

BLOCKCHAIN TECHNOLOGY

Dr. Neha Sharma

Founder Secretary, Society for Data Science

Execom Member, IEEE Pune Section



WHERE SHOULD
WE FOCUS
THIS YEAR?



"BLOCKCHAIN"



IT WILL
CHANGE
EVERYTHING.



EVERYBODY
IS TALKING
ABOUT IT.



THE POTENTIAL
APPLICATIONS
ARE ENDLESS.



WE DON'T
WANT TO BE
LEFT BEHIND.



WHAT
EXACTLY IS
BLOCKCHAIN?

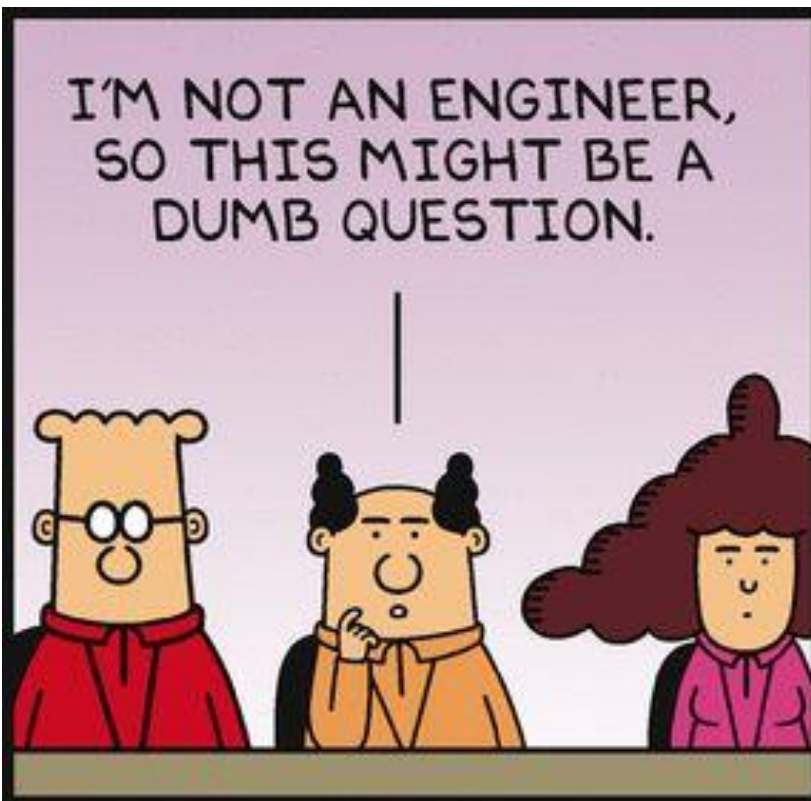


ALSO,
"ARTIFICIAL
INTELLIGENCE"

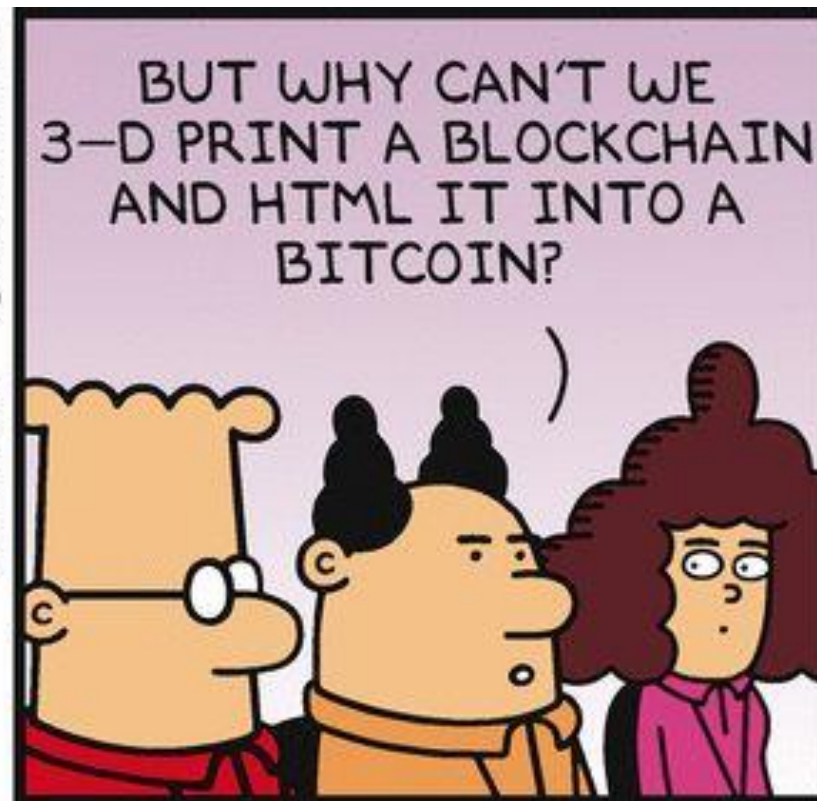


TOM
FISH
BURNE

WHAT'S A BLOCKCHAIN??



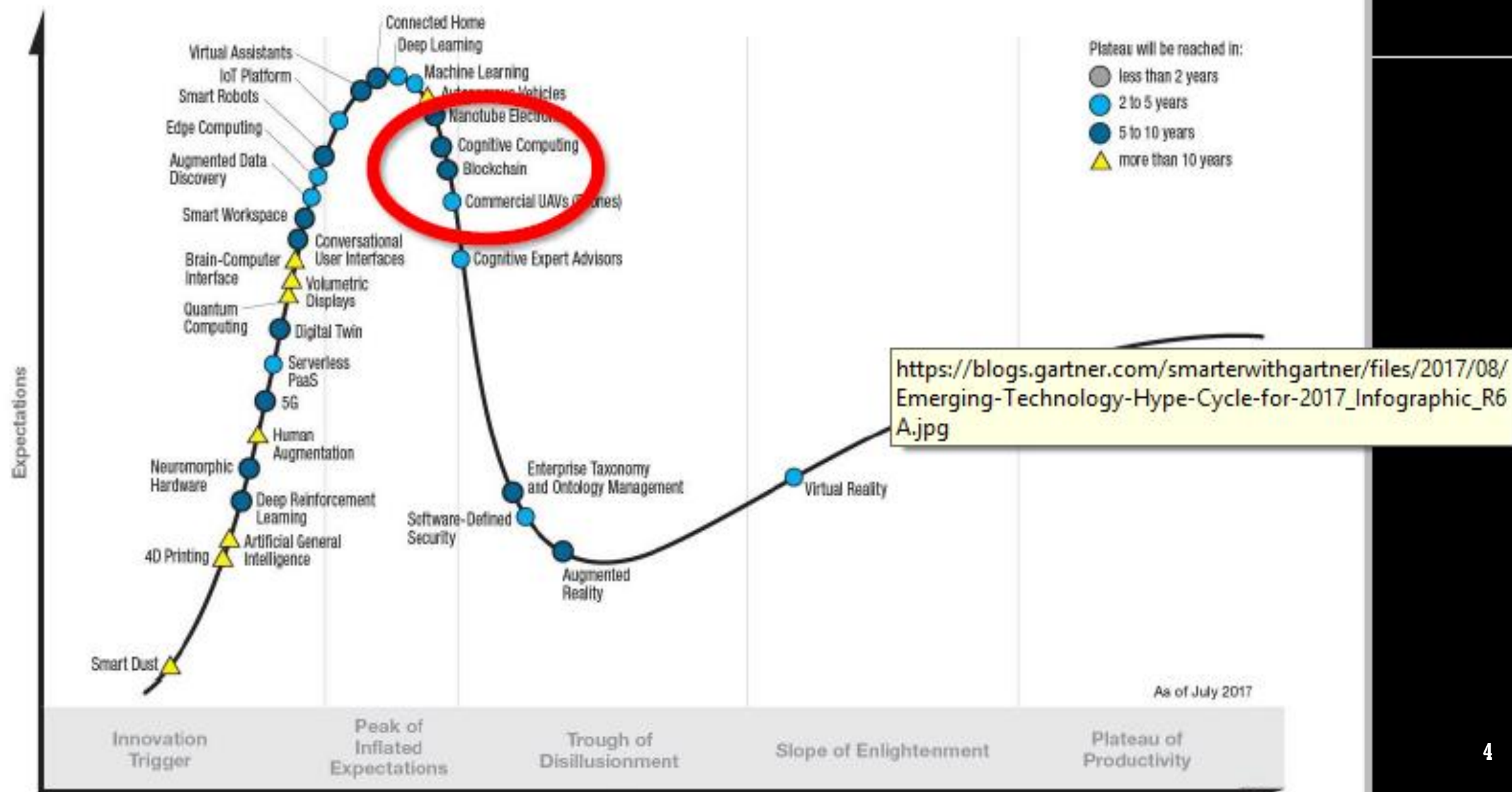
DILBERT.COM @SCOTTADAMSSAYS



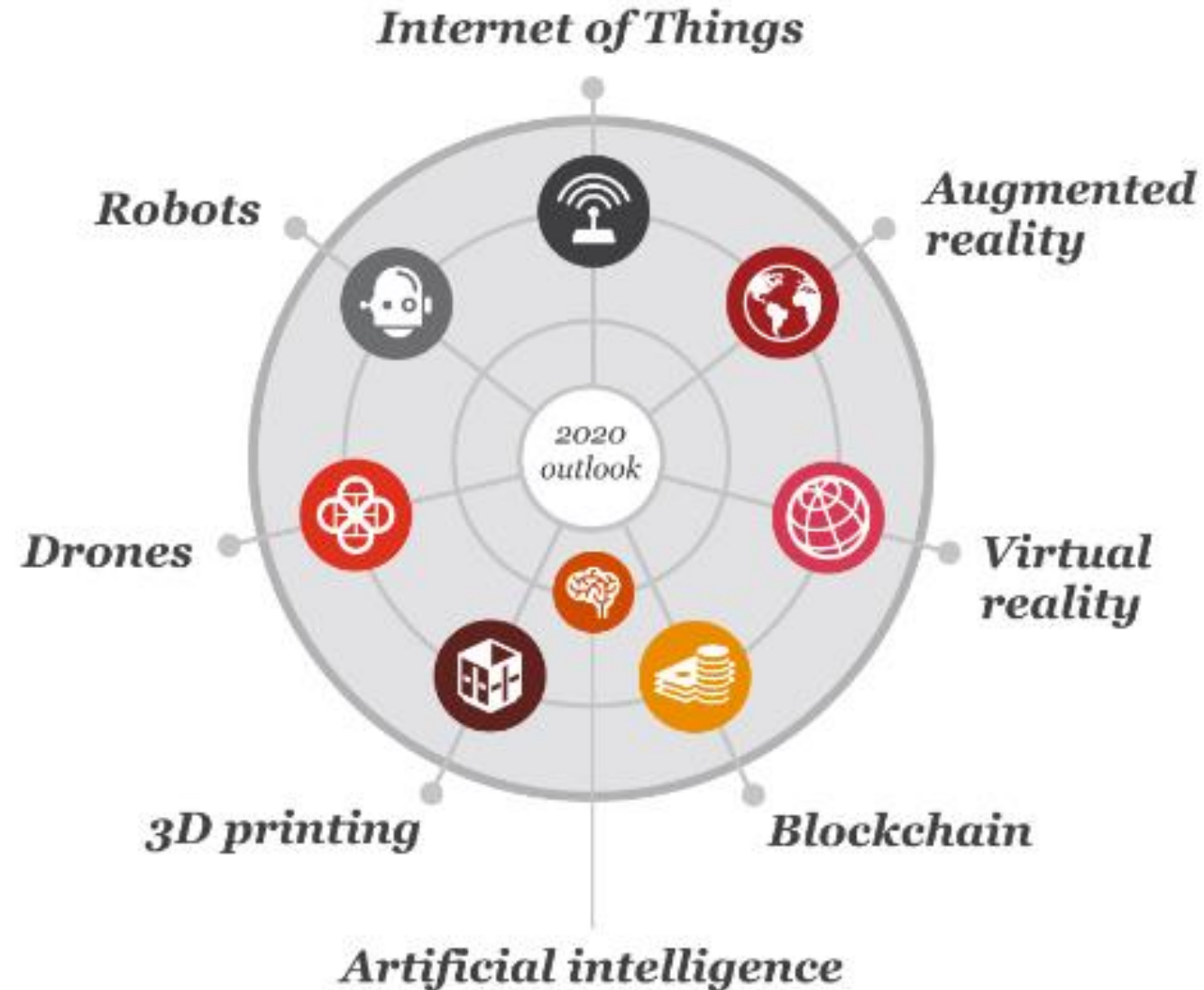
4-20-18 ©2018 Scott Adams, Inc./Dist. by Andrews McMeel



Gartner Hype Cycle for Emerging Technologies, 2017



THE ESSENTIAL EIGHT TECHNOLOGIES



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Drones

Air or water-based devices and vehicles, for example, Unmanned Aerial Vehicles (UAV), that fly or move without an onboard human pilot. Drones can operate autonomously (via on-board computers) on a predefined flight plan or be controlled remotely.

Top business potential applications

- Insurance claim validation
- Precision farming
- Infrastructure inspections
- Cargo delivery



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Internet of Things (IoT)

Network of objects – devices, vehicles, etc. – embedded with sensors, software, network connectivity and compute capability that can collect and exchange data over the Internet. IoT enables devices to be connected and remotely monitored or controlled. The term IoT has come to represent any device that is now “connected” and accessible via a network connection. The Industrial IoT is a subset of IoT and refers to its use in manufacturing and industrial sectors.

Top business potential applications

- Inventory and material tracking
- Usage and performance benchmarking
- Connected service parts management
- Real time market insights



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Robots

Electro-mechanical machines or virtual agents that automate augment or assist human activities, autonomously or according to a set of instructions – often a computer program.

Top business potential applications

- Hazardous industries
- Hotels and tourism
- Automation of predictable tasks
- Data management



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

3D Printing

Additive manufacturing techniques used to create three-dimensional objects based on digital models by layering or “printing” successive layers of materials. 3D printing relies on innovative “inks” including plastic, and more recently, glass and wood.

Top business potential applications

- Healthcare and smart medical devices
- Prototyping
- Customized products
- Remote location production



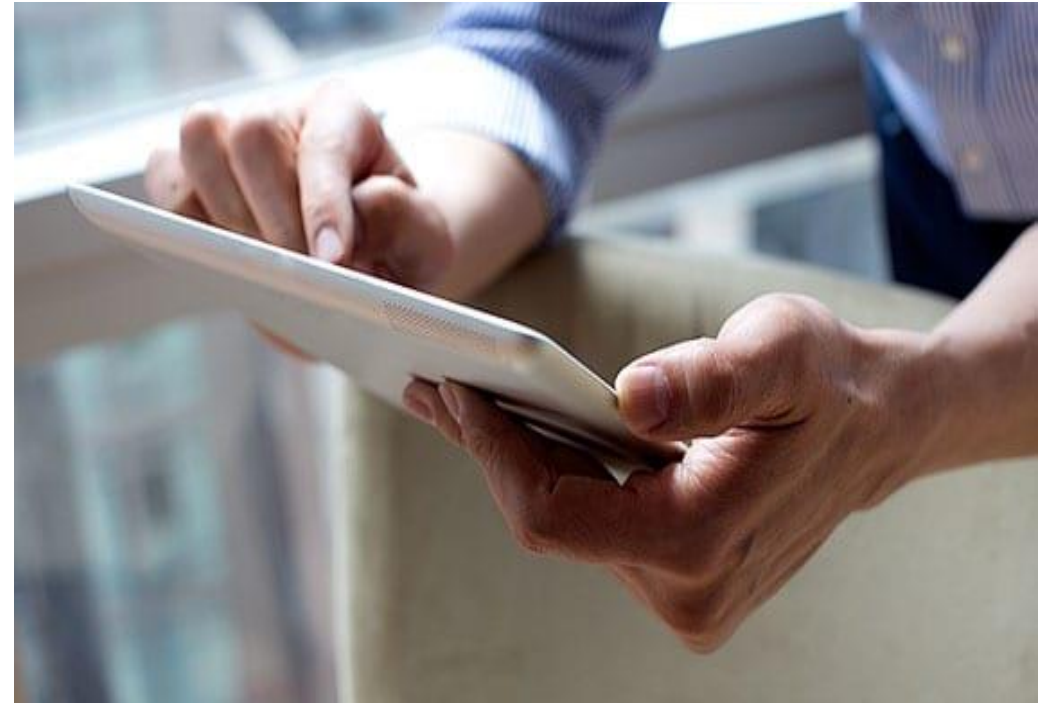
THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Virtual Reality (VR)

Computer-generated simulation of a three dimensional image or a complete environment, within a defined and contained space, that viewers can interact with in realistic ways. VR is intended to be an immersive experience and typically requires equipment, most commonly a helmet/headset.

Top business potential applications

- Manufacturing/ product design
- Architecture & construction
- Education & Training
- Merchandising



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Augmented Reality (AR)

Addition of information or visuals to the physical world, via a graphics and/or audio overlay, to improve the user experience for a task or a product. This “augmentation” of the real world is achieved via supplemental devices that render and display said information.

Top business potential applications

- Virtual showrooms
- Education
- Printing and advertisers
- Retail environments



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Artificial Intelligence (AI)

Software algorithms that are capable of performing tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making and language translation. AI is an “umbrella” concept that is made up of numerous subfields, such as machine learning, which focuses on the development of programs that can teach themselves to learn, understand, reason, plan, and act when exposed to new data in the right quantities.

Top business potential applications

- Managing personal finances
- Real time fraud and risk management
- Automated virtual assistants
- Customer support, transactions and helpdesks



THE ESSENTIAL TECHNOLOGIES AND HOW THEY CAN BE APPLIED

Block Chain

Distributed electronic ledger that uses software algorithms to record and confirm transactions with reliability and anonymity. The record of events is shared between many parties and information once entered cannot be altered, as the downstream chain reinforces upstream transactions.

Top business potential applications

- Voting
- Smart contracting
- Provenance / traceability
- Asset registration / ownership



AGENDA

Current Existing
Monetary System

How can Blockchain and
Bitcoin help?

What is Blockchain?

Blockchain Concepts



BLOCKCHAIN

Bitcoin Transaction

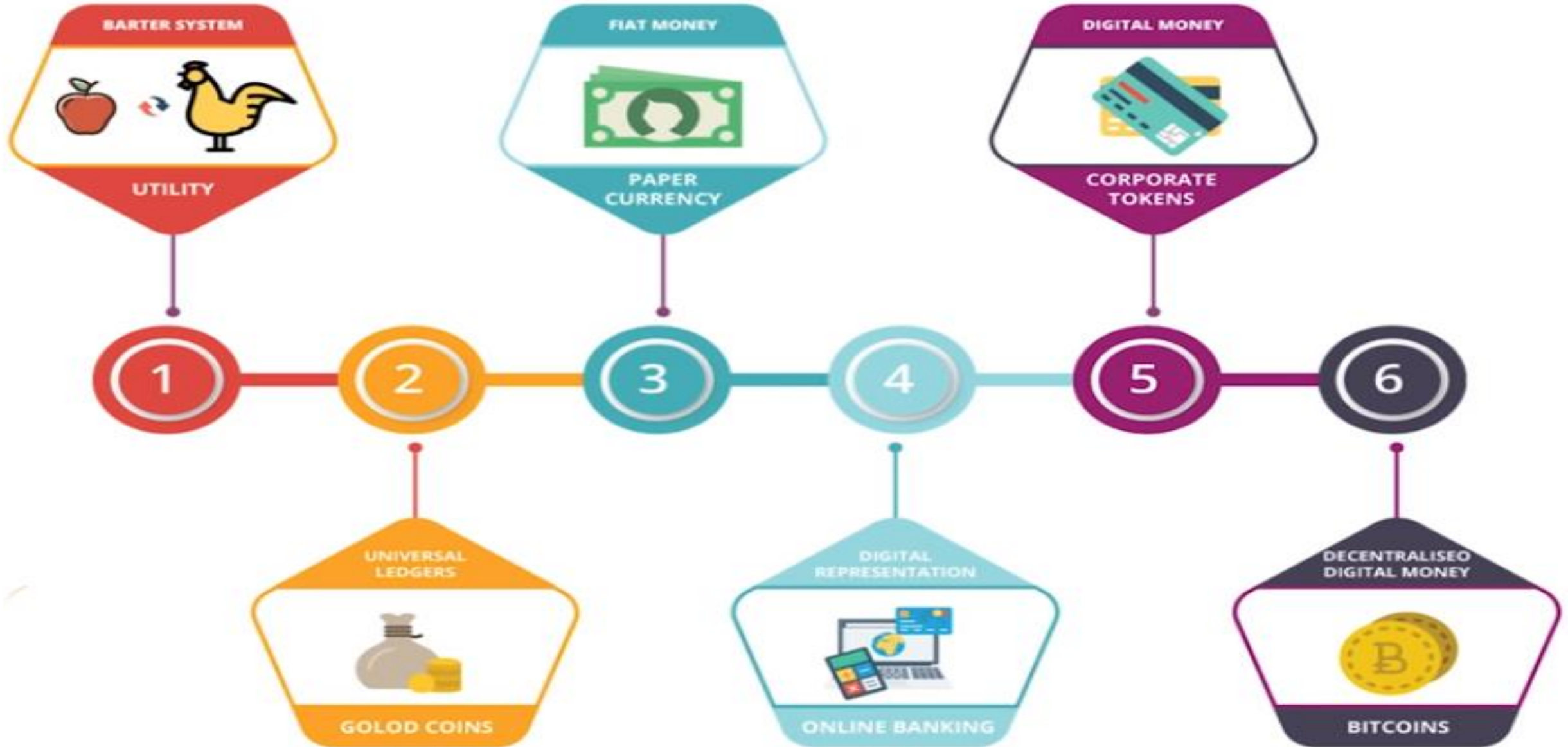
Blockchain Features

Blockchain Use Cases

TRACING BLOCKCHAIN'S ORIGIN

- Need for an **efficient, cost-effective, reliable, and secure system** for conducting and recording financial and business transactions.
- Throughout history, **instruments of trust**, such as minted coins, paper money, letters of credit, and banking systems, have emerged **to facilitate the exchange of value** and protect buyers and sellers.

CHANGE OF MONETARY SYSTEM OVER TIME



TRACING BLOCKCHAIN'S ORIGIN

- Need for an **efficient, cost-effective, reliable, and secure system** for conducting and recording financial and business transactions.
- Throughout history, **instruments of trust**, such as minted coins, paper money, letters of credit, and banking systems, have emerged to facilitate the exchange of value and protect buyers and sellers.
- Important **innovations**, including telephone lines, credit card systems, the Internet, and mobile technologies have **improved the convenience, speed, and efficiency of transactions** while shrinking and sometimes virtually eliminating the distance between buyers and sellers.

LANDMARK TECHNOLOGICAL ADVANCES

Digital

- Computer



Network

- Internet



Communication

- Usenet
- Email
- Messaging



Web

- Information
- Ecommerce
- Enterprise



Crypto

- Bitcoin
- Blockchain
- Smart contracts
- Internet of Money
- Internet of Value



Data

- Analytics
- Machine Learning
- Internet of Things



Social

- Media
- Networks



Mobile

- Apps
- Maps
- Snaps

TRACING BLOCKCHAIN'S ORIGIN

- Need for an **efficient, cost-effective, reliable, and secure system** for conducting and recording financial and business transactions.
- Throughout history, **instruments of trust**, such as minted coins, paper money, letters of credit, and banking systems, have emerged to facilitate the exchange of value and protect buyers and sellers.
- Important **innovations**, including telephone lines, credit card systems, the Internet, and mobile technologies have improved the convenience, speed, and efficiency of transactions while shrinking and sometimes virtually eliminating the distance between buyers and sellers.

STILL, THERE ARE MANY CHALLENGES WITH EXISTING BANKING & BUSINESS SYSTEMS

TRADING IN THE CURRENT SYSTEM



Trade is Recorded in Bookkeeping (An offline ledger where transaction details are stored)



Bookkeeping is isolated and closed to the public



For this reason we use trusted third parties or middle men we trust to facilitate and approve our transactions

ISSUES WITH THE CURRENT BANKING SYSTEM

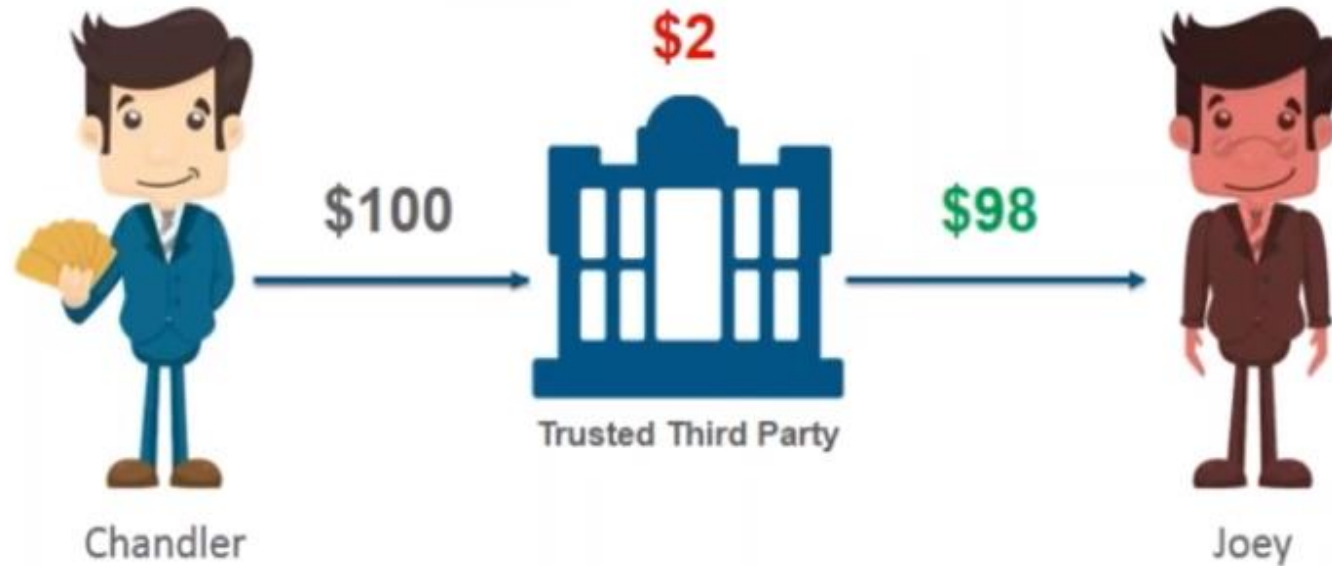
Transaction Delays



Transactions require a lot of time to be **Verified** and completed causing huge delays.

