Introduction to Blockchain

Lecture 1. Blockchain technology: definition and examples

Alexey Frolov, Yury Yanovich
Stanislav Kruglik, Evgeny Marshakov, Anton Glebov

Skolkovo Institute of Science and Technology

October 30, 2018

Let us introduce ourselves

Alexey Frolov

- PhD in Computer science.
- Research topics: Information theory, data security, machine learning
- Author of more than thirty scientific articles and white papers
- Assistant professor at Skoltech.

Yury Yanovich

- PhD in Mathematics.
- Research topics: Machine Learning, Statistics, Blockchain.
- Author of tens scientific articles and white papers including ten about Bitcoin and blockchain.
- Researcher at Bitfury (a diversified blocking company, the largest industrial miner outside of China, a developer of software and hardware for working with Bitcoin and blockchain) for three plus years.
- Research scientist at Skoltech.
- Research scientist at IITP RAS and lecture at HSE.

Stanislav Kruglik

- PhD student in CDISE, Skoltech
- Research topics: Data security, information theory
- Research scientist at IITP RAS and teacher at DREC MIPT

Table of Contents

Edelman
trustbarometer
I ANNUAL GLOBAL STUDY

- **28** countries
- **33 000+** people
- Informed public

Edelman trustbarometer | ANNUAL GLOBAL STUDY

Trust index 2018

Non Governmental Organizations

Mass Media

Business

Government

Edelman trustbarometer | ANNUAL GLOBAL STUDY

Trust index 2018

53 %

0

Non Govermental Organizations

43 %

0

Mass Media

52 %

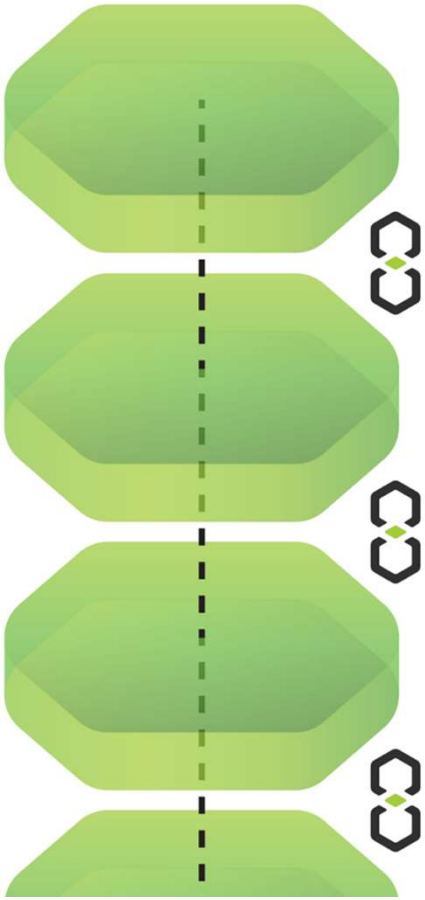
0

Business

43 %

+2

Government



Blockchain is

a decentralized database with tamper-resistant log and built-in auditability

- A way of storing information: in atomic transactions, grouped in blocks
- Blocks joined in a chain with the aid of cryptography

Let’s imagine Blockchain

As a Paper Book

Chain of book pages = chain of blocks in Blockchain.

Paper Book

- Impossible to remove pages unnoticed.
- Impossible to change the existing text.
- Book is stored in many copies.

Blockchain

- Data can’t be deleted in any way.
- Data can’t be manipulated in any way.
- Data is stored on many nodes.

Advantages

Security

One cannot unnoticeably erase the data stored in a blockchain

Trust

The architecture of the network removes the necessity of trust to a platform maintainer

Built-in Auditability

Audit can be performed by any entity in the network. The validity of any change is proved with PKI & cryptography.

Economics

Removing the middleman and online audit reduce total solution cost dramatically

Public blockchain

Anyone can become a miner:

- Built-in cryptocurrency with mining
- Single platform for everybody

Security: **High**

Performance: **Low**

Private blockchain

Only restricted set of nodes are validators:

- ‘Mining’ incentivizing is outside the solution
- Transaction creation and audit is regulated by blockchain maintainer

Security: **Low**

Performance: **High**

Definitions

- **Initial definition:** The blockchain is the technology running the Bitcoin.

Definitions

- **Initial definition:** The blockchain is the technology running the Bitcoin.
- **Wikipedia:** A blockchain – originally block chain – is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data.

Definitions

- **Initial definition:** The blockchain is the technology running the Bitcoin.
- **Wikipedia:** A blockchain – originally block chain – is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data.
- **Alternative (Jerome Kehrli):** Blockchain is a secured protocol enabling peer-to-peer exchanges on a distributed network in a secured, public and non-repudiable way.

A tiny little bit of history

- Architecture and principle first designed for **Bitcoin**
  - A solution to make the database both **secured** and **widely distributed**
  - Actually the main innovation of the Bitcoin

A tiny little bit of history

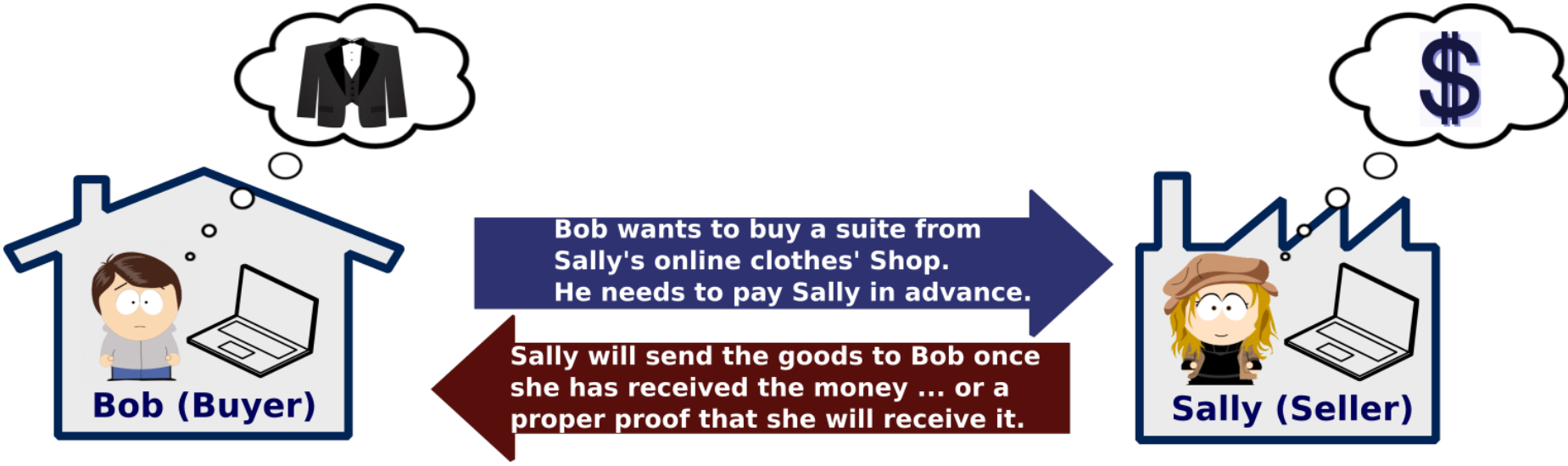
- Architecture and principle first designed for **Bitcoin**
  - A solution to make the database both **secured** and **widely distributed**
  - Actually the main innovation of the Bitcoin
- Conceived in 2008 and implemented in 2009
  - Satoshi Nakamoto

A tiny little bit of history

- Architecture and principle first designed for **Bitcoin**
  - A solution to make the database both **secured** and **widely distributed**
  - Actually the main innovation of the Bitcoin
- Conceived in 2008 and implemented in 2009
  - Satoshi Nakamoto
- As of 2014 : "Blockchain 2.0"
  - Evolution over the initial blockchain
  - From simple transactions to actual **Software Programs**
  - From simply a distributed transaction ledger to a **globally decentralized, unownable, digital computer.**

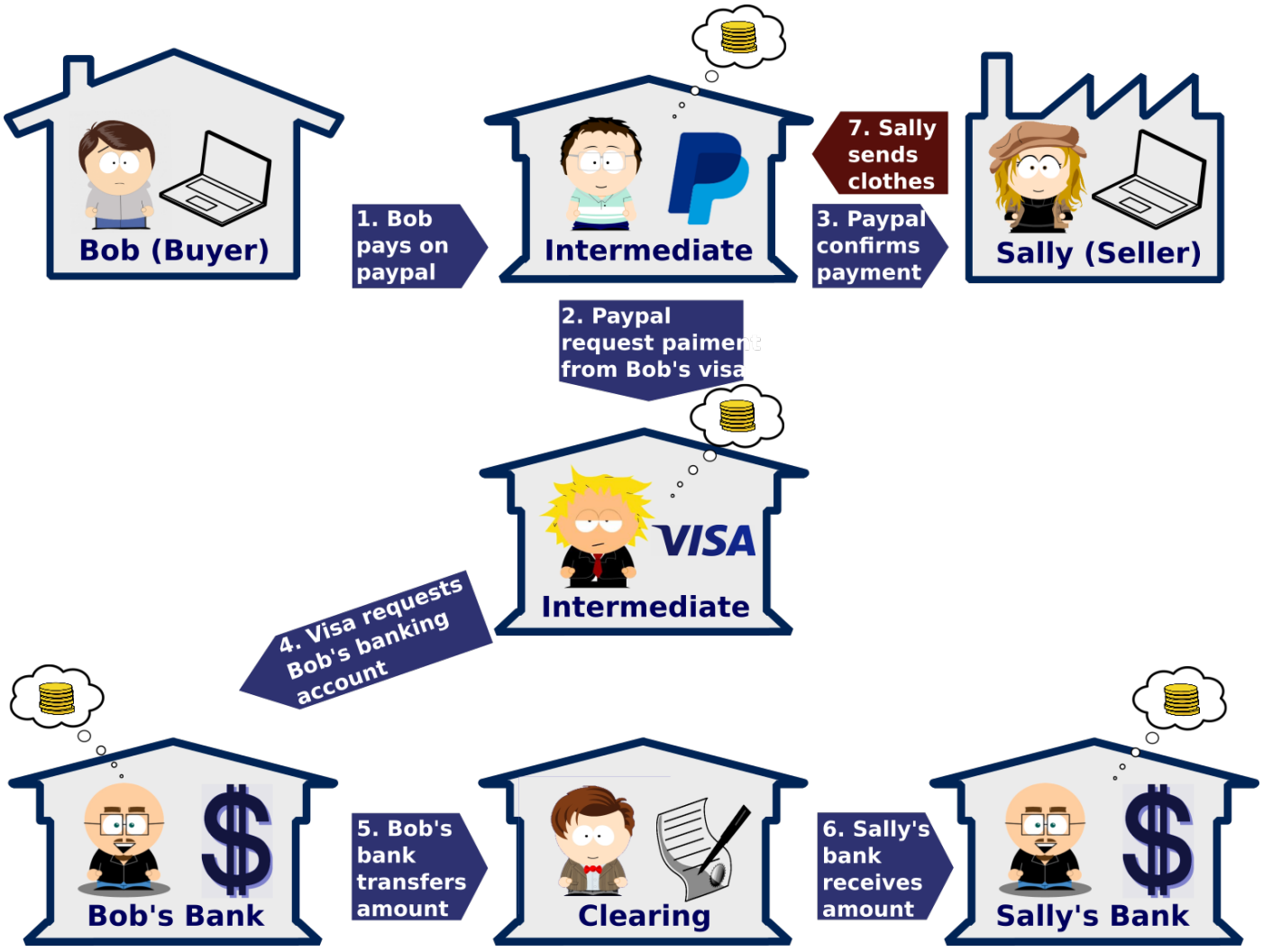
Table of Contents

Introduction Example



- Bob is an online web surfer and is looking for a suite. He wants to buy it online.
- Sally runs an online shop and sells clothes.

Usual Situation



Problems with this model

- The financial system is opaque and lacks transparency and fairness.

Problems with this model

- The financial system is opaque and lacks transparency and fairness.
- All these intermediates are no volunteers. They work for money and get paid for their services.

Problems with this model

- The financial system is opaque and lacks transparency and fairness.
- All these intermediates are no volunteers. They work for money and get paid for their services.
  - The transaction costs money to both the buyer and the seller.
  - There are interest rates, fees, surcharges, etc.
  - Credit transactions can cost several percent of the transaction.

Problems with this model

- The financial system is opaque and lacks transparency and fairness.
- All these intermediates are no volunteers. They work for money and get paid for their services.
  - The transaction costs money to both the buyer and the seller.
  - There are interest rates, fees, surcharges, etc.
  - Credit transactions can cost several percent of the transaction.
- All these exchanges are error prone.
  - Banks make mistakes.
  - Credit card informations are often stolen.

Problems with this model

- The financial system is opaque and lacks transparency and fairness.
- All these intermediates are no volunteers. They work for money and get paid for their services.
  - The transaction costs money to both the buyer and the seller.
  - There are interest rates, fees, surcharges, etc.
  - Credit transactions can cost several percent of the transaction.
- All these exchanges are error prone.
  - Banks make mistakes.
  - Credit card informations are often stolen.
- An account holder is eventually not even the actual owner of his account.
  - The bank really owns the account.
  - Funds can be garnished, even frozen completely.
  - Banks and other payment processors like PayPal, Visa, and Mastercard may refuse to process payments for certain legal entities.

Problems with this model

- The financial system is opaque and lacks transparency and fairness.
- All these intermediates are no volunteers. They work for money and get paid for their services.
  - The transaction costs money to both the buyer and the seller.
  - There are interest rates, fees, surcharges, etc.
  - Credit transactions can cost several percent of the transaction.
- All these exchanges are error prone.
  - Banks make mistakes.
  - Credit card informations are often stolen.
- An account holder is eventually not even the actual owner of his account.
  - The bank really owns the account.
  - Funds can be garnished, even frozen completely.
  - Banks and other payment processors like PayPal, Visa, and Mastercard may refuse to process payments for certain legal entities.
- Financial exchanges are slow.
  - Checking and low cost wire services take days to complete.

