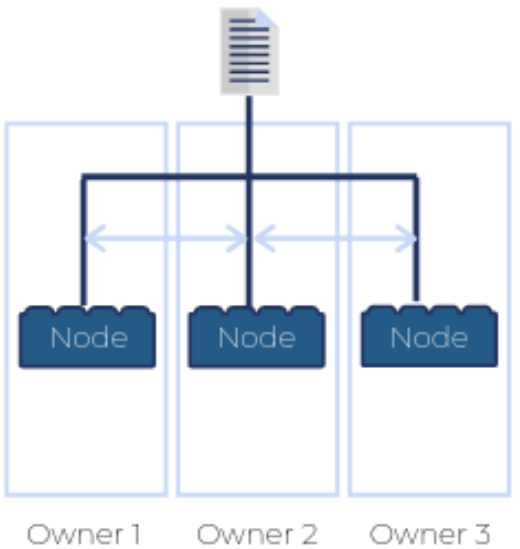


Centralized

- One database, one owner
- Example: Excel Spreadsheet
- Data was lost if owner left company or machine broke

Distributed

- Many database copies, but still one owner
- Example: Cloud Computing
- Is resilient to technical failure, but not to organizational



Decentralized

- Many database copies, everyone in the blockchain is an owner, no master
- Example: Blockchain
- Can withstand technical and organizational failure

Centralized vs Distributed vs Decentralized

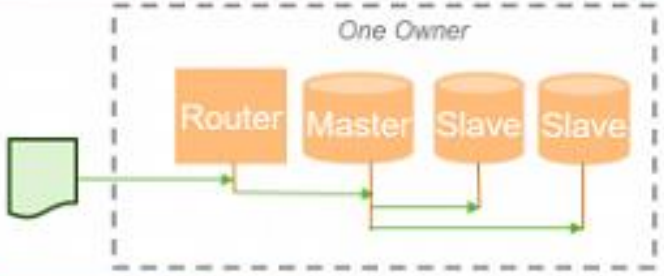
[ledger]

Centralized

- One database, one owner
- Not resilient to organizational failure
- Not resilient to technical failure

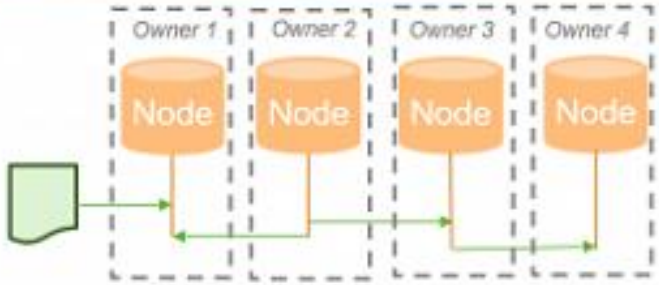
Distributed

- Many database copies, one owner
- Resilient to technical failure
- Not resilient to organizational failure



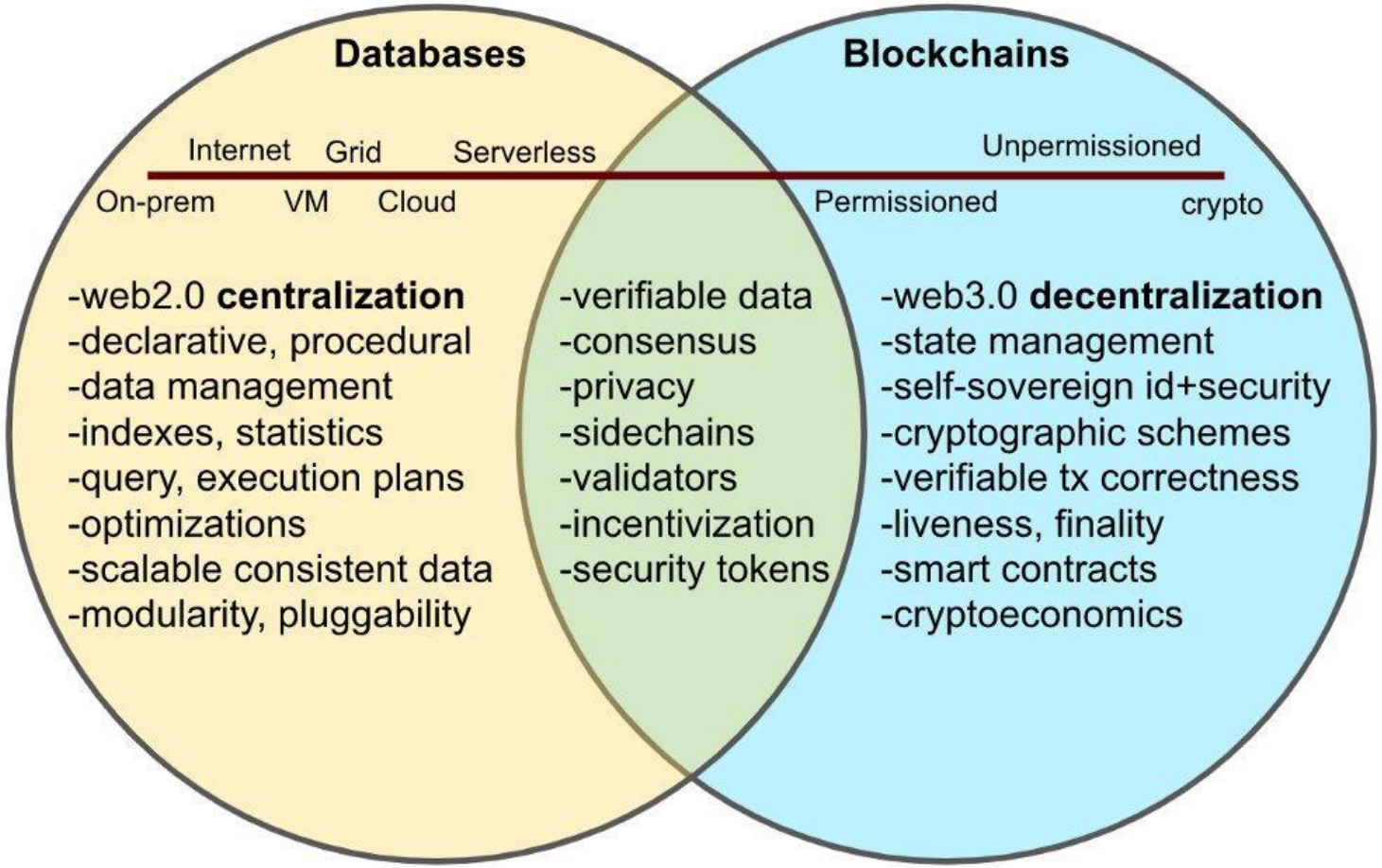
Decentralized

- Many database copies, many owners, no one “master”
- Resilient to technical failure
- Resilient to organizational failure



So what is Blockchain/Bitcoin?