ISSUES WITH THE CURRENT BANKING SYSTEM

High Transaction Fees

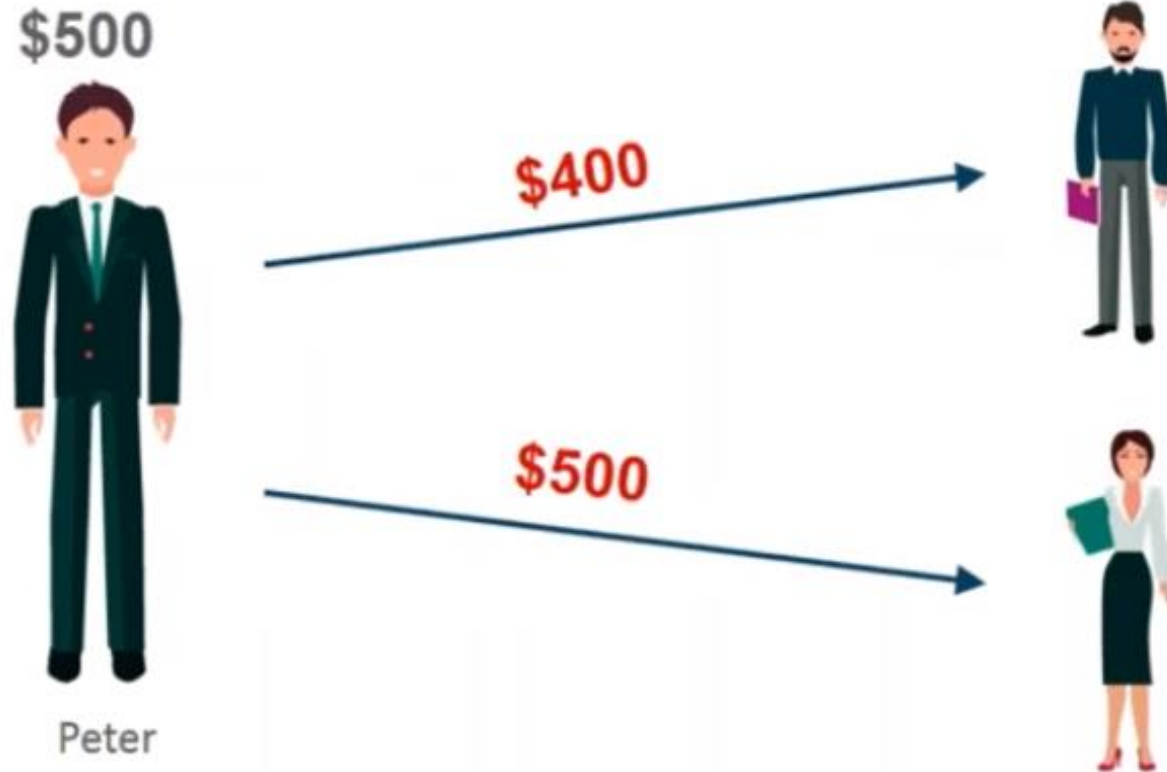


JPMorgan Chase, Bank of America and Wells Fargo

alone earned more than **\$6 billion** from **ATM** and **overdraft fees** in **2015** (SNL Financial and CNNMoney Report)

ISSUES WITH THE CURRENT BANKING SYSTEM

Double Spending



Bank transactions are prone to double spending

ISSUES WITH THE CURRENT BANKING SYSTEM



Reserve Bank of India



US Federal Reserve

Banks have become synonymous with crises and crashes due to depression and fractional reserve banking



ISSUES WITH THE BUSINESS TRANSACTION

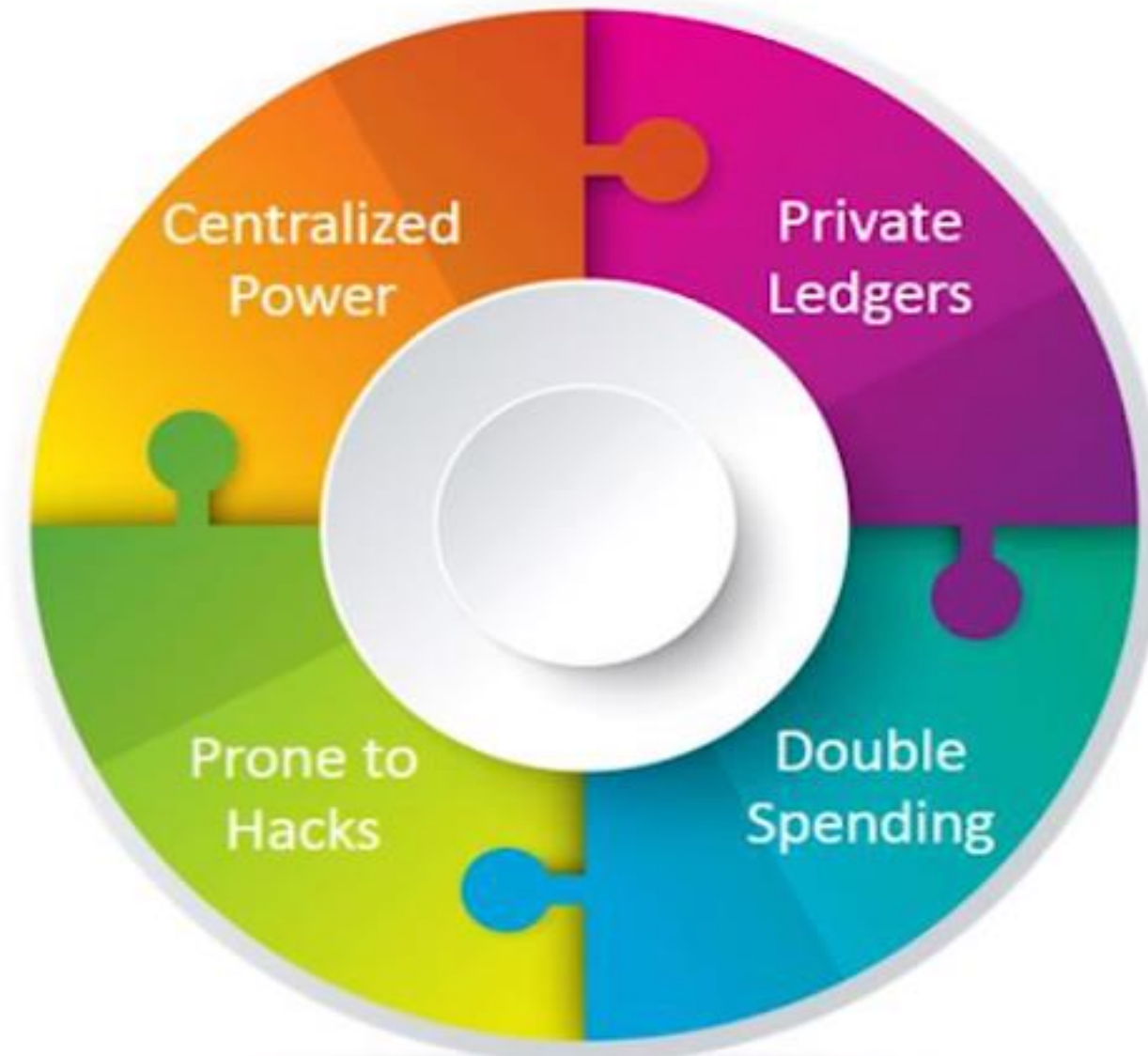
Many business transactions remain inefficient, expensive, and vulnerable, suffering from the following limitations:

- **Cash** is useful only in local transactions and in relatively small amounts.
- The **time** between transaction and settlement can be long.
- **Duplication** of effort and the need for **third-party validation** and/or the presence of intermediaries add to the inefficiencies.
- **Fraud, cyber-attacks**, and simple **mistakes** add to the cost and complexity of doing business, and they expose all participants in the network to risk if a central system, such as a bank, is compromised.
- Credit card organizations have essentially created **walled gardens** with a high price of entry. Merchants must pay the high costs of onboarding, which often involves considerable paperwork and a time-consuming vetting process.
- Half of the people in the world **don't have access to a bank account** and have had to develop parallel payment systems to conduct transactions.

LIMITATION OF EXISTING SYSTEM

- Previously, we had to **trust** the financial institutes and other **third parties** with our money, not knowing if they are as safe and secured as they claim.
- The transactions in the differed databases takes **time**, costs **money** or transaction charges, **vulnerable** to hacking or can be **error prone** due to any human intervention.
- We are subjected to all such difficulties and hassles, but with the emergence of Blockchain all these issues can be resolved in a **safe, secure and effective** manner by **revolutionizing the way of managing data and databases**.

LIMITATION OF EXISTING SYSTEM



Issues with centralized banks

NEED FOR BLOCKCHAIN

- Transaction volumes worldwide are growing exponentially due to growth of ecommerce, online banking, in-app purchases, and the increasing mobility of people around the world.
- Which will magnify the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems.
- Transaction volumes will explode with the rise of Internet of Things (IoT) — autonomous objects, such as refrigerators that buy groceries when supplies are running low and cars that deliver themselves to your door, stopping for fuel along the way.
- To address these challenges and others, the world needs **transaction / payment networks** that are
 - **Fast** and that provide a mechanism that establishes **trust**,
 - Requires **no specialized** equipment,
 - Has **no chargebacks** or monthly fees,
 - Provides a **collective bookkeeping** solution for ensuring transparency and trust.

BLOCKCHAIN

BLOCKCHAIN



Stuart Haber

How to Time-Stamp a Digital Document

By Stuart Haber & W. Scott Stornetta (1991)



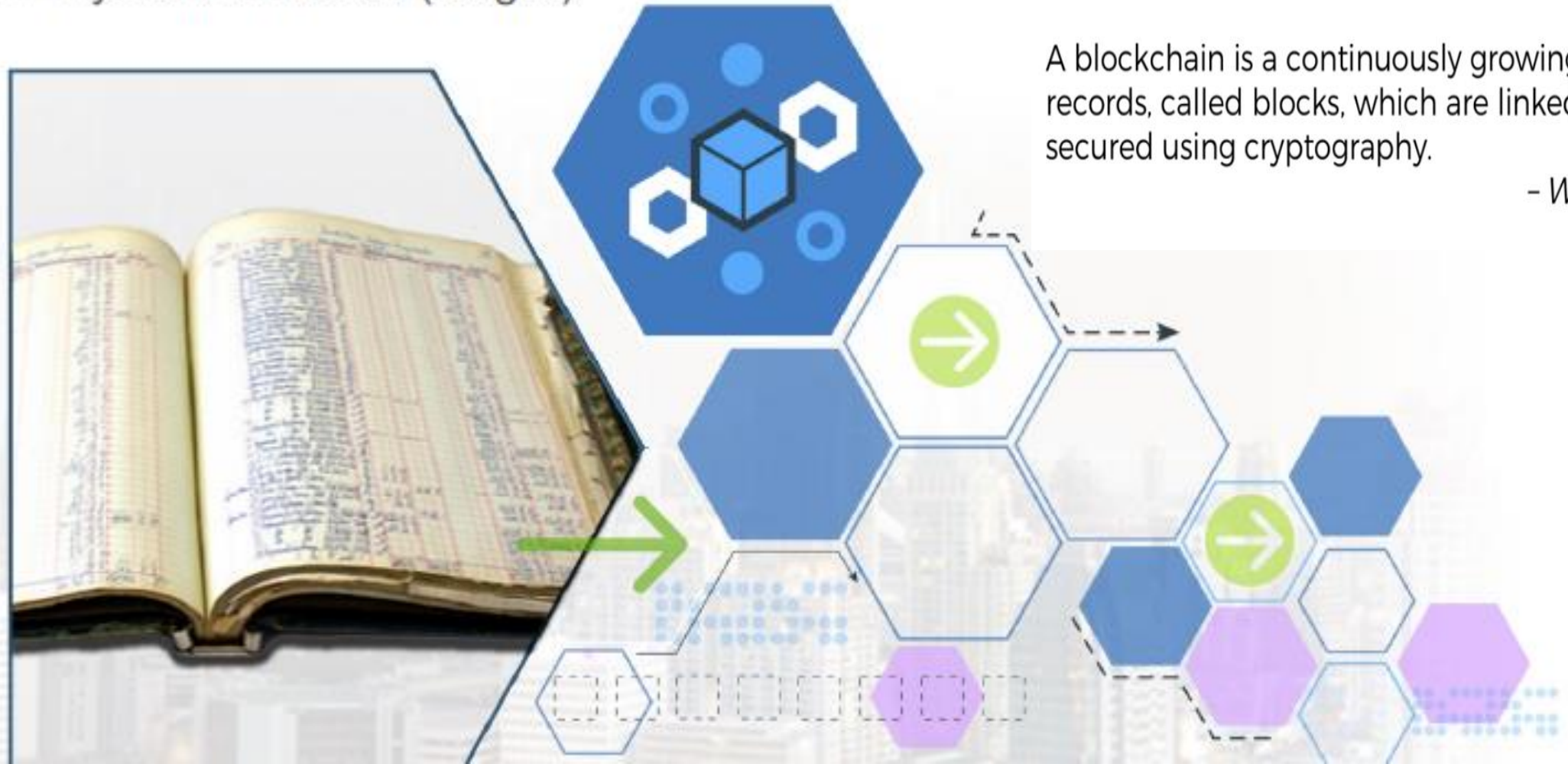
W. Scott Stornetta

Link:

https://www.anf.es/pdf/Haber_Stornetta.pdf

Introducing Blockchain

A shared ledger technology allowing any participant in the business network to see THE system of record (ledger)



A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

- Wikipedia

BLOCKCHAIN



Technical Definition

A blockchain is a **linked list** that is built with **hash pointers** instead of regular pointers.

Socio-political-economic-semi-technical libertarian definition

A blockchain is an **open***, **borderless**, **decentralized**, **public**, **trustless**, **permissionless**, **immutable record of transactions**

Financial-accounting definition

A blockchain is a **public**, distributed **ledger** of peer-to-peer transactions

BLOCKCHAIN

- Blockchain is a new type of Database and Transaction Management System.
- A blockchain is **an open, decentralized, distributed database / ledger** that can
 - - **Record** transactions between two parties efficiently
 - - **Track** assets in a business network
 - - **Maintain** a continuously growing list of records, called blocks, in a **verifiable** and **permanent** way.
- An *asset* can be **tangible** — a house, a car, cash, land — or **intangible** like intellectual property, such as patents, copyrights, or branding.
- Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

BLOCKCHAIN



Transferring assets, building value

Anything that is capable of being owned or controlled to produce value, is an asset



Two fundamental types of asset

- Tangible, e.g. a house
- Intangible, e.g. a mortgage



Intangible assets subdivide

- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. music

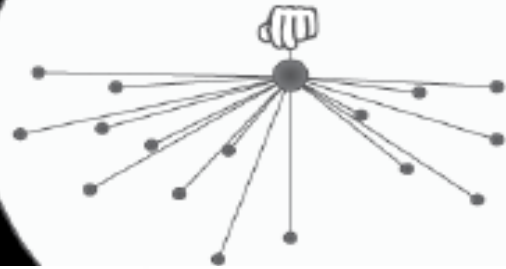


Cash is also an asset

- Has property of anonymity

Types of networks (from the viewpoint of control)

Centralized



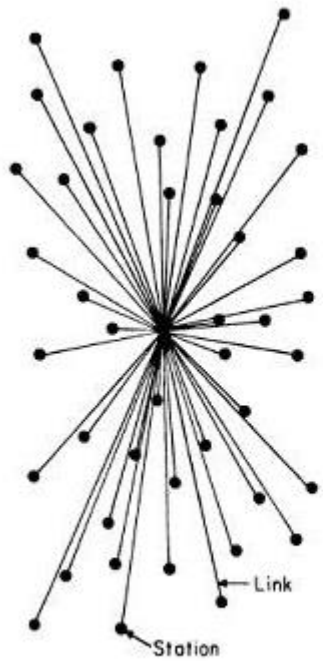
Distributed



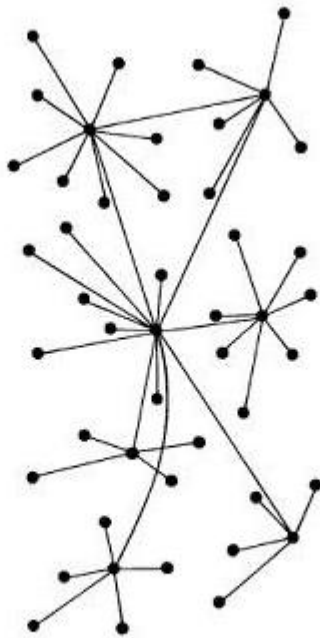
Decentralized



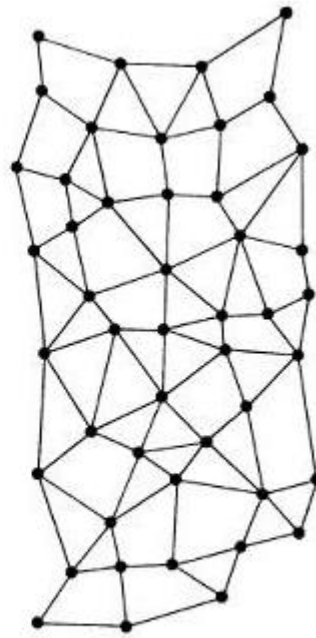
Peer-to-peer



CENTRALIZED
(A)



DECENTRALIZED
(B)



DISTRIBUTED
(C)

BLOCKCHAIN



1. Data: "Hello World!"



1. Data: "Hello World!"
2. Prev.Hash: 034DFA357



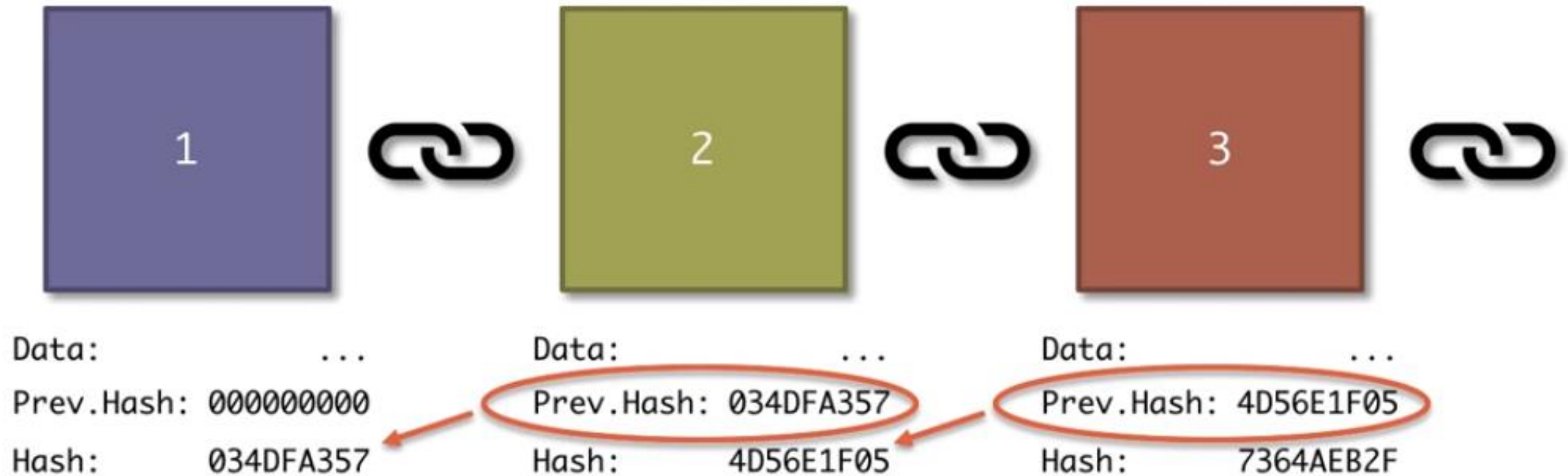
1. Data: "Hello World!"
2. Prev.Hash: 034DFA357
3. Hash: 4D56E1F05



1. Data: "Hello World!"
2. Prev.Hash: 034DFA357
3. Hash: 4D56E1F05

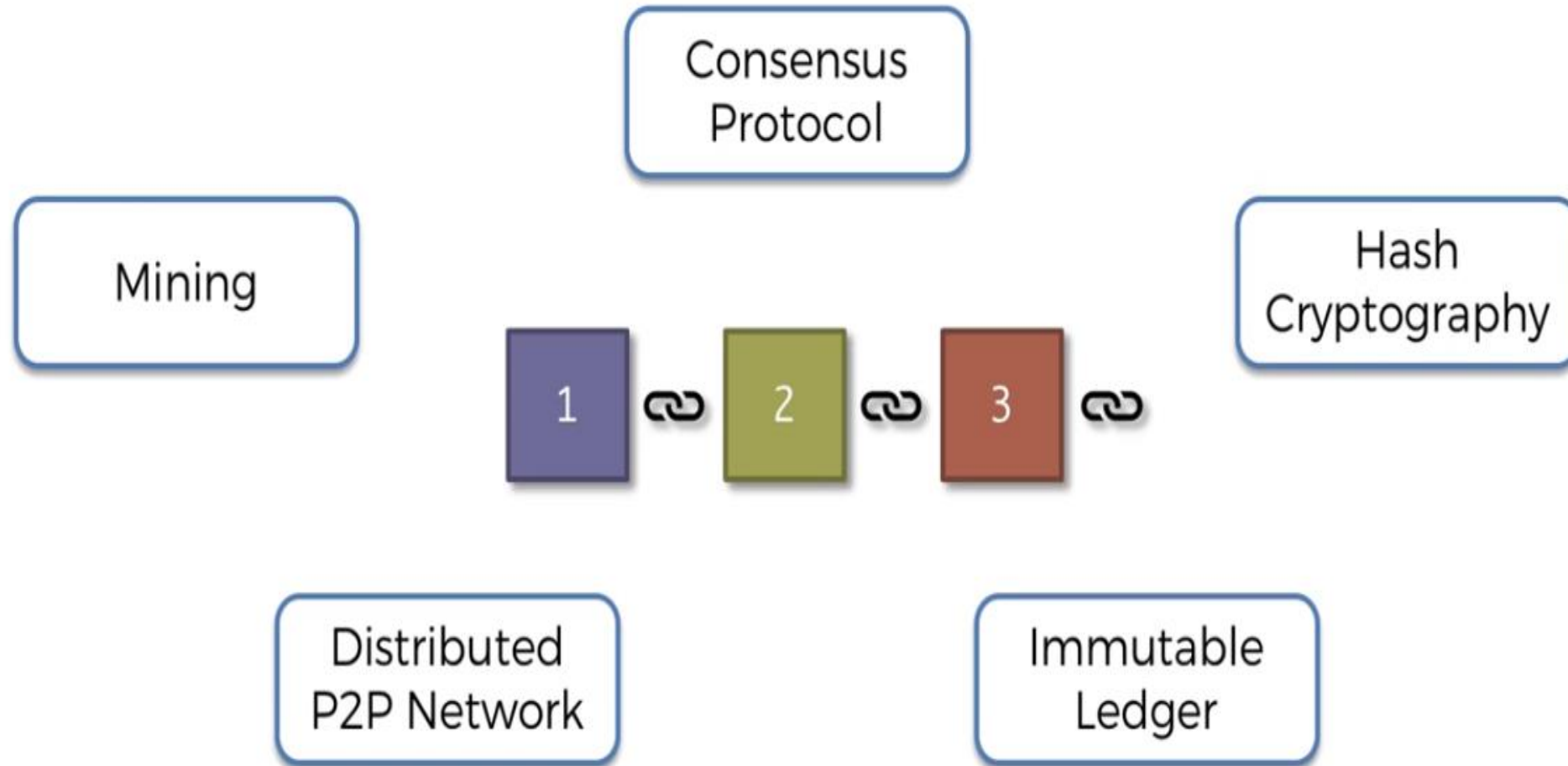
BLOCKCHAIN

GENESIS BLOCK



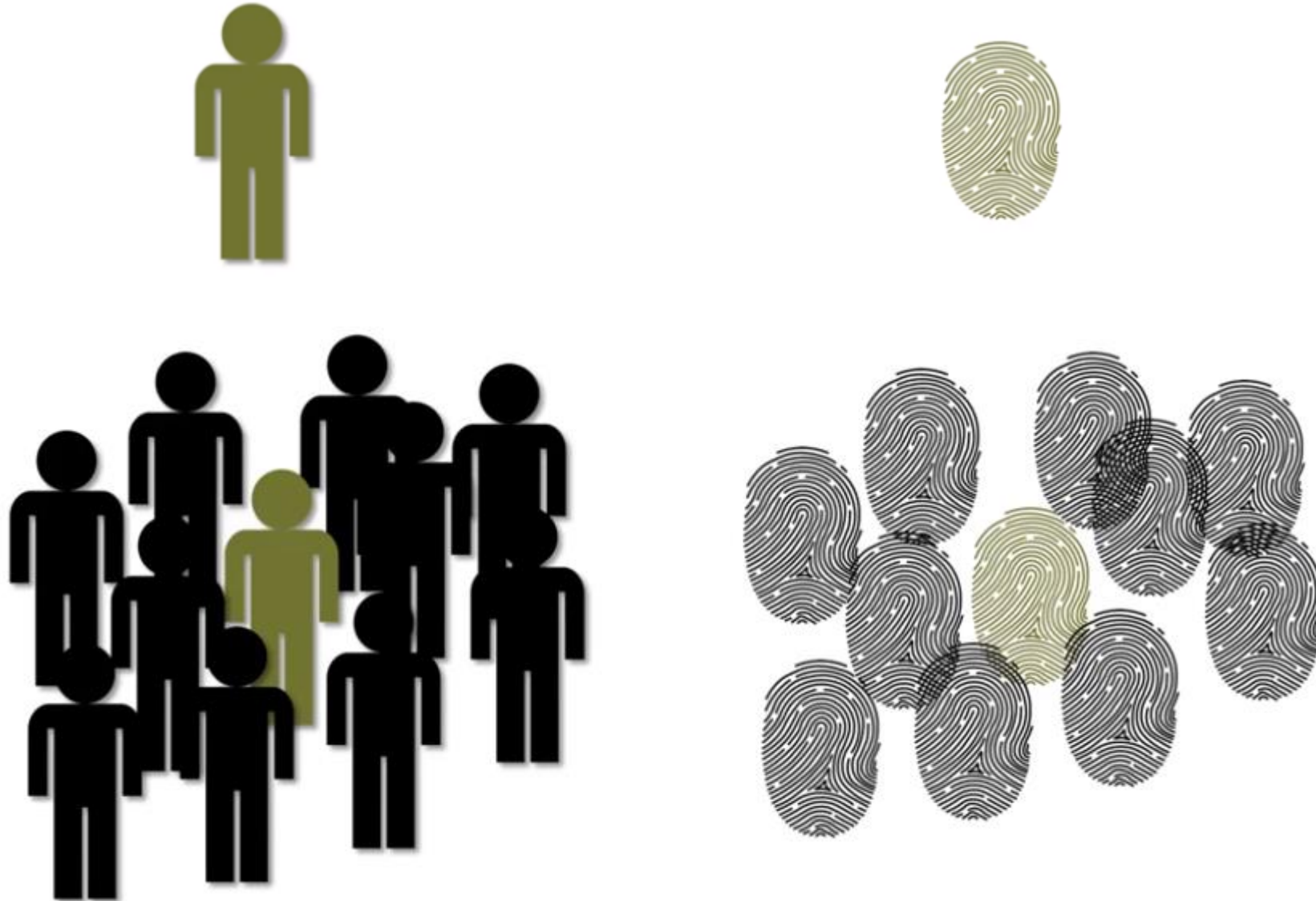
“Blocks are cryptographically linked together”

BLOCKCHAIN



SHA256 HASH

UNDERSTANDING SHA256 HASH



UNDERSTANDING SHA256 HASH



UNDERSTANDING SHA256 HASH



UNDERSTANDING SHA256 HASH



0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F



SHA256 takes 256 bits in memory
Represented by 64 characters

2a89bf1700a91
40aa496380fd0
b4443921bbeef
b9cdb9ef6ea74
07cf82286afc

NSA
'SHA256'
64 characters

Creates hash for all types of digital documents like – text, pdf, video, audio, executable or operating systems

05 REQUIREMENTS OF HASH ALGORITHMS

1. One-Way

2. Deterministic

- Same hash will be generated each time for a particular document

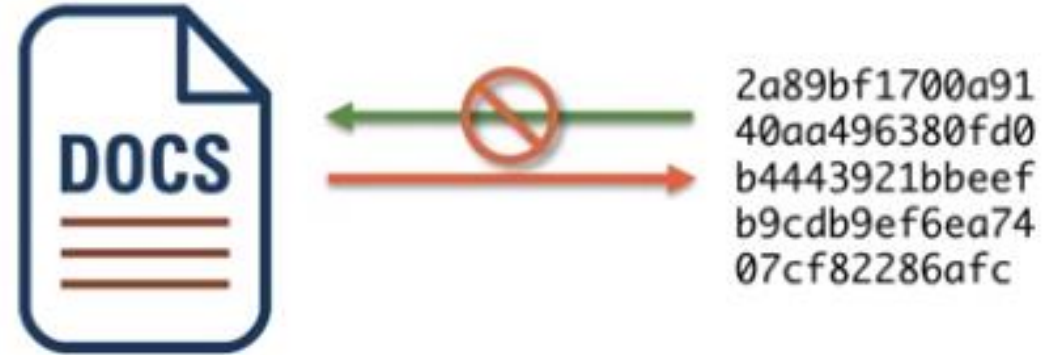
3. Fast Computation

4. Avalanche Effect

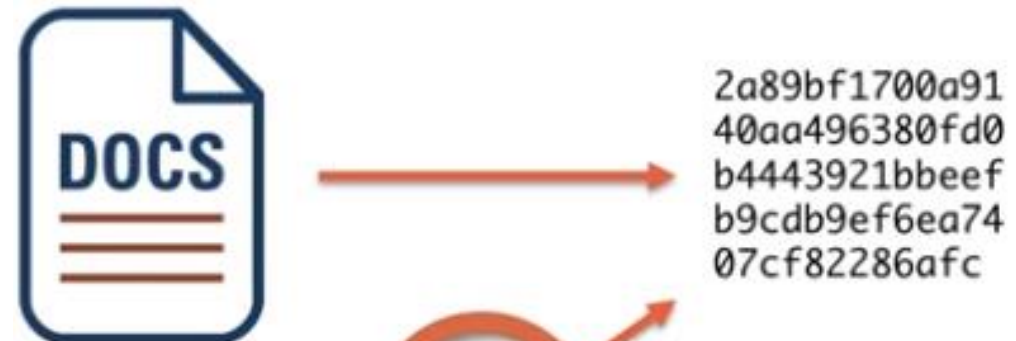
- A small change in document will change the hash completely

5. Must withstand Collision

- Accommodate a rare similar hash but avoid fraudulently created similar document



