A technical introduction to Blockchain technology

Gerard Bosch (gerard.bosch@gmail.com)

September 27, 2018

(Last build: October 5, 2021)

Outline

1. Preliminary concepts
2. How does it work?
3. Blockchain by generations
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
7. Some conclusions

Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

Ledger

The foundation of accounting, are as ancient as writing and money (Mesopotamia $<$ 5000 B.C.).

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

Cryptographic

The procedures and protocols to append new data to the ledger implies the use of cryptographic techniques.

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

Distributed

Not a single entity is the owner of the data, but it is replicated in every participant of the network.

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

Bitcoin

was the first and most popular *peer-to-peer* **value** exchange network.

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

Satoshi Nakamoto

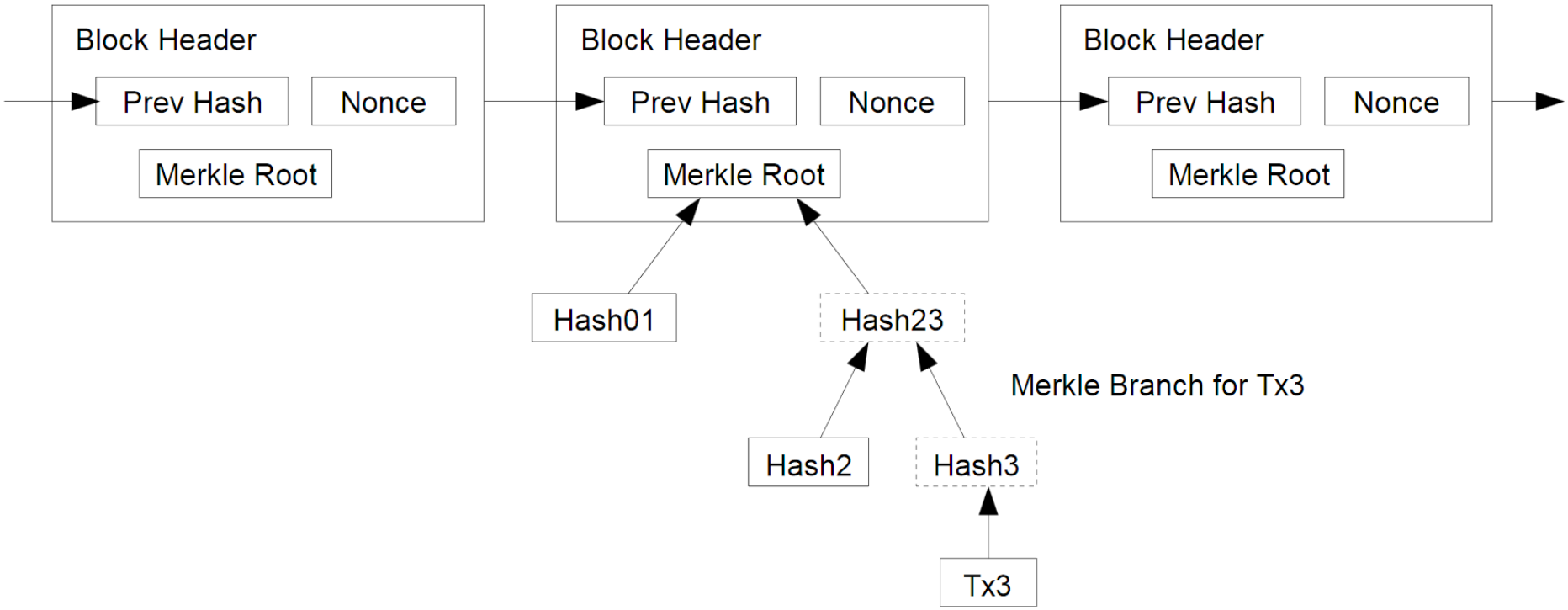
is a pseudonym of an anonymous individual or group that developed the idea of Blockchain and Bitcoin.

What is a Blockchain?

Now we know, but. . . how does it look like?

What is a Blockchain?

Now we know, but. . . how does it look like?



What is a Blockchain?

Cool! But why?

What is a Blockchain?