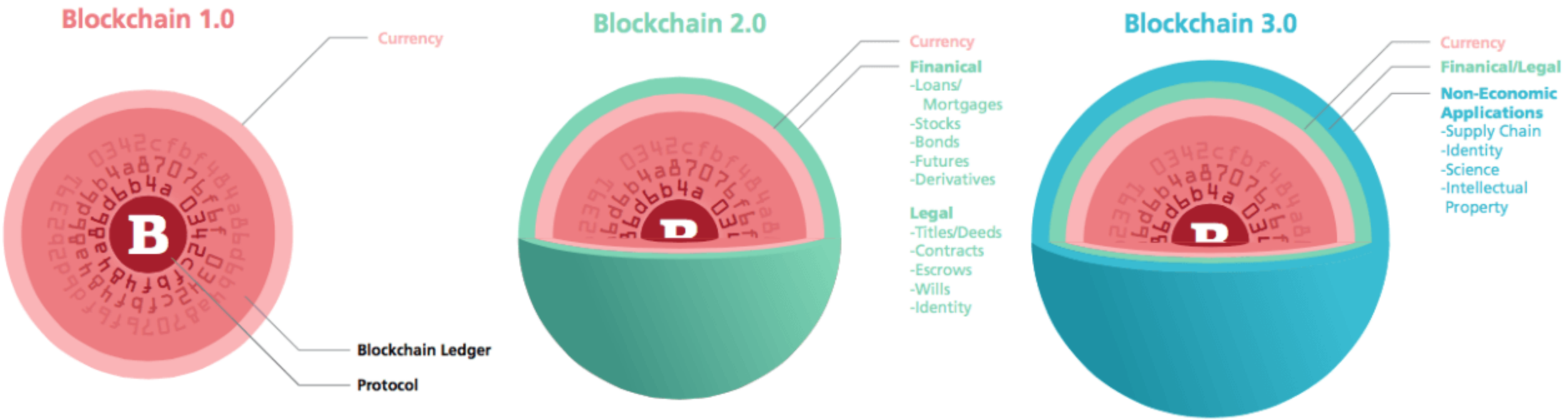
- Network Protocol
- Currency
- Database/Ledger



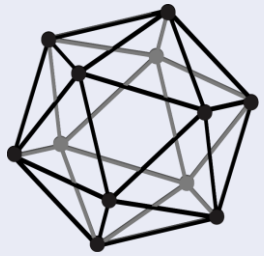
Bitcoin

- Consists of:
  - A **decentralized peer-to-peer network** (*the bitcoin protocol*);
  - A public transaction **ledger** (*the blockchain*);
  - A **set of rules** for independent transaction validation and currency issuance (*consensus rules*);
  - A **mechanism** for reaching a global **decentralized consensus** on the valid blockchain (*Proof-of-Work*) algorithm;

Blockchain Evolution



Blockchain Evolution (2009 – present)

2009 Bitcoin		• A hard-coded **cryptocurrency application** with limited stack-based scripting language; • Proof-of-Work consensus; • Native cryptocurrency (BTC); • **Permisionless blockchain** system;	Blockchain 1.0
2014 Ethereum		• Distributed applications (**smart contracts**) in a domain-specific language (Solidity); • Prof-of-Work consensus (transition to Proof-of-Stake); • Native cryptocurrency (ETH); • **Permisionless blockchain** system	Blockchain 2.0
2017 Hyperledger Fabric		• **Distributed applications** (chaincodes) if different general-purpose languages (e.g. golang, Java, Node); • Modular/pluggable consensus; • **No native cryptocurrency**; • **Permissioned blockchain** system;	Blockchain 3.0

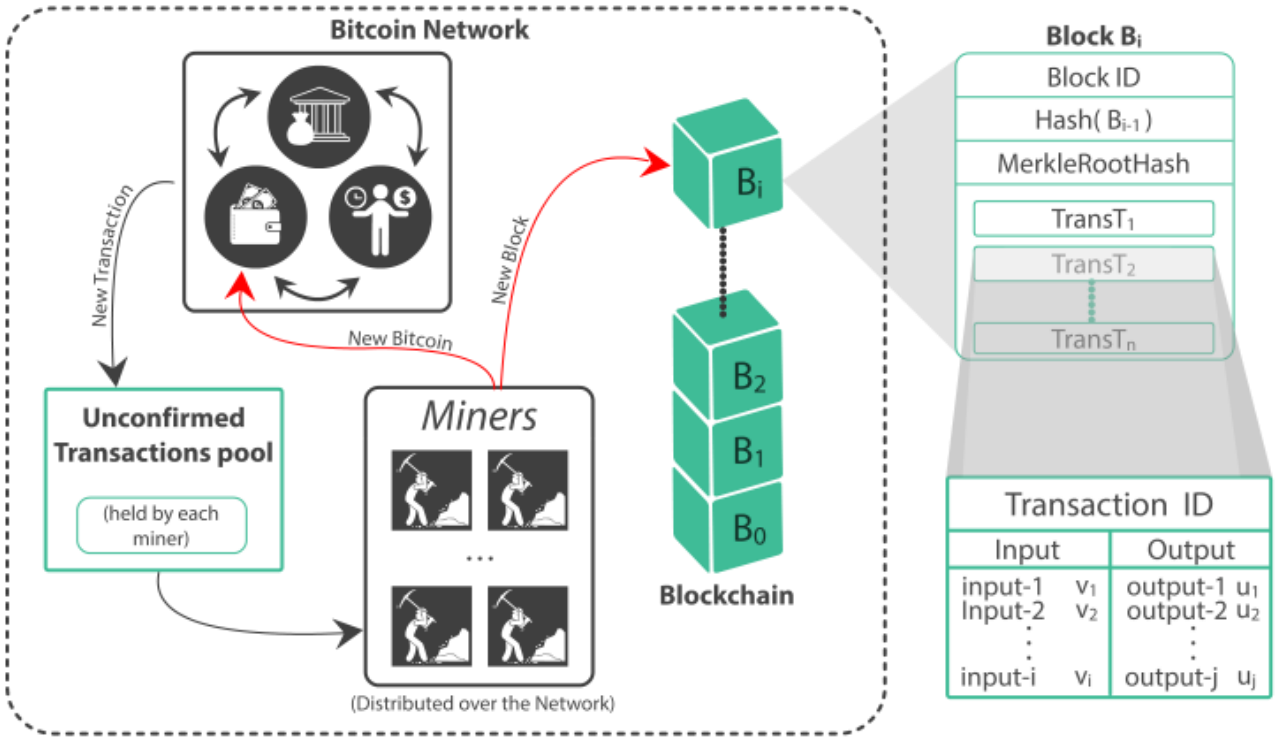
‘Simple’ Block Creation

- Step that a transaction goes through in a Bitcoin network…
- What is a block made of…
- How is a block created and linked with the rest of the chain of blocks…
- What does it involve and what are the other innovations and discoveries used to achieve the blockchain technology…

Simplified explanation

[100,000 ft view from Space]

- The bitcoin transaction
- Creation of a block
- Block consists of many parts not only transaction
- Mining
- Consensus
- Block created, added, linked



10,000 ft view

[a simplified '**simple English**' approach]

- John wants to send some money (digital currency) to Anna electronically.
- John uses a digital wallet app to transfer the money to Anna. The app stamps the transaction with John's digital signature. This transaction now need to be verified by the blockchain.
- John's transaction is grouped with other transactions that occur at the same time into a block. The block has a unique ID, the transaction time and the ID of the previous block in the chain.
- The block containing John's transaction is then broadcasted to the entire network to be verified.
- Once verified, the block is added to the head of the blockchain, forming a permanent and transparent record of transactions.
- After the verification process, Anna receives the money from John.