2a89bf1700a91
40aa496380fd0
b4443921bbeef
b9cdb9ef6ea74
07cf82286afc



2a89bf1700a91
40aa496380fd0
b4443921bbeef
b9cdb9ef6ea74
07cf82286afc

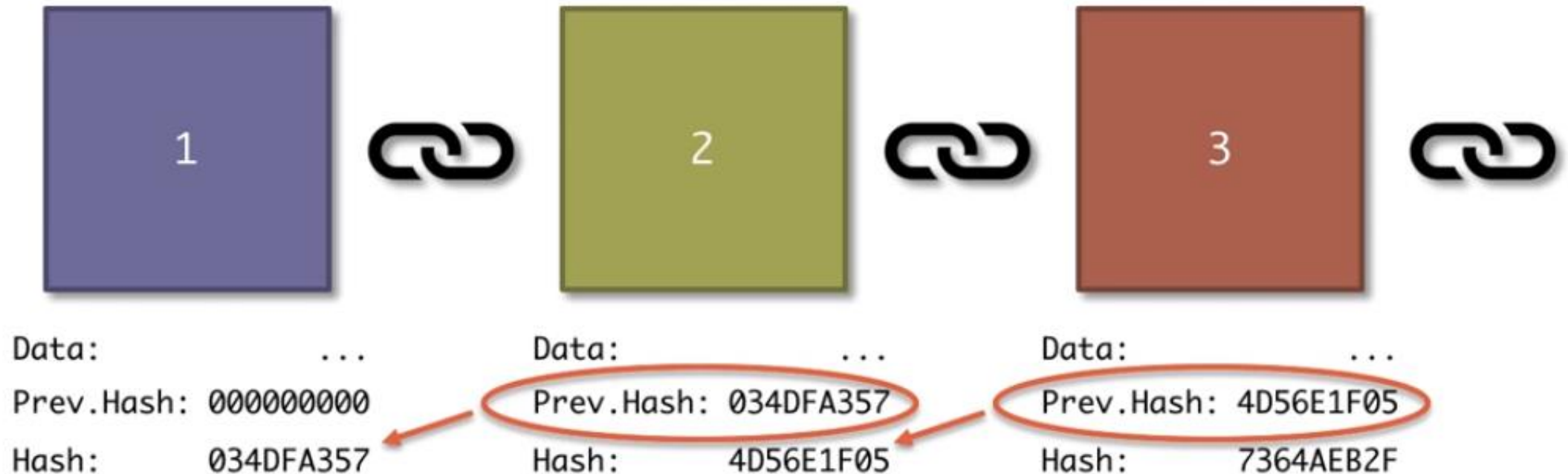


IMMUTABLE LEDGER

45

OUR UNDERSTANDING ON BLOCKCHAIN

GENESIS BLOCK



“Blocks are cryptographically linked together”

IMMUTABLE LEDGERS

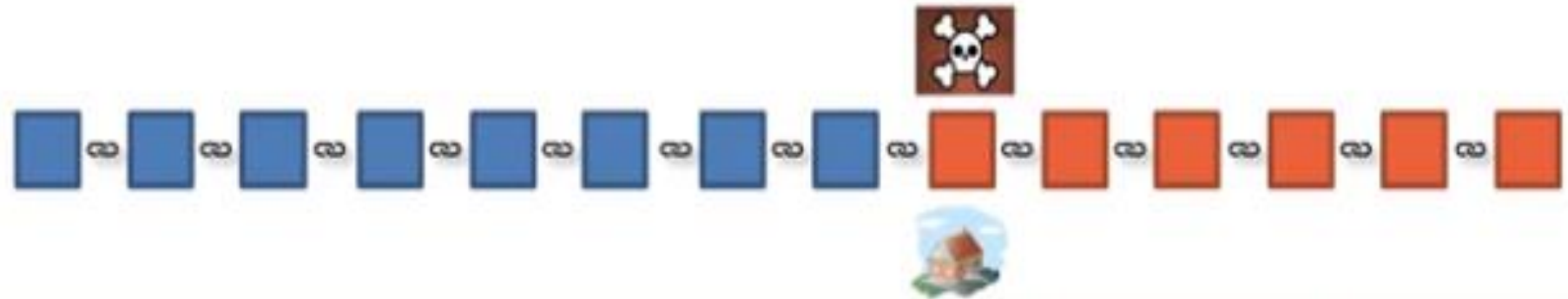
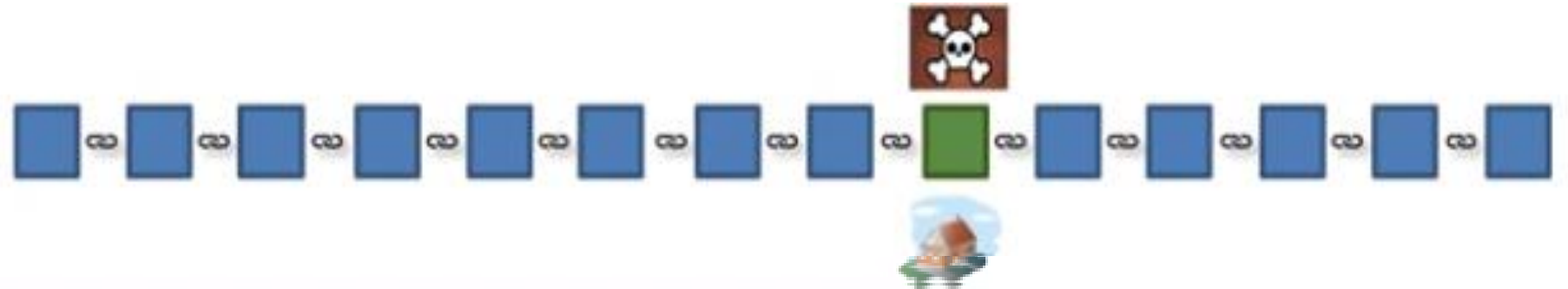


Traditional Ledger

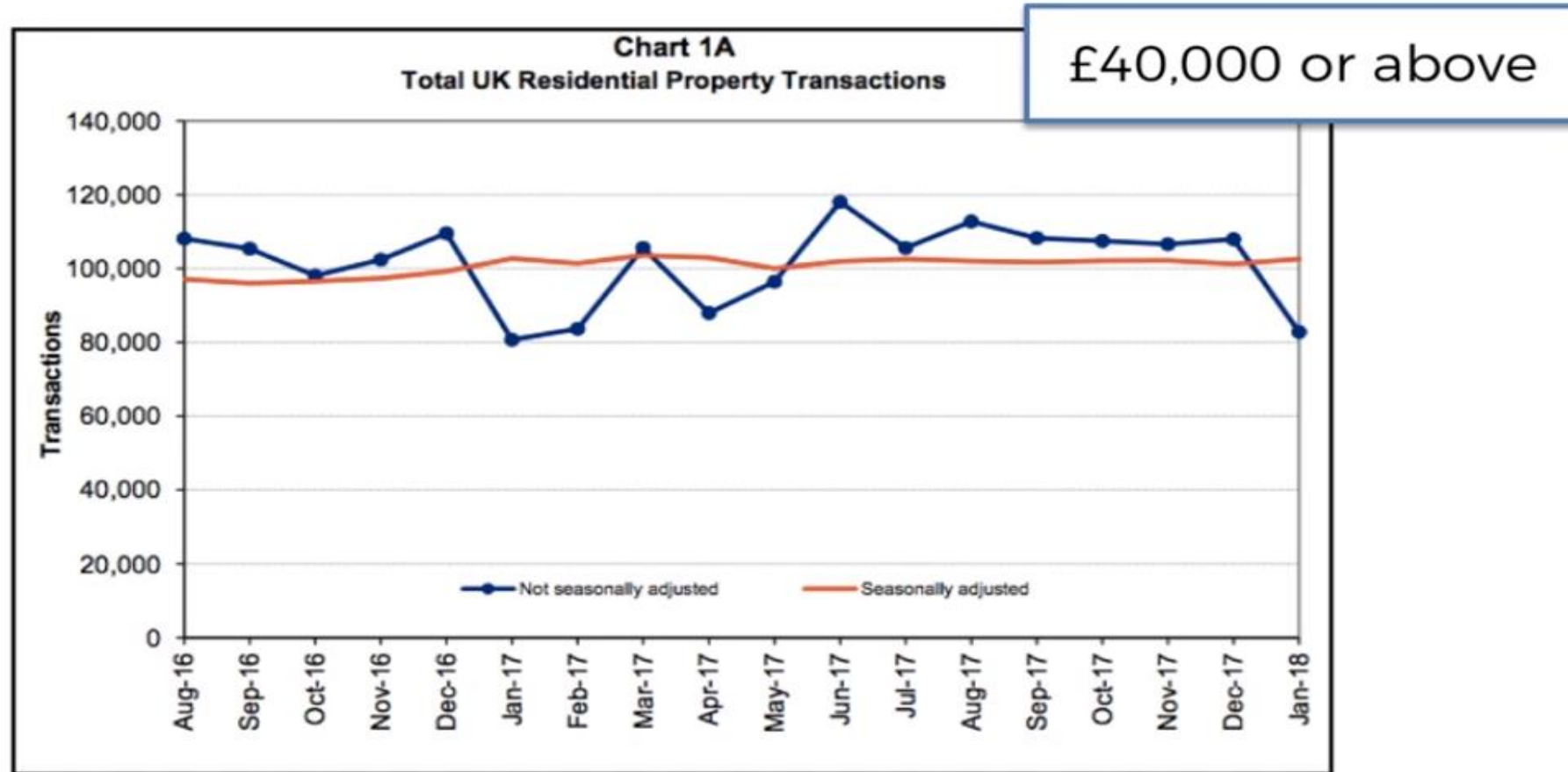


IMMUTABLE LEDGERS

Blockchain



IMMUTABLE LEDGER

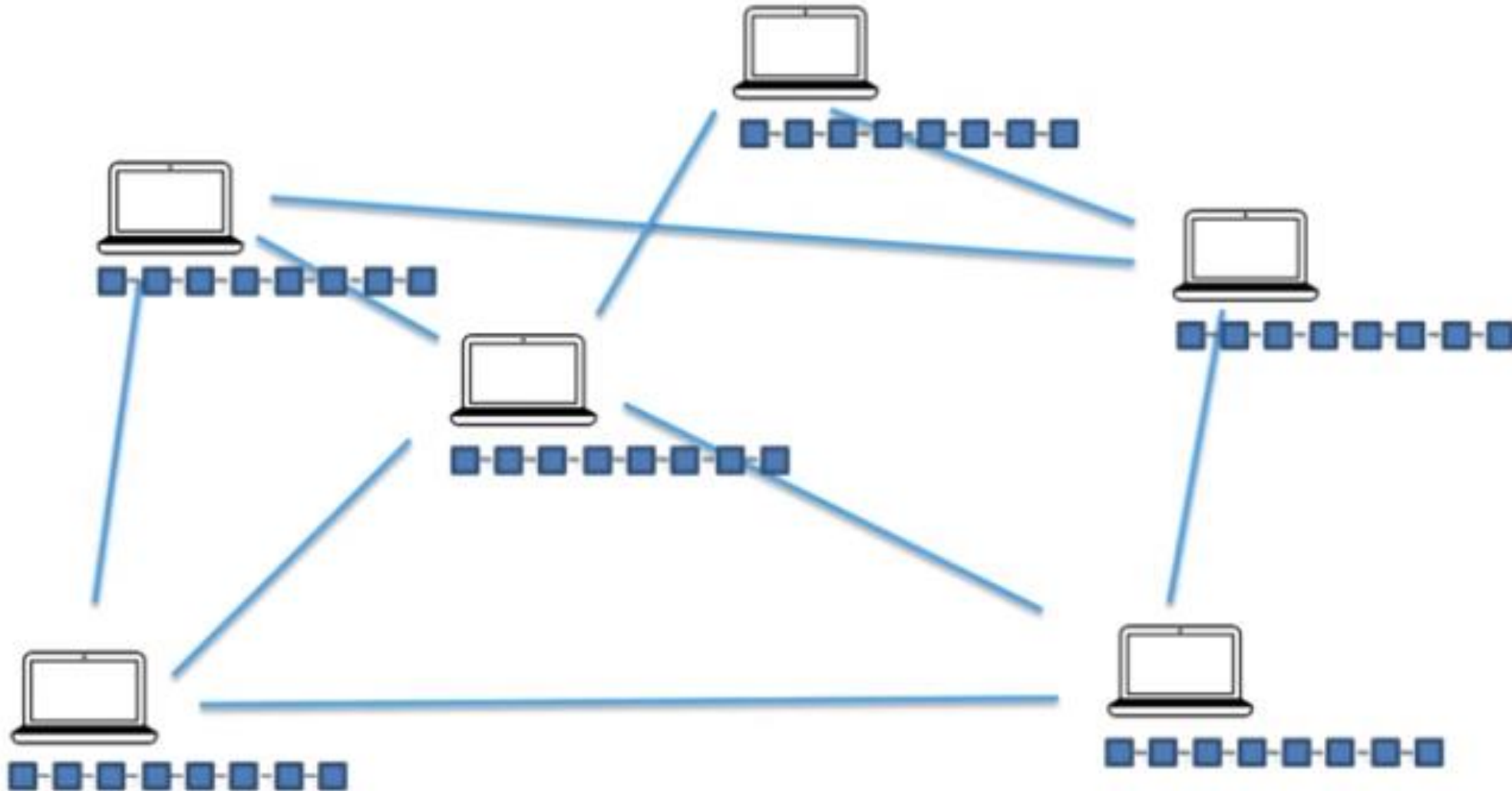


Source: <https://www.gov.uk>

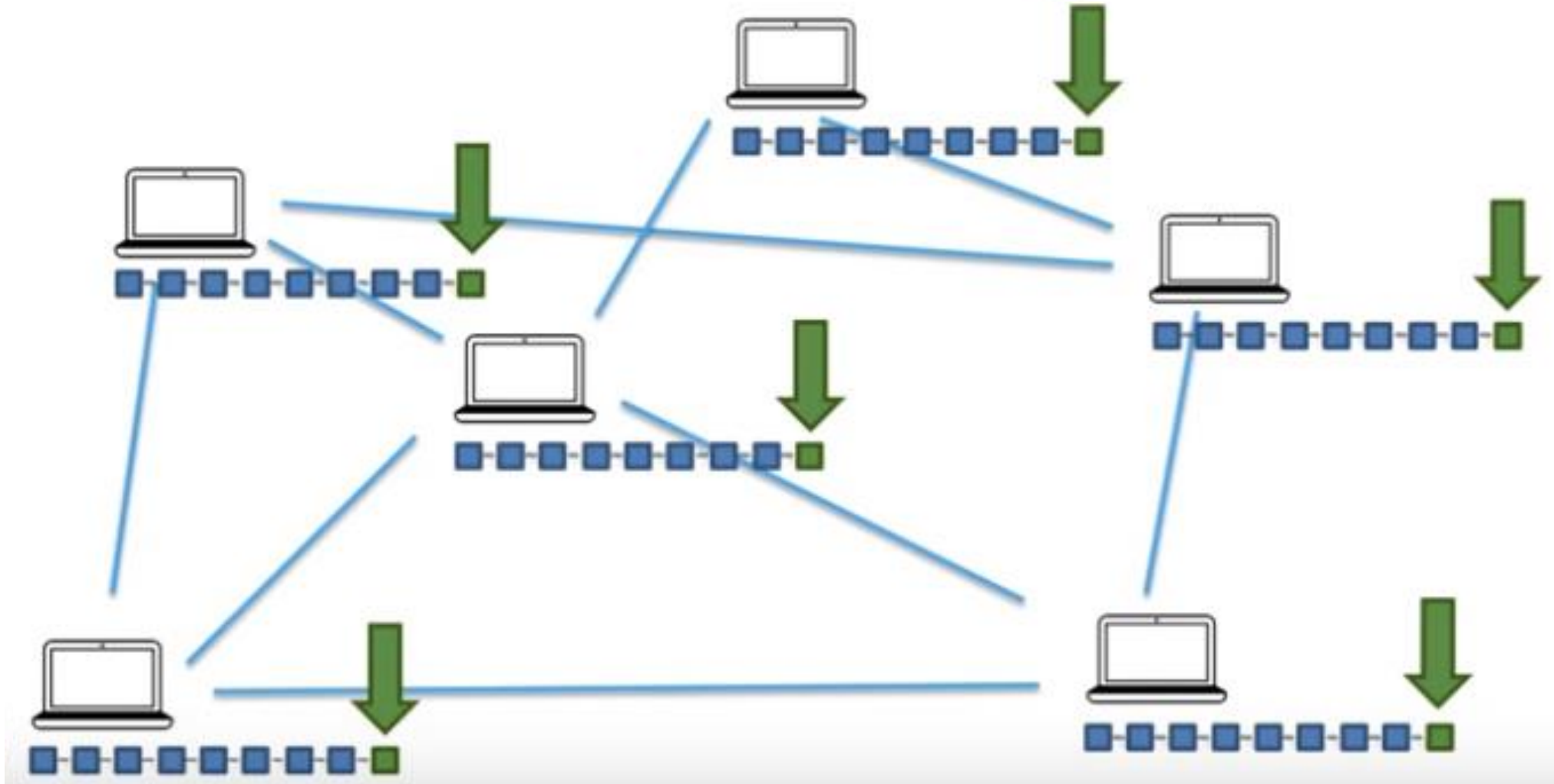
DISTRIBUTED P2P NETWORK

50

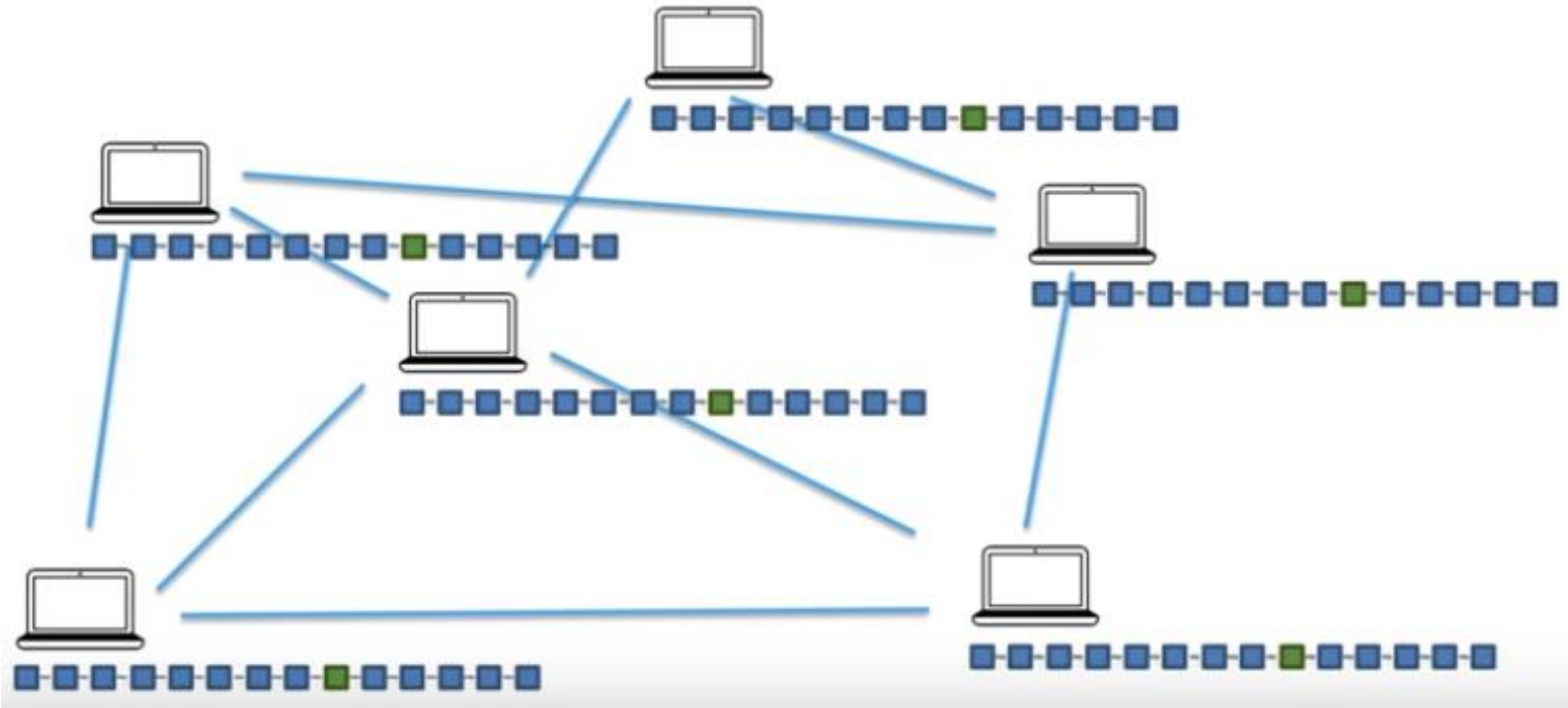
DISTRIBUTED P2P NETWORK



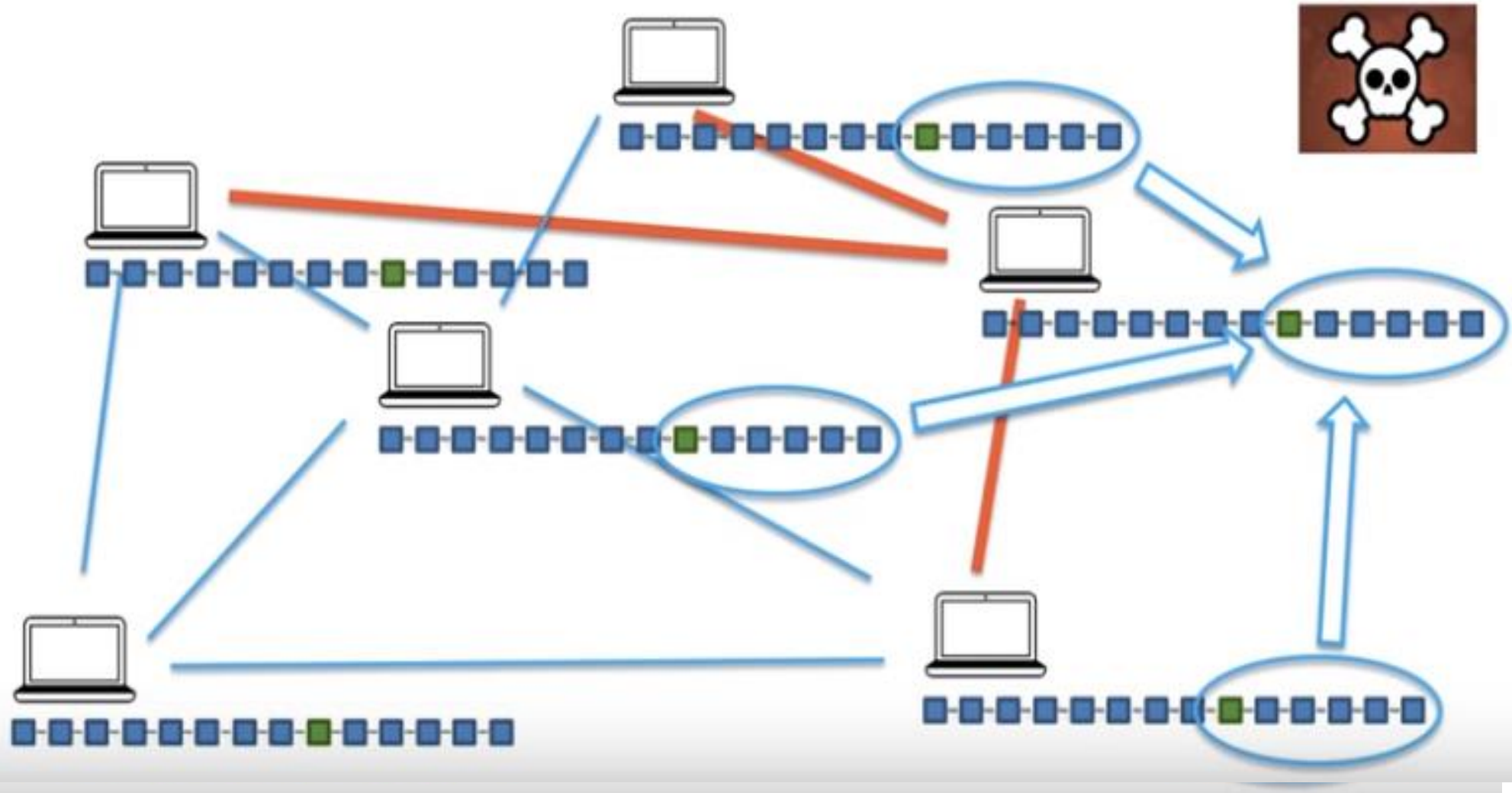
DISTRIBUTED P2P NETWORK



DISTRIBUTED P2P NETWORK



DISTRIBUTED P2P NETWORK



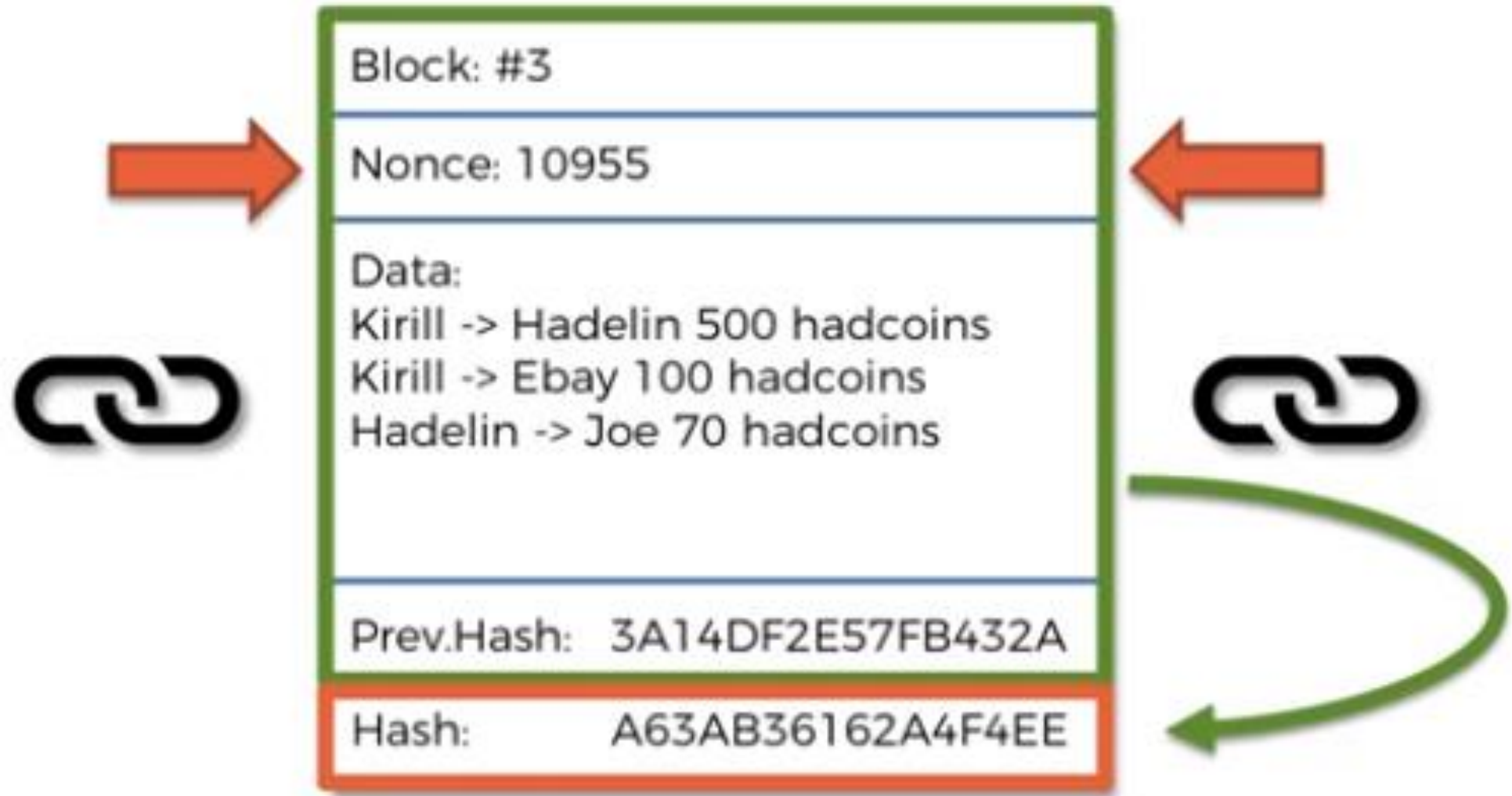
MINING

55

HOW MINING WORKS



HOW MINING WORKS



HOW MINING WORKS

A Hash is a Number

18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68
=11232962686236154915841062771303455665105266333
445130312258268457057784990824

```
00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923
      =0000000000000000218420711603109937116824492054445
      852323869008912526075378993443
```

[illegible]

HOW MINING WORKS

 18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

[illegible]

TIP: Express Target with leading Zeroes
E.g. '0000'