Clearing House

A clearing house

- is a financial institution that provides clearing and settlement services for financial and commodities derivatives and securities transactions

Clearing House

A clearing house

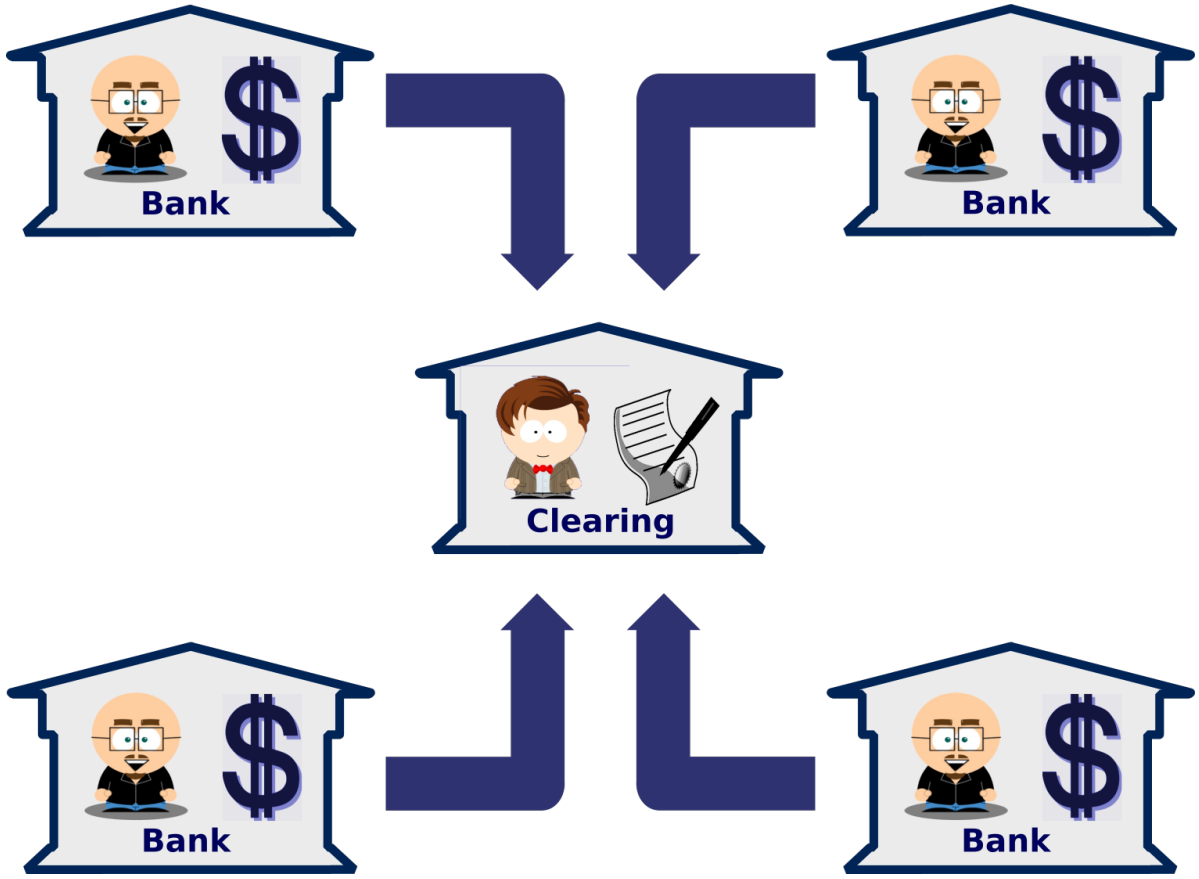
- is a financial institution that provides clearing and settlement services for financial and commodities derivatives and securities transactions
- stands between two clearing participants / firms (banks)

Clearing House

A clearing house

- is a financial institution that provides clearing and settlement services for financial and commodities derivatives and securities transactions
- stands between two clearing participants / firms (banks)
- reduces the risk of one (or more) clearing firm failing to honor its trade settlement obligations.
  - It nets offsetting transactions between multiple counterparties.

Clearing House (2)



Buyers and sellers use intermediaries because they may not trust the other party, but they trust that the intermediary will assure the transaction is completed faithfully. This is the fundamental role of a clearing house.

The problems with Clearing Houses

- When one bank sends money to another, no physical currency changes hands.

The problems with Clearing Houses

- When one bank sends money to another, no physical currency changes hands.
- Banks and settlement systems use central electronic ledgers to track assets.
  - But such central ledgers - or clearing houses - can be slow and inefficient, often relying on faxes or manual input.
  - That not only wastes time but racks up fees.

The problems with Clearing Houses

- When one bank sends money to another, no physical currency changes hands.
- Banks and settlement systems use central electronic ledgers to track assets.
  - But such central ledgers - or clearing houses - can be slow and inefficient, often relying on faxes or manual input.
  - That not only wastes time but racks up fees.
- The system is also open to hacking and fraud.

The problems with Clearing Houses

- When one bank sends money to another, no physical currency changes hands.
- Banks and settlement systems use central electronic ledgers to track assets.
  - But such central ledgers - or clearing houses - can be slow and inefficient, often relying on faxes or manual input.
  - That not only wastes time but racks up fees.
- The system is also open to hacking and fraud.
- These central institutions gets fees to cover such risks of course as well as many other services. The price is high
  - It prevents, for instance, micro-payments services who are not able to support the charge asked by these central structures.

Distributed Ledgers

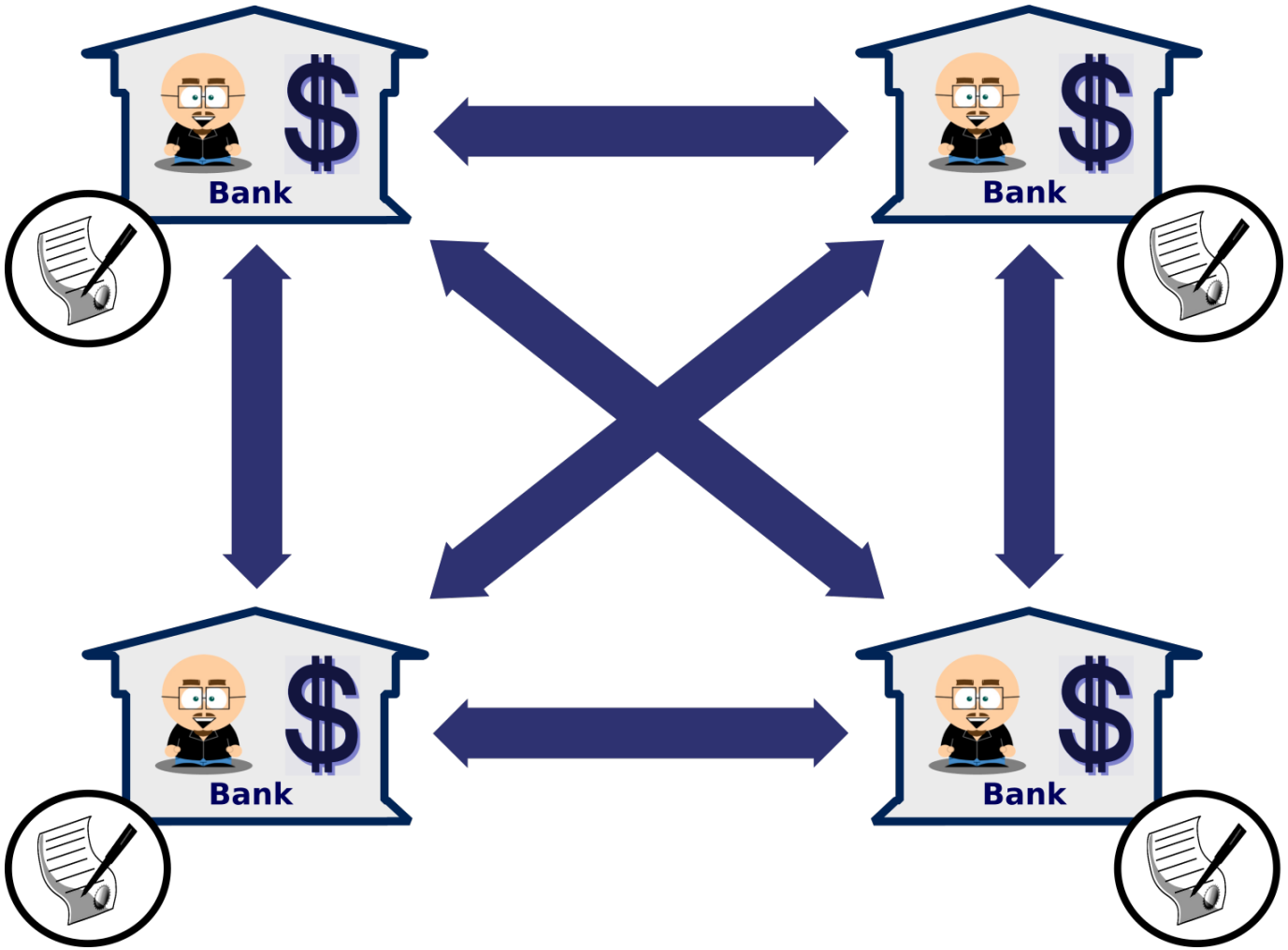
- A distributed ledger (also called shared ledger) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions.
- Every node in the decentralized system has a copy of the ledger.
- No centralized "official" copy exists and no user is "trusted" more than any other.

Distributed Ledgers

- A distributed ledger (also called shared ledger) is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions.
- Every node in the decentralized system has a copy of the ledger.
- No centralized "official" copy exists and no user is "trusted" more than any other.

Other definition: A blockchain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks.

Distributed Ledger instead of Central Ledger

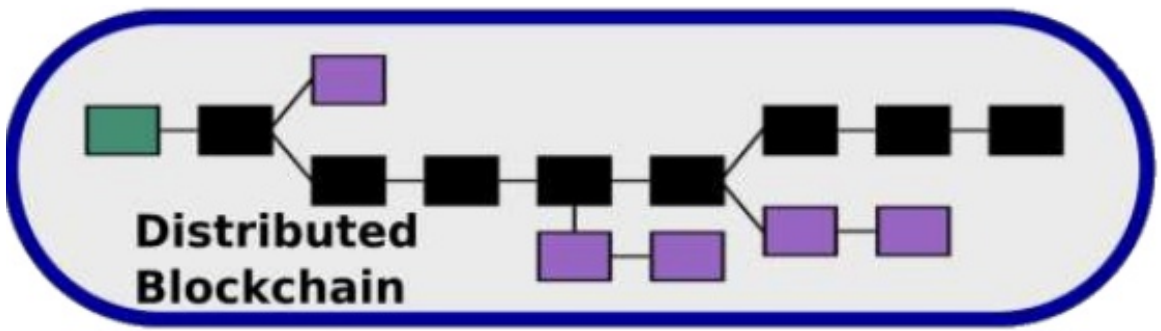


Blockchain overview

- The blockchain itself is a list of blocks.
  - These digitally recorded "blocks" of data are stored in a linear chain.
  - Each block in the chain contains data (e.g. bitcoin transaction) and is cryptographically hashed.

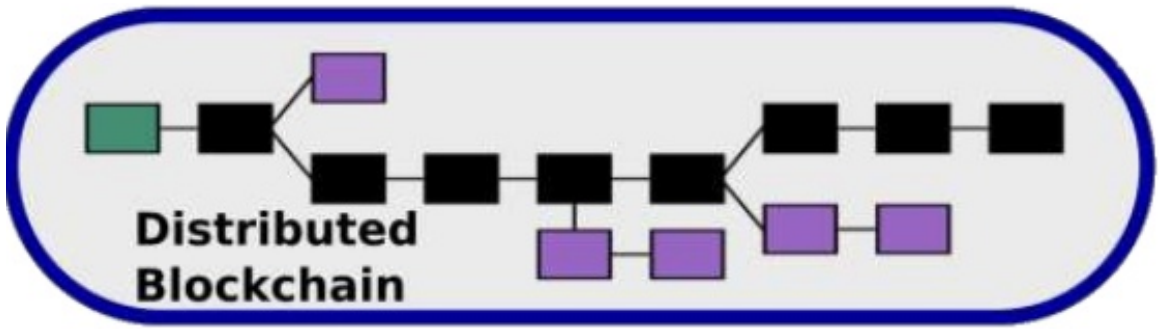
Blockchain overview

- The blockchain itself is a list of blocks.
  - These digitally recorded "blocks" of data are stored in a linear chain.
  - Each block in the chain contains data (e.g. bitcoin transaction) and is cryptographically hashed.
- Each block includes the hash of the prior block in the blockchain, linking the two, ensuring all data in the overall "blockchain" has not been tampered with and remains unchanged.



Blockchain overview

- The blockchain itself is a list of blocks.
  - These digitally recorded "blocks" of data are stored in a linear chain.
  - Each block in the chain contains data (e.g. bitcoin transaction) and is cryptographically hashed.
- Each block includes the hash of the prior block in the blockchain, linking the two, ensuring all data in the overall "blockchain" has not been tampered with and remains unchanged.



- This has the effect of creating a chain of blocks from the genesis block to the current block.
  - Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known.

Blockchain overview (2)

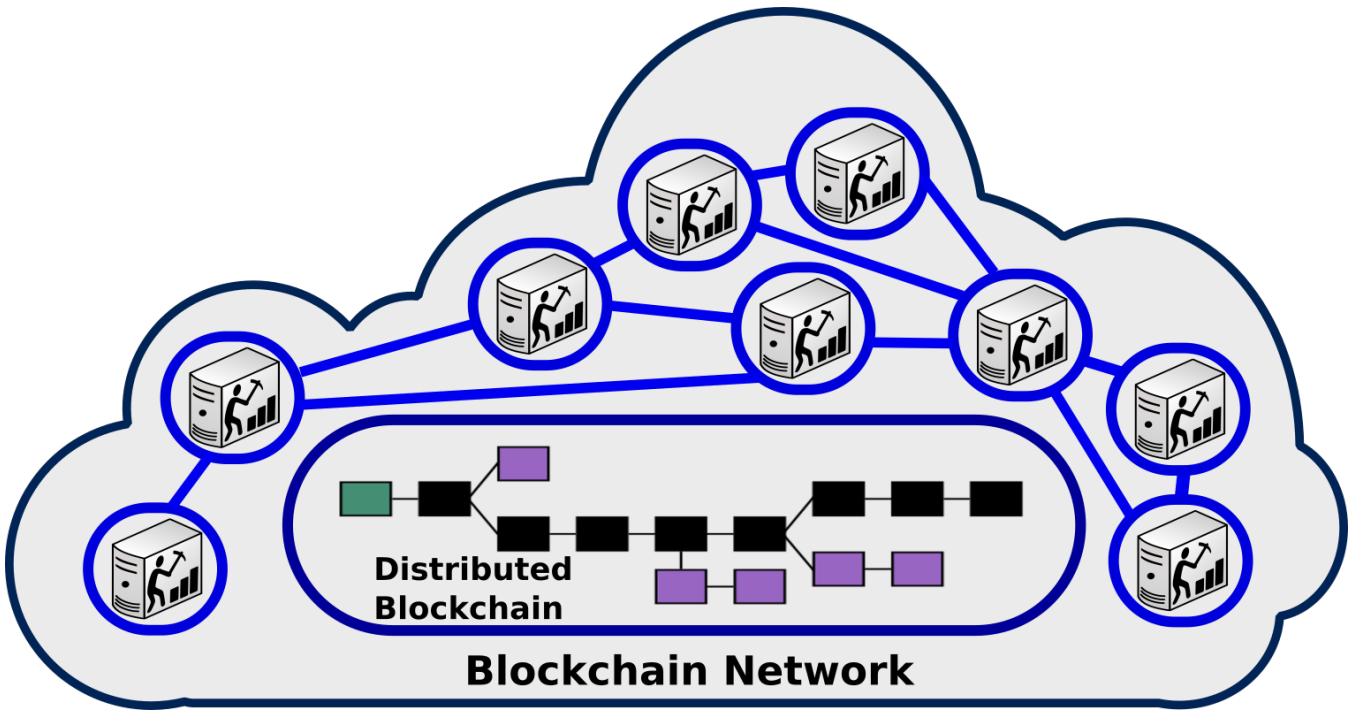
- The blockchain network is a peer-to-peer network of independent nodes communicating together by message broadcasting.