10,000 ft view

[in ‘tech & blockchain’ terms]

- **INITIATE THE TRANSACTION**
  - ✓Multiple parities transact;
  - ✓All transactions are recorded, including the transactions time, date, parties and amounts;
- **POST AND RECORD THE TRANSACTIONS TO THE NETWORK**
  - ✓The transaction is added in order into a network’s ‘block’ and presented;
  - ✓Each node in the network owns a copy of the ledger;

10,000 ft view

[in tech & blockchain terms]

- **BROADCAST**
  - ✓The ‘block is broadcasted to every node in the network.
  - ✓The network of computer nodes verify and validate by running a software that continuously replicated the ledger;
- **VALIDATE VIA CONSENSUS AND CONFIRM**
  - ✓multiple parities transact; all transactions are recorded, including the transactions time, date, parties and amounts;
  - ✓Consensus (agreed mathematical mechanism) is recorded and provides the basis for the trust mechanism.

10,000 ft view

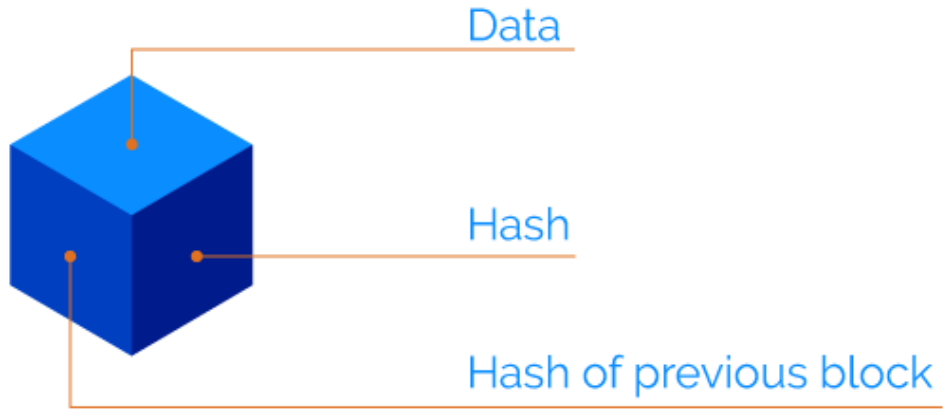
[in tech & blockchain terms]

- **IMMUTABLE, ENCRYPTED BLOCK**
  - ✓The confirmed block is added in linear and chronological order to the chain;
  - ✓This provides a transparent record of transactions, audit trail, and traceable digital fingerprints;
  - ✓Data creates a reliable transaction record;
- **TRANSACTION COMPLETED**
  - ✓Nodes have access to a single shared source of truth;

BLOCK

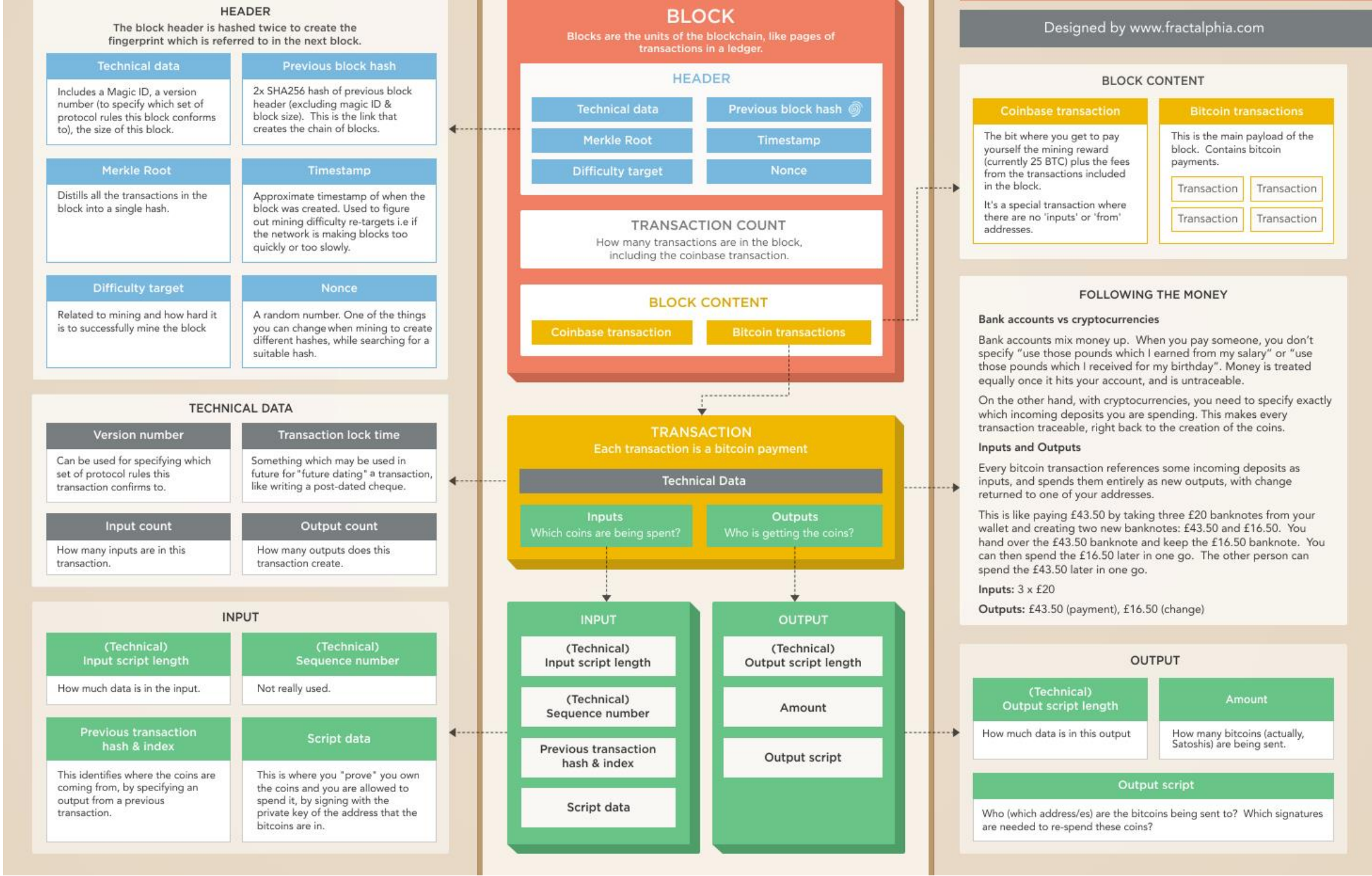
[in blockchain]

- Each block references the previous one and contains data, its own hash, and the hash of the previous block.
- Data stored inside a block may be represented by any value depending on the type of the blockchain.
- A block can store any amount of money, a share in a company, a digital certificate of ownership, a vote, or any other value.



source: rubygarage.org

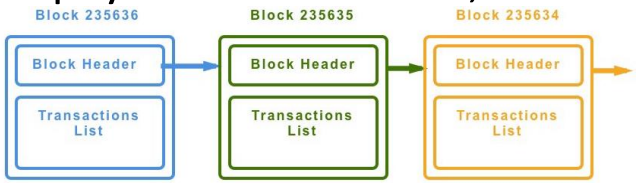
Inside Bitcoin's Blockchain



What data does each block consists of?