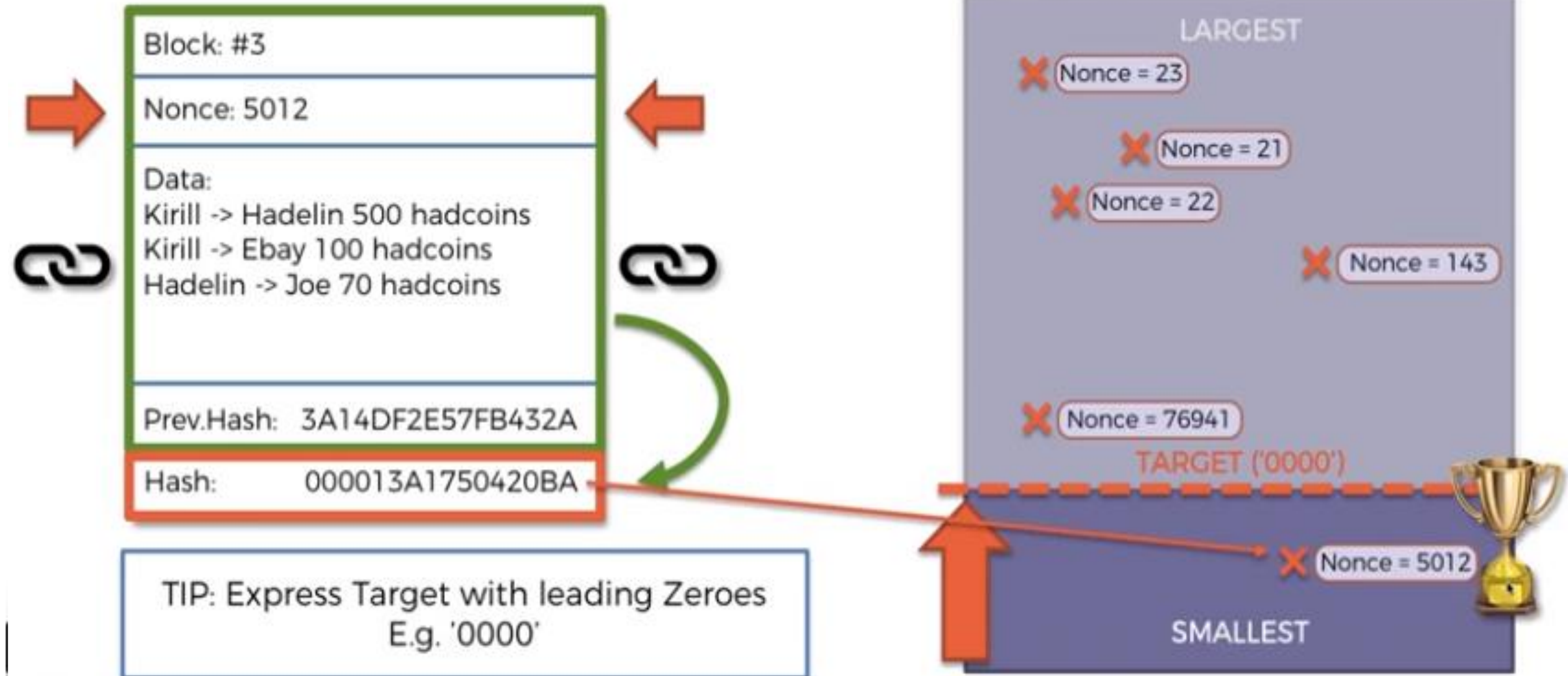
- ALL POSSIBLE HASHES -

LARGEST

TARGET ('0000')

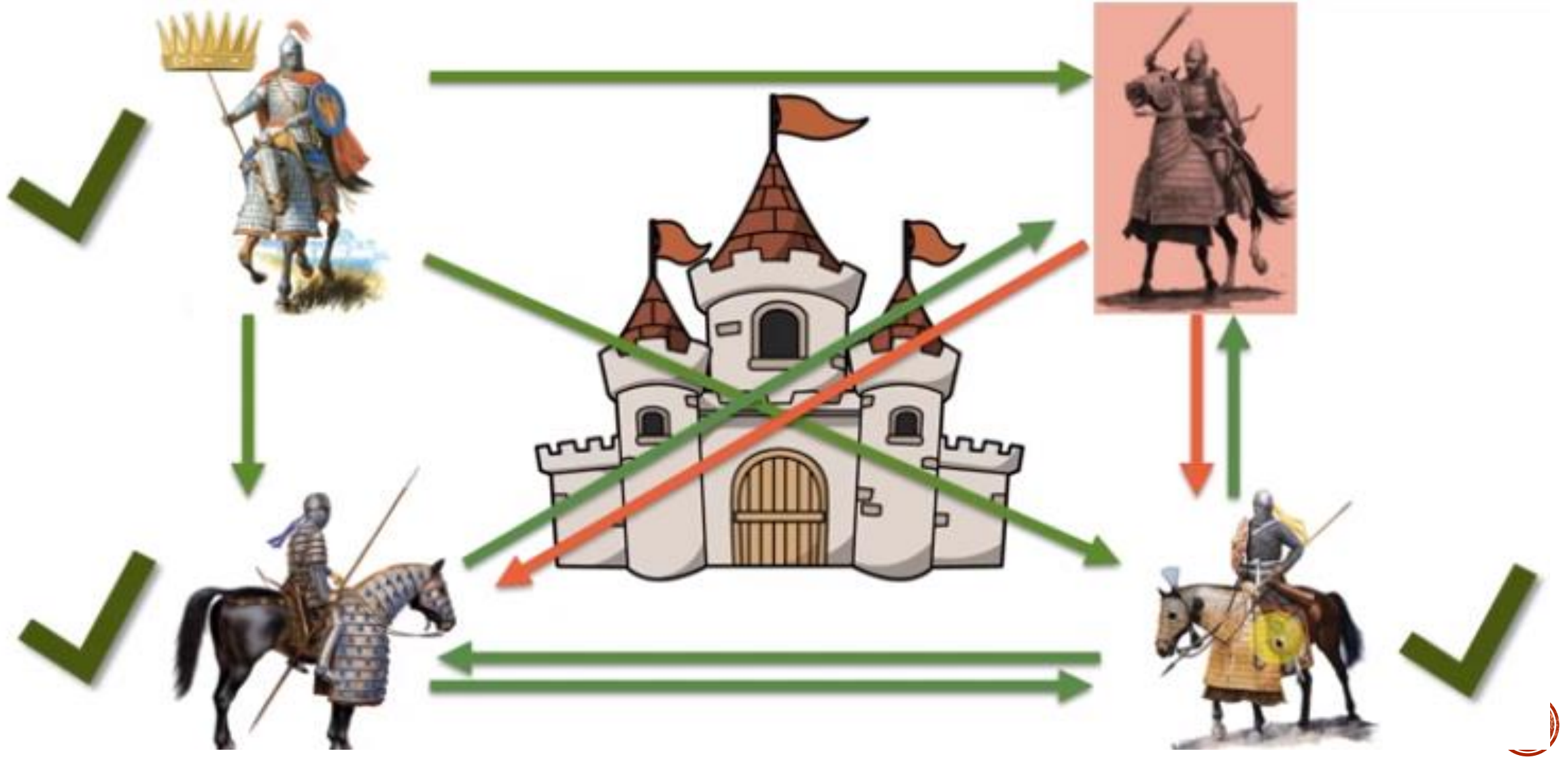
X
SMALLEST

HOW MINING WORKS

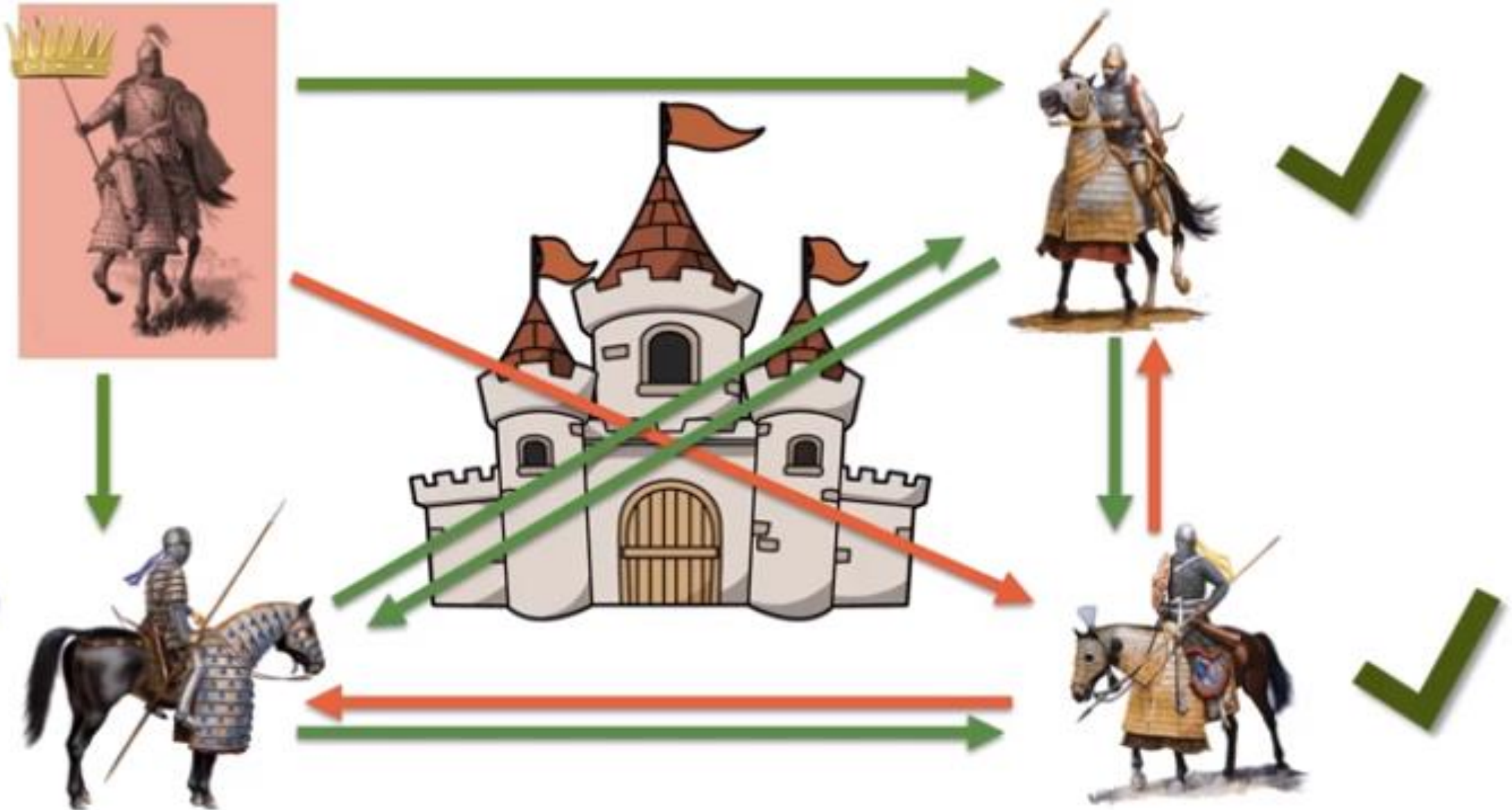


BYZANTINE FAULT TOLERANCE

BYZANTINE FAULT TOLERANCE



BYZANTINE FAULT TOLERANCE



BYZANTINE FAULT TOLERANCE

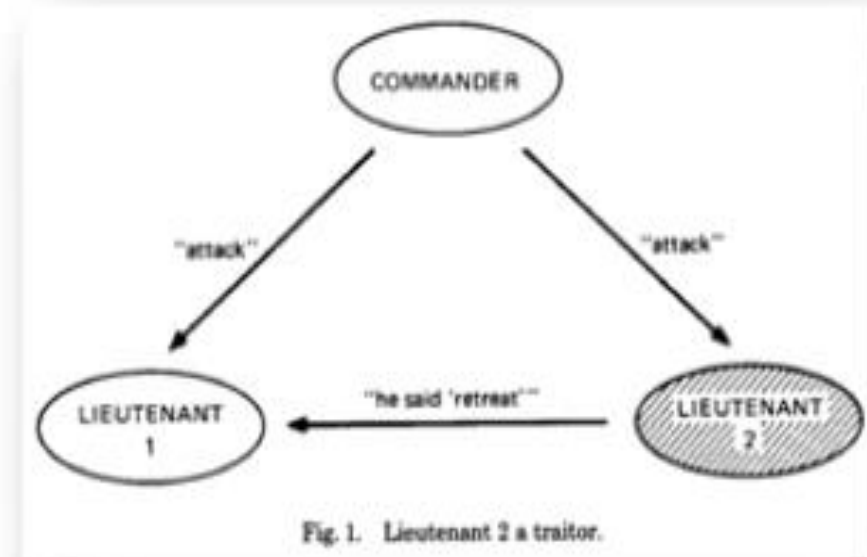
Additional Reading:

The Byzantine Generals Problem

Leslie Lamport, Robert Shostak,
and Marshall Pease (1982)

Link:

<https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf>

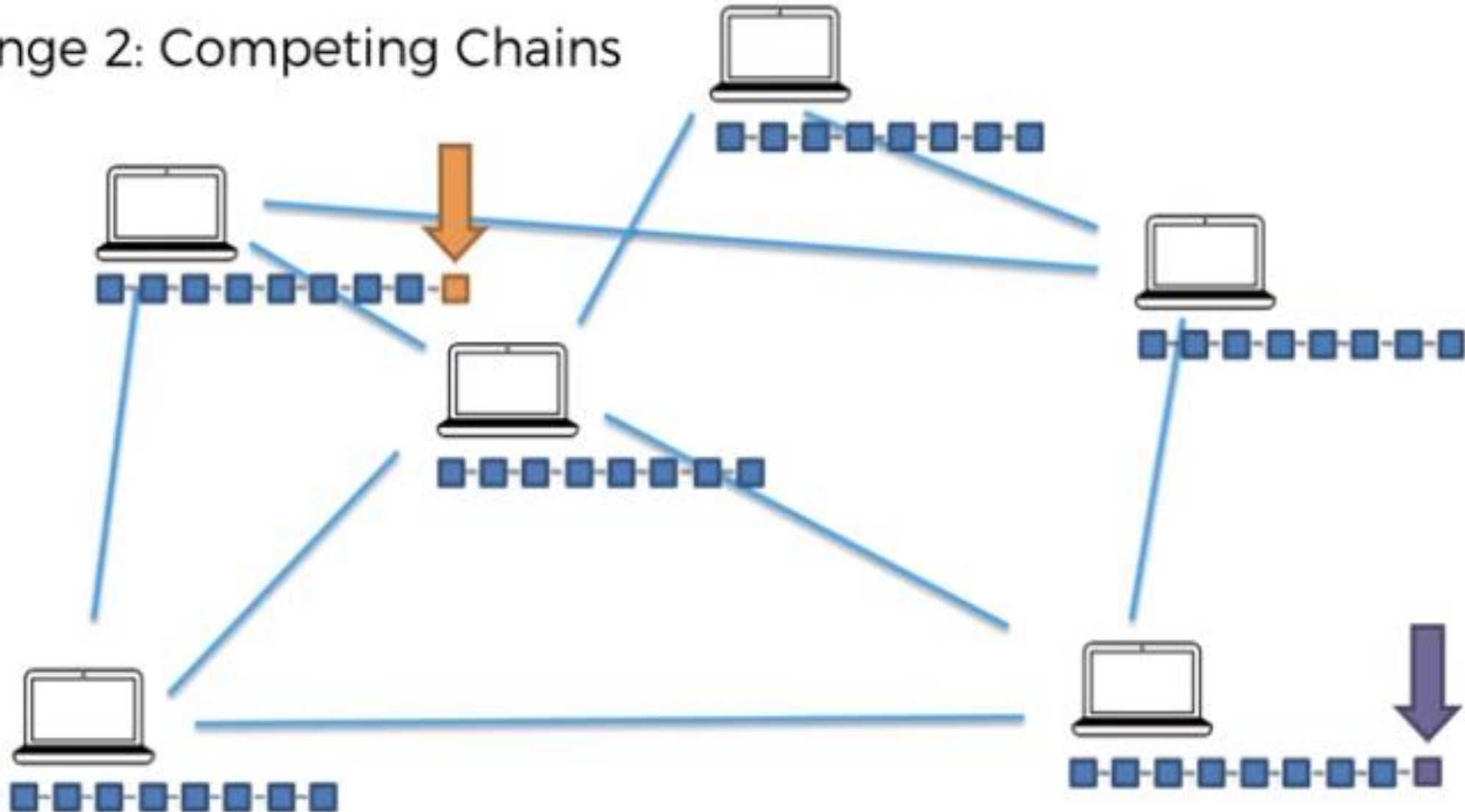


CONSENSUS PROTOCOL

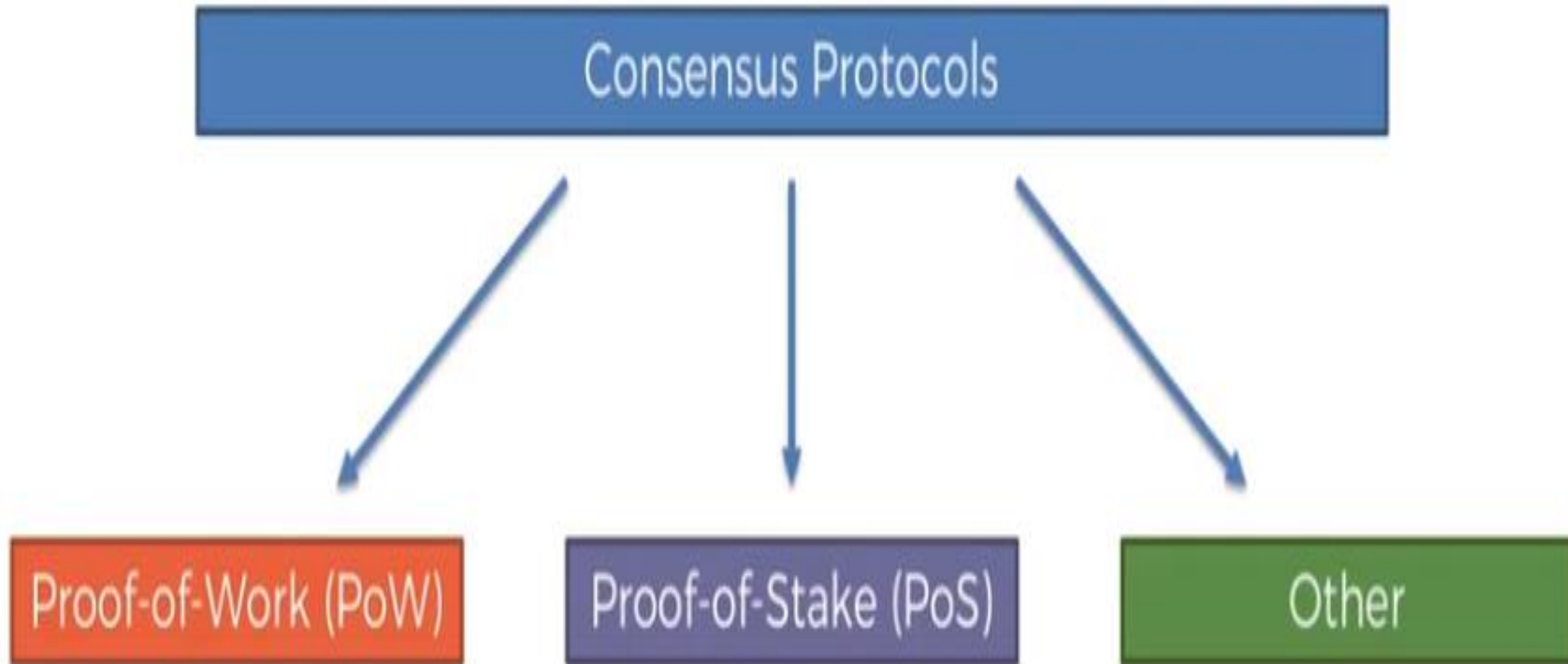
65

CONSENSUS PROTOCOL: HANDLES 02 PROBLEMS

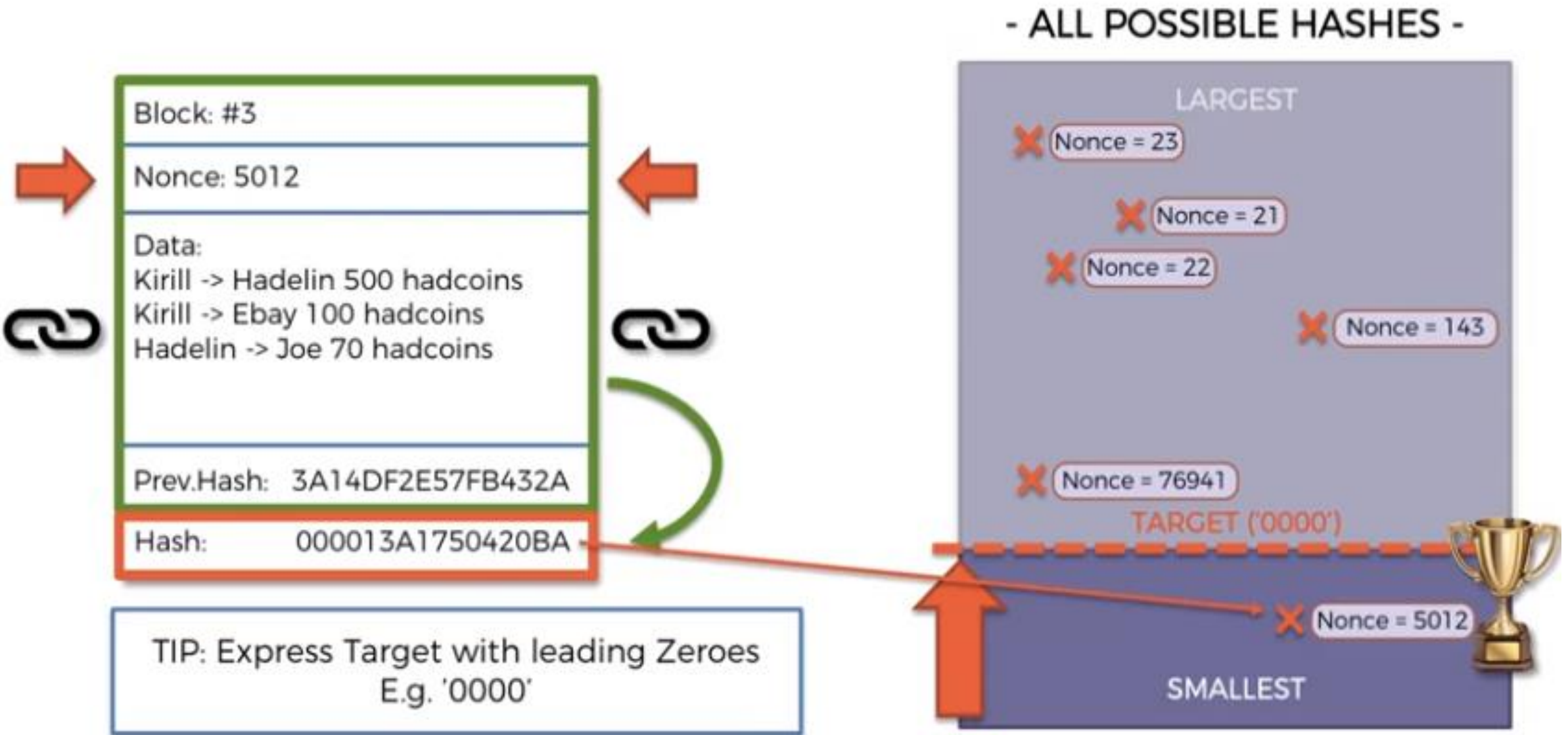
Challenge 2: Competing Chains



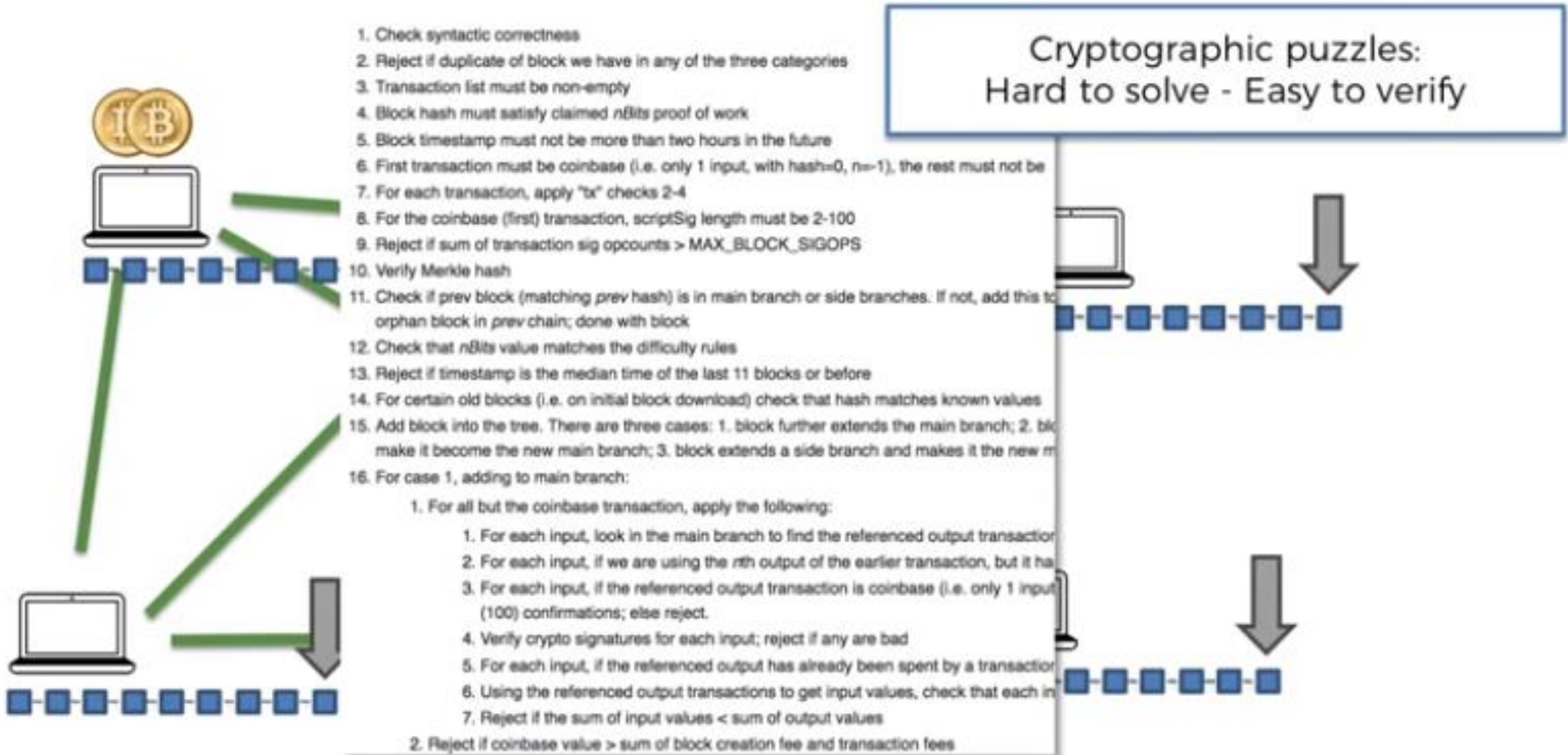
CONSENSUS PROTOCOL



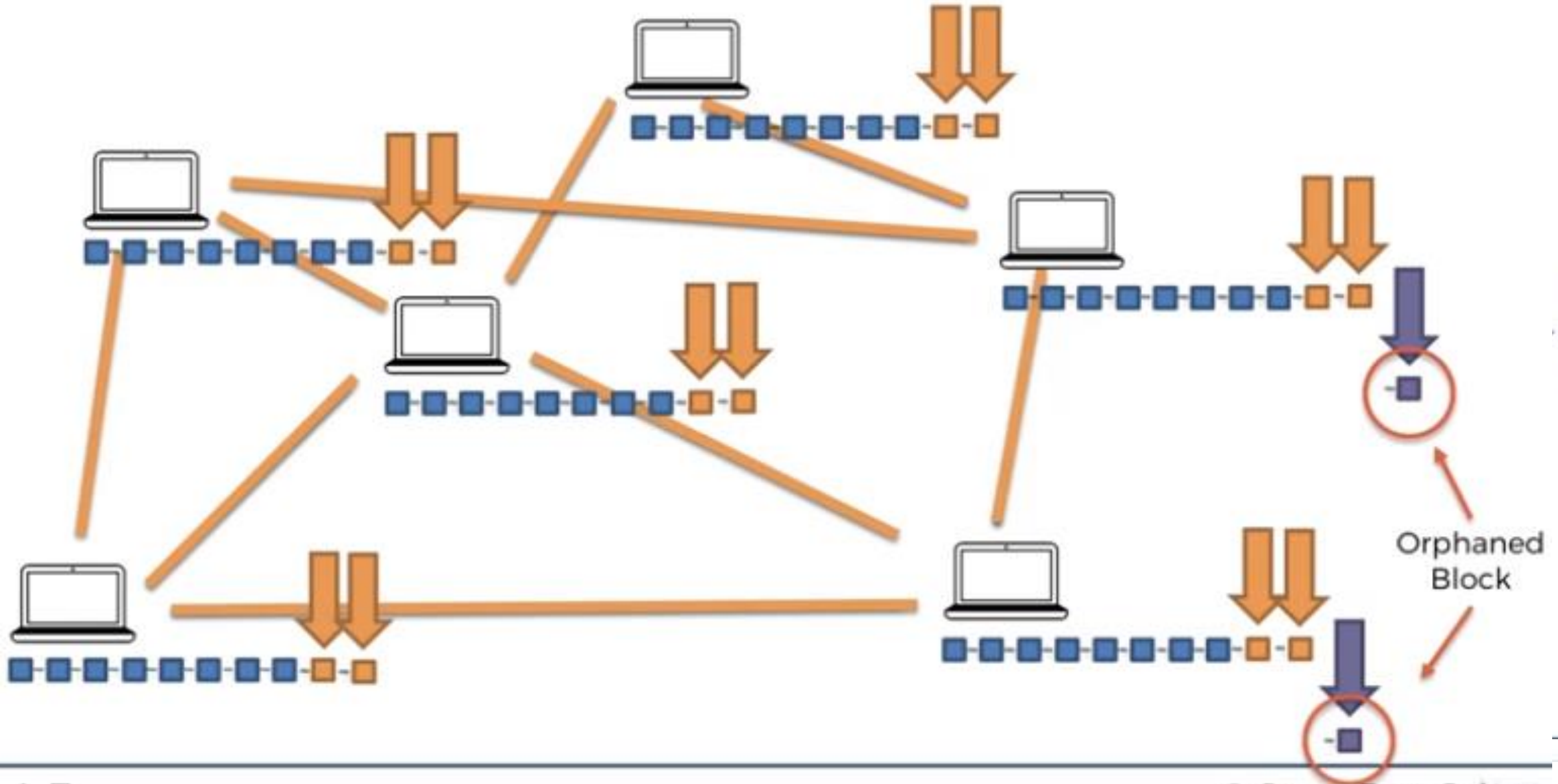
CONSENSUS PROTOCOL



CONSENSUS PROTOCOL: TO HANDLE ATTACKERS



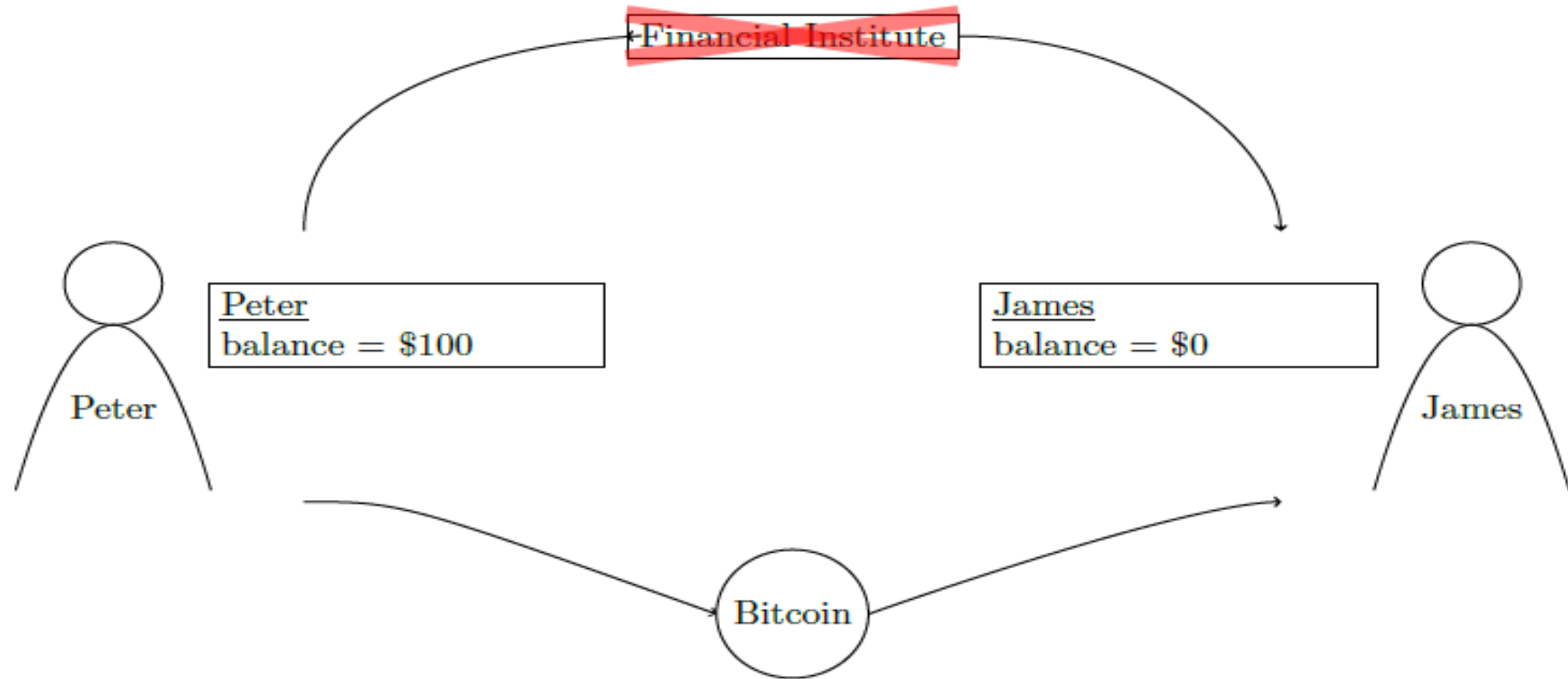
CONSENSUS PROTOCOL-COMPETING CHAIN



BLOCKCHAIN SOLUTIONS

71

HIGH TRANSACTION FEE: BLOCKCHAIN IS THE SOLUTION



DOUBLE SPENDING: BLOCKCHAIN IS THE SOLUTION

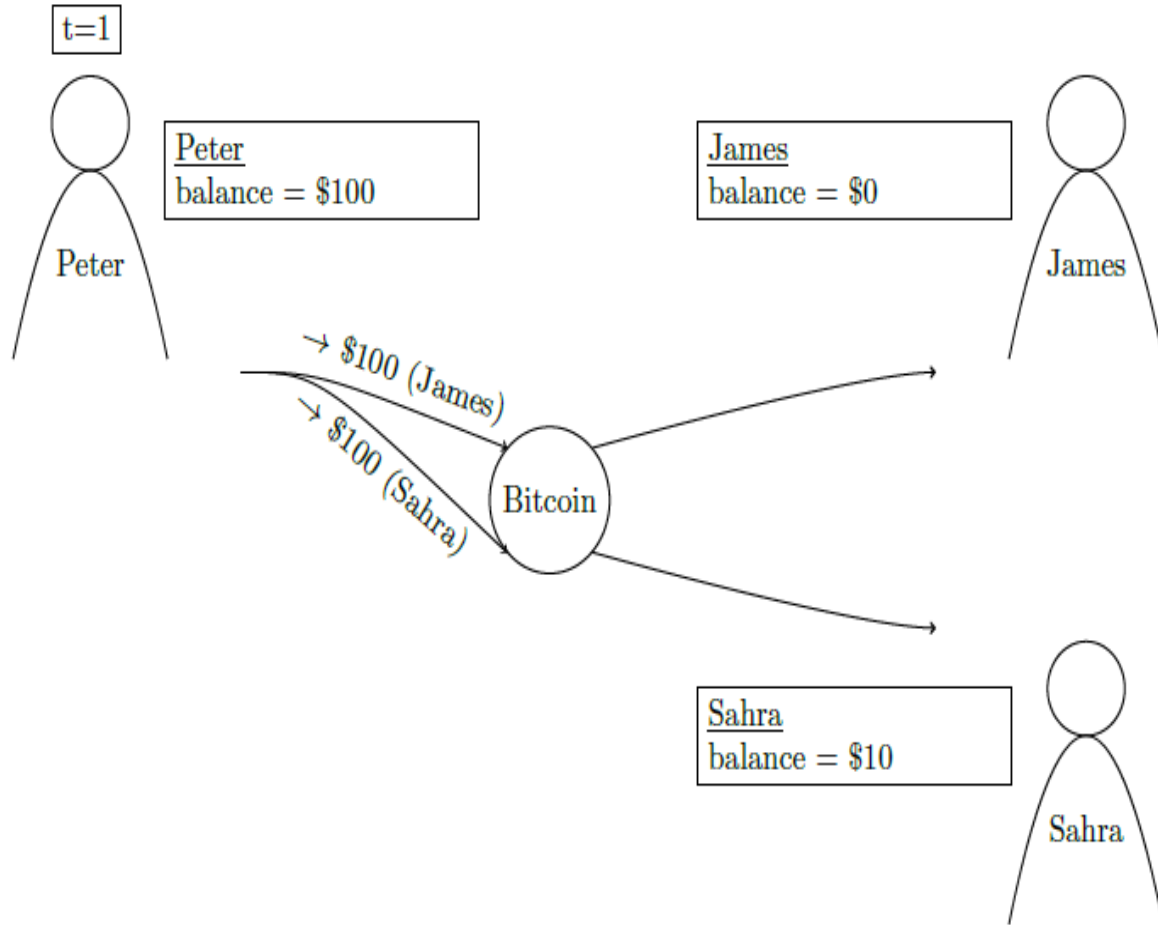


Figure 1.2: Peter promised his \$100 to both James and Sahra!

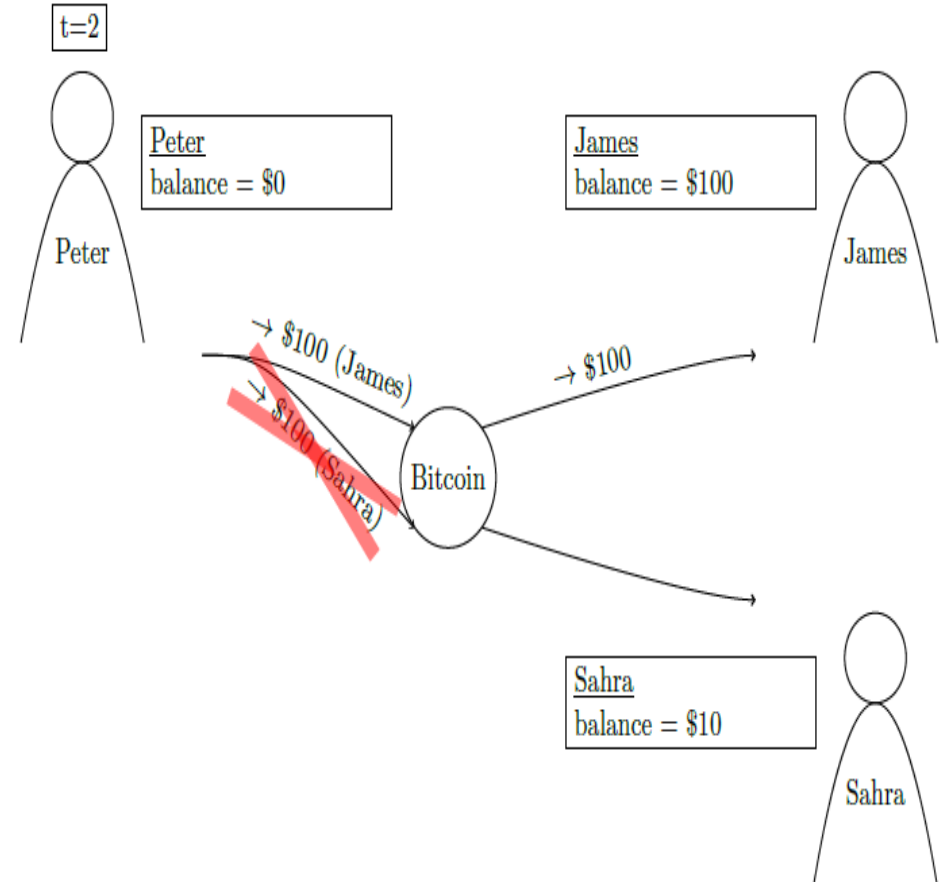
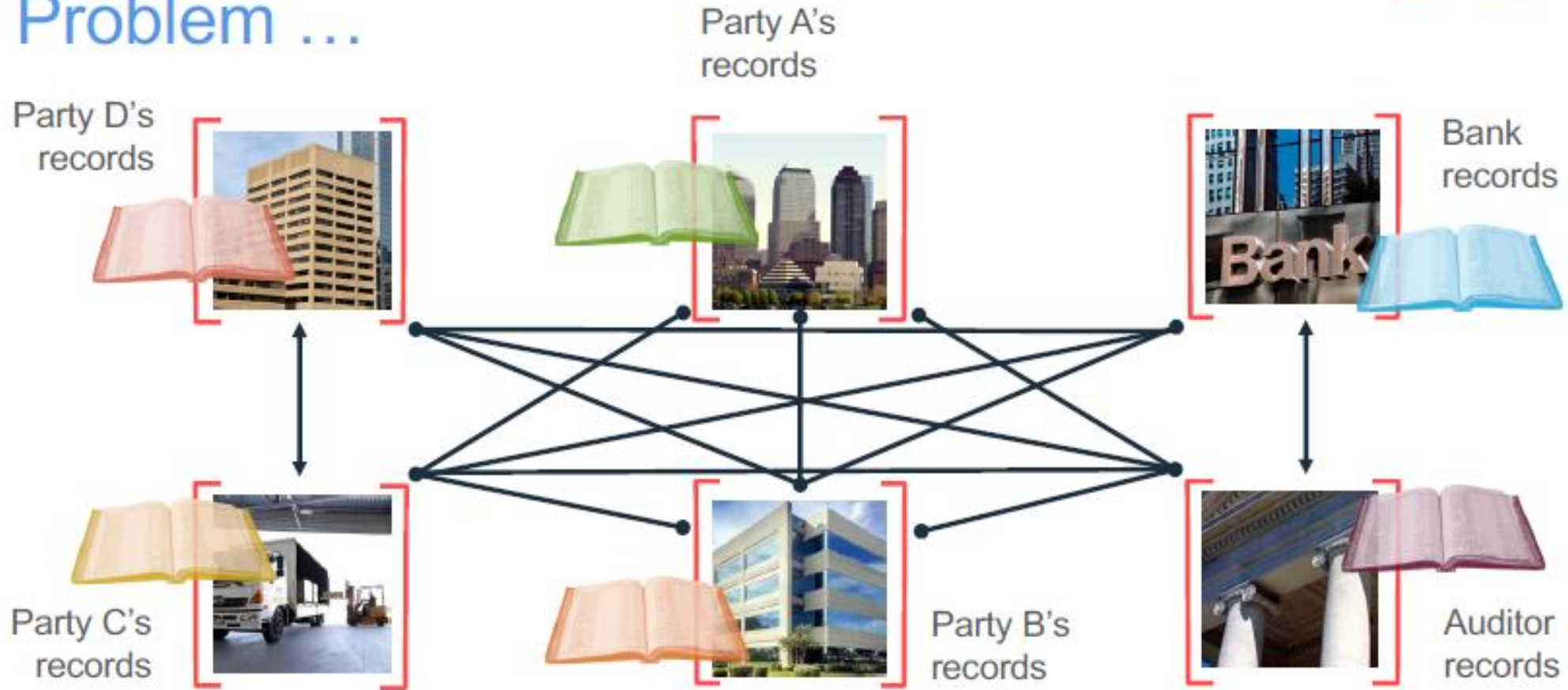


Figure 1.3: Blockchain checks this, and only the first promised, will receive the money

TRADITIONAL BUSINESS NETWORK



Problem ...

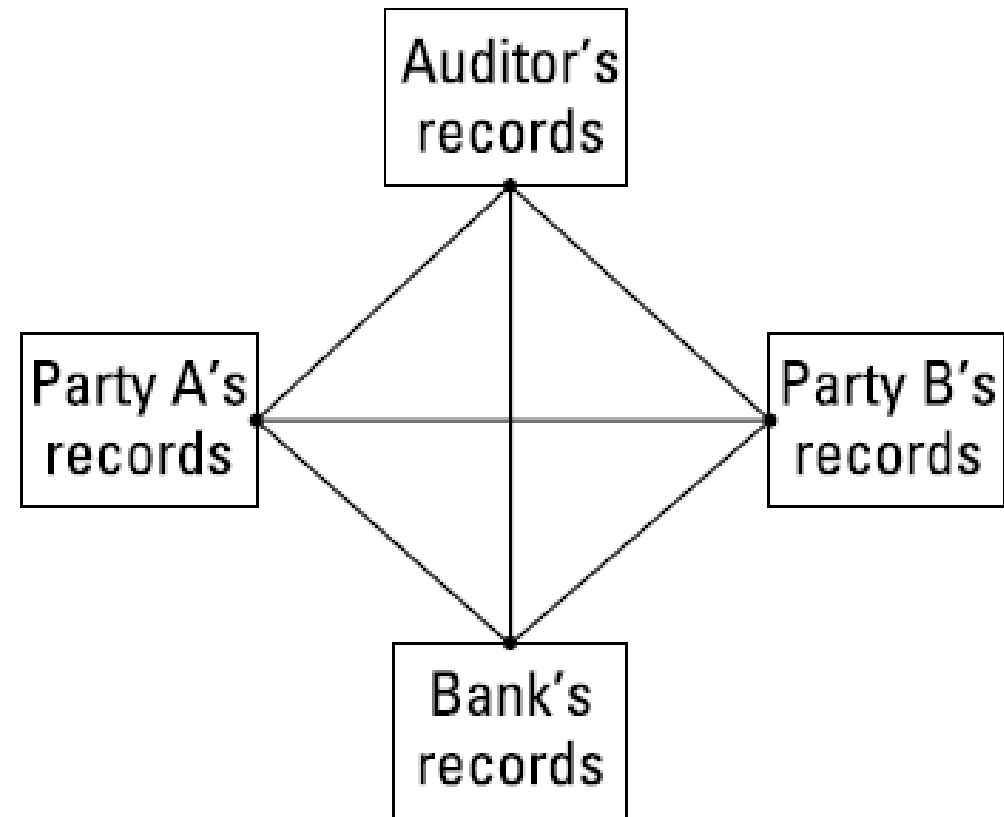


... Inefficient, expensive, vulnerable

TRADITIONAL BUSINESS NETWORK

Traditional method is:

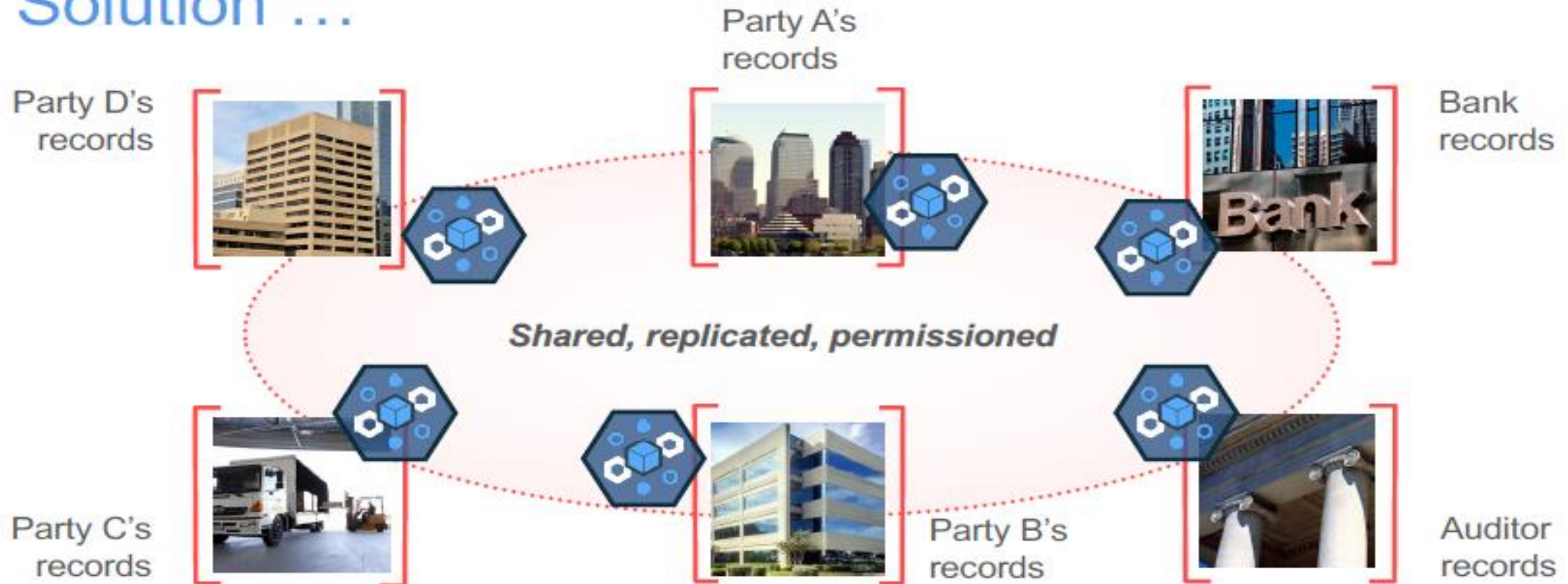
1. **Expensive** as it involves intermediaries that charge fee for their services.
2. **Inefficient** due to delays in executing agreements
3. **Duplication** of efforts to maintain numerous ledgers
4. **Vulnerable** – if the central system (eg. Bank) is compromised due to fraud, cyber-attack, simple mistake, the entire business network is affected.



BUSINESS NETWORK ON BLOCKCHAIN



Solution ...

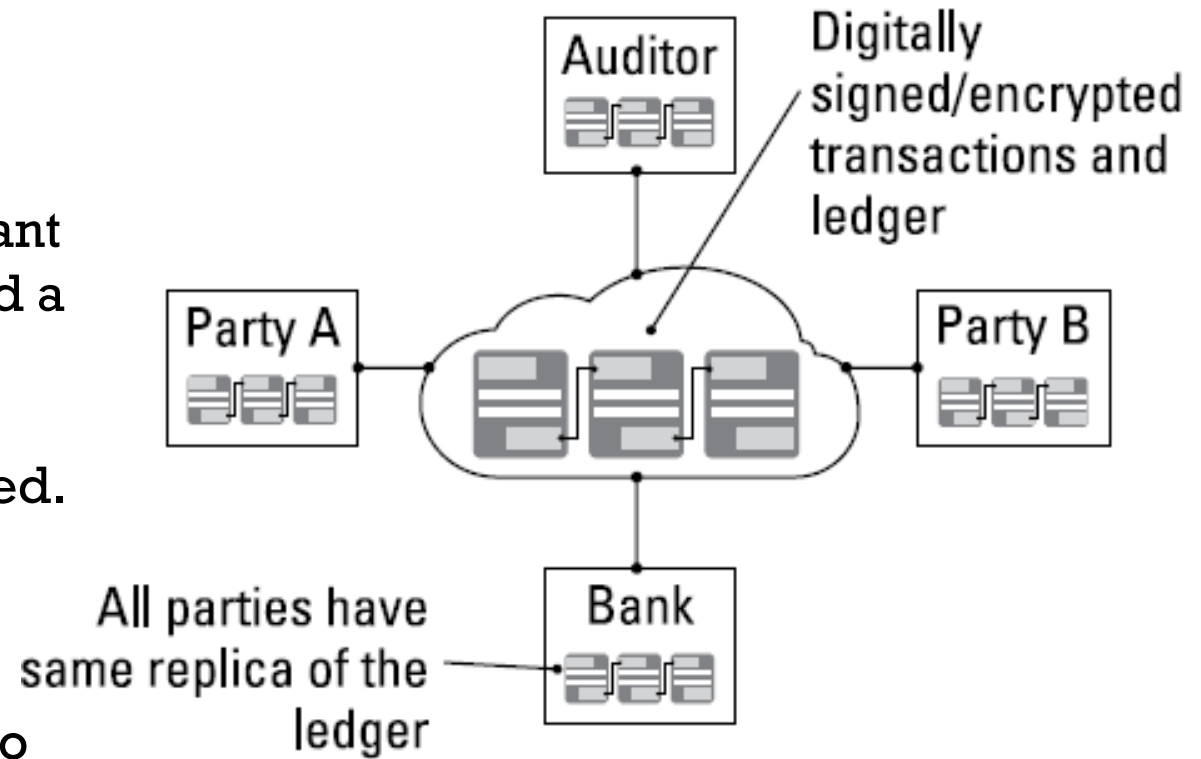


... Consensus, provenance, immutability, finality

BUSINESS NETWORK ON BLOCKCHAIN

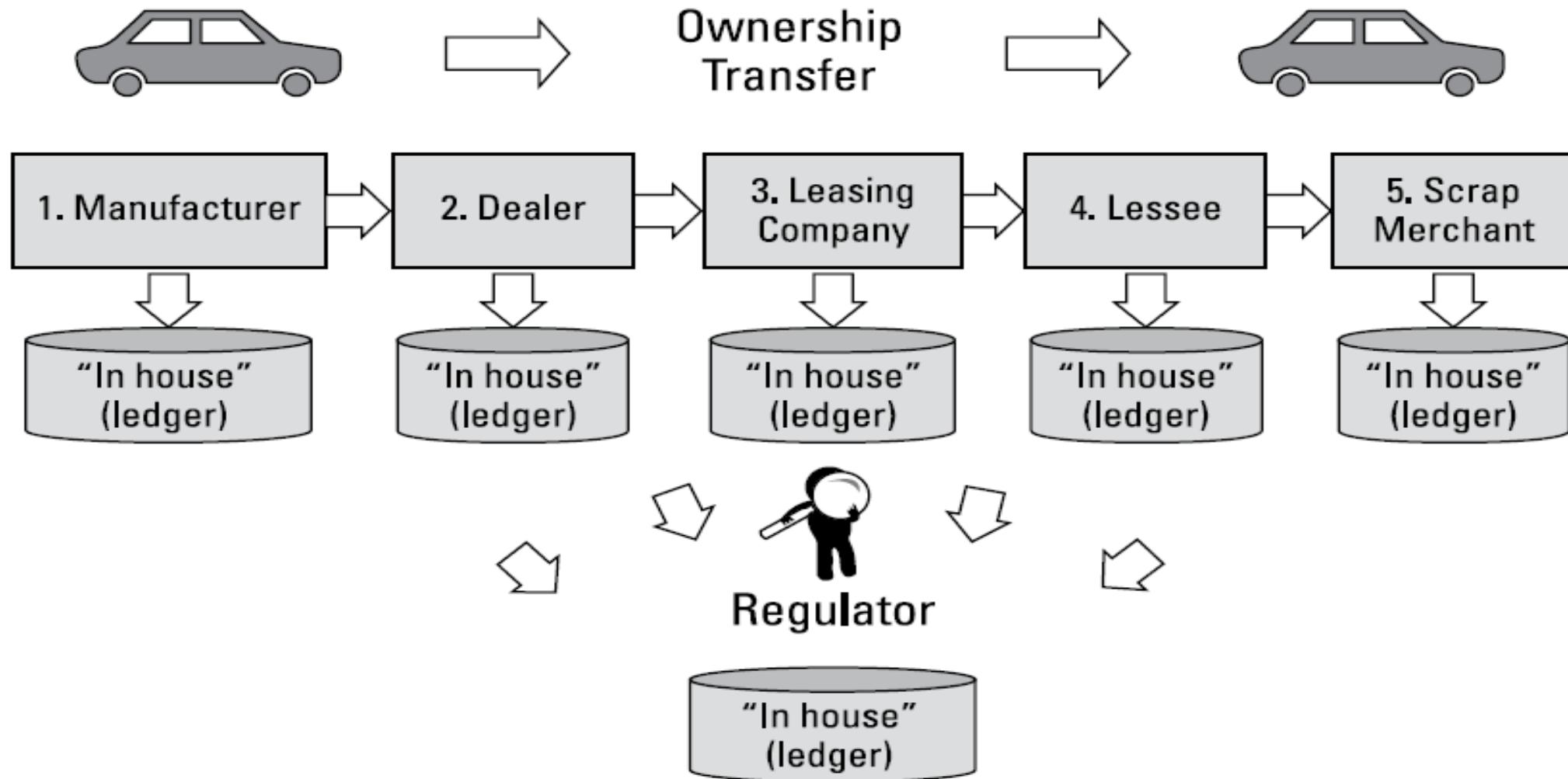
The blockchain architecture gives the participants the ability to:

1. **Share a ledger** that is updated, through peer-to-peer replication, every time a transaction occurs. *Peer-to-peer replication* means that each participant (node) in the network acts as both a publisher and a subscriber. Each node can receive or send transactions to other nodes, and the data is synchronized across the network as it is transferred.
2. More **economical and efficient**, as it eliminates duplication of efforts and reduces the need of intermediaries
3. **Less vulnerable**, as it uses the consensus model to validate the information



Transaction on Blockchain are Secure, Authenticate and Verifiable.