Cool! But why?

- Suppress the necessity of trusted third-party (i.e. financial institutions and banks).
- Move trust from central authorities to decentralized secure protocol.
- Create an economical system not driven by central institutions.
- Empower people.
- Enable almost immediate transactions.
- Offer lower fees than traditional banking.
- Let people become their own bank.

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of asymmetric cryptography the integrity of the data is guaranteed.

Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of asymmetric cryptography the integrity of the data is guaranteed.

Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of asymmetric cryptography the integrity of the data is guaranteed.

Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of asymmetric cryptography the integrity of the data is guaranteed.

Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of asymmetric cryptography the integrity of the data is guaranteed.

Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of asymmetric cryptography the integrity of the data is guaranteed.

Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

A bit more background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based in some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that provides at least 2 out of the 3 properties of CIA triad: integrity and availability.

> *" We can see it as an Internet-native way to store and exchange value "*

Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

How does it work?

"It is all about consensus"

How does it work?

"It is all about consensus"

- Blockchain concept is in continuous evolution and new protocols are continuously created to improve the current flaws.
- Earliest implementations (which includes Bitcoin and Ethereum) are using a system called *Proof of Work* (PoW) to validate the transactions.
- Validation is required in order to **append** a new block of transactions to the chain; preventing things such as double spend.
- The process of block validation is known as mining.
- Lately a new system called *Proof of Stake* (PoS) was developed to address PoW flaws.

How does it work?

"It is all about consensus"

- Blockchain concept is in continuous evolution and new protocols are continuously created to improve the current flaws.
- Earliest implementations (which includes Bitcoin and Ethereum) are using a system called *Proof of Work* (PoW) to validate the transactions.
- Validation is required in order to **append** a new block of transactions to the chain; preventing things such as double spend.
- The process of block validation is known as mining.
- Lately a new system called *Proof of Stake* (PoS) was developed to address PoW flaws.

How does it work?

"It is all about consensus"

- Blockchain concept is in continuous evolution and new protocols are continuously created to improve the current flaws.
- Earliest implementations (which includes Bitcoin and Ethereum) are using a system called *Proof of Work* (PoW) to validate the transactions.
- Validation is required in order to **append** a new block of transactions to the chain; preventing things such as double spend.
- The process of block validation is known as mining.
- Lately a new system called *Proof of Stake* (PoS) was developed to address PoW flaws.

How does it work?

"It is all about consensus"

- Blockchain concept is in continuous evolution and new protocols are continuously created to improve the current flaws.
- Earliest implementations (which includes Bitcoin and Ethereum) are using a system called *Proof of Work* (PoW) to validate the transactions.
- Validation is required in order to **append** a new block of transactions to the chain; preventing things such as double spend.
- The process of block validation is known as mining.
- Lately a new system called *Proof of Stake* (PoS) was developed to address PoW flaws.

How does it work?

"It is all about consensus"

- Blockchain concept is in continuous evolution and new protocols are continuously created to improve the current flaws.
- Earliest implementations (which includes Bitcoin and Ethereum) are using a system called *Proof of Work* (PoW) to validate the transactions.
- Validation is required in order to **append** a new block of transactions to the chain; preventing things such as double spend.
- The process of block validation is known as mining.
- Lately a new system called *Proof of Stake* (PoS) was developed to address PoW flaws.

How does it work?

"It is all about consensus"

- Nodes are motivated to maintain the network with a reward coming from transaction fees.
- Hence, consensus is achieved though these systems (PoW/PoS).

How does it work?

"It is all about consensus"

- Nodes are motivated to maintain the network with a reward coming from transaction fees.
- Hence, consensus is achieved though these systems (PoW/PoS).

Transaction work-flow

1. Clients **create** and sign transactions (TX) using their private key, then they broadcast TX to the network.
2. Network nodes (miners) receive transactions and store them in the so called mempool.
3. Miners prioritize transactions based on fees, validate and put them in a block.
4. Once successfully created and verified by the network, the block is finally appended to the chain.

But how does it work under the hood?

Proof of Work: The Bitcoin case

Block creation (mining)

Participants of a Blockchain network put computational resources to validate transactions by solving the so called cryptographic puzzles.