Blockchain overview (2)

- The blockchain network is a peer-to-peer network of independent nodes communicating together by message broadcasting.
- A node is not necessarily connected to every other node, but at least some of them.

Blockchain overview (2)

- The blockchain network is a peer-to-peer network of independent nodes communicating together by message broadcasting.
- A node is not necessarily connected to every other node, but at least some of them.



Blockchain principle

The operation principle of is pretty straightforward to understand. We'll illustrate it her on the Bitcoin blockchain. Principle is as follows:

Blockchain principle

The operation principle of is pretty straightforward to understand. We'll illustrate it her on the Bitcoin blockchain. Principle is as follows:

1. A user wants to pay another user some bitcoins, he broadcasts a transaction to the network.

Blockchain principle

The operation principle of is pretty straightforward to understand. We'll illustrate it her on the Bitcoin blockchain. Principle is as follows:

1. A user wants to pay another user some bitcoins, he broadcasts a transaction to the network.
2. Miners add the transaction as they receive it to their current block, the one they are currently working on

Blockchain principle

The operation principle of is pretty straightforward to understand. We'll illustrate it her on the Bitcoin blockchain. Principle is as follows:

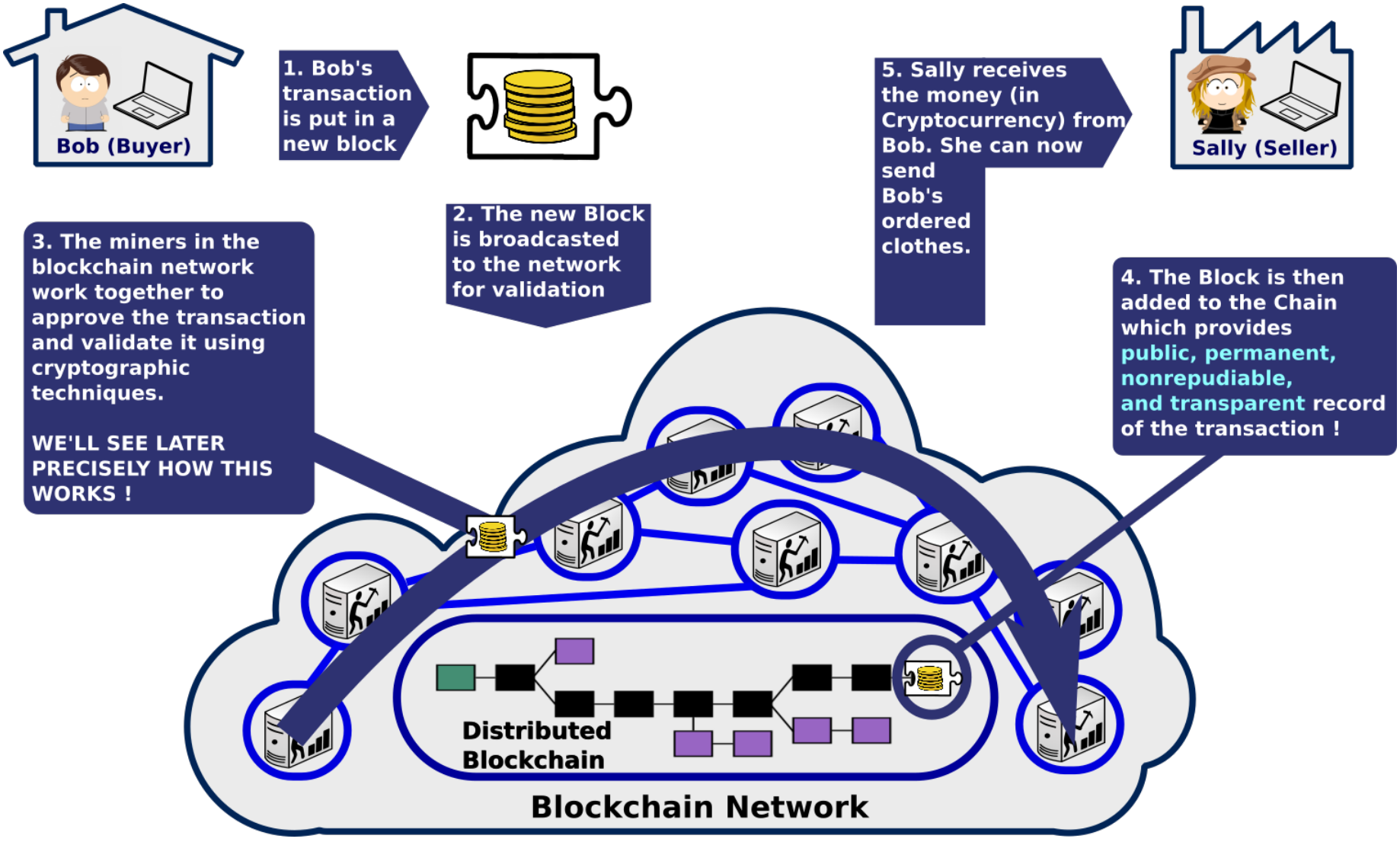
1. A user wants to pay another user some bitcoins, he broadcasts a transaction to the network.
2. Miners add the transaction as they receive it to their current block, the one they are currently working on
3. Randomly, one of the miner may win the lottery and "mine" the block (we'll get back to that)

Blockchain principle

The operation principle of is pretty straightforward to understand. We'll illustrate it her on the Bitcoin blockchain. Principle is as follows:

1. A user wants to pay another user some bitcoins, he broadcasts a transaction to the network.
2. Miners add the transaction as they receive it to their current block, the one they are currently working on
3. Randomly, one of the miner may win the lottery and "mine" the block (we'll get back to that)
4. At that moment, this new "definitive" block is broadcasted to the network and added to everyone's copy of the blockchain

Blockchain principle (2)



Proof of Work

- In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block.

Proof of Work

- In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block.
  - The proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements.
  - Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.
  - Bitcoin uses the Hashcash proof of work system.

Proof of Work

- In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block.
  - The proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements.
  - Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated.
  - Bitcoin uses the Hashcash proof of work system.
- For a block to be valid it must hash to a value less than the current target; this means that each block indicates that work has been done generating it.

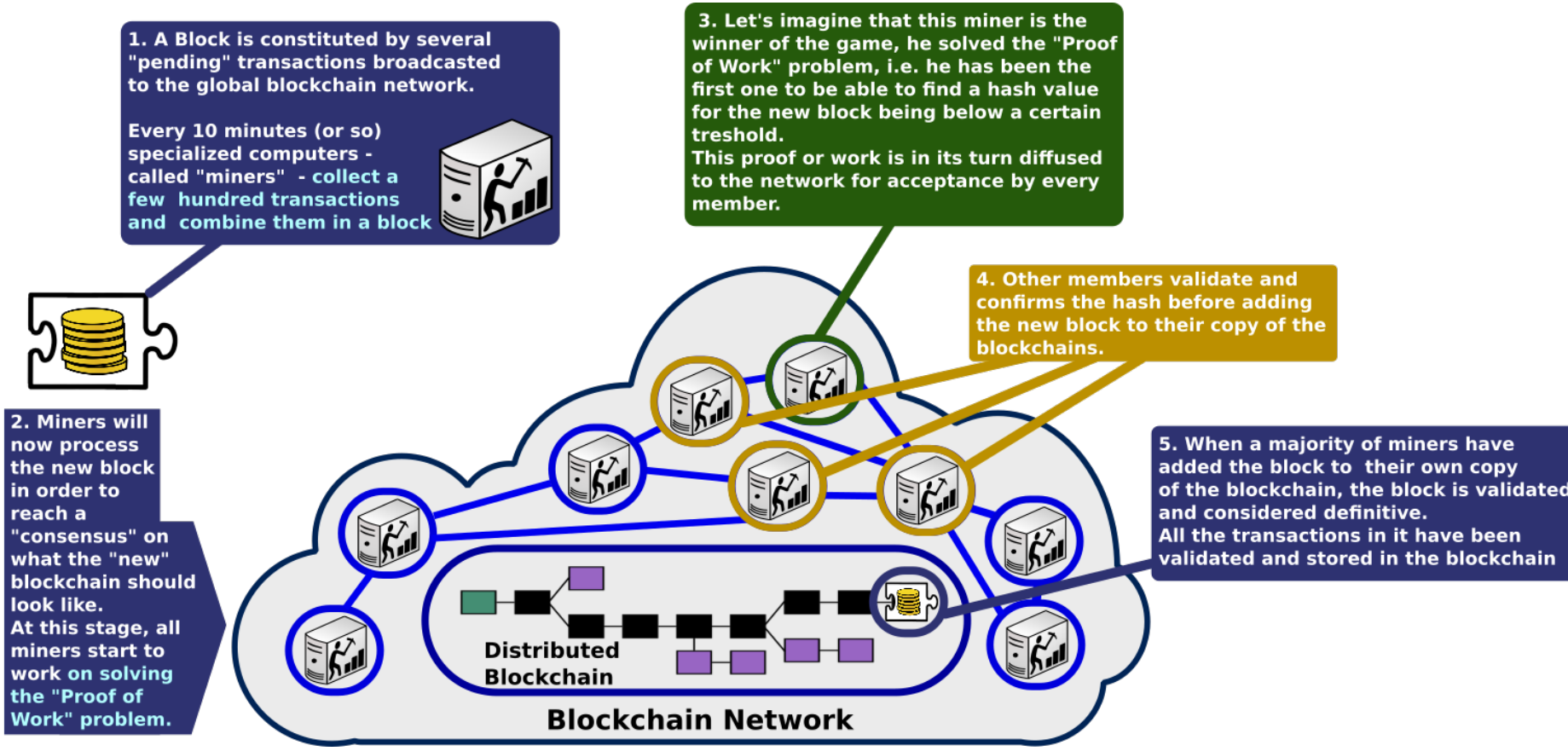
Proof of Work (2)

- Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work.

Proof of Work (2)

- Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work.
- Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain.
  - This protects the block chain from tampering.
  - The amount of successors is relevant when qualifying the validity of a block: at least 6 successors are required to consider a block valid

Mining principle



Blockchain structure

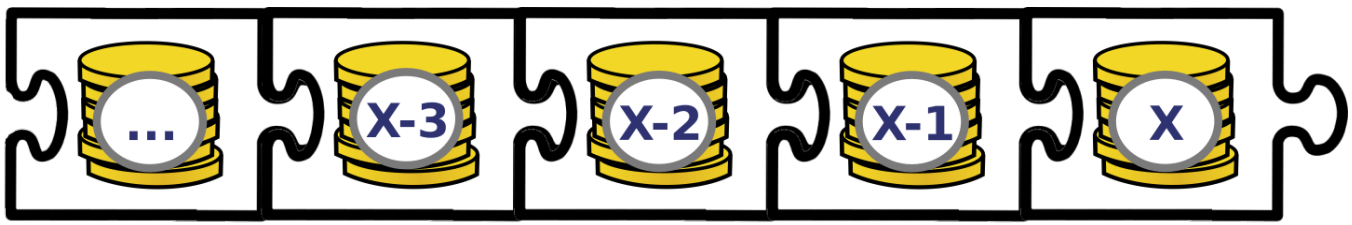
- The blockchain data structure is an ordered, back-linked list of blocks of transactions.

Blockchain structure

- The blockchain data structure is an ordered, back-linked list of blocks of transactions.
  - Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block.

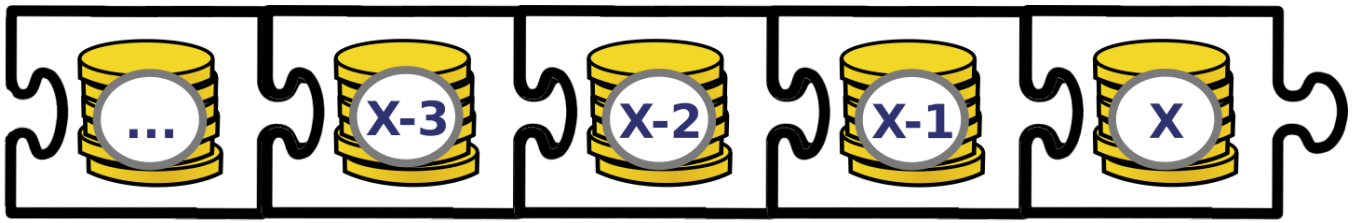
Blockchain structure

- The blockchain data structure is an ordered, back-linked list of blocks of transactions.
  - Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block.
  - Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known.