EXPLORING BLOCKCHAIN APPLICATION

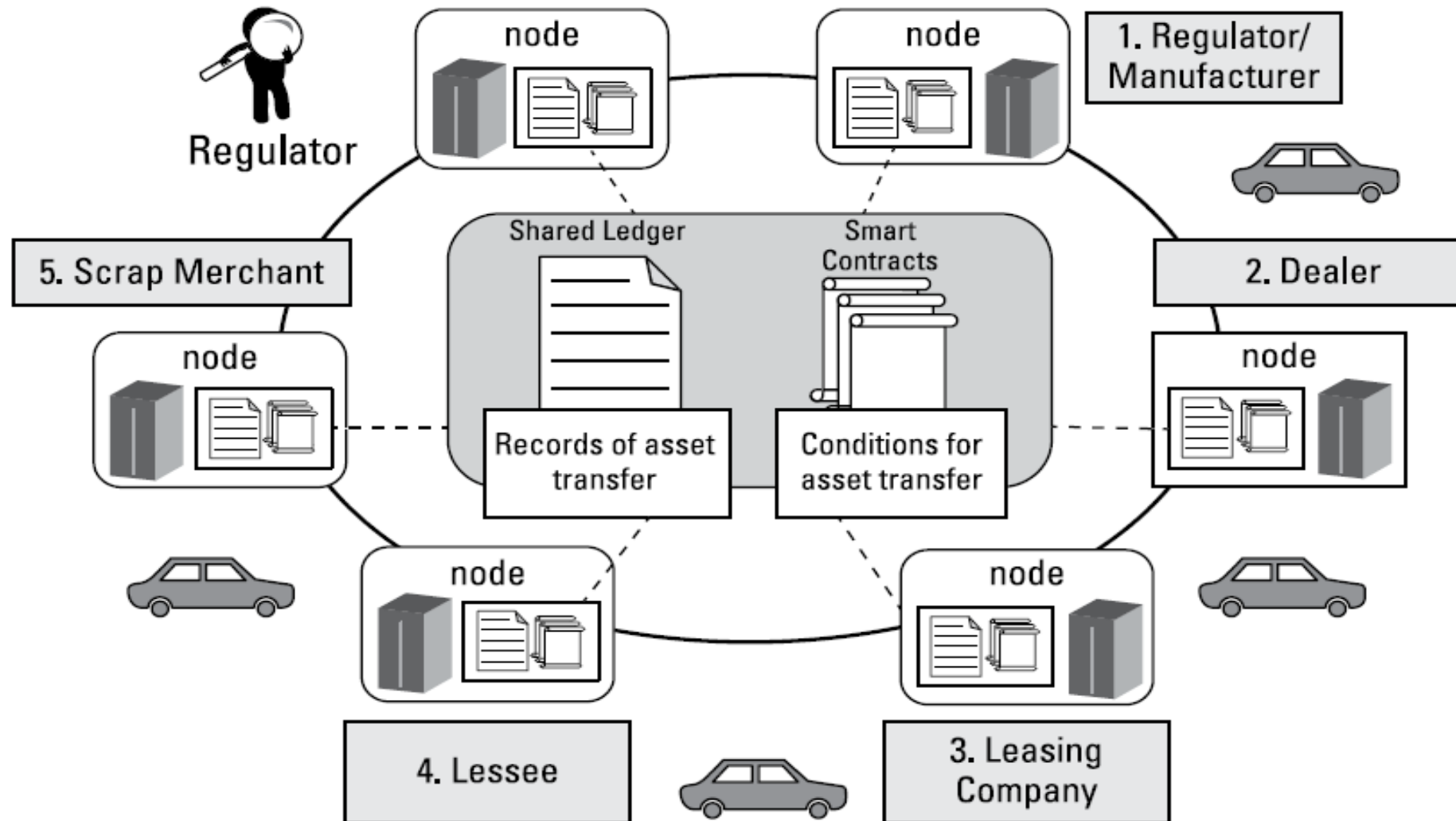


Even though the physical supply chain is usually integrated, the support system is fragmented. Each party maintains its own ledger, which can take days or weeks to synchronize.

TRACKING VEHICLE OWNERSHIP WITH BLOCKCHAIN

- The **government regulator** creates and populates the registration for the new vehicle on the blockchain and transfers the ownership of the vehicle to the manufacturer.
- The **manufacturer** adds the make, model, and vehicle identification number to the vehicle template within the parameters allowed by the ***smart contract***
- The **dealer** can see the new stock availability, and ownership of the vehicle can be transferred from the manufacturer to the dealership after a smart contract is executed to validate the sale.
- The **leasing company** can see the dealer's inventory. Ownership of the vehicle can be transferred from the dealer to the leasing company after a smart contract is executed to validate the transfer.
- The **lessee** can see the cars available for lease and complete any form required to execute the lease agreement.
- The leasing process continues between various lessees and the leasing company until the leasing company is ready to retire the vehicle. At this point, ownership of the asset is transferred to the **scrap merchant**, who, according to another smart contract, has permission to dispose of the vehicle.

EXPLORING BLOCKCHAIN APPLICATION



By using a Shared Ledger on the Blockchain network, every participants can access, monitor, and analyze the state of vehicle irrespective of where it is within its life cycle

RECOGNIZING THE KEY BUSINESS BENEFITS

- **Time savings:** Transaction times for complex, multi-party interactions are slashed from days to minutes. Transaction settlement is faster, because it doesn't require verification by a central authority.
- **Cost savings:** A blockchain network reduces expenses in several ways:
 - Less oversight is needed because the network is self policed by network participants, all of whom are known on the network.
 - Intermediaries are reduced because participants can exchange items of value directly.
 - Duplication of effort is eliminated because all participants have access to the shared ledger.
- **Tighter security:** Blockchain's security features protect against tampering, fraud, and cybercrime. If a network is permissioned, it enables the creation of a members-only network with proof that members are who they say they are and that goods or assets traded are exactly as represented.

RECOGNIZING THE KEY BUSINESS BENEFITS

- Not all blockchains are built for business. Some are permissioned while others aren't. A permissioned network is critical for a blockchain for business, especially within a regulated industry. It offers:
- **Enhanced privacy:** Through the use of IDs and permissions, users can specify which transaction details they want other participants to be permitted to view. Permissions can be expanded for special users, such as auditors, who may need access to more transaction detail.
- **Improved auditability:** Having a shared ledger that serves as a single source of truth improves the ability to monitor and audit transactions.
- **Increased operational efficiency:** Pure digitization of assets streamlines transfer of ownership, so transactions can be conducted

HOW CAN BLOCKCHAIN HELP?

Following are the ways by which Blockchain and Bitcoins solves these Issues:

Bitcoin Blockchain
has a distributed
ledger

Transactions are
immutable, thus
cannot be hacked



The ledger is public
for all to access

Double spending is
not allowed because
of the basic structure
of block transactions

BITCOIN

84

WHAT IS BITCOIN?



Satoshi Nakamoto

EMERGENCE OF BITCOIN

- ~ 1990 – Start of the movement from cash to digital
- 1991 - **Digicash** – David Chaum (focuses on making transactions anonymous)
- 1992: Start of the Cypherpunks. Publication of “A Cypherpunk’s Manifesto”.
- 1997: **Hashcash** – Adam Back
- 1998: **B-Money** – Wei Dai
- 2005: **BitGold** – Nick Szabo
- 2008: **Bitcoin** – Satoshi Nakamoto

EMERGENCE OF BITCOIN

- To address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems
- BitCoin is a digital currency that was launched in 2009 by a mysterious person (or persons) known only by the pseudonym Satoshi Nakamoto.
- - No Central Authority, like tradition currency
- - Not printed, but **MINED** by the people and businesses using software that solves mathematical puzzles.
- - Rather than rely on a central monetary authority to monitor, verify, and approve transactions and manage the money supply, bitcoin is enabled by a peer-to-peer computer network

BITCOIN



The first decentralized digital currency

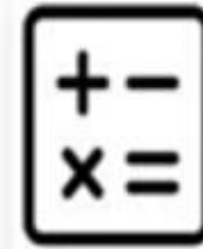
Uses cryptography to control its creation and management



Account Number	Balance
19KAgp1W9kU52U2	27
57D9M7Pua5U4b6	42.67
17BmK26DfHfH50...	842
29K5U9H98K22K6	512.809
3Fv4K8u5d87746	562
5u8d9h5d5h2465	974.25

Created and held electronically in a peer to peer open ledger called the blockchain

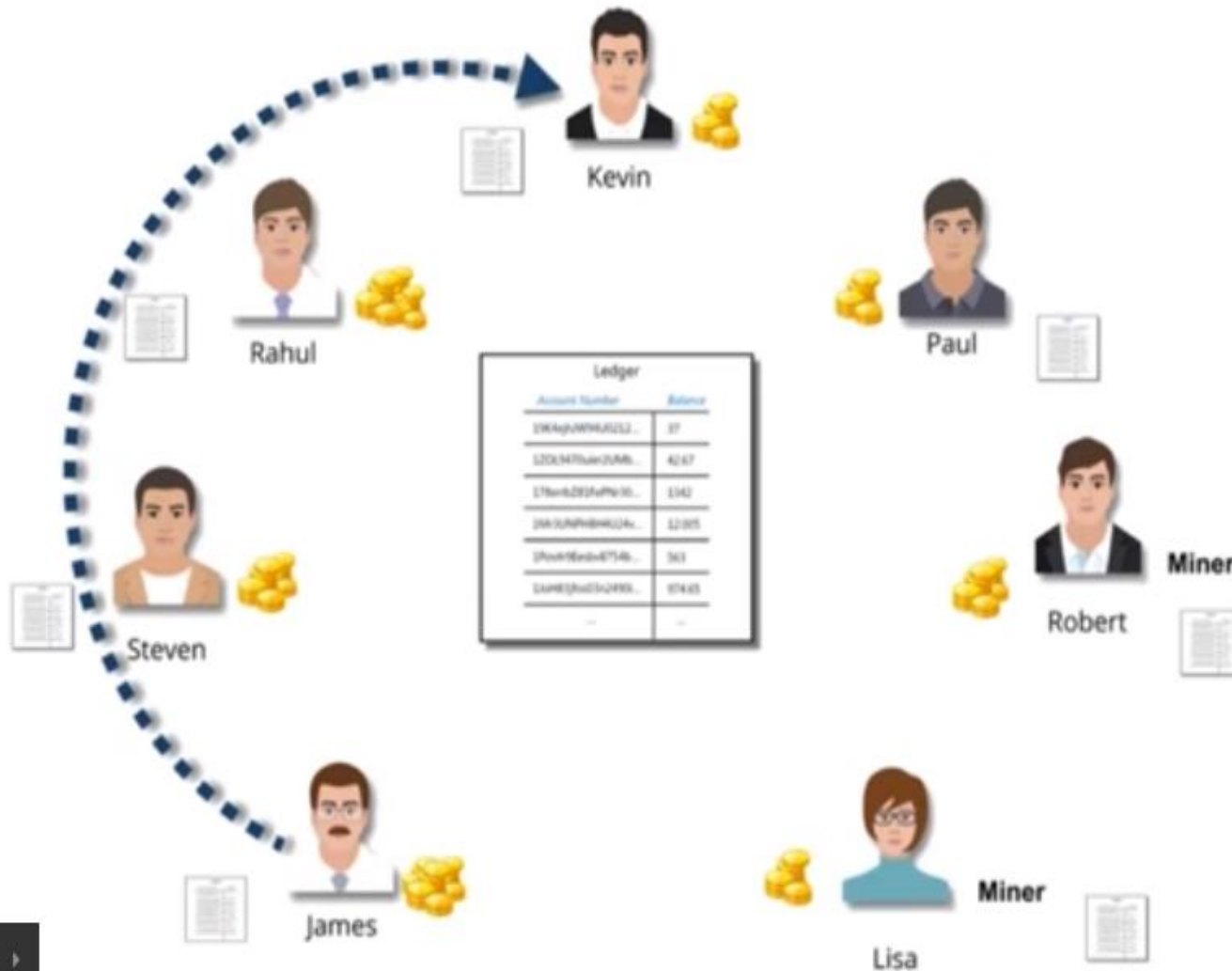
Ledger is produced by people using software that solves mathematical problems



BITCOIN

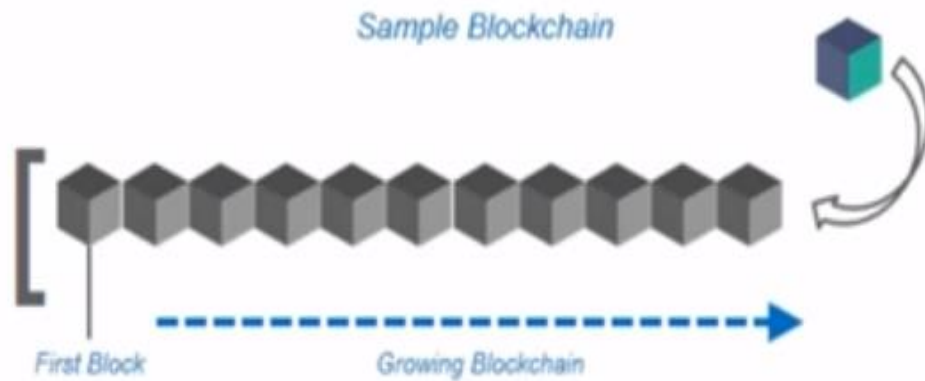
- Bitcoin has several advantages over other current transaction systems, including the following:
- **Cost-effective:** Bitcoin eliminates the need for intermediaries.
- **Efficient:** Transaction information is recorded once and is available to all parties through the distributed network.
- **Safe and secure:** The underlying ledger is tamper-evident. A transaction can't be changed; it can only be reversed with another transaction, in which case both transactions are visible.

BITCOIN TRANSACTION



- ❑ Let us take a Bitcoin transaction where James wants to transfer 500 BTC to Kevin.
- ❑ The transaction is a part of the new block that will be validated by miners Lisa and Robert.

BITCOIN TRANSACTION

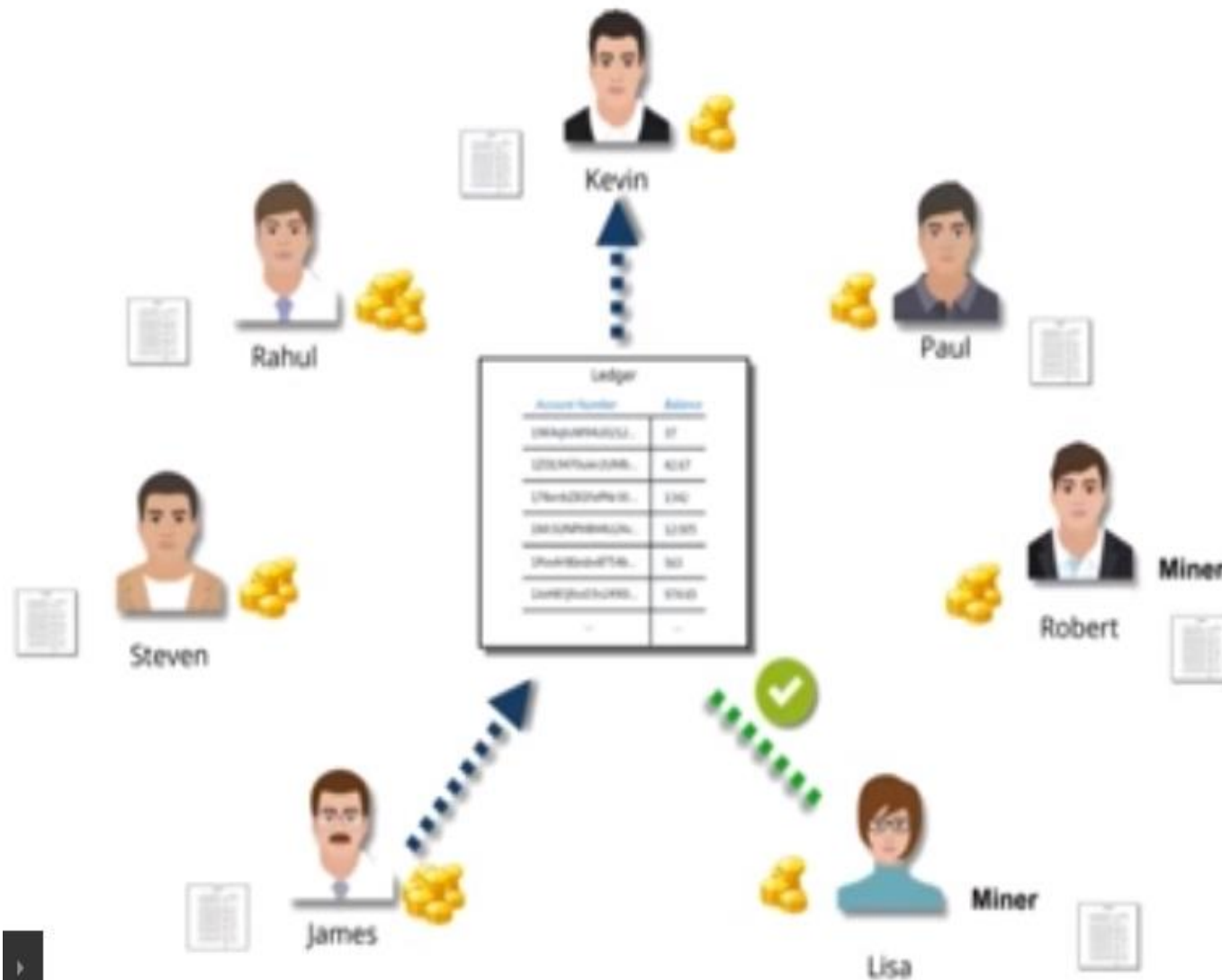


Account Number	Balance
19K4ejhJW94U0212...	37
1ZOL9470uier2UMb...	42.67
178errbZ81FePNr30...	1342
1Mr3UNPH8H4U24v...	12.005
1Pos4r9Eesbv8754b...	563
1JoH83jfos03n2490i...	974.65
...	...

Ledger

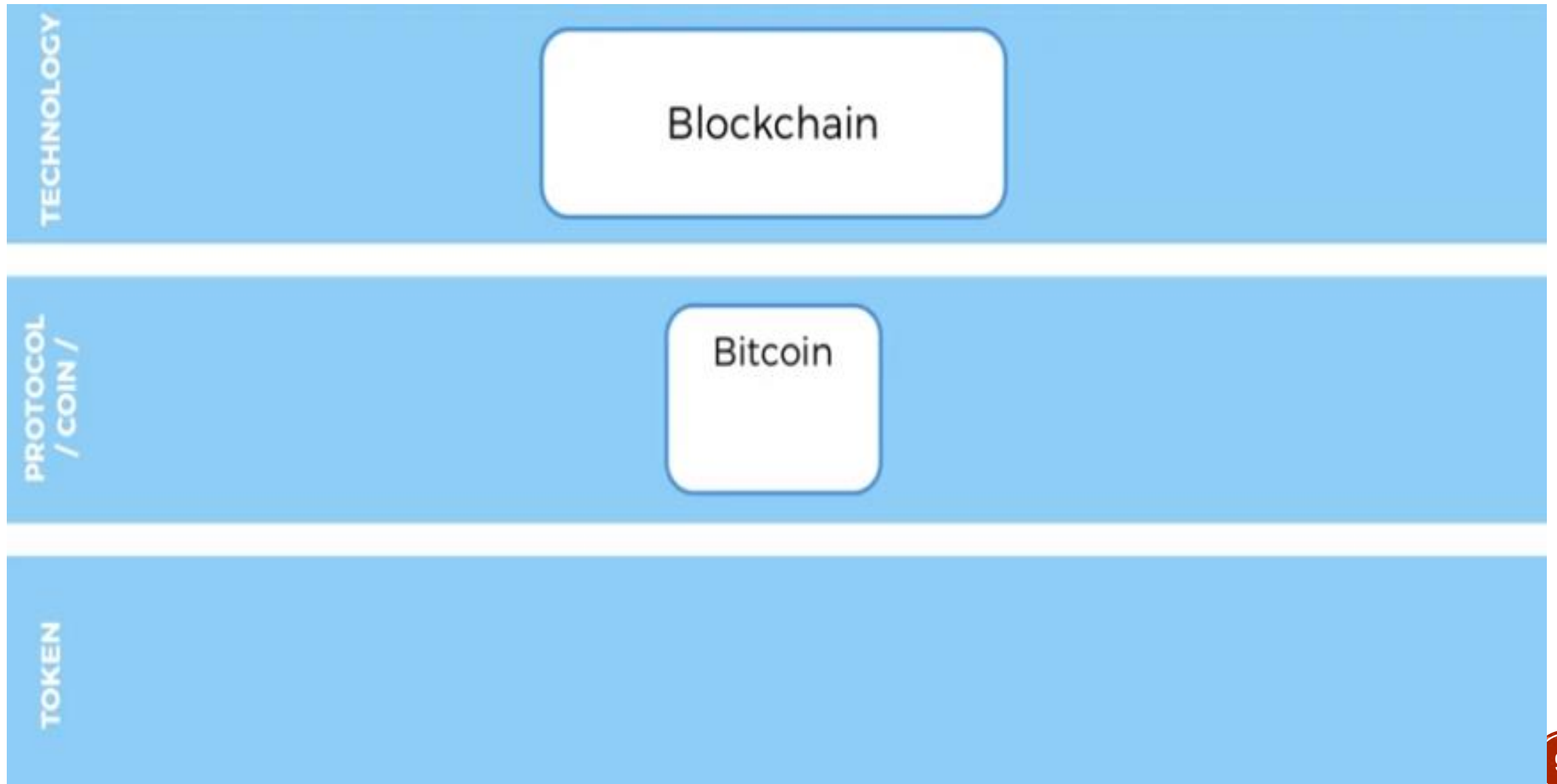
- ❑ Every transaction holds details of the transfer of currency from one account to the another.
- ❑ The balance of any account is not stored explicitly. It is always calculated by adding up all the blockchain transactions ever recorded.

BITCOIN TRANSACTION



- ❑ Once the **block** is **validated**, money is deducted from James' account and is transferred to Kevin's Bitcoin account.
- ❑ This solves the problem of *Double Spending*.

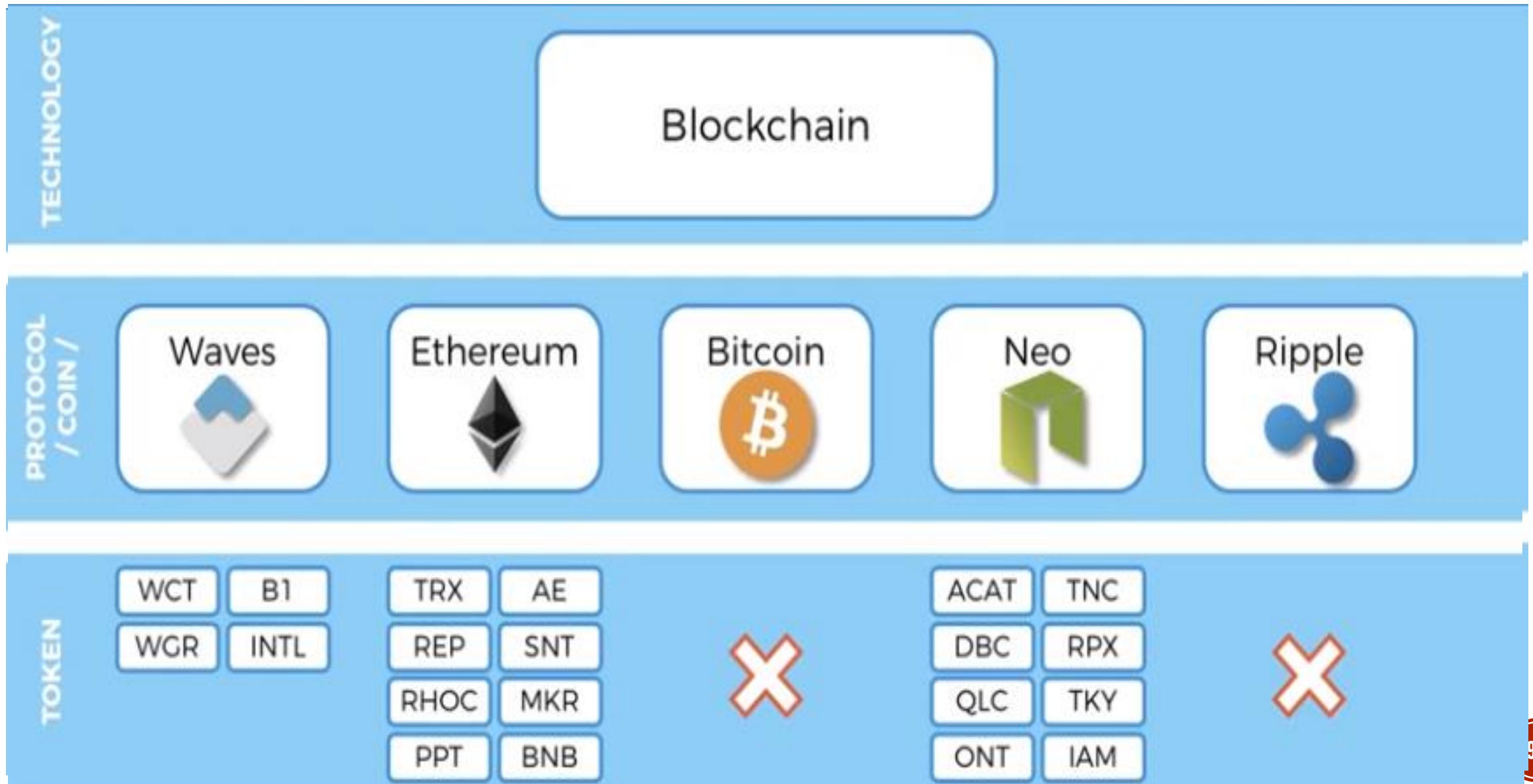
WHAT IS BITCOIN?



WHAT IS BITCOIN?

- **Bitcoin is not just a coin / currency, but is a set of protocols, to help the participants of bitcoin blockchain network to communicate with each other and agree on things**
- **Bitcoin protocol dictates-**
 - **How we can come to consensus?**
 - **How public keys and signature can be used for authentication?**
 - **Agree on update of protocols itself.**
 - **Other things to update efficiently**

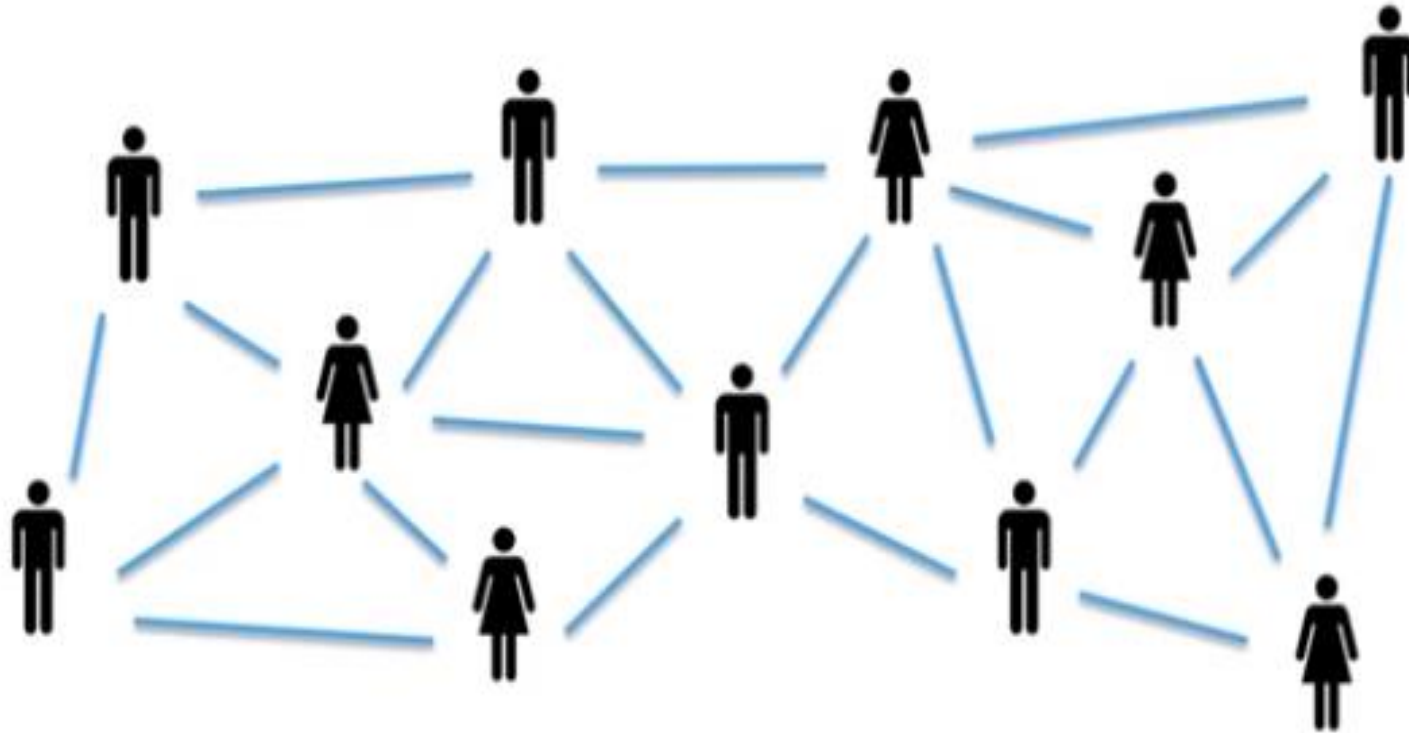
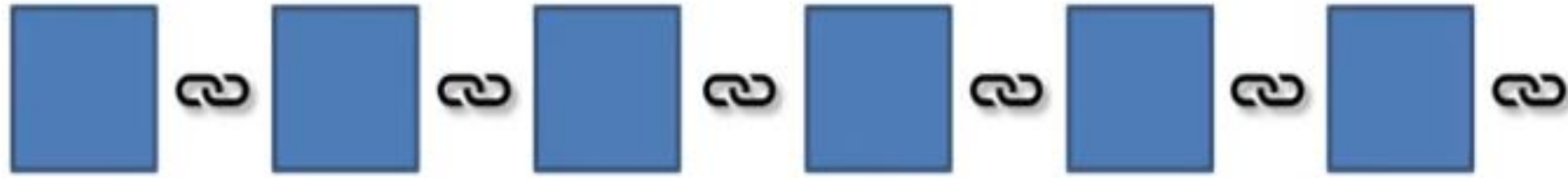
WHAT IS BITCOIN?