[fly by at 1,000ft – a closer look]

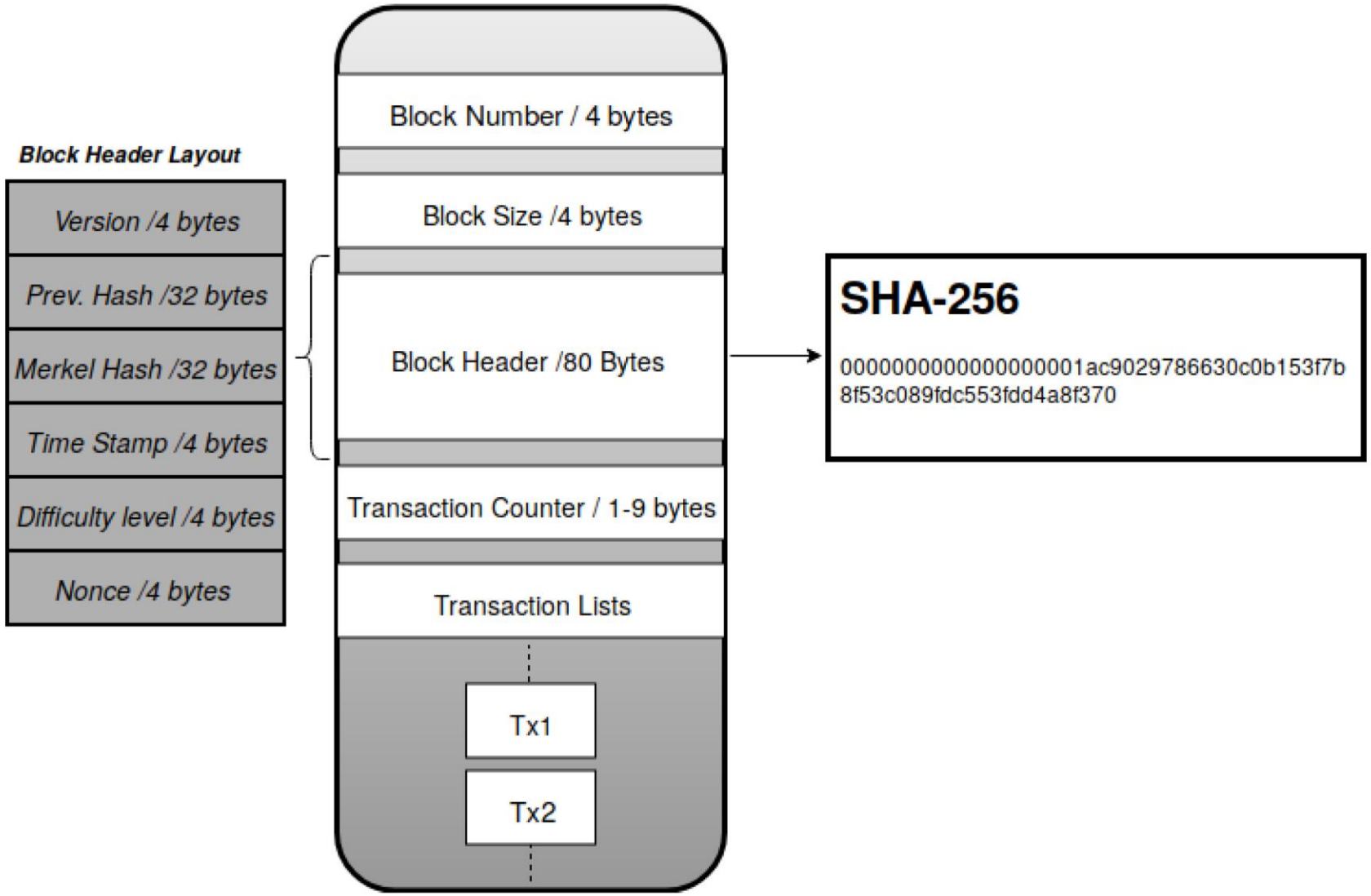
- **HEADER** (the block header is hashed twice to create fingerprint which is referred to in the next block
  - **Tech Data** – size of the block, Magic ID, version;
  - **Previous Block Hash** – SHA256 of previous block header (excluding ID and block size);
  - **Merkel Root** – distils all transactions in the block into a single hash;
  - **Time Stamp** – when the block was created, used to figure out the mining difficulty re-targets i.e. if the network is making the block too quickly or too slowly;
  - **Difficulty Target** – related to the mining and how hard is to successfully mine the block;
  - **Nonce** – A random number, you change while mining to create a different hashes, while searching for a suitable hash (target below the current difficulty level).
- **BITCOIN TRANSACTIONS**
  - **Coinbase Transaction** – mining reward + transaction fees to the one who solves the puzzle first;
  - **Bitcoin Transactions** – main payload of the block, contains bitcoin payments;



source: bitsonblocks.net

BLOCK STRUCTURE

[bitcoin block]



HASH – securing of the data

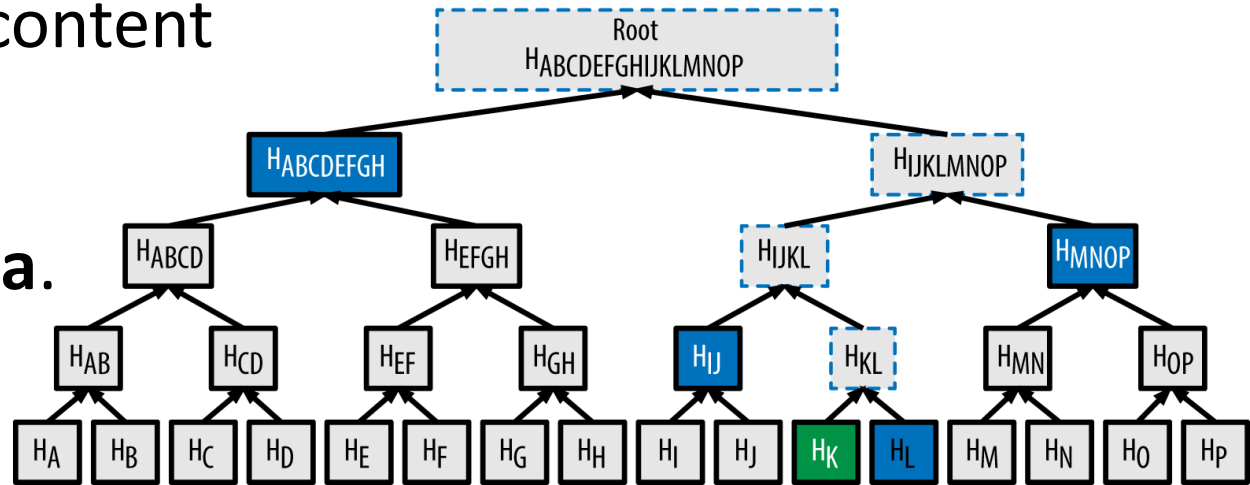
- Bitcoin uses a **SHA256** hash algorithm, email uses a MD5 hash algorithm. Hash is a mathematical function that takes an any size input and converts into encrypted fixed size output;
- A **hash is a fingerprint**, as each **hash is unique** – some qualities are:
  - ✓ Impossible to produce same hash value for different inputs.
  - ✓ The same input will always produce the same output.
  - ✓ Quick to produce a hash for any given data.
  - ✓ Impossible to determine input based on the output (one way only).
  - ✓ Even the slightest change to an input data drastically alters the output.