Blockchain structure

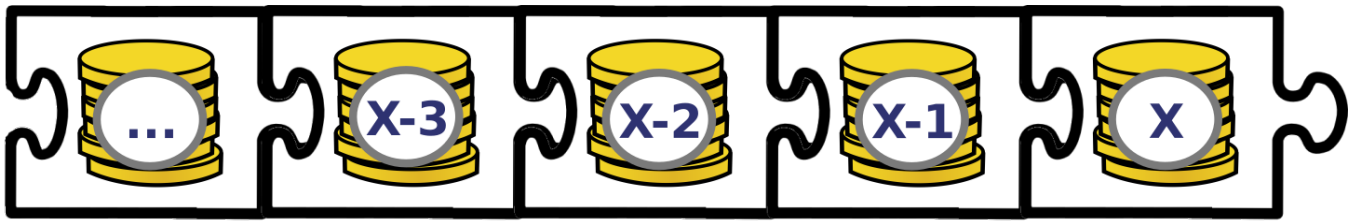
- The blockchain data structure is an ordered, back-linked list of blocks of transactions.
  - Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block.
  - Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known.



- Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated.

Blockchain structure

- The blockchain data structure is an ordered, back-linked list of blocks of transactions.
  - Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block.
  - Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known.



- Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated.
- New transactions are constantly being processes by miners into new blocks which are added to the end of the chain and can never be changed or removed once accepted by the network.

Block Structure

Each block contains, among other things:

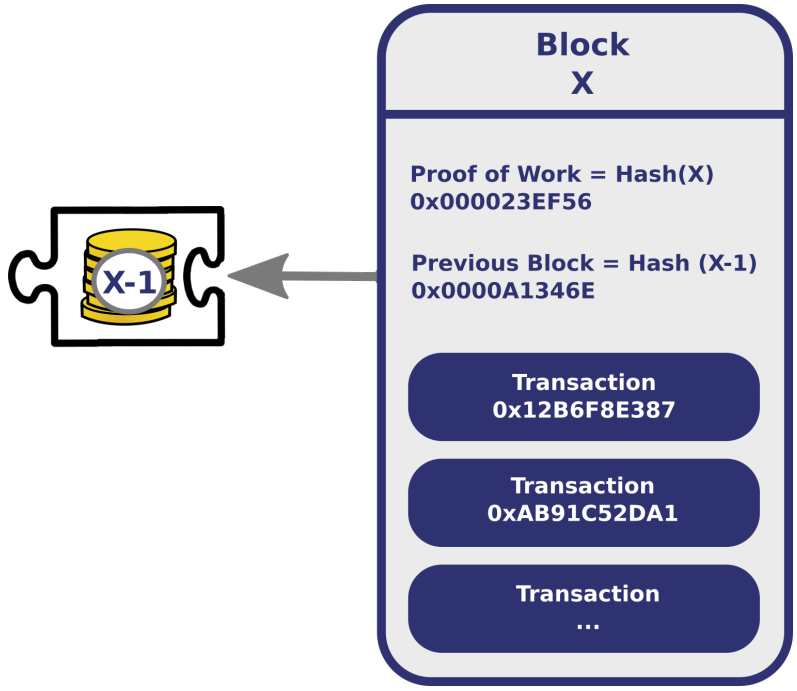
- a record of some or all recent transactions, and
- a reference to the block that came immediately before it.

Block Structure

Each block contains, among other things:

- a record of some or all recent transactions, and
- a reference to the block that came immediately before it.

It also contains an answer to a difficult-to-solve mathematical puzzle, the hash or Proof of Work.



Mining

- In the Bitcoin world, transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. This is called Mining.

Mining

- In the Bitcoin world, transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. This is called Mining.
  - Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions. This ledger of past transactions is called the block chain as it is a chain of blocks.

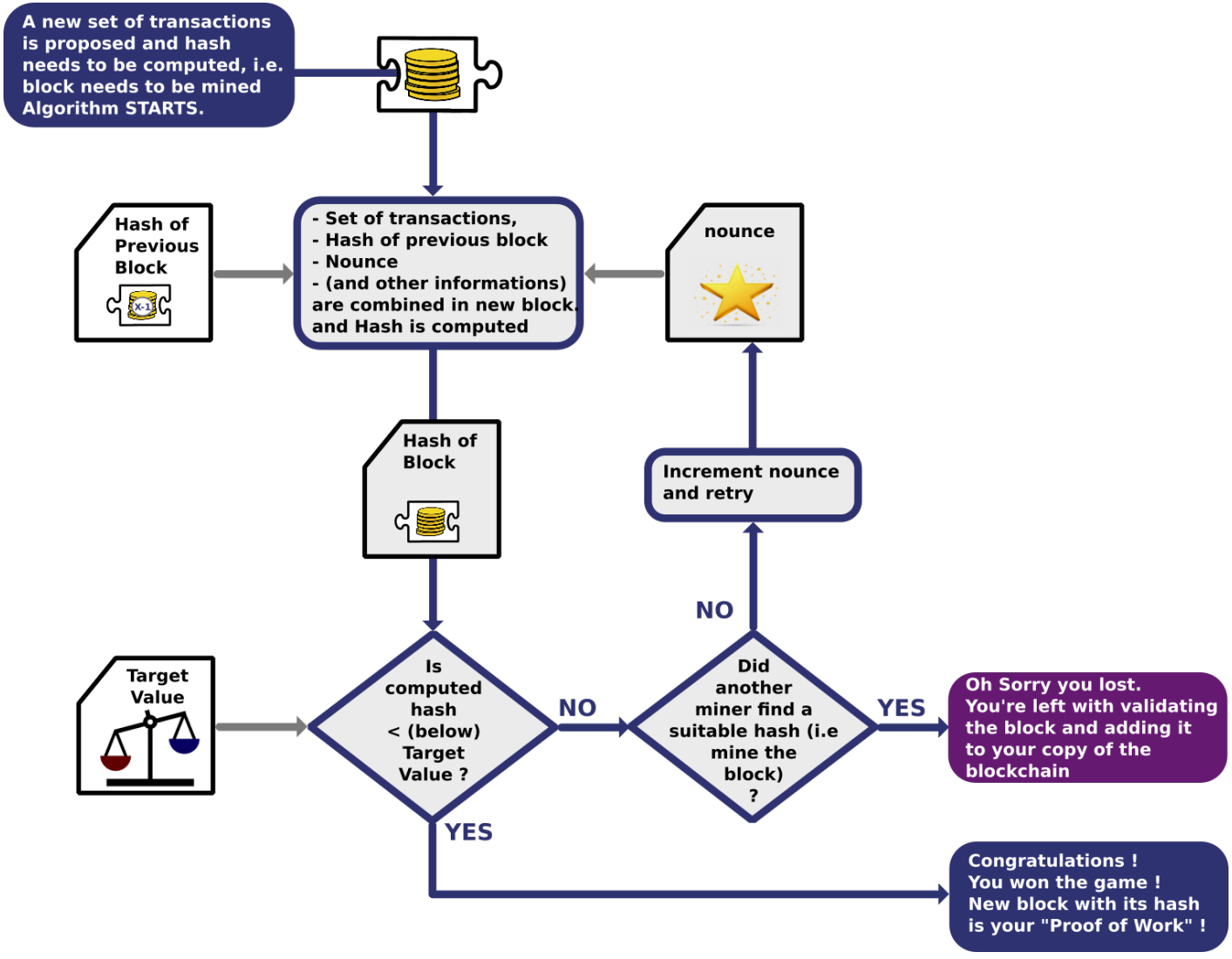
Mining

- In the Bitcoin world, transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. This is called Mining.
  - Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions. This ledger of past transactions is called the block chain as it is a chain of blocks.
  - Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid.

Mining

- In the Bitcoin world, transactions are broadcast to the network by the sender, and all peers trying to solve blocks collect the transaction records and add them to the block they are working to solve. This is called Mining.
  - Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions. This ledger of past transactions is called the block chain as it is a chain of blocks.
  - Mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of work to be considered valid.
- The primary purpose of mining is to allow Bitcoin nodes to reach a secure, tamper-resistant consensus.

Mining algorithm



Difficulty Adjustment

- The difficulty is the measure of how difficult it is to find a new block compared to the easiest it can ever be.

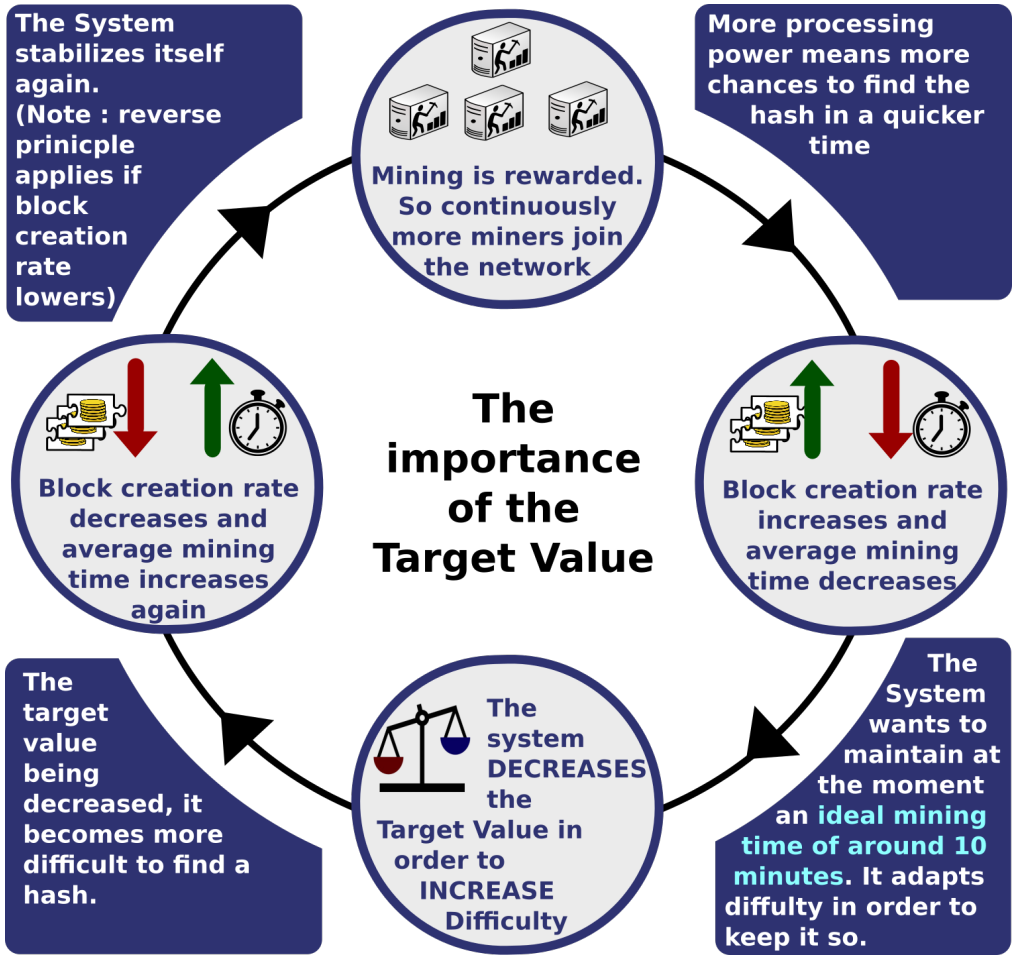
Difficulty Adjustment

- The difficulty is the measure of how difficult it is to find a new block compared to the easiest it can ever be.
- It is recalculated every $2016 = 14 \cdot 24 \cdot 6$ blocks to a value such that the previous 2016 blocks would have been generated in exactly two weeks had everyone been mining at this difficulty.

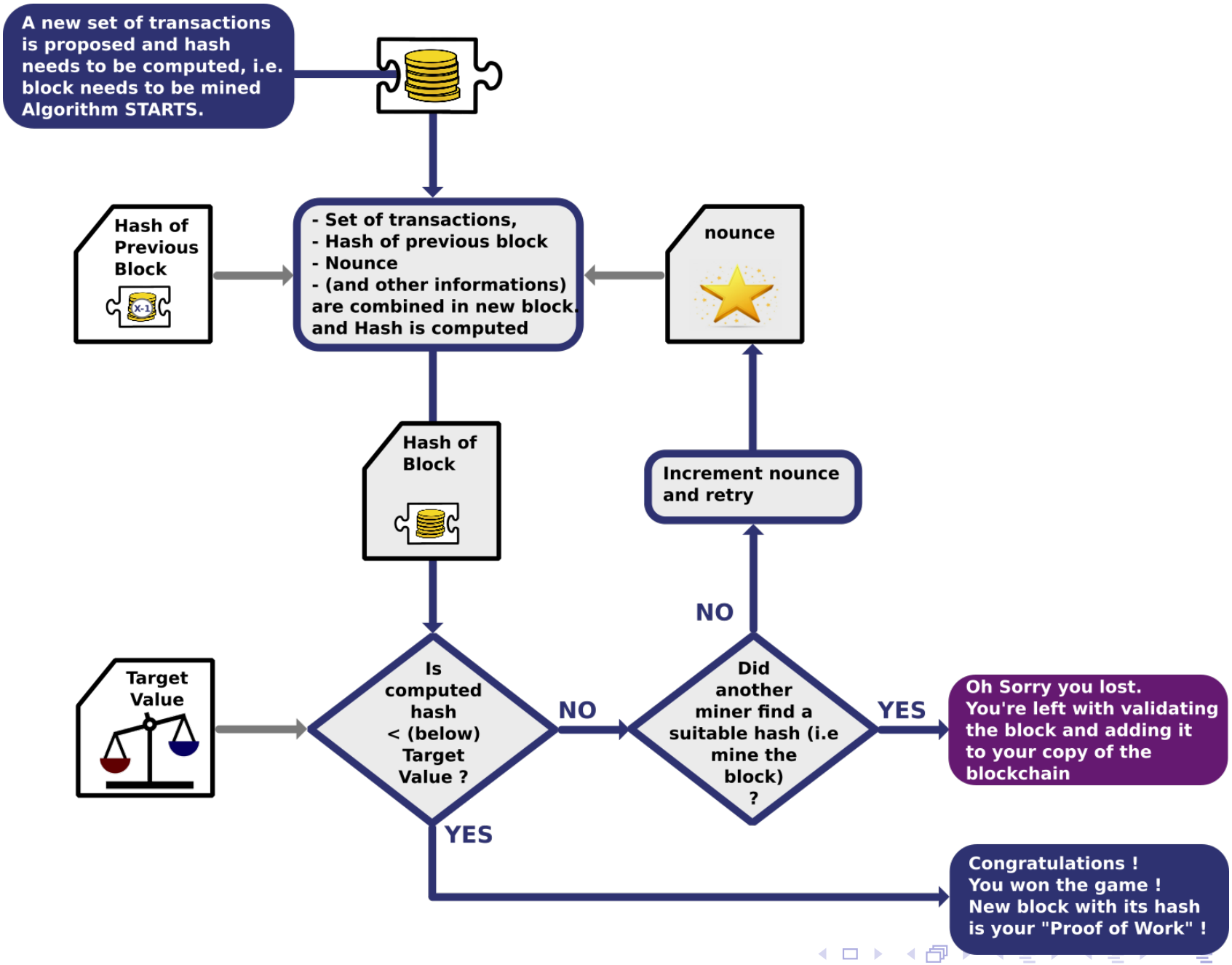
Difficulty Adjustment

- The difficulty is the measure of how difficult it is to find a new block compared to the easiest it can ever be.
- It is recalculated every $2016 = 14 \cdot 24 \cdot 6$ blocks to a value such that the previous 2016 blocks would have been generated in exactly two weeks had everyone been mining at this difficulty.
- This will yield, on average, one block every ten minutes.