WHAT IS BITCOIN?

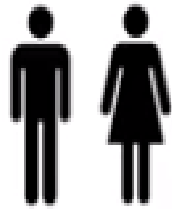
- **Bitcoin Token** (BTK) is a digital currency.
- It uses peer-to-peer technology to operate with no central authority or banks; managing transactions are carried out collectively by the network.
- There is no central control over the **token**. **Bitcoin Token** is open source, community driven, decentralized.
- Once the transaction ledger has been created, however, it is necessary to issue **tokens** that are actually exchanged among cryptocurrency users, and whose exchanges will be **transactions stored on the distributed ledger** (ie on the blockchain).
- **Visit coinmarketcap.com**
- **Investing in coin is investing in protocol**
- **Investing in token is investing in Idea**
- **Blockchain is used by multiple industries, healthcare, logistics, supplychain etc. are build on the top of protocols build by bitcoins**

WHAT IS BITCOIN?

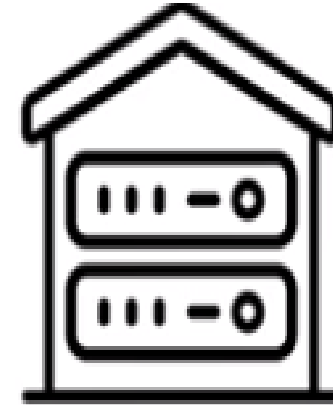


BITCOIN ECOSYSTEM

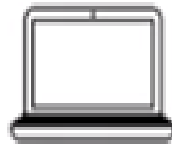
- Nodes



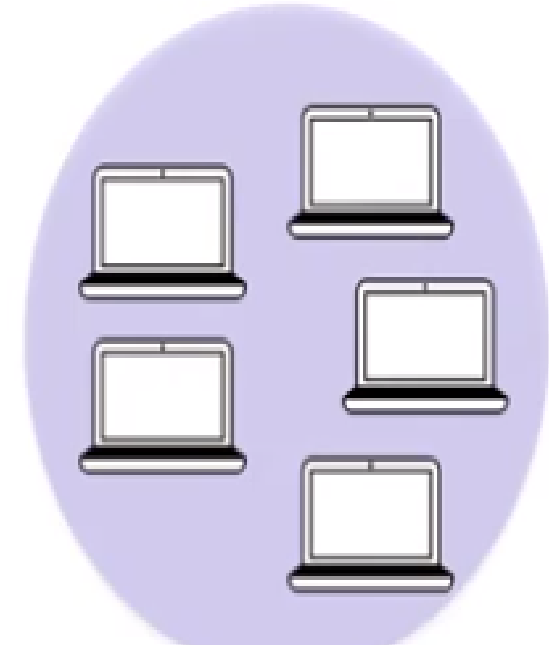
- Large Mines



- Miners



- Mining Pools



WHAT IS BITCOIN?

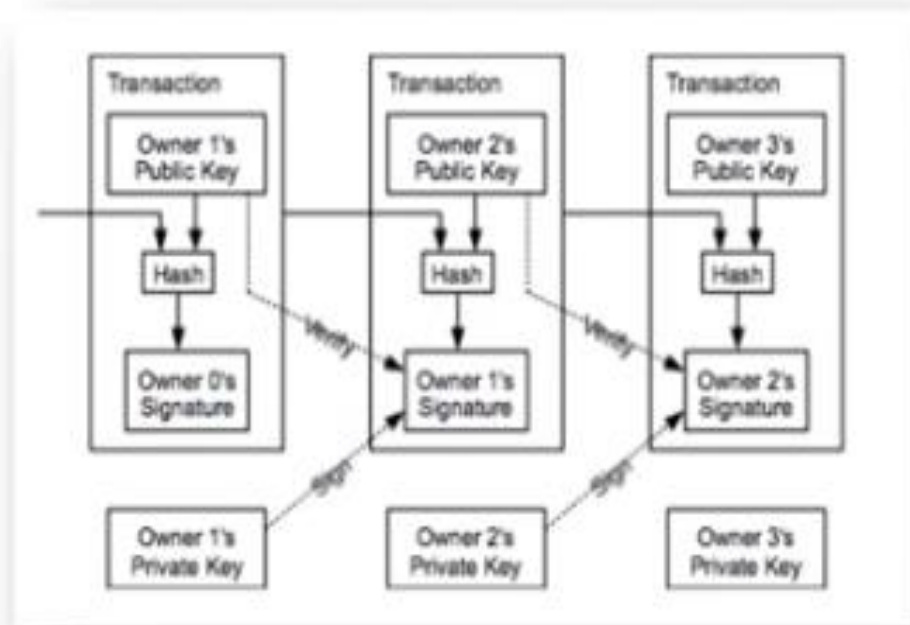
Additional Reading:

Bitcoin: A Peer-to-Peer Electronic Cash System

By Satoshi Nakamoto (2008)

Link:

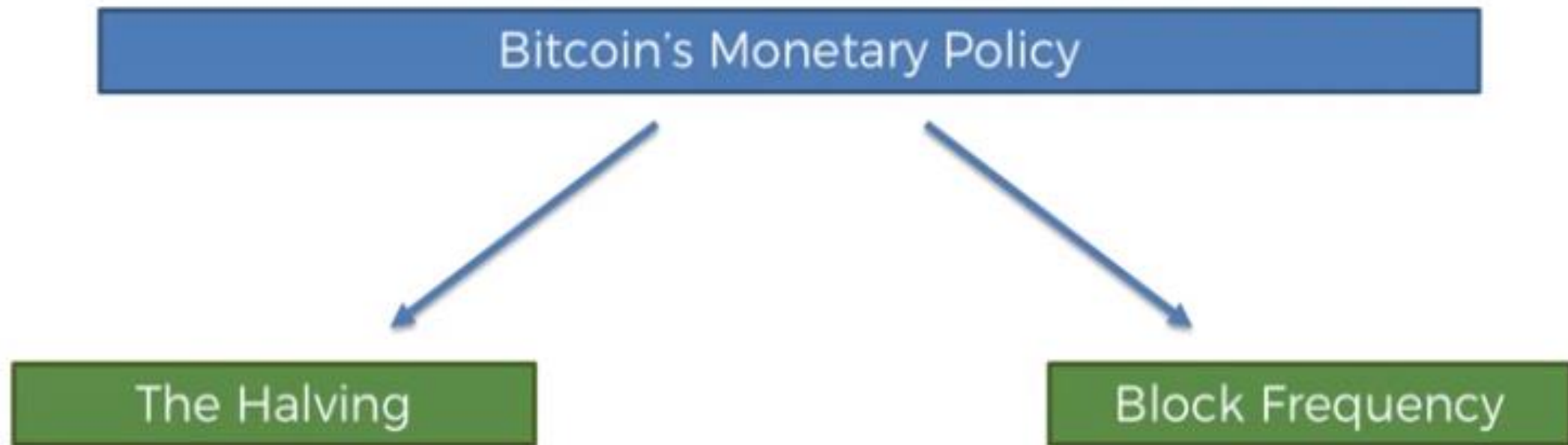
<https://bitcoin.org/bitcoin.pdf>



BITCOIN MONETARY POLICY

100

BITCOIN MONETARY POLICY



The number of bitcoins released in the system is halved every 04 years (every 210000 blocks)

Monetary policy is entirely under the control of computer algorithms and is not controlled manually.

BITCOIN MONETARY POLICY – THE HALVING

The Halving

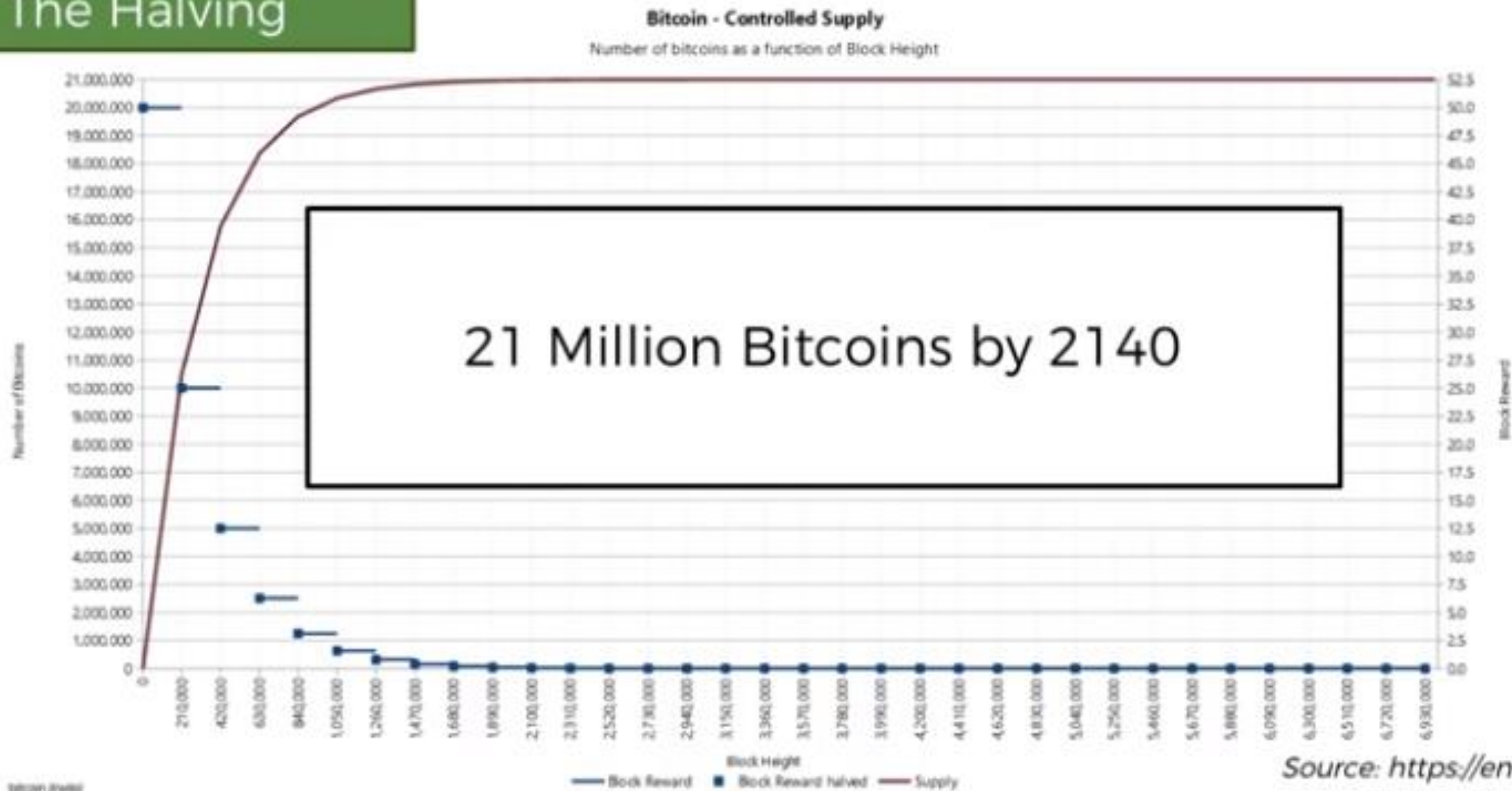
Date reached	Block	Reward Era	BTC/block
2009-01-03	0	1	50.00
2010-04-22	52500	1	50.00
2011-01-28	105000	1	50.00
2011-12-14	157500	1	50.00
2012-11-28	210000	2	25.00
2013-10-09	262500	2	25.00
2014-08-11	315000	2	25.00
2015-07-29	367500	2	25.00
2016-07-09	420000	3	12.50
2017-06-23	472500	3	12.50

~2020: 6.25

~2024: 3.125

BITCOIN MONETARY POLICY – THE HALVING

The Halving



BITCOIN MONETARY POLICY – THE HALVING




The Halving

TRANSACTION FEES ARE MEANT TO
REPLACE BLOCK REWARDS

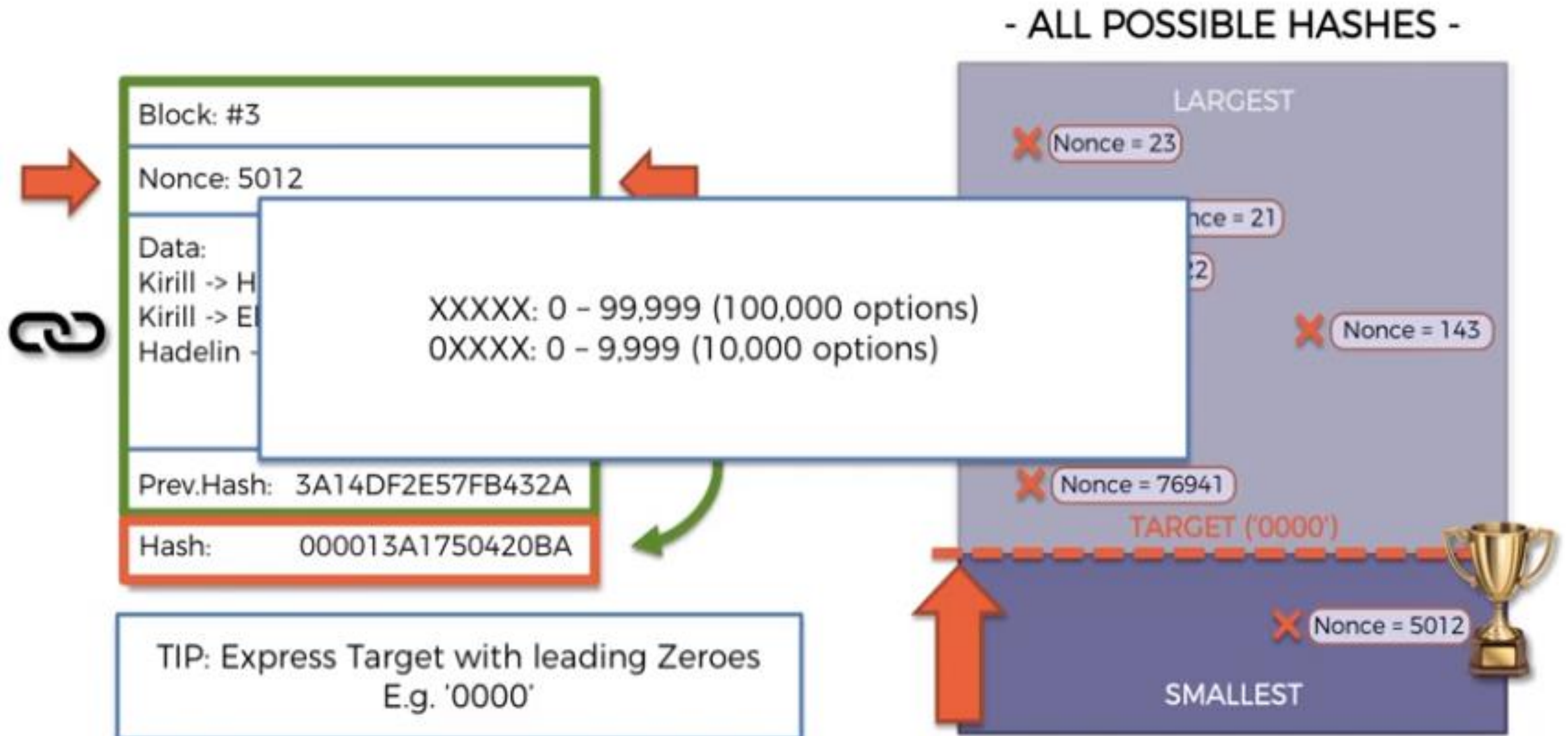


BITCOIN MONETARY POLICY – BLOCK FREQUENCY

Block Frequency


Cryptocurrency	Average block time
 bitcoin	10 min
 ethereum	15 sec
 ripple	3.5 sec
 litecoin	2.5 min

UNDERSTANDING THE MINING DIFFICULTY



UNDERSTANDING THE MINING DIFFICULTY

Current target = 000000000000000000005d97dc000000000000000000000000000000000000000


18 zeros

Let's do some estimations:

Probability:

Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \dots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx 10^{77}$

Total valid hashes (with 18 leading zeros): $16 \times 16 \times \dots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.0000000000000000000002\%$

HOW BLOCKCHAIN WORKS?

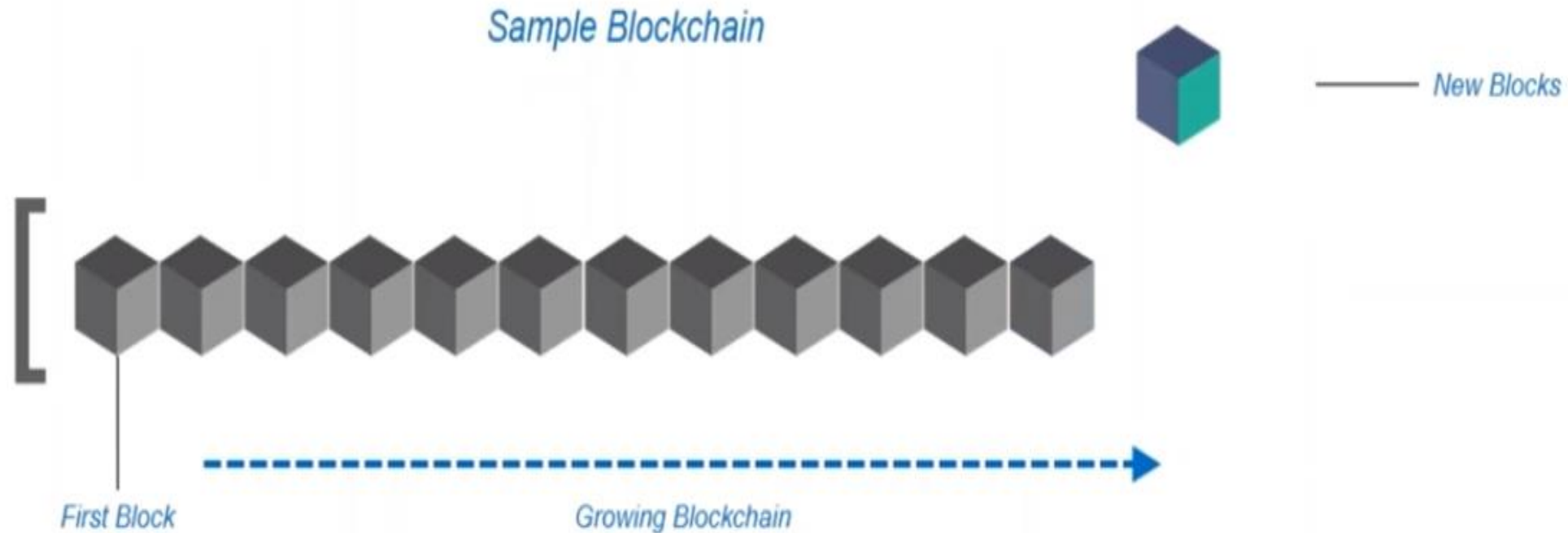
108

BIRTH OF BLOCKCHAIN: REVOLUTIONIZING THE TRADITIONAL BUSINESS NETWORK

- Blockchain is a core technology and spine of bitcoin, which serves as a bitcoin's shared ledger.
- Think of blockchain as an Operating System, such as Microsoft Windows or MacOS and bitcoin is only one of the many applications that can be run on operating system.
- Blockchain provides bitcoin a platform to record the transaction in a shared ledger, However the shared ledger can be used to record any transaction and track the movement of any asset (tangible, intangible and digital)
- **Blockchain and Bitcoin are not same. Bitcoin is only the first usecase of Blockchain.**

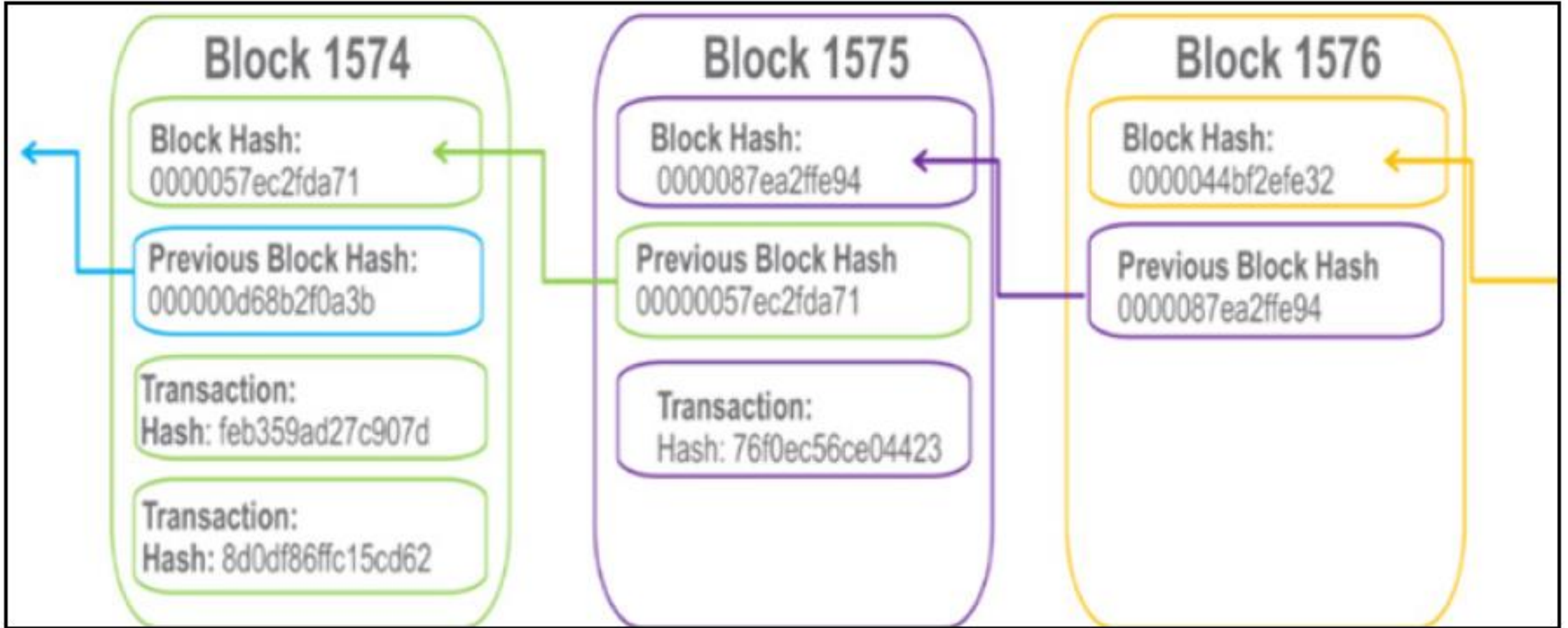
BLOCKCHAIN OVERVIEW

Blockchain is the technology used in Bitcoin. It is a public distributed database holding encrypted ledgers.



A block is the 'current' part of a blockchain which records some or all of the recent transactions, and once completed goes into the blockchain as permanent database. Each time a block gets completed, a new block is generated.

WHY IT IS CALLED BLOCKCHAIN?



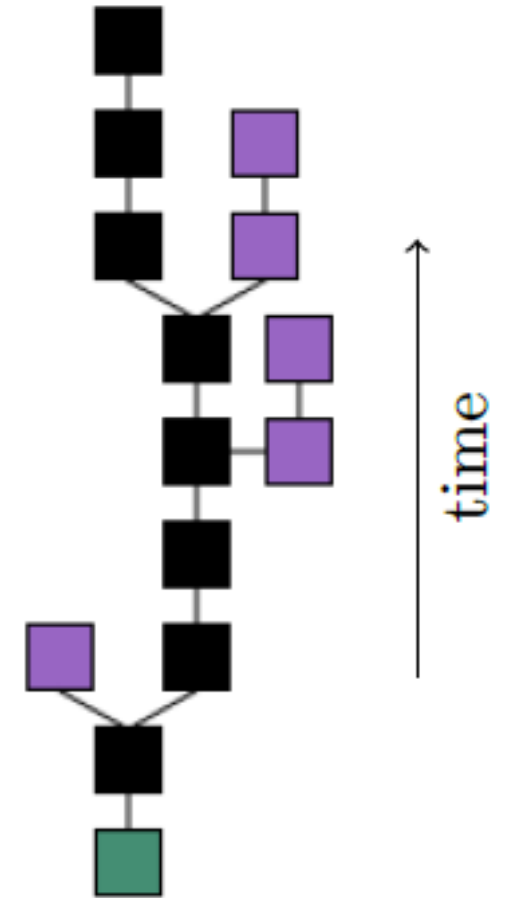
Blockchain stores transaction records in a series of connected blocks

WHY IT IS CALLED BLOCKCHAIN?

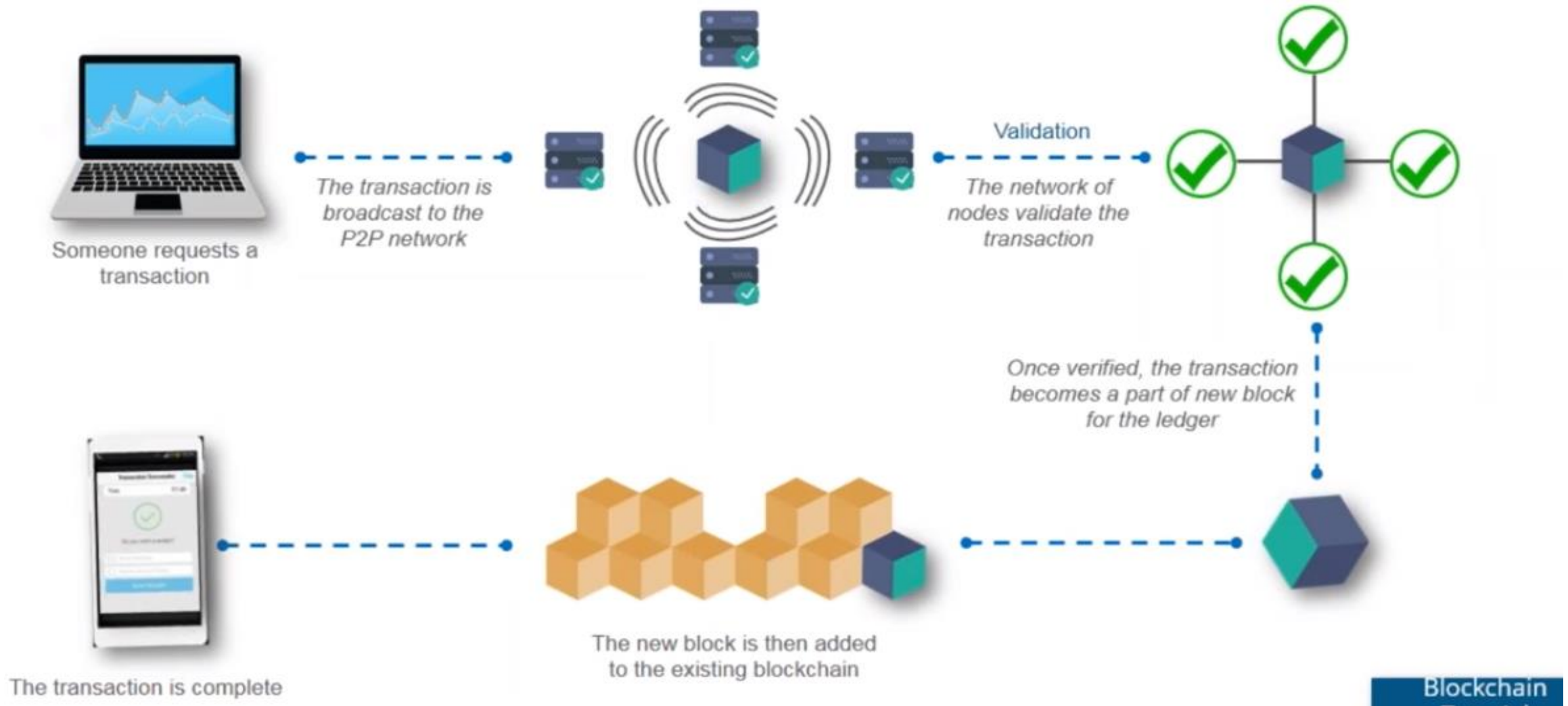
- Each block contains a
 - *Hash* (a digital fingerprint or unique identifier),
 - Timestamped batches of recent valid transactions,
 - and the hash of the previous block.
- The previous block hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain.
- The method renders the blockchain tamper-evident, lending to the key attribute of immutability.
- To be clear, while the blockchain contains transaction data, it's *not* a replacement for databases, messaging technology, transaction processing, or business processes. The blockchain contains verified proof of transactions. However, while blockchain essentially serves as a database for recording transactions, its benefits extend far beyond those of a traditional database.