source: lisk.io

Merkle Root (Hash Tree)

[has nothing to do with Angela Merkel in Germany]

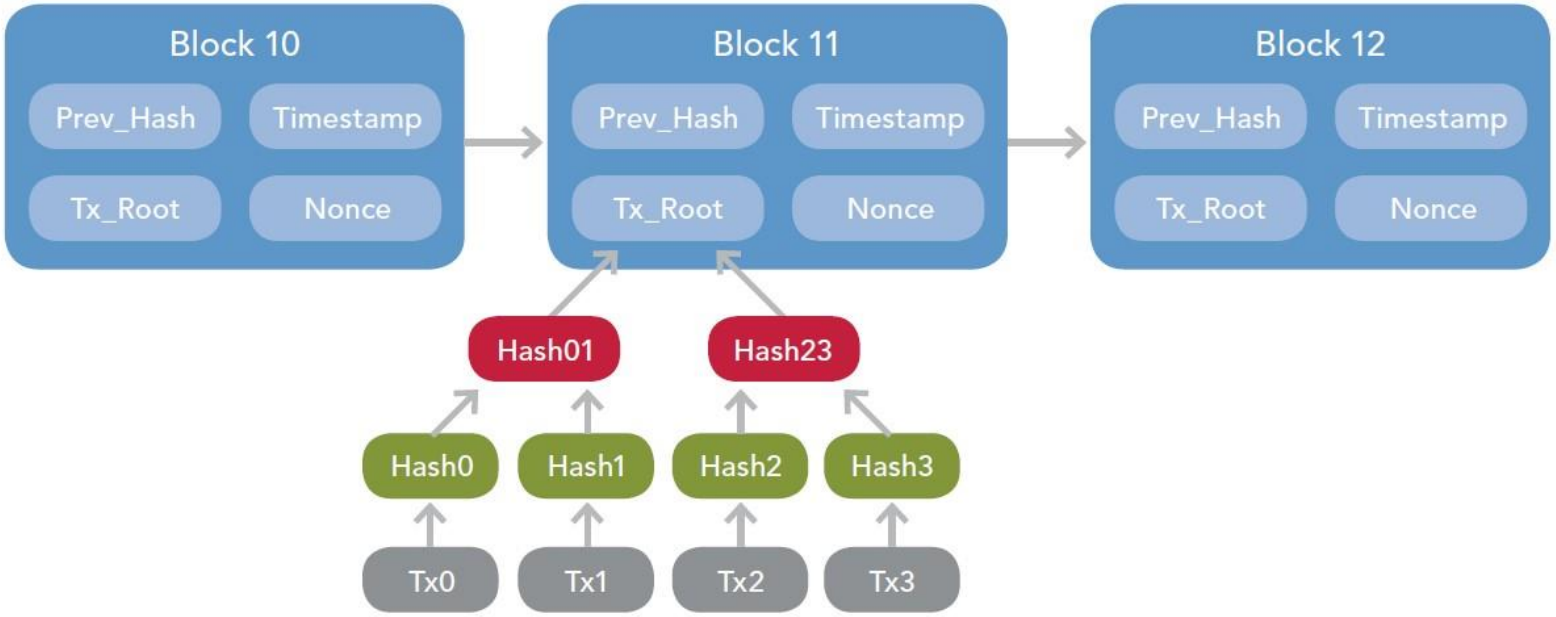
- Fundamental part of blockchain technology - **maintains the integrity of data** – the truth.
- Each transaction in the block (bitcoin blockchain) in hashed. **Hash values are further combined in a system known as a Merkle Tree**. Thus, a Merkle tree **summarizes all the transactions in a block by producing a digital fingerprint** of the entire set of transactions.
- A Merkle tree is a structure that allows for efficient and secure verification of content in a large body of data.
- This structure **helps verify the consistency and content of the data**.



Merkle Root (Tree)

[has nothing to do with Angela Merkel in Germany]

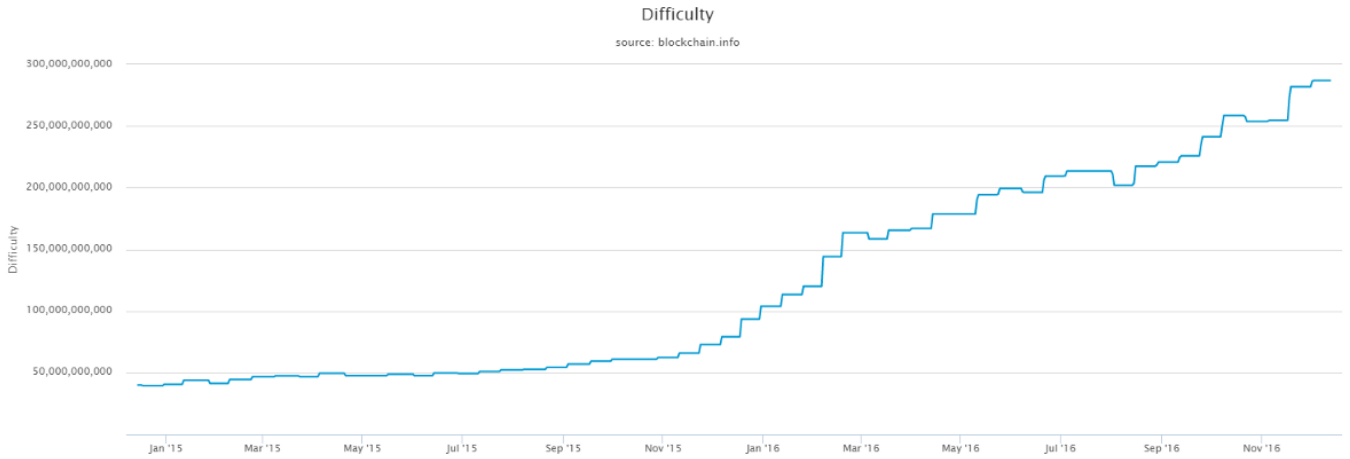
- They are constructed bottom up from hashes of individual transactions known Transaction IDs.
- Using a Merkle tree allows for a quick and simple test of whether a specific transaction is included in the set or not.



DIFICULTY TARGET

- **As more miners (nodes) join the network the more difficult it is to solve the puzzle, and vice versa**.
- Difficulty level adjusts every approximately 2 weeks or 2016 blocks, to **make sure it takes 10 minutes to create a block**.
- Difficulty is set by the protocol. [link]
- As the difficulty increases, so the target value for the hash decreases. This means there have to be more zeros at the start of the hash number.