Target Value



Mining algorithm



Miner retribution

- Mining is also the mechanism used to introduce Bitcoins into the system:
  - Miners are paid any transaction fees as well as
  - a "subsidy" of newly created coins.

Miner retribution

- Mining is also the mechanism used to introduce Bitcoins into the system:
  - Miners are paid any transaction fees as well as
  - a "subsidy" of newly created coins.
- These both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system.

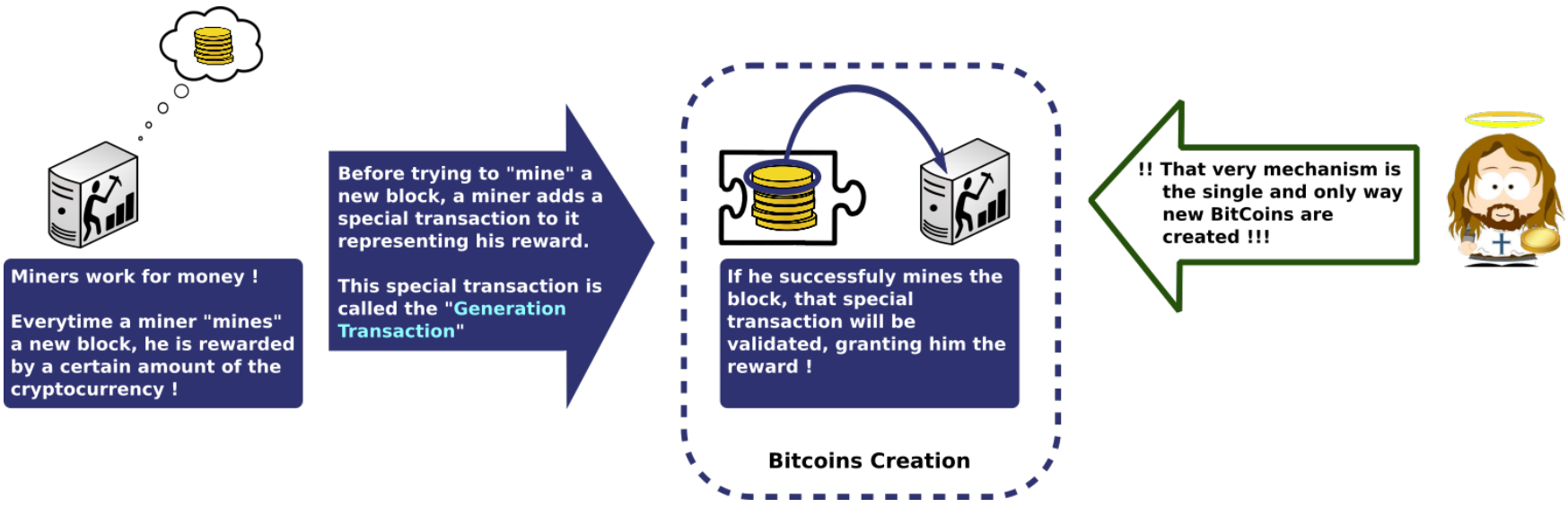
Miner retribution

- Mining is also the mechanism used to introduce Bitcoins into the system:
  - Miners are paid any transaction fees as well as
  - a "subsidy" of newly created coins.
- These both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system.
- It gives miners incentive to put their computation power at the disposal of the blockchain network.

Miner retribution

- Mining is also the mechanism used to introduce Bitcoins into the system:
  - Miners are paid any transaction fees as well as
  - a "subsidy" of newly created coins.
- These both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system.
- It gives miners incentive to put their computation power at the disposal of the blockchain network.
- Because there is a reward of brand new bitcoins for solving each block, every block also contains a record of which Bitcoin addresses or scripts are entitled to receive the reward.
  - This record is known as a generation transaction (or a coinbase transaction) and is always the first transaction appearing in every block.

Mining algorithm



Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.
  - The monetary base is controlled by this central bank.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.
  - The monetary base is controlled by this central bank.
  - In the United States, the Fed increases the monetary base by issuing currency, increasing the amount banks have on reserve, and more recently, printing money electronically in a process called Quantitative Easing.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.
  - The monetary base is controlled by this central bank.
  - In the United States, the Fed increases the monetary base by issuing currency, increasing the amount banks have on reserve, and more recently, printing money electronically in a process called Quantitative Easing.
- In a fully decentralized monetary system, there is no central authority that regulates the monetary base.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.
  - The monetary base is controlled by this central bank.
  - In the United States, the Fed increases the monetary base by issuing currency, increasing the amount banks have on reserve, and more recently, printing money electronically in a process called Quantitative Easing.
- In a fully decentralized monetary system, there is no central authority that regulates the monetary base.
  - Instead, currency is created by the nodes of a peer-to-peer network.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.
  - The monetary base is controlled by this central bank.
  - In the United States, the Fed increases the monetary base by issuing currency, increasing the amount banks have on reserve, and more recently, printing money electronically in a process called Quantitative Easing.
- In a fully decentralized monetary system, there is no central authority that regulates the monetary base.
  - Instead, currency is created by the nodes of a peer-to-peer network.
  - The Bitcoin generation algorithm defines, in advance, how currency will be created and at what rate.

Bitcoin limited supply

- In the specific case of the bitcoin, Satoshi had very soon the idea of limiting the bitcoin supply.
  - In a centralized economy, currency is issued by a central bank at a rate that is supposed to match the growth of the amount of goods that are exchanged so that these goods can be traded with stable prices.
  - The monetary base is controlled by this central bank.
  - In the United States, the Fed increases the monetary base by issuing currency, increasing the amount banks have on reserve, and more recently, printing money electronically in a process called Quantitative Easing.
- In a fully decentralized monetary system, there is no central authority that regulates the monetary base.
  - Instead, currency is created by the nodes of a peer-to-peer network.
  - The Bitcoin generation algorithm defines, in advance, how currency will be created and at what rate.
  - Any currency that is generated by a malicious user that does not follow the rules will be rejected by the network and thus is worthless.

Bitcoin limited supply (2)

- Bitcoins are created each time a user discovers a new block.

Bitcoin limited supply (2)

- Bitcoins are created each time a user discovers a new block.
  - The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period (equivalent to 6 per hour)

Bitcoin limited supply (2)

- Bitcoins are created each time a user discovers a new block.
  - The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period (equivalent to 6 per hour)
  - The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years.

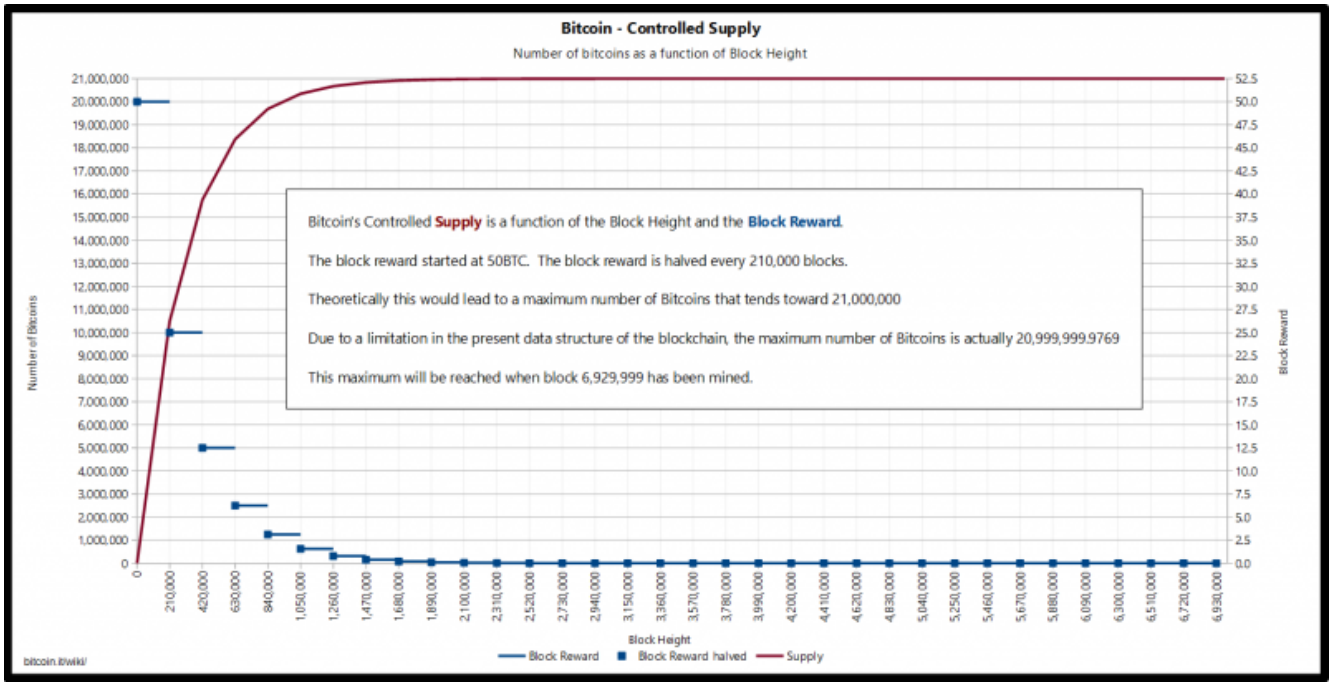
Bitcoin limited supply (2)

- Bitcoins are created each time a user discovers a new block.
  - The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period (equivalent to 6 per hour)
  - The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years.
  - The result is that the number of bitcoins in existence is not expected to exceed 21 million.

Bitcoin limited supply (2)

- Bitcoins are created each time a user discovers a new block.
  - The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period (equivalent to 6 per hour)
  - The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years.
  - The result is that the number of bitcoins in existence is not expected to exceed 21 million.
- Speculated justifications for the unintuitive value "21 million" are that it matches a 4-year reward halving schedule; or the ultimate total number of bitcoins that will be mined is close to the maximum capacity of a 64-bit floating point number.

Bitcoin Monetary Inflation



Bitcoin Wallet Cryptography

- A wallet is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others.

Bitcoin Wallet Cryptography

- A wallet is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others.
  - The name "Bitcoin wallet" is a bit of a misnomer. Bitcoin wallets don't hold actual Bitcoins, those are essentially stored on the blockchain.

Bitcoin Wallet Cryptography

- A wallet is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others.
  - The name "Bitcoin wallet" is a bit of a misnomer. Bitcoin wallets don't hold actual Bitcoins, those are essentially stored on the blockchain.
  - Instead, Bitcoin wallets hold the private keys that give users the right to use those coins.

Bitcoin Wallet Cryptography

- A wallet is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others.
  - The name "Bitcoin wallet" is a bit of a misnomer. Bitcoin wallets don't hold actual Bitcoins, those are essentially stored on the blockchain.
  - Instead, Bitcoin wallets hold the private keys that give users the right to use those coins.
  - Each Bitcoin wallet comes with at least two keys: one public, and one private.

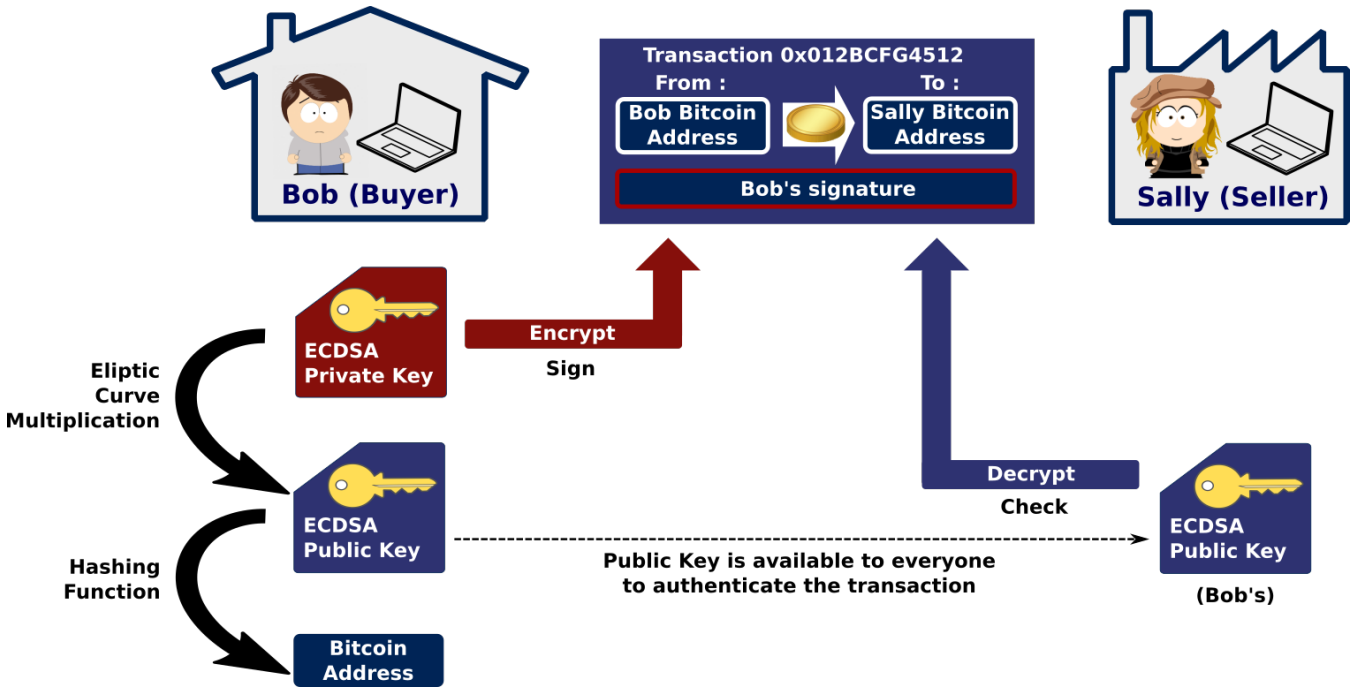
Bitcoin Wallet Cryptography

- A wallet is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others.
  - The name "Bitcoin wallet" is a bit of a misnomer. Bitcoin wallets don't hold actual Bitcoins, those are essentially stored on the blockchain.
  - Instead, Bitcoin wallets hold the private keys that give users the right to use those coins.
  - Each Bitcoin wallet comes with at least two keys: one public, and one private.
- A Bitcoin address, or simply address, is an identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3, that represents a possible destination for a bitcoin payment.