Proof of Work: The Bitcoin case

Block creation (mining)

Participants of a Blockchain network put computational resources to validate transactions by solving the so called cryptographic puzzles.

- Block creation consists in finding a nonce (number) for the block that satisfies a property of the block's hash (a number of leading zeros) known as difficulty.
- This is a trial and error procedure (a kind of brute-force).
- The first node that finds a successful solution announces it to the network.
- The rest of the nodes can easily verify that the solution (and hence the block) is valid.
- If a node acts dishonestly, the rest of nodes will discard the block.

Proof of Work: The Bitcoin case

Drawbacks

- Huge energy consumption.
- Susceptible to a 51% attack.
- Democratization of the network (hardware, electricity price,...)

Proof of Stake

Given the aforementioned problems that PoW presents, the new Proof of Stake (PoS) model was developed.

Block creation (forging)

Participants of the network stake an amount of currency they hold (a kind of deposit) to be able to forge and send a block to the network.

Proof of Stake

Given the aforementioned problems that PoW presents, the new Proof of Stake (PoS) model was developed.

Block creation (forging)

Participants of the network stake an amount of currency they hold (a kind of deposit) to be able to forge and send a block to the network.

- The next block creator (called forger) will be chosen randomly following certain criteria.
- The forger verifies transactions, forges a new block and sends it to the network.
- As in PoW, new block is added to the chain and forger receives transaction fees (and its stake back).
- If the forger acts dishonestly, the rest of nodes will discard the block and forger will lose the stake.

Proof of Stake

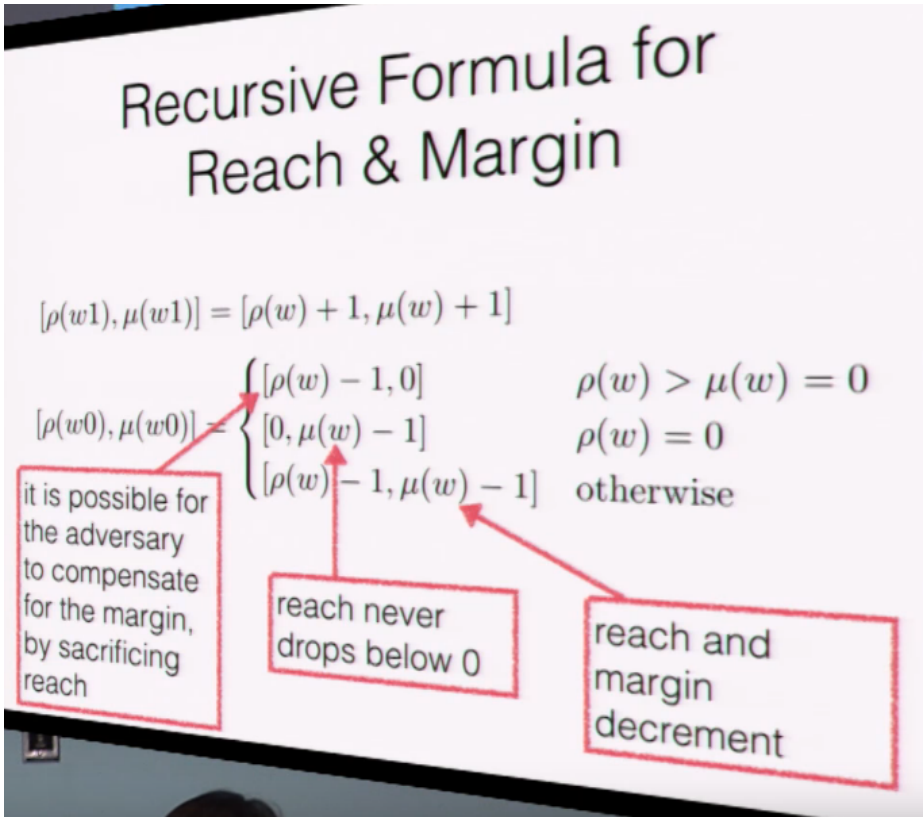
Pros