Date: Mar 24 2019
Difficulty: 6,379,265,451,411
Hash rate: 45,664,560,811 GH/s



NONCE

- Only blocks whose hashes start with a certain number of 0's can be added to the ledger. Why?
- **The idea is to create competition among the miner.** Who will find the number that will contain a run of leading zeros below the difficulty target first. Remember the **SHA256 hash is unpredictable**.
- Thus, the miners has to **add an arbitrary number to the block, known as nonce** (i.e. 9876879).
- Finding the a block with a certain number of 0's is a **brute force task**, and can **only be achieved by testing different combinations** as fast as possible (lots of random guesses/trail and error – which keeps it fair).
- Hash value is unique for the combination of a nonce and input data
- The guessing game is called 'hashing'.

Transactions (Tx)

[private & public key]

- Cryptography also helps one more puzzle – **authenticity**.
- To be part of the bitcoin network all you need is access to internet. Every user in the network is **identified by** a string of characters, known as the **bitcoin address**.
- To transact with someone in bitcoins you need to know their bitcoin address (i.e. email).
- **Your bitcoin address is derived from a public key which is derived from a private key.** Private key should be kept secret like your password to an email.

Transactions (Tx)

[private & public key]

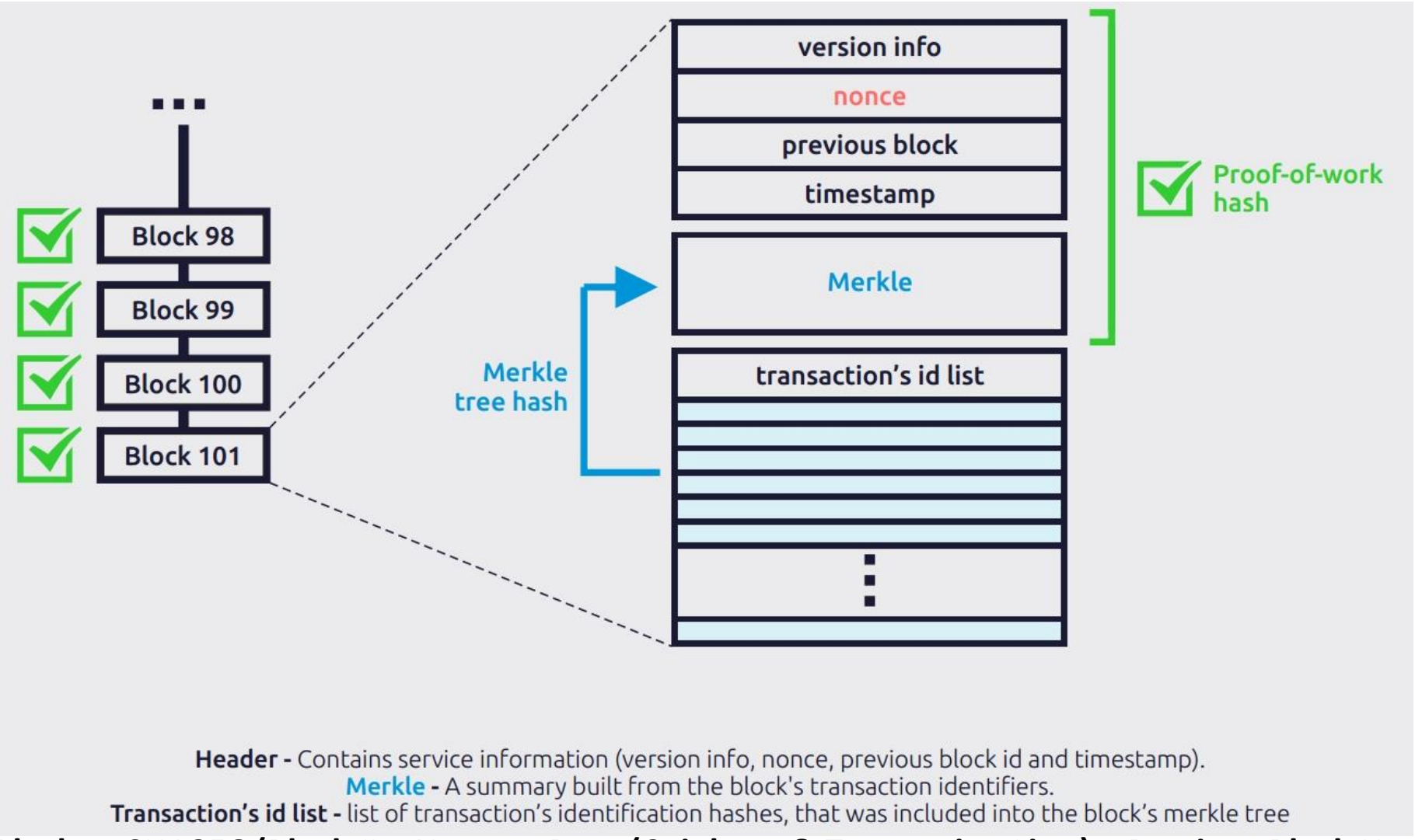
- A transaction signature = hash (private key + bitcoin amount)
- So when sending a bitcoin to someone it includes:
  - My **signature**: hash output of my transaction and my private key
  - My **transaction**: since you can’t determine the amount from the signature
  - My **public key**: to identify myself as the sender

- Where do I send it? To someone's bitcoin address which is derived from his public key.

- Thus, when a transaction is picked up from the mempool by the miner they check if all the components match.

What does a block look like?

[simplified block structure]



SHA256 Hash of Blocks = SHA256 (Block # + Nonce + Data (Coinbase & Transaction Lists) + Previous Block Hash + Time-Stamp)


Block 0xaf013c45
Block 0x43a5fc78

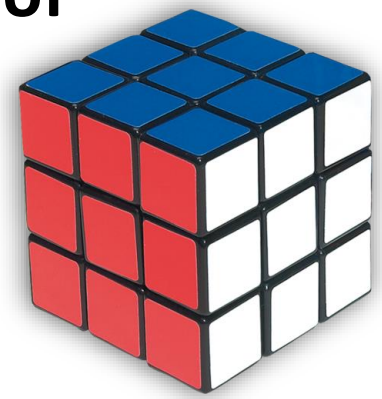
Consensus Mechanisms

- Most blockchains have a lot of things in common and function in similar ways, but one of the ways in which **blockchains can be unique is the way consensus is reached**.
- Consensus mechanisms are protocols that make sure all nodes (device on the blockchain that maintains the blockchain and sometimes processes transactions) are synchronized with each other and **agree on which transactions are legitimate** and are added to the blockchain.
- These consensus mechanisms are crucial for a blockchain in order to function correctly. **Without a good consensus mechanisms, blockchains are at risk of various attacks**.

Proof of Work

[mining]

- It is one of many consensus mechanism; this algorithm is used to **confirm transactions and produce a new block to the chain**.
- **Miners compete** with each other by solving the PoW algorithm in order **to receive the reward.**
- Mining is done with dedicated computer machines which **costs processing power (hardware, energy, and time).**
- Miners are using their hardware to test these nonce, at a **rate of millions per second.**
- Difficult to solve but very easy to verify the correct value!