Bitcoin Wallet Cryptography

- A wallet is basically the Bitcoin equivalent of a bank account. It allows you to receive bitcoins, store them, and then send them to others.
  - The name "Bitcoin wallet" is a bit of a misnomer. Bitcoin wallets don't hold actual Bitcoins, those are essentially stored on the blockchain.
  - Instead, Bitcoin wallets hold the private keys that give users the right to use those coins.
  - Each Bitcoin wallet comes with at least two keys: one public, and one private.
- A Bitcoin address, or simply address, is an identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3, that represents a possible destination for a bitcoin payment.
  - Addresses can be generated at no cost by any user of Bitcoin.

Bitcoin Wallet Cryptography



Merkle Trees

- A Merkle Tree is a tree constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains, the merkle root.

Merkle Trees

- A Merkle Tree is a tree constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains, the merkle root.
- The construction of the Merke tree is such that if any single leaf transaction is changed, all hashes along the branch would be changed and ultimately the merkle root as well.

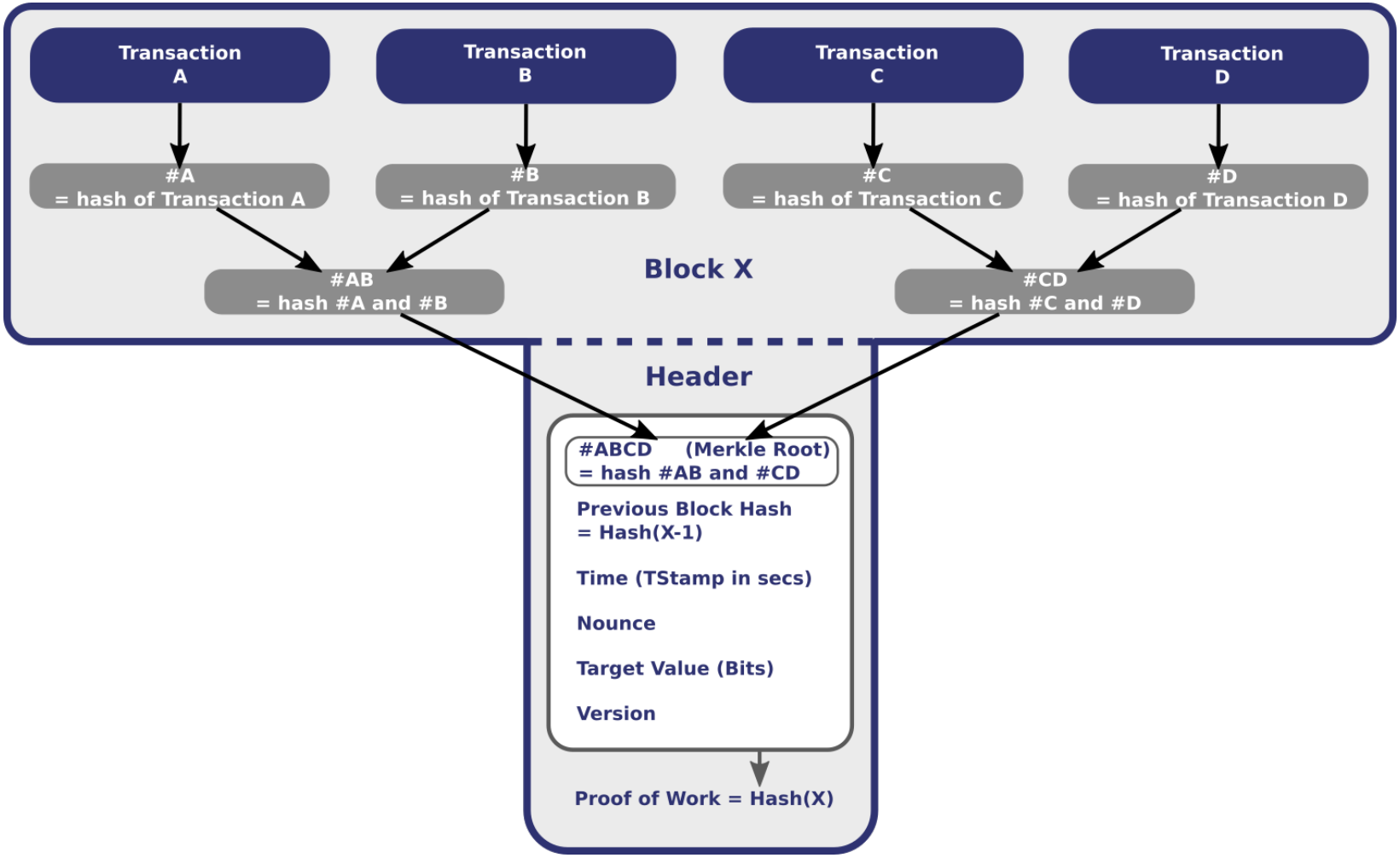
Merkle Trees

- A Merkle Tree is a tree constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains, the merkle root.
- The construction of the Merke tree is such that if any single leaf transaction is changed, all hashes along the branch would be changed and ultimately the merkle root as well.
  - This is a key property ensuring security of the blockchain.

Merkle Trees

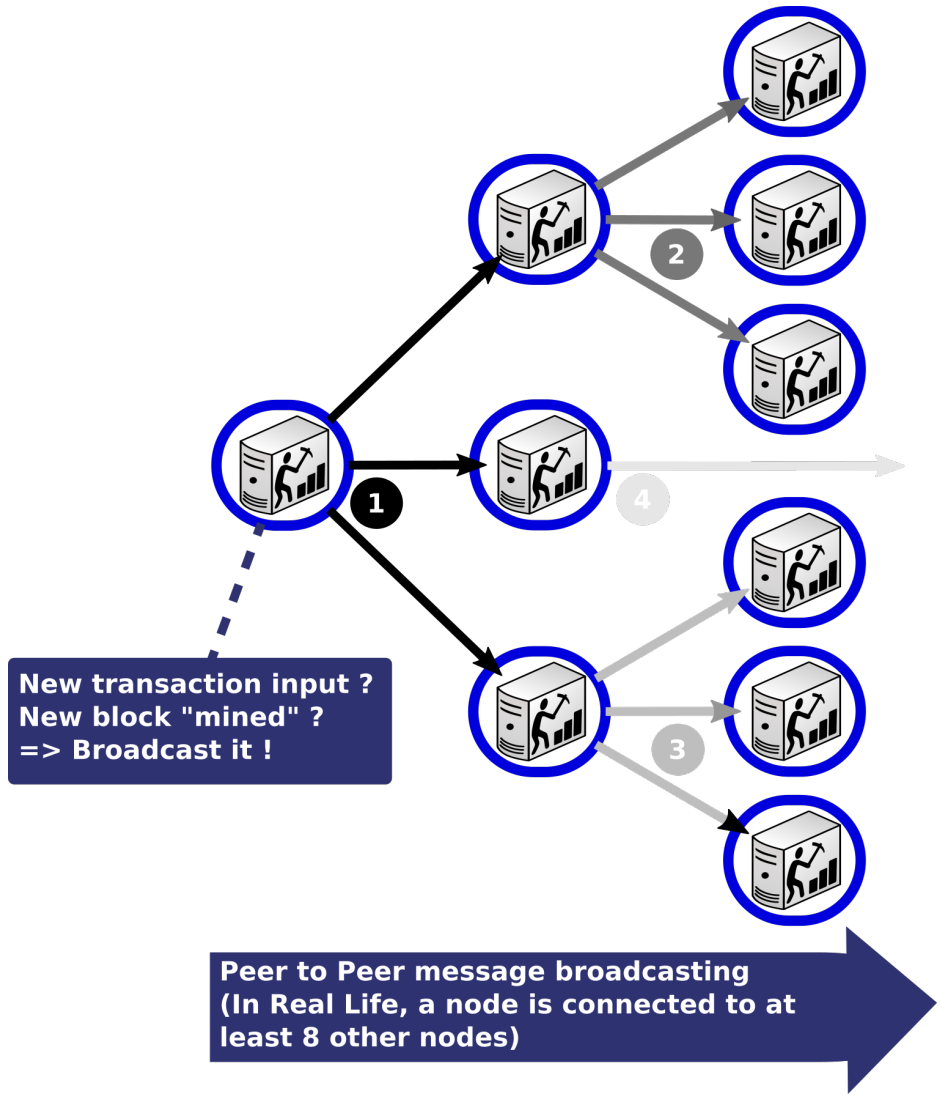
- A Merkle Tree is a tree constructed by hashing paired data (the leaves), then pairing and hashing the results until a single hash remains, the merkle root.
- The construction of the Merke tree is such that if any single leaf transaction is changed, all hashes along the branch would be changed and ultimately the merkle root as well.
  - This is a key property ensuring security of the blockchain.
- Merkle trees in Bitcoin use a double SHA-256, the SHA-256 hash of the SHA- 256 hash of something.

Merkle Tree


Transaction A
Transaction B
Transaction C
Transaction D
#A = hash of Transaction A
#B = hash of Transaction B
#C = hash of Transaction C
#D = hash of Transaction D
#AB = hash #A and #B
#CD = hash #C and #D
Block X
Header
#ABCD (Merkle Root) = hash #AB and #CD
Previous Block Hash = Hash(X-1)
Time (TStamp in secs)
Nounce
Target Value (Bits)
Version
Proof of Work = Hash(X)

Replication

Both new transactions and newly mined blocked are broadcasted to the peer-to- peer network using the Flood Protocol.



Orphaned, Extinct and Staled Blocks

- It's possible for the blockchain to have temporary splits

Orphaned, Extinct and Staled Blocks

- It's possible for the blockchain to have temporary splits
  - for instance, if two miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another.

Orphaned, Extinct and Staled Blocks

- It's possible for the blockchain to have temporary splits
  - for instance, if two miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another.
- The peer-to-peer network is designed to resolve these splits within a short period of time, so that eventually only one branch of the chain survives.

Orphaned, Extinct and Staled Blocks

- It's possible for the blockchain to have temporary splits
  - for instance, if two miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another.
- The peer-to-peer network is designed to resolve these splits within a short period of time, so that eventually only one branch of the chain survives.
- The client accepts the longest chain of blocks as valid.

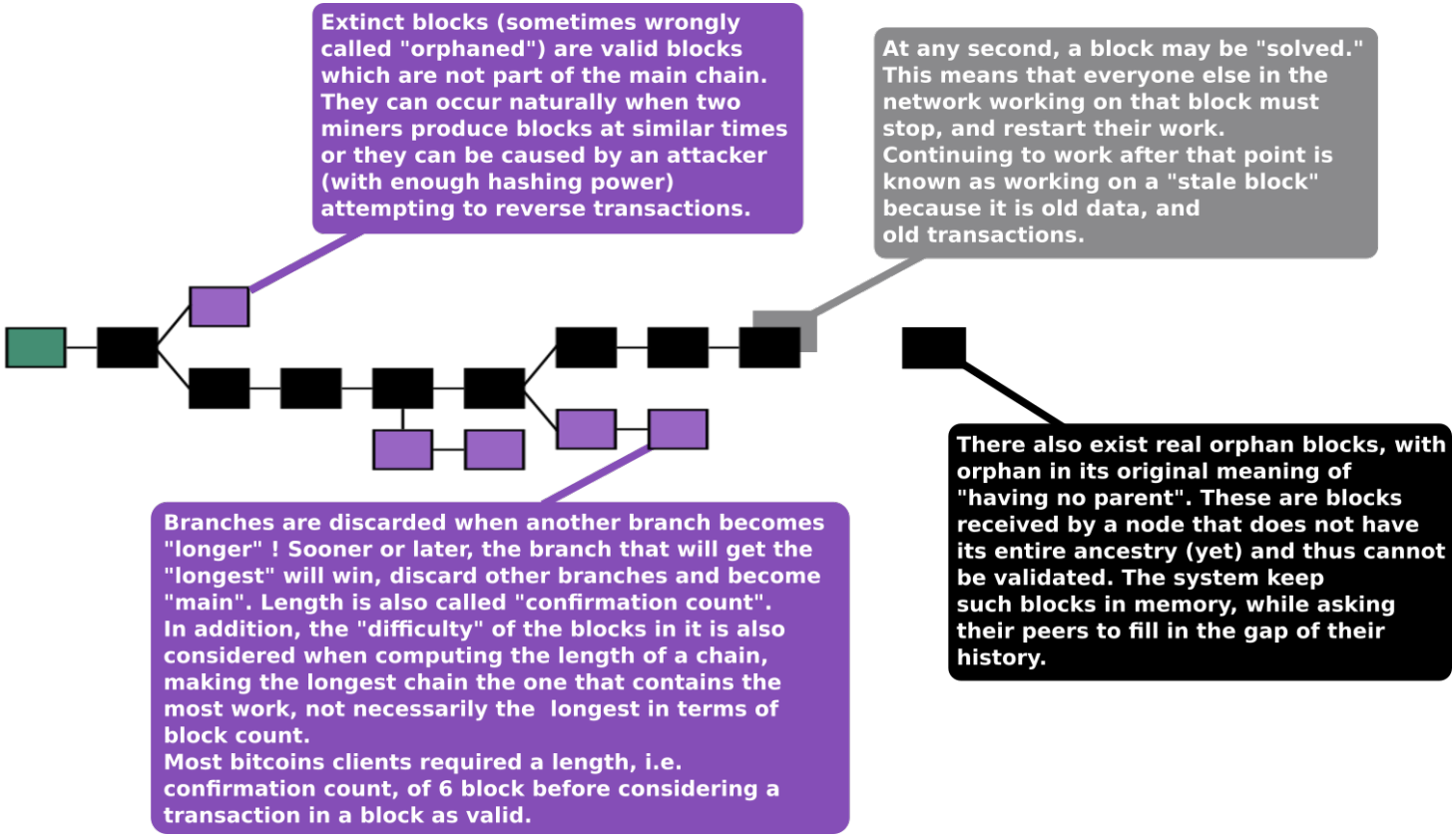
Orphaned, Extinct and Staled Blocks

- It's possible for the blockchain to have temporary splits
  - for instance, if two miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another.
- The peer-to-peer network is designed to resolve these splits within a short period of time, so that eventually only one branch of the chain survives.
- The client accepts the longest chain of blocks as valid.
  - The "length" of the entire block chain refers to the chain with the most combined difficulty, not the one with the most blocks.

Orphaned, Extinct and Staled Blocks

- It's possible for the blockchain to have temporary splits
  - for instance, if two miners arrive at two different valid solutions for the same block at the same time, unbeknownst to one another.
- The peer-to-peer network is designed to resolve these splits within a short period of time, so that eventually only one branch of the chain survives.
- The client accepts the longest chain of blocks as valid.
  - The "length" of the entire block chain refers to the chain with the most combined difficulty, not the one with the most blocks.
  - This prevents someone from forking the chain and creating a large number of low- difficulty blocks, and having it accepted by the network as "longest".

Blockchain branches



Blockchain 2.0

- The Blockchain 2.0 is an evolution of the blockchain protocol enabling not only to exchange transaction but rather code and programs in the form of Smart Contracts

Blockchain 2.0

- The Blockchain 2.0 is an evolution of the blockchain protocol enabling not only to exchange transaction but rather code and programs in the form of Smart Contracts
  - Now developers are allowed to build programs and API's on the Blockchain Protocol.

Blockchain 2.0

- The Blockchain 2.0 is an evolution of the blockchain protocol enabling not only to exchange transaction but rather code and programs in the form of Smart Contracts
  - Now developers are allowed to build programs and API's on the Blockchain Protocol.
  - This relatively new concept involves the development of programs that can be entrusted with money.

Blockchain 2.0

- The Blockchain 2.0 is an evolution of the blockchain protocol enabling not only to exchange transaction but rather code and programs in the form of Smart Contracts
  - Now developers are allowed to build programs and API's on the Blockchain Protocol.
  - This relatively new concept involves the development of programs that can be entrusted with money.
  - Smart contracts are programs that encode certain conditions and outcomes.

Blockchain 2.0 (2)

- By developing ready to use programs that function on predetermined conditions between the supplier and the client, smart programs ensure a secure escrow service in real time at near zero marginal cost

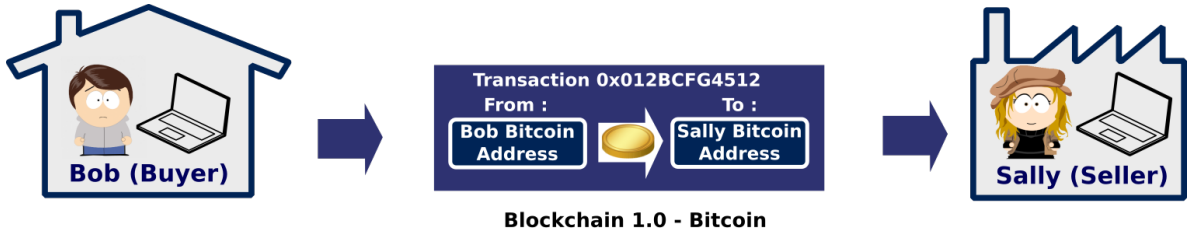
Blockchain 2.0 (2)

- By developing ready to use programs that function on predetermined conditions between the supplier and the client, smart programs ensure a secure escrow service in real time at near zero marginal cost
- Apart from Financial transactions, smart contracts makes the blockchain technology entering a whole lot of different industry.

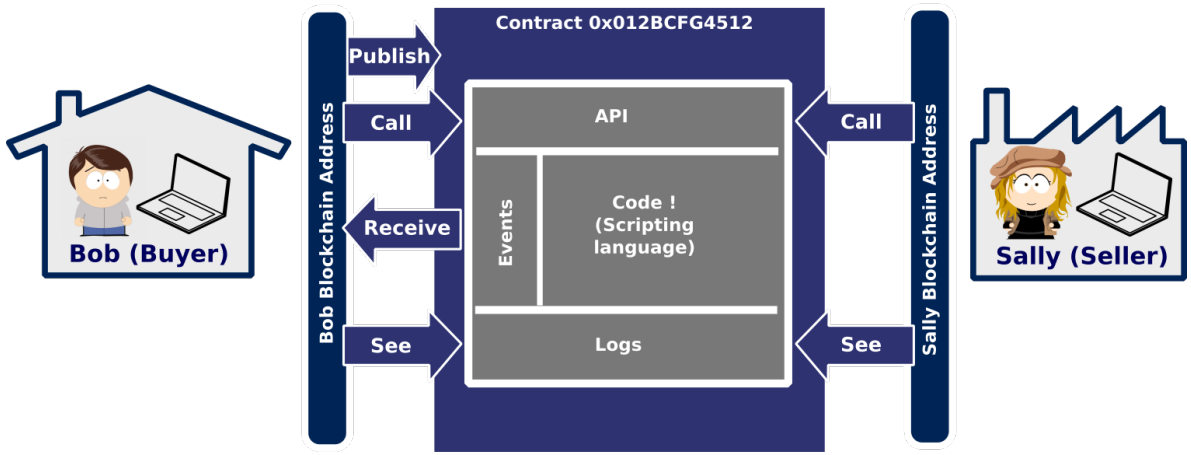
Blockchain 2.0 (2)

- By developing ready to use programs that function on predetermined conditions between the supplier and the client, smart programs ensure a secure escrow service in real time at near zero marginal cost
- Apart from Financial transactions, smart contracts makes the blockchain technology entering a whole lot of different industry.
  - For instance in the Legal System, companies like Empowered Law use the public distributed ledger of transactions that makes up the Block Chain to provide Multi- Signature account services for asset protection, estate planning, dispute resolution, leasing and corporate governance.

Smart Contract



Blockchain 1.0 - Bitcoin



Blockchain 2.0 - e.g. Ethereum, ...

Advances in blockchain

Advanced definition: The blockchain is a distributed database using state machine replication, with atomic changes to the database (transactions) grouped into blocks, with the integrity and tamper-resistance of the transaction log assured via hash links among blocks.

Advances in blockchain

Advanced definition: The blockchain is a distributed database using state machine replication, with atomic changes to the database (transactions) grouped into blocks, with the integrity and tamper-resistance of the transaction log assured via hash links among blocks.

Blockchain is usually understood to be decentralized, i.e., jointly maintained by a plurality of independent parties (maintainers), with the security assumptions postulating that a certain fraction of these parties may be non-responsive or compromised at any moment during blockchain operation

Blockchain key points

- **Linked timestamping:** blockchain by design makes it possible to provide a universally verifiable proof of existence or absence of certain data or a state transition in the blockchain database. These proofs would be computationally unforgeable by third parties (i.e., anyone but a collusion of a supermajority of the blockchain maintainers), provided that underlying cryptographic primitives (hash functions and signature schemes) are computationally secure.

Blockchain key points

- **Linked timestamping:** blockchain by design makes it possible to provide a universally verifiable proof of existence or absence of certain data or a state transition in the blockchain database. These proofs would be computationally unforgeable by third parties (i.e., anyone but a collusion of a supermajority of the blockchain maintainers), provided that underlying cryptographic primitives (hash functions and signature schemes) are computationally secure.
- Blockchain uses a **consensus algorithm**, which guarantees that non-compromised database copies have the same views as to the database state. In other words, consensus ensures that transactions in the log are eventually propagated to all non-compromised nodes and lead to the identical changes.

Blockchain key points

- **Linked timestamping:** blockchain by design makes it possible to provide a universally verifiable proof of existence or absence of certain data or a state transition in the blockchain database. These proofs would be computationally unforgeable by third parties (i.e., anyone but a collusion of a supermajority of the blockchain maintainers), provided that underlying cryptographic primitives (hash functions and signature schemes) are computationally secure.
- Blockchain uses a **consensus algorithm**, which guarantees that non-compromised database copies have the same views as to the database state. In other words, consensus ensures that transactions in the log are eventually propagated to all non-compromised nodes and lead to the identical changes.
- Applied cryptography routines (e.g., public-key digital signatures) are used to **decentralize authentication and authorization** of transactions taking place within the network. That is, transactions are created externally to the blockchain nodes, which limits the repercussions of a node compromise.

Blockchain users

- **Maintainers** of the blockchain infrastructure, who decide business logic on the blockchain. The maintainers store full replica of the entire blockchain data, thus have full read access to it and decide on the rules of transaction processing, and are active participants of the consensus algorithm on the blockchain.

Blockchain users

- **Maintainers** of the blockchain infrastructure, who decide business logic on the blockchain. The maintainers store full replica of the entire blockchain data, thus have full read access to it and decide on the rules of transaction processing, and are active participants of the consensus algorithm on the blockchain.
- External **auditors** of the blockchain operation (e.g., regulators, non-government organizations, law enforcement), who verify the correctness of the whole transaction processing in real time and/or retrospectively. Auditors assumed to store replica of the entire blockchain data (or at least a logically complete portion of it) and read access to it to be able to perform complete audits.

Blockchain users

- **Maintainers** of the blockchain infrastructure, who decide business logic on the blockchain. The maintainers store full replica of the entire blockchain data, thus have full read access to it and decide on the rules of transaction processing, and are active participants of the consensus algorithm on the blockchain.
- External **auditors** of the blockchain operation (e.g., regulators, non-government organizations, law enforcement), who verify the correctness of the whole transaction processing in real time and/or retrospectively. Auditors assumed to store replica of the entire blockchain data (or at least a logically complete portion of it) and read access to it to be able to perform complete audits.
- **Clients** who are the end users of the services provided by maintainers. Each client may have access to a relatively small portion of blockchain data, but her software may utilize cryptographic proofs to verify (with reasonable accuracy) the authenticity of the blockchain data provided by maintainers

Blockchain types (by Bitfury)

- In **public permissionless** blockchains, all blockchain data is public. Furthermore, the consensus algorithm is censorship-resistant (e.g., proof of work used in Bitcoin), which ensures that maintainers are free to enter and leave the system; i.e., write access to the blockchain is public, too.

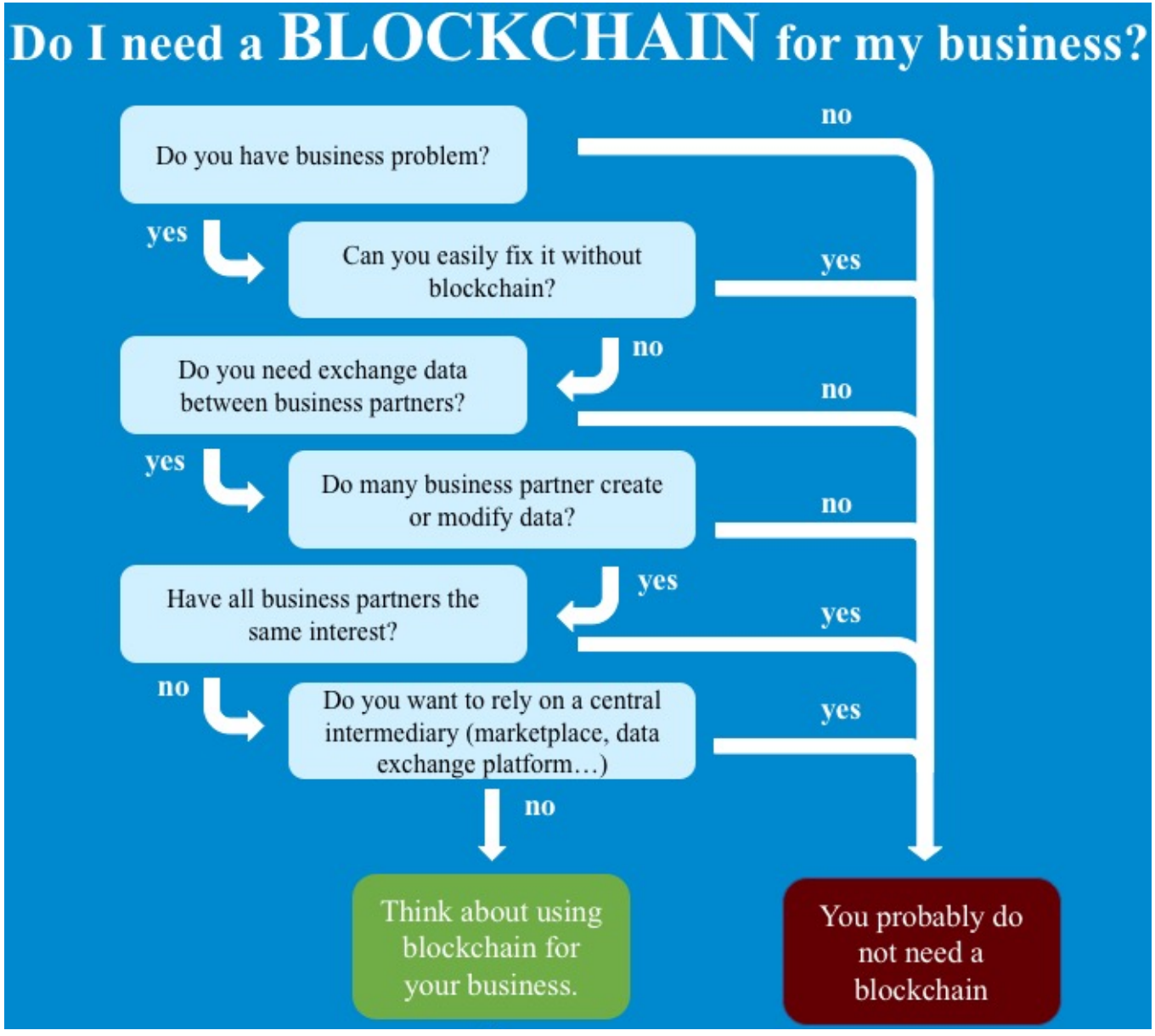
Blockchain types (by Bitfury)

- In **public permissionless** blockchains, all blockchain data is public. Furthermore, the consensus algorithm is censorship-resistant (e.g., proof of work used in Bitcoin), which ensures that maintainers are free to enter and leave the system; i.e., write access to the blockchain is public, too.
- **Private** blockchains have a well-defined and restricted list of entities having read and write access to the blockchain (e.g., a group of banks, the regulator and law enforcement in a hypothetical banking blockchain).

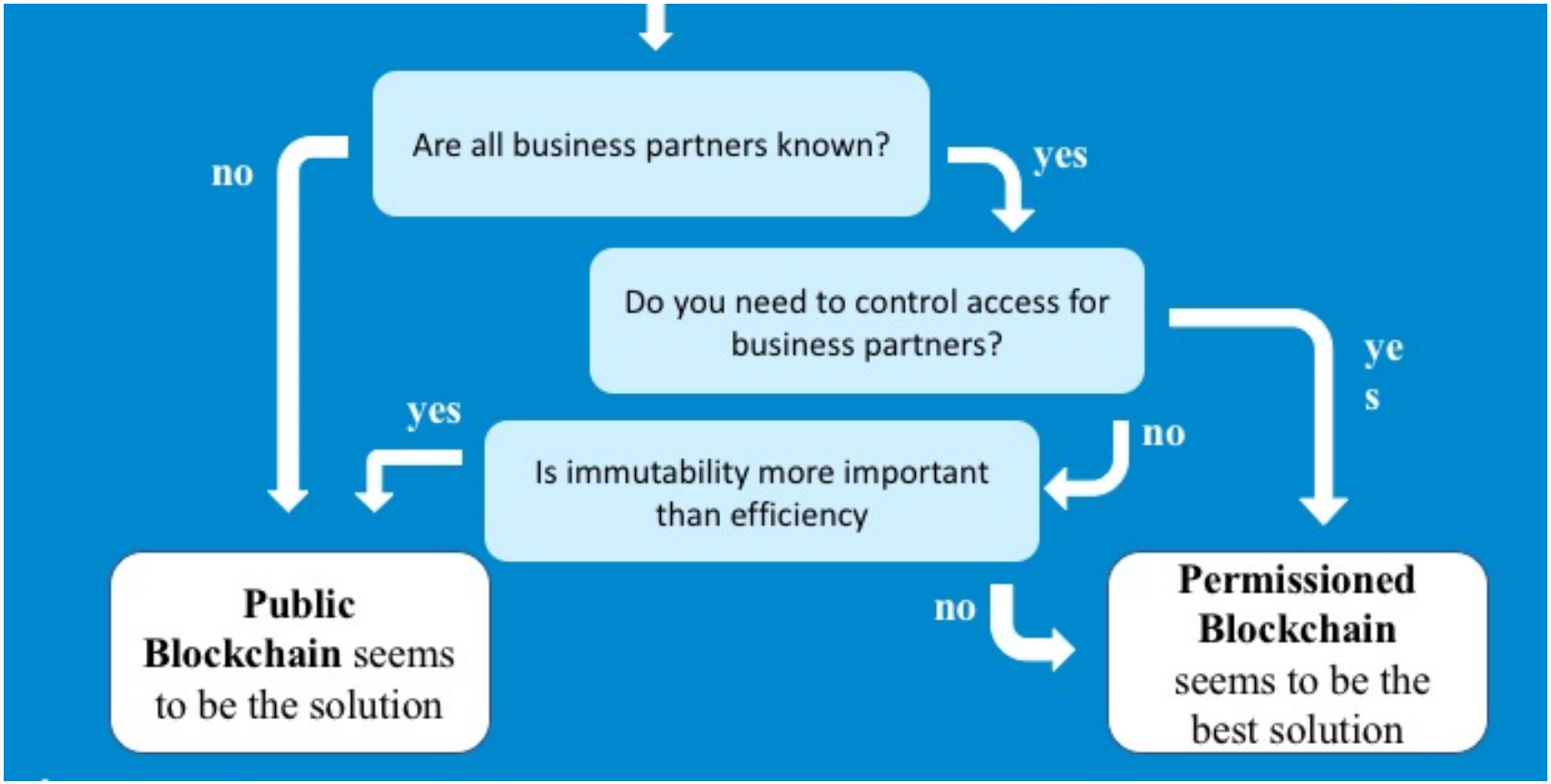
Blockchain types (by Bitfury)

- In **public permissionless** blockchains, all blockchain data is public. Furthermore, the consensus algorithm is censorship-resistant (e.g., proof of work used in Bitcoin), which ensures that maintainers are free to enter and leave the system; i.e., write access to the blockchain is public, too.
- **Private** blockchains have a well-defined and restricted list of entities having read and write access to the blockchain (e.g., a group of banks, the regulator and law enforcement in a hypothetical banking blockchain).
- **Public permissioned** blockchains restrict write access to the blockchain data similarly to private blockchains, but are engineered to be universally auditable and thus oriented for wide read access by end users.

Does the project need blockchain (by Contractus)?



What kind of blockchain do you need?



Cryptocurrancy

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$42,420,200,186	$2581.69	16,431,175 BTC	$896,716,000	1.05%	
2	Ethereum	$25,586,441,675	$274.91	93,071,389 ETH	$816,457,000	3.74%	
3	Ripple	$9,754,348,126	$0.254740	38,291,387,790 XRP *	$55,301,700	-0.53%	
4	Litecoin	$2,599,298,962	$50.12	51,866,582 LTC	$534,796,000	-4.58%	
5	Ethereum Classic	$1,673,064,710	$17.93	93,286,462 ETC	$74,895,000	2.23%	
6	NEM	$1,536,813,000	$0.170757	8,999,999,999 XEM *	$3,627,450	-2.62%	

***

540	OctoCoin	$124,030	$0.002513	49,358,142 888	Low Vol	33.38%	
541	Bitcloud	$118,214	$0.010547	11,207,895 BTD	Low Vol	64.08%	
542	Tattoocoin (S...	$113,509	$0.001258	90,245,635 TSE *	Low Vol	-16.04%	
543	UniCoin	$112,529	$0.038408	2,929,838 UNIC	Low Vol	24.17%	
544	Guncoin	$109,437	$0.000592	184,959,628 GUN	Low Vol	1.01%	

***

Distributed Timestamping

A new way to prove document authenticity — distributed trusted timestamping. Each document will receive a digital fingerprint that will be stored in Exonum Blockchain to enable verification of document existence and integrity at a certain point in time. Notarial and other certificates, prescriptions, coupons are a few of use cases where Exonum platform — protected from forgery and backdating — can be of benefit.

Supply Chain

In the modern reality where different parties use different internal systems to manage their workflow understanding a particular situation at a specific moment in time may become an obstacle. In this case blockchain can act as a single point of truth providing relevant information to all participants. Blockchain framework can manage any business logic to establish a system where all parties are sure they have all relevant information

Digital Rights Management

Big publishing companies are dictating their ways of rights management and leave artists a tiny part of their earnings — just because of numerous intermediaries. Blockchain can help to establish an automatic platform that can ensure all parties are taking the rules into account. By using powerful smart-contract system, you can create a transparent and robust money flow control system.

P2P Lending

Complicated KYC/AML procedures, aggressive risk scoring makes p2p lending a “high risk — high gain” area to invest money in. Blockchain can affect value chain in a very positive way, providing unprecedented level of transparency and thus making the investments and borrowings protected by the technology. It allows performing audit on a real-time basis.

E-Voting

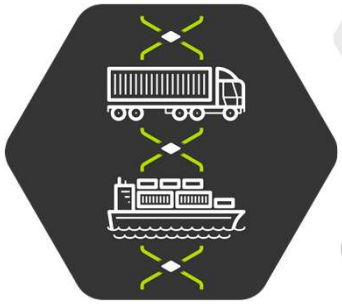
Existing e-voting solutions are not able to work without central authority and guarantee vote secrecy. Blockchain is a natural way to solve these problems and guarantee voting process integrity to all participants. Blockchain's modular architecture allows easy integration of specific cryptography tools to provide the highest level of transparency while also keeping sensitive data secure.

Government Registry

Your Blockchain can be used to create an entirely new process for citizen-government interactions. It can keep records safe while also offering a citizen true control of his or her assets.

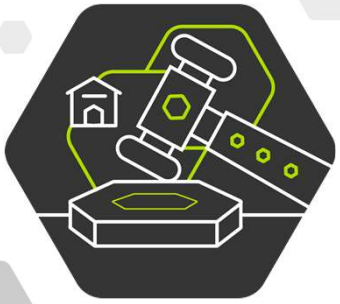
Peer-to-peer cloud storage

A peer-to-peer cloud storage network implementing client-side encryption would allow users to transfer and share data without reliance on a third party storage provider. The removal of central controls would mitigate most traditional data failures and outages, as well as significantly increase security, privacy, and data control.



Supply Chain

Government Registry



E-auction

Digital Rights Management

And many others

Registry of Workers' Contracts

Coca Cola

- Protection of workers' rights
- Increase transparency and efficiency of the verification process related to labor policies within supply chain

Venue 345	Workers	Open
One Factory	345 343	348

Workers

Karl Peterson	Plummer	05.02.2018
Dima Lagoda	Designer	13.02.2017
Alex Kovach	Counter	02.11.2012

DevOps Process

Speeding Product Development

- Multiple companies involved
- Trust and consistent information
- **Up to 50%** increase in development time
- **+33%** developer productivity

Aricent DSCI DIGITAL·SUPPLY·CHAIN·INSTITUTE

Task 345 231	Committee	Status
Commit	John Doe	5/8

Rewievers

Michael Fawler	Accepted	1 min ago
Nicolas Mage	Accepted	5 hours ago
Jennifer Rens	Accepted	Yesterday

Blockchain based Land Titling

NAPR, Republic of Georgia

- Secure
- Transparent
- People-friendly
- Enables smart contract economy

Object 345 231	Price
House	$25 000 000

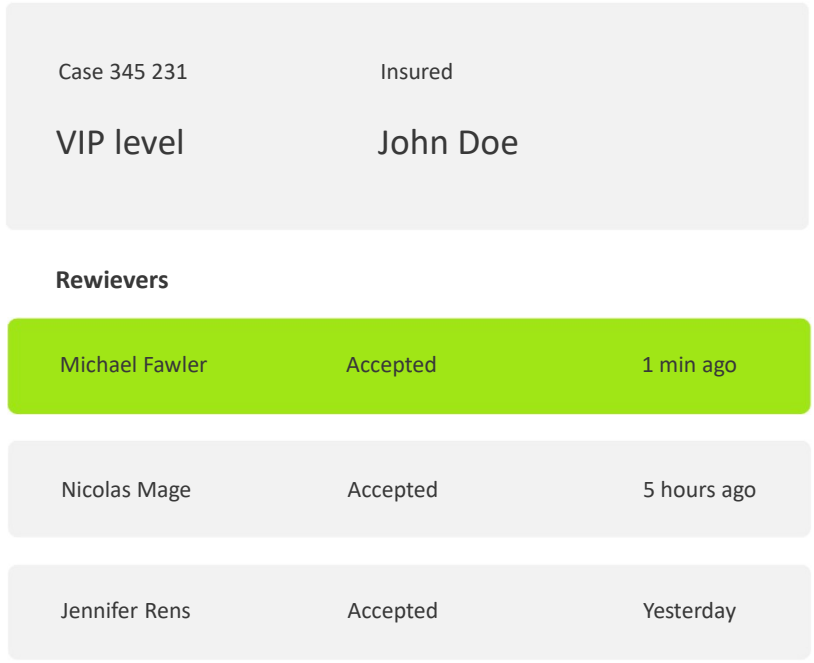
Owners

John Doe	$24M	May 5, 2018
George Goe	$23M	March 16, 1986
King David IV	$22M	August 11, 1098

Insurance on blockchain

Risk Cooperative, USA

- Trust between participants
- Savings on audit
- Quick decision making



Auction on blockchain

SETAM (OpenMarket), Ukraine

- Enhance the trust
- Growth of the number of potential partners and users
- Secure & auditable bids

OpenMarket

Lot 345 231	Next Price	Time Left
Boeing B 737/524	$1,5M	0:06.233
John Doe	$1,4M	17:59:06.4353
Sam Peterson	$1,3M	17:56:06.3543
Peter Samson	$1,2M	14:25:06.8697

Pre-qualification selection

Samruk-Kazyna, Kazakhstan

- Automated regular purchases
- Same documents for each auction
- Third-party audit of the process

Documents

Purchase	Verified	May 5, 2018
Invoice	Verified	May 4, 2018
Agreement	Verified	May 3, 2018
Registration	Verified	May 2, 2018

Equity Participation Agreements

Rosreestr, Russia

- Elimination of the problem of poor-quality entry of the data, loss or improper correction of data
- Transparent way to track the current status of each application for organizations, developers and buyers

РОСРЕЕСТР
Федеральная служба государственной регистрации, кадастра и картографии

Requests

Public Fund	Processing	
Organization	Verified	May 4, 2018
Purchase	Verified	May 3, 2018
Development	Completed	May 2, 2018

Lectures plan

The order and content may change!

Lectures plan

The order and content may change!

1. Blockchain introduction.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.
6. Proof-of-Work and public key cryptography practice.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.
6. Proof-of-Work and public key cryptography practice.
7. Bitcoin and lightning.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.
6. Proof-of-Work and public key cryptography practice.
7. Bitcoin and lightning.
8. Introduction into distributed databases.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.
6. Proof-of-Work and public key cryptography practice.
7. Bitcoin and lightning.
8. Introduction into distributed databases.
9. Ethereum and smart contracts. Initial coin offering.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.
6. Proof-of-Work and public key cryptography practice.
7. Bitcoin and lightning.
8. Introduction into distributed databases.
9. Ethereum and smart contracts. Initial coin offering.
10. Proof-of-work alternatives. Consensus problem and why Byzantine generals.

Lectures plan

The order and content may change!

1. Blockchain introduction.
2. Introduction into cryptography. Hash functions.
3. Public key cryptography (1).
4. Public key cryptography (2).
5. Threshold and secret sharing cryptography. Zero knowledge proofs.
6. Proof-of-Work and public key cryptography practice.
7. Bitcoin and lightning.
8. Introduction into distributed databases.
9. Ethereum and smart contracts. Initial coin offering.
10. Proof-of-work alternatives. Consensus problem and why Byzantine generals.
11. Blockchain platforms overview and practice: Ethereum, Fabric, Exonum.

Marks

There will be two home assignments (15% for each one in final grade) as well as final exam (35% of final grade) and final project (35% of final grade). The grading policy is the following:
>80% – A
>70% – B
>60% – C
>50% – D
>40% – E
<=40% – F

Thank you for your attention!