WHY IT IS CALLED BLOCKCHAIN?

- *Blockchain* owes its name to the way it stores transaction data — in *blocks* that are linked together to form a *chain*. As the number of transactions grows, so does the blockchain.
- Blocks record and confirm the **time** and **sequence** of transactions, which are then logged into the blockchain, within a discrete network governed by rules agreed on by the network participants
- The black blocks are the 'normal' blocks. These are the blocks which form the longest (and thus official) chain. The purple blocks form so called 'forks'. These form when two blocks are found at exactly the same moment. For a short moment in time there are two chains of equal length. Until for one of the chains a new block is found quicker than for the other chain it is undecided which of the two is the 'official' chain.



BLOCKCHAIN – FLOW DIAGRAM



BLOCKCHAIN - SUMMURIZED

- It is a **public distributed database** which hold the **encrypted ledger** to keep the details of the people involved in it, completely anonymous.
- Block is a collection of all the recent transaction that has happened and are verified.
- Group all the transaction details in a block. Create a hashcode and store it in a block.
- Once the transaction is verified, then it becomes permanent part of the blockchain and chain keeps growing.
- Every 10mins a block is added.
- Blockchain is a core technology and spine of bitcoin that relies on the exchange of cryptocurrencies with anonymous users on a public network
- Blockchain for business is a private, permissioned network with known identities and without the need for cryptocurrencies.

WHAT MAKES BLOCKCHAIN SUITABLE FOR BUSINESS

Four key concepts of Blockchain for business



Blockchain for business ...

Append-only
distributed system of
record shared across
business network



Business terms
embedded in
transaction database
& executed with
transactions

Ensuring appropriate
visibility; transactions are
secure, authenticated
& verifiable



All parties agree
to network verified
transaction

... Broader participation, lower cost, increased efficiency

SHARED LEDGER

- Ledgers are nothing new; they've been used in double-entry bookkeeping since the 13th century.
- What is new is the concept of a shared, distributed ledger — an immutable record of all transactions on the network, a record that all network participants can access.
- With a shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.



Records all transactions across business network

- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- THE shared system of record

PRIVACY



Ledger is shared, but participants require privacy

- Participants need:
 - Transactions to be private
 - Identity not linked to a transaction
- Transactions need to be authenticated
- Cryptography central to these processes

PERMISSIONS

- Blockchains can be permissioned or permissionless.
- With a permissioned blockchain, each participant has a unique identity, which enables the use of policies to constrain network participation and access to transaction details. With the ability to constrain network participation, organizations can more easily comply with data protection regulations, such as those stipulated in the Health Insurance Portability and Accountability Act (HIPAA). Permissioned blockchains are also more effective at controlling the consistency of the data that gets appended to the blockchain.
- With the ability to restrict access to transaction details, more transaction detail can be stored in the blockchain, and participants can specify the transaction information they're willing to allow others to view. In addition, some participants may be authorized to view only certain transactions, while others, such as auditors, may be given access to a broader range of transactions. (With a public blockchain, the level of transaction detail may be limited to protect confidentiality and anonymity.)
- For example, if Party A transfers an asset to Party B, both Party A and Party B can see the details of the transaction. Party C can see that A and B have transacted but can't see the details of the asset transfer. If an auditor or regulator joins the network, privacy services can ensure that they see full details of all transactions on the network. **Cryptographic technology — this time through the use of *digital certificates* — makes this possible.**
- Just like a passport, a digital certificate provides identifying information, is forgery resistant, and can be verified because it was issued by a trusted agency. The blockchain network will include a certification authority who issues the digital certificate.

CONSENSUS



... the process by which transactions are verified

- Anonymous participants
 - Bitcoin *cryptographic mining* provides randomized selection among anonymous participants
 - Significant compute cost (proof of work)
- Known & trusted participants
 - Commitment possible at low cost
 - Byzantine fault tolerance (BFT)
- Multiple alternatives
 - Proof of stake, where influence is determined by risk of validators
 - Multi-signatures, validation needs consent from 3 out of 5 validators
- Industrial Blockchain needs “pluggable” consensus

CONSENSUS

In a business network where participants are known and trusted, transactions can be verified and committed to the ledger through various means of *consensus* (agreement), including the following:

Proof of stake: To validate transactions, validators must hold a certain percentage of the network's total value. Proof-of-stake might provide increased protection from a malicious attack on the network by reducing incentives for attack and making it very expensive to execute attacks.

Multi-signature: A majority of validators (for example, three out of five) must agree that a transaction is valid.

Practical Byzantine Fault Tolerance (PBFT): An algorithm designed to settle disputes among computing *nodes* (network participants) when one node in a set of nodes generates different output from the others in the set.

Blockchain for business features *pluggable consensus* — a way to implement whichever consensus mechanism is deemed best for any given industry segment.

CONSENSUS: PROOF OF WORK

When participants are anonymous (such as in the bitcoin world), commitment is expensive. On the bitcoin network, consensus is reached through *proof of work*.

The network challenges every machine that stores a copy of the ledger to solve a complex puzzle based on its version of the ledger. Machines with identical copies of the ledger “team up” to solve the puzzle they’ve been given.

The first team to solve the puzzle wins, and all other machines update their ledgers to match that of the winning team. The idea is that the majority wins because it has the most computing power to solve its puzzle first.

Proof of work is useful on a public blockchain, such as the one used for bitcoin, but it consumes considerable computing power and electricity, making it an expensive way to reach consensus. Such an expense is unnecessary on a private business network where all participants are known.

BLOCKCHAIN BENEFITS



Saves time

Transaction time
from days to near
instantaneous



Removes cost

Overheads and
cost intermediaries



Reduces risk

Tampering, fraud
& cyber crime

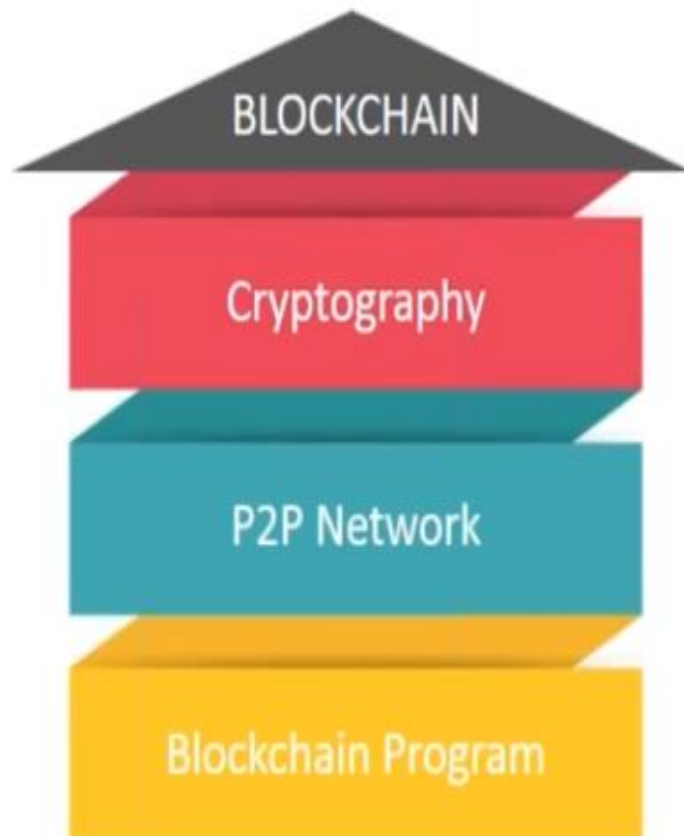


Increases trust

Through shared
processes and
recordkeeping

BLOCKCHAIN TECHNOLOGIES

Blockchains are built from 3 technologies:



Blockchain uses **Private Key Cryptography** to secure identities and **hash** functions to make the **blockchain** immutable

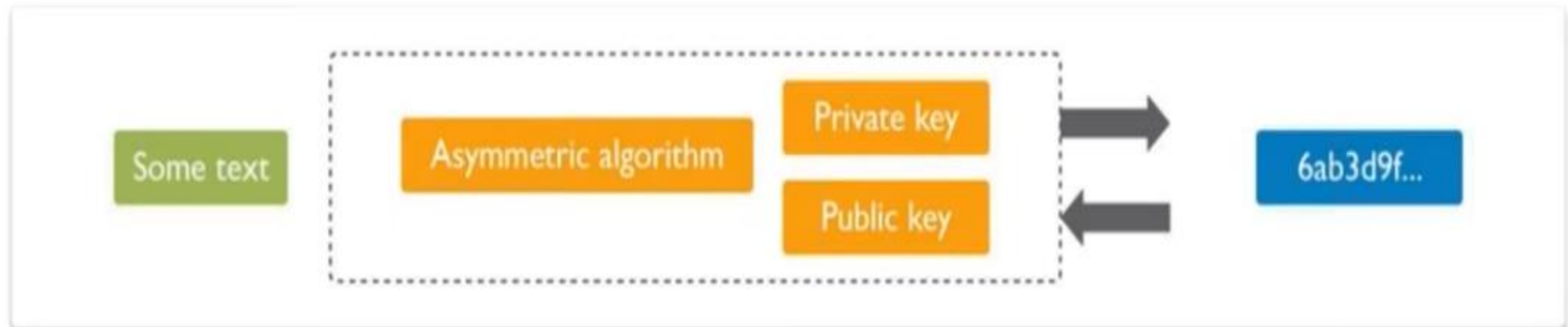
P2P machines on the network help in maintaining the consistency of the distributed **ledger**

The **program** gives the blockchain its **protocol** based on the requirement

PUBLIC KEY CRYPTOGRAPHY

This approach involves two different keys

- ❑ One key is purposely kept **private**, the other is provided to the other party (or often the **public**)
- ❑ If you use **private key to encrypt** then the **public key can decrypt**
- ❑ If you use the public key to encrypt then you use the private key to decrypt. This is called **asymmetric encryption**



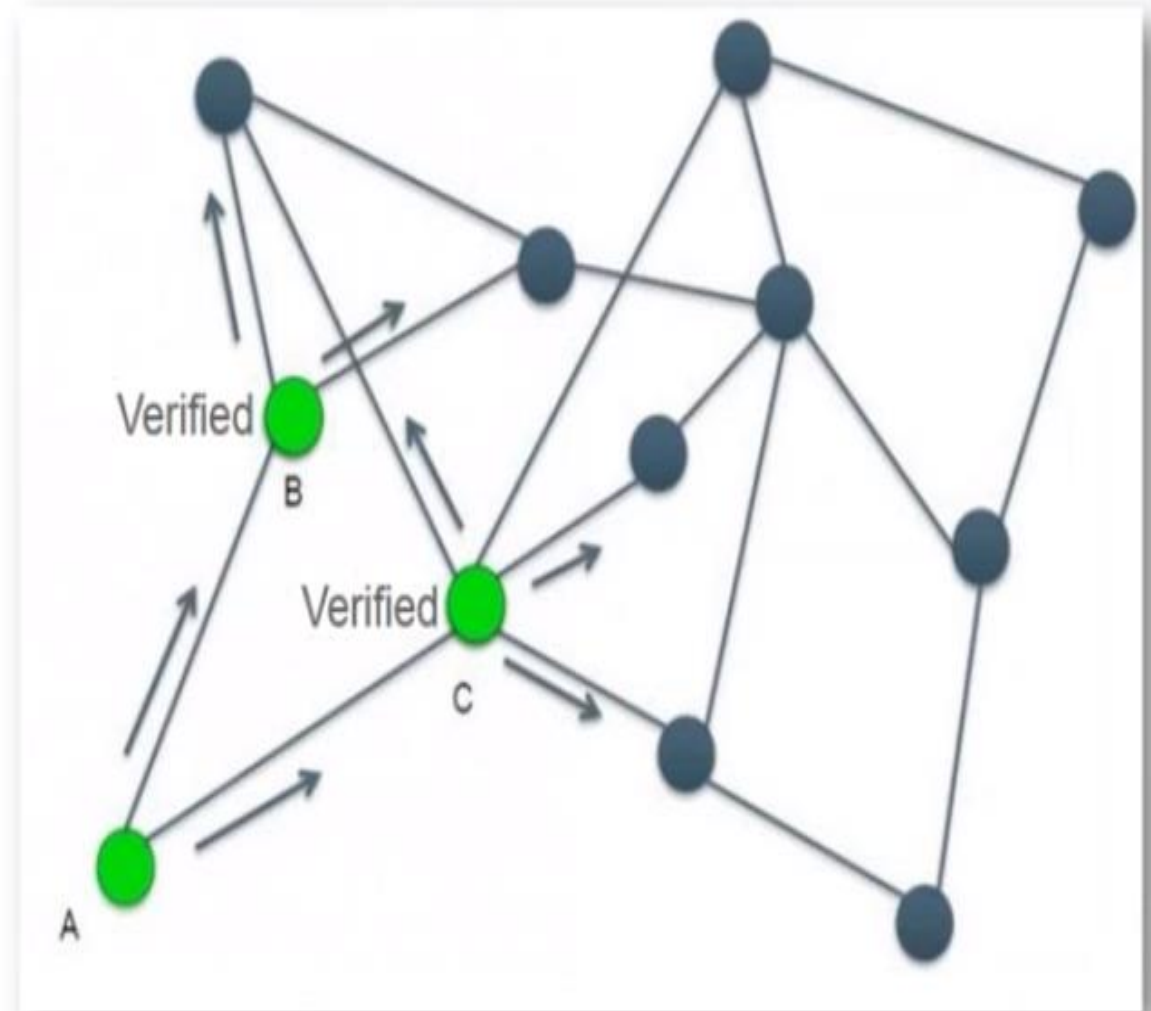
PEER TO PEER NETWORK

Suppose A finds the transaction: Bobby (B) pays 5 coins to Cindy (C)

Node A broadcasts to the peers B and C in the network

If the transaction is verified, the peers (here, B & C) forward the transaction to their peers

The transactions propagate rapidly across the network



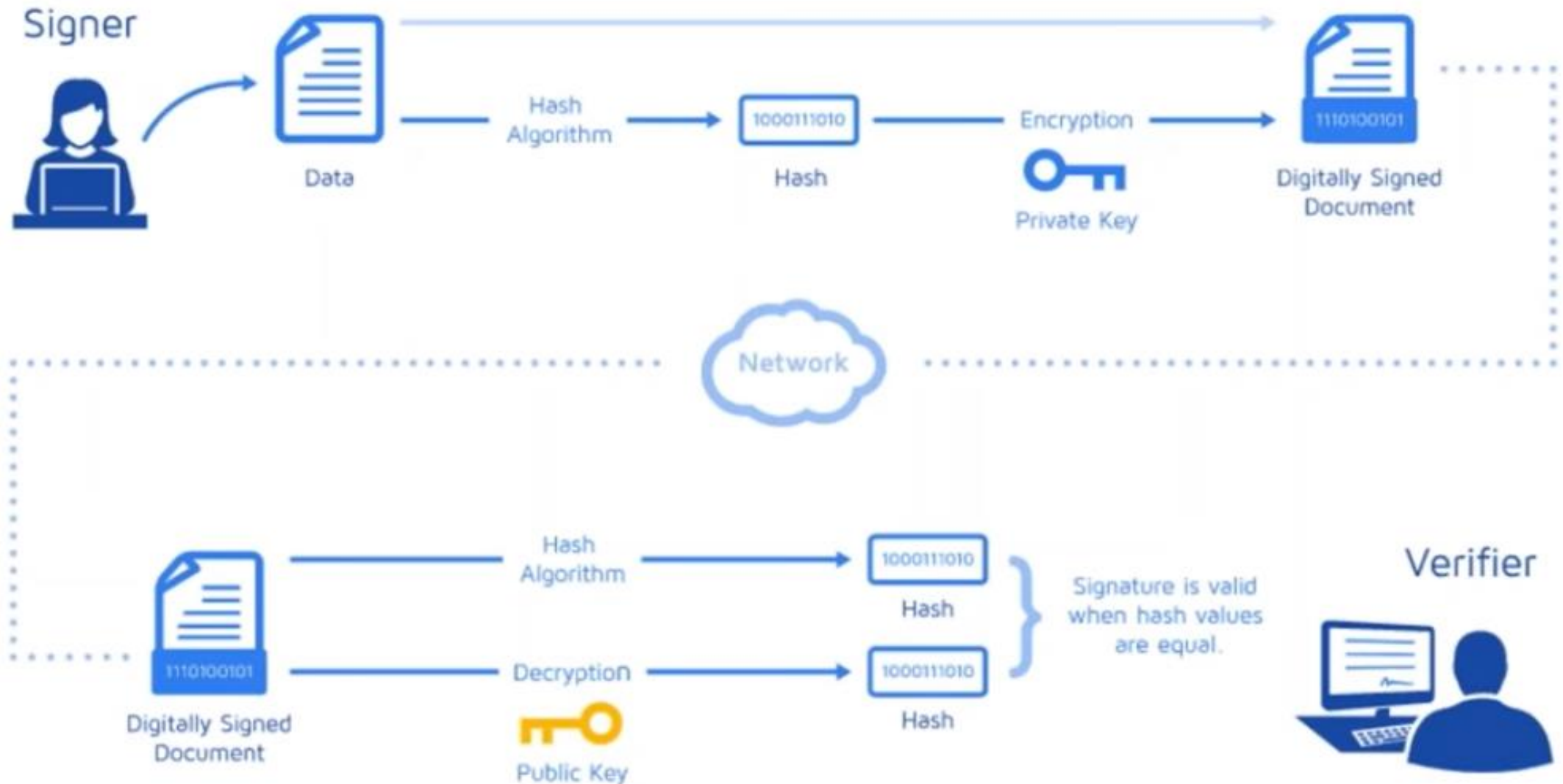
P2P NETWORK – DISTRIBUTED LEDGER



P2P NETWORK – DISTRIBUTED LEDGER



P2P NETWORK – DIGITAL SIGNATURE

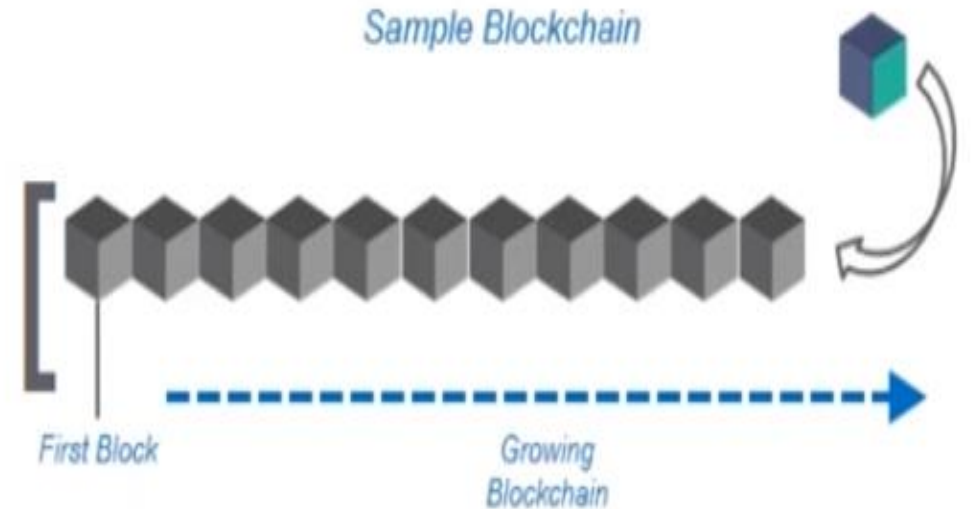


BLOCKCHAIN PROGRAM

The Blockchain is the way of implementing any solution/ use case

Blockchain is a concept and can be implemented by any language

Solidity is the most preferred default for writing programs in Blockchain



BLOCKCHAIN TRANSACTION

In any blockchain:

- All transactions are logged including information on the time, date, participants and amount of every single transaction
- Each node in the network owns a full copy of the blockchain



BLOCKCHAIN TRANSACTION



Transactions are verified by the **Miners** after solving complex math puzzles and maintain the ledger



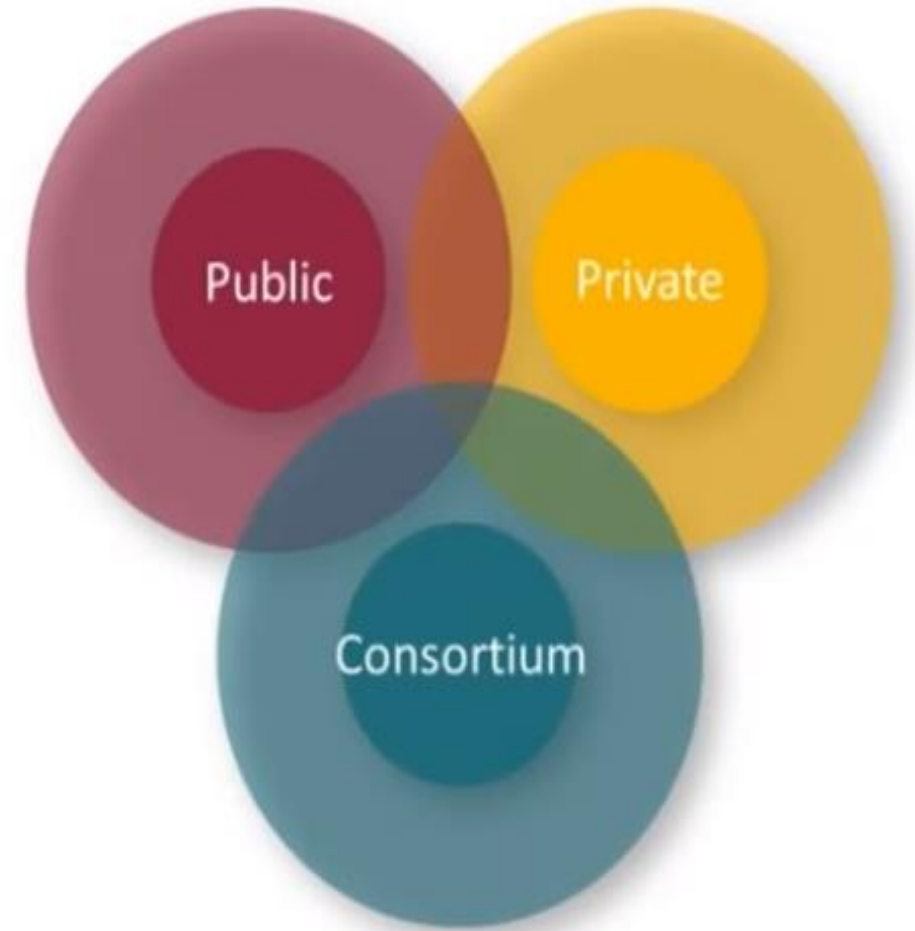
The **mathematical principle** ensures that the nodes **automatically** and **continuously** agree to the current state of the ledger and every transaction in it.



If anyone **attempts to corrupt a transaction**, the nodes will not arrive at a consensus and hence will **refuse to incorporate** the transaction in the blockchain.

BLOCKCHAIN TYPES

- ❑ **Public:** Public blockchains have ledgers visible to everyone on the internet and anyone can verify and add a block of transactions to the block chain.
- ❑ **Private:** Private blockchains allow only specific people in the organization to verify and add transaction blocks but everyone on the internet is generally allowed to view.
- ❑ **Consortium:** Here, only a group of organizations (such as banks) can verify and add transactions but the ledger can open or restricted to select groups.



Blockchain Types

BLOCKCHAIN IN A NUTSHELL



The use of



Mathematics



To create a
secure



distributed
ledger



which enables
transactions



without the
need for



third



parties

BLOCKCHAIN USE CASES



Banking



Payment & Transfers



Healthcare



Law Enforcement



Voting



Internet Of Things



Online Music



Real Estate

BLOCKCHAIN USE CASES



Banking

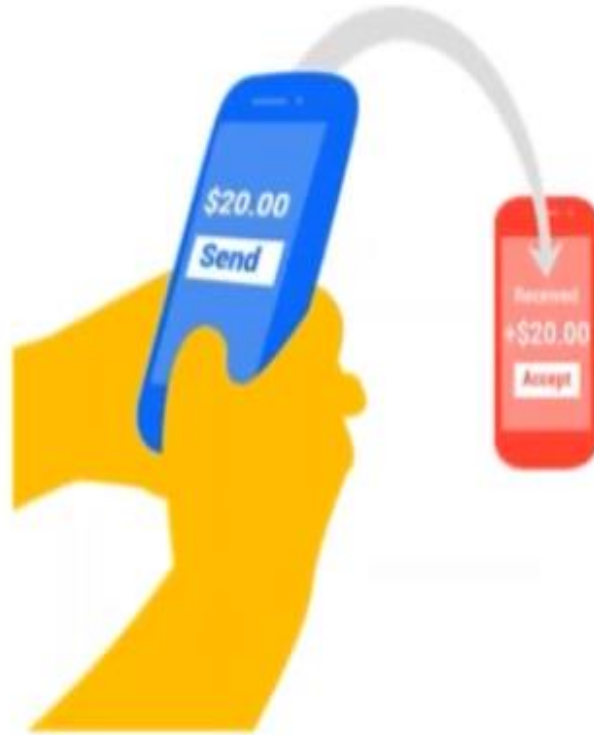
Blockchains could cut up to **\$20 billion** in middle-man costs per year

Hacking into banking ledgers becomes close to **impossible**

Solves the **double spending** problem

Reduces bank **crises** by a large extent

BLOCKCHAIN USE CASES



Payment & Transfers

Blockchains transfers are the **highest** in terms of **security**

Currently **Bitcoin** runs on **no** fixed **transaction fees**

No bank account required

Anonymity is maintained

BLOCKCHAIN USE CASES



Voting

Elections require authentication of voters' identity, secure record keeping and trusted tallies

Blockchains are the medium for casting, tracking and counting votes without voter-fraud, lost records or fowl-play.

Increases voter turnout

APPLICATIONS

Banking and Finance sector



- Peer to Peer
 - Lending
 - Insurance
 - Financial Services
- Payment Transfers
 - Inter branch/ bank
 - International
- Stock Exchanges
- Derivatives

Supply Chain Management



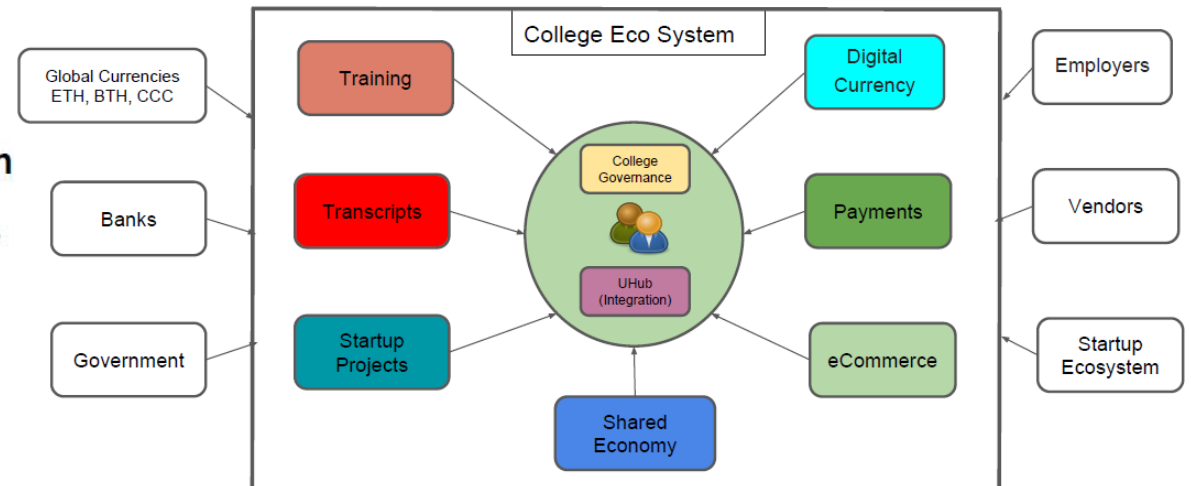
- Global end to end supply chain
- Traceability
- No reconciliation of records of multiple agencies
- Visibility
- No frauds possible
- Trade Finance
- Insurance

Governance and Public Services



- Public Records
 - Marriage, Birth
 - Land Title
 - Legal registered documents
- Voting
- Social services
- Benefits distribution
- Legal services/ Justice
- Identification
- Financial Inclusion

Education



<10> WHERE CAN YOU BUY CRYPTOCURRENCY?

<A> A PRIVATE TRANSACTION

** AN EXCHANGE**

<C> A BITCOIN ATM

<D> ALL OF THE ABOVE

THANK YOU

- Dr. Neha Sharma
- www.drnehasharma.in
- nvsharma@rediffmail.com
- 9923602490