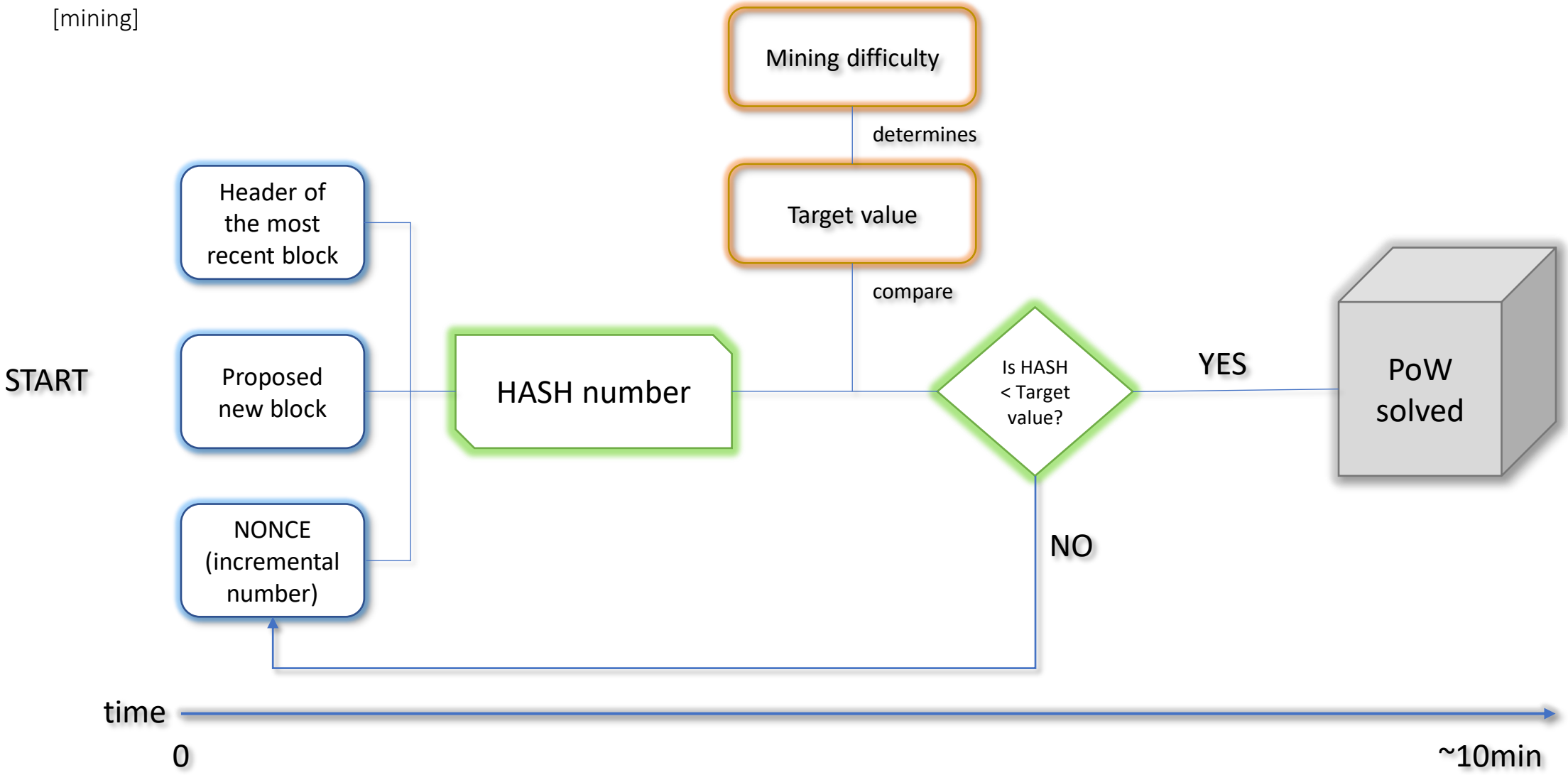
Proof of Work

[mining]

- **The Proof Of Work process is known as mining** and the nodes are known as miners. Miners **solve complex mathematical puzzles** which require a lot computational power.
- **First** of all, they are asymmetric, meaning it **takes a lot of time to find the answer, yet it's easy to verify if an answer is correct**.
- **Secondly**, the only way **to solve these puzzles is to 'guess' the answer**. It is not possible to solve the puzzles quicker using any other **method than trial and error.**
- **Lastly**, the **difficulty of these puzzles changes depending on how fast blocks are mined.** To maintain a consistent supply of new coins, blocks have to be created within a certain time frame. If blocks are created too fast, the puzzles get harder, and if they are created too slow, the puzzles get easier.

Proof of Work

[mining]

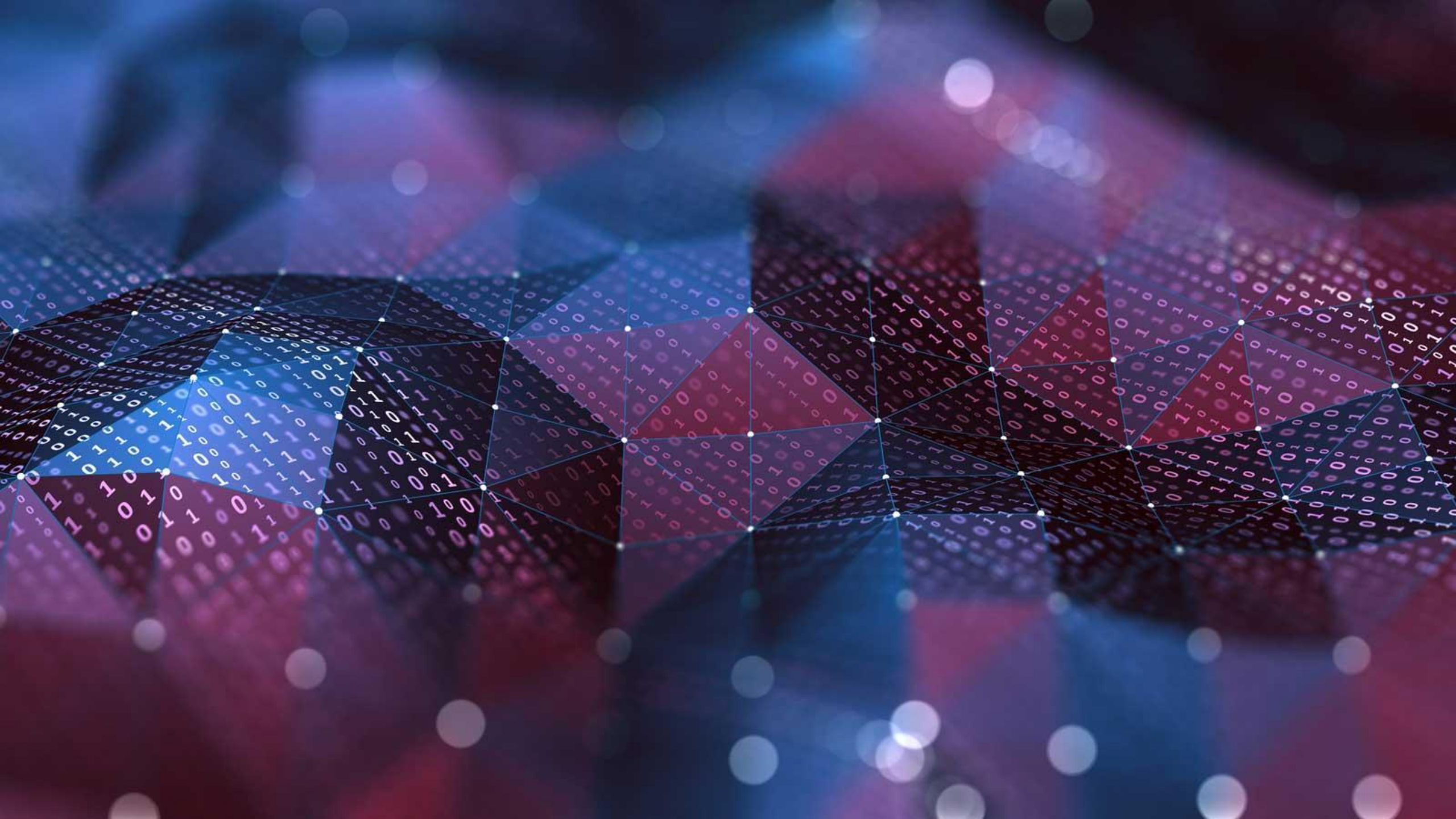


BLOCKCHAIN

Block #	1
Nonce	44029
Data	coin-base/transactions...
Timestamp	12.12.2017-04:10:10
Previous	0000000000000000000000000000000000000000000000000000000000000000
Hash	0000d89cfa9bee16d7a2a67ab7c9b8795b22362dfa7c46e5bff514320a809beb

Block #	2
Nonce	78048
Data	coin-base/transactions...
Timestamp	12.12.2017-04:20:10
Previous	0000d89cfa9bee16d7a2a67ab7c9b8795b22362dfa7c46e5bff514320a809beb
Hash	0000b556851cc13ebf2c3497c7422249e3965226b3de1fbd81409d2cb6d9c856

Block #	3
Nonce	97713
Data	coin-base/transactions...
Timestamp	12.12.2017-04:30:10
Previous	0000b556851cc13ebf2c3497c7422249e3965226b3de1fbd81409d2cb6d9c856
Hash	0000r6bf41d8137b48e8a2beaff4a3d7c2a32ac52662d37d0f6ac6cdb543f5a6



Smart Contract – Characteristics

[smart contract are not a technical issue but a business one]

1. Smart contracts can call other contracts, if needed. This means that if there are two parts of a contract, wherein the first part is concerned with checking a requirement, then after the condition gets validated the second part of the contract where the task might be to carry out a transaction, will receive the output of the first part and the transaction will take place successfully.
2. Smart contracts act as accounts that need multiple signatures. Unless a required number of people sign, funds won't be transferred.
3. Smart contracts help in managing the agreement between two or more users, for example if one person sells an insurance to the other.

source: https://hackernoon.com/smart-contracts-a-time-saving-primer-b3060e3e5667

Smart Contract - Characteristics

4. You don’t need to rely on any intermediaries to carry out or confirm your agreements. This removes the risk of a third party manipulation, as execution is done by the network in an automated way.

5. All the documents are encrypted in a shared ledger so nobody can claim to have lost something of yours.

6. Everything is backed up in the blockchain, as all the nodes have a copy of it so you can’t really worry about losing data.

7. The smart contracts are built on a blockchain environment so everything is well encrypted so it would take a really smart hacker to tamper with data.

source: https://hackernoon.com/smart-contracts-a-time-saving-primer-b3060e3e5667

Smart Contract - Characteristics

8. Smart contracts save your time as all tasks are automated due to them written in software code. This also removes the paperwork and endless settlements and other legalities.

9. Smart contracts also save you money since no middleman is being paid here, thanks to the blockchain environment!

10. Smart contracts are pretty accurate as they are automated, which removes the possibility of human errors that may occur in filling out heaps of forms.

source: https://hackernoon.com/smart-contracts-a-time-saving-primer-b3060e3e5667

USE CASE | Manufacturing Supply Chain

[quick demo i.e. laptop]

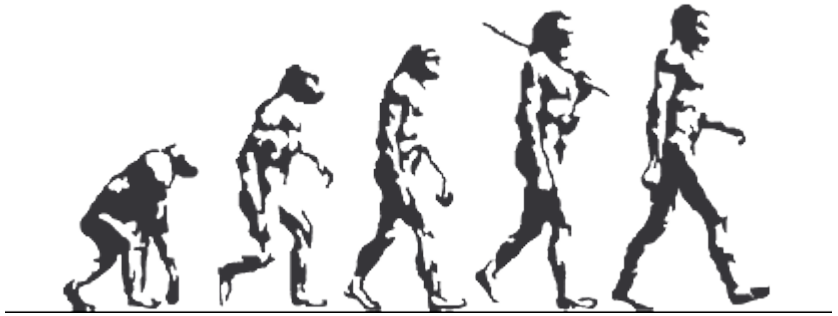
- A computer company decides to produce some amount of laptops for the following year. They will make an order to the laptop manufacturer.
- Manufacturer will contact its hardware suppliers (chips, monitors, HD, ram, video cards, etc.) in order to produce the final product.
- Once all parts are assembled together to produce the final product (laptop) they will be shipped via logistic companies to a distribution center.

source: transformationworx.com

USE CASE | Manufacturing Supply Chain

[quick demo i.e. laptop]

- Problem statement:
  - When there is an issue (problem) with a laptop and its called back it is difficult to know were it originated and if it's a single laptop issue or the whole series of them. The investigations can last for months.
  - Inability or very expensive means to identify point of original source. What came from where?
  - Root cause opaque* in the system and individual components are not connected one with each other in a reliable manner. (digital does not mean reliable)



(Not able to see through, not transparent, unclear, uncertain)

source: transformationworx.com

What is Solution Architecture?

- **Solution** – a way to describe the answer to some problem; and addressing them with appropriate system that provide measurable improvements in place of previously deployed systems.

- **Architecture** – complex or carefully designed structure of something

- **Solution Architect** (job) – involved with the crafting the business need (usually a technical one) and is tasked with crafting the description of solutions that can be to address that need. (choice of weapon – diagrams or other visual aids is a key to success)

Future

The use of blockchain combined with smartphones, RFID, IoT networks, and mobility applications could create (by 2030) or make almost every if not all industries with near-perfect records.

Further Readings and Resources

- Andreas Antonopoulos [link]
- Try to go over the Blockchain Demo by Anders [link]
- (**Advanced**) How to set up a private Ethereum blockchain and deploy a Solidity Smart Contract on the blockchain — in less than 20 mins! [link]

Cryptocurrency Realtime Visualization Websites

[interactive websites]

- Market Capitalization and Volume – crypto info [link]
- Watch live bitcoin transactions presented as balls – [link]
- Bitnodes across the globe – [link]
- Network Map – [link]

MORE TO FOLLOW IN NEXT SESSION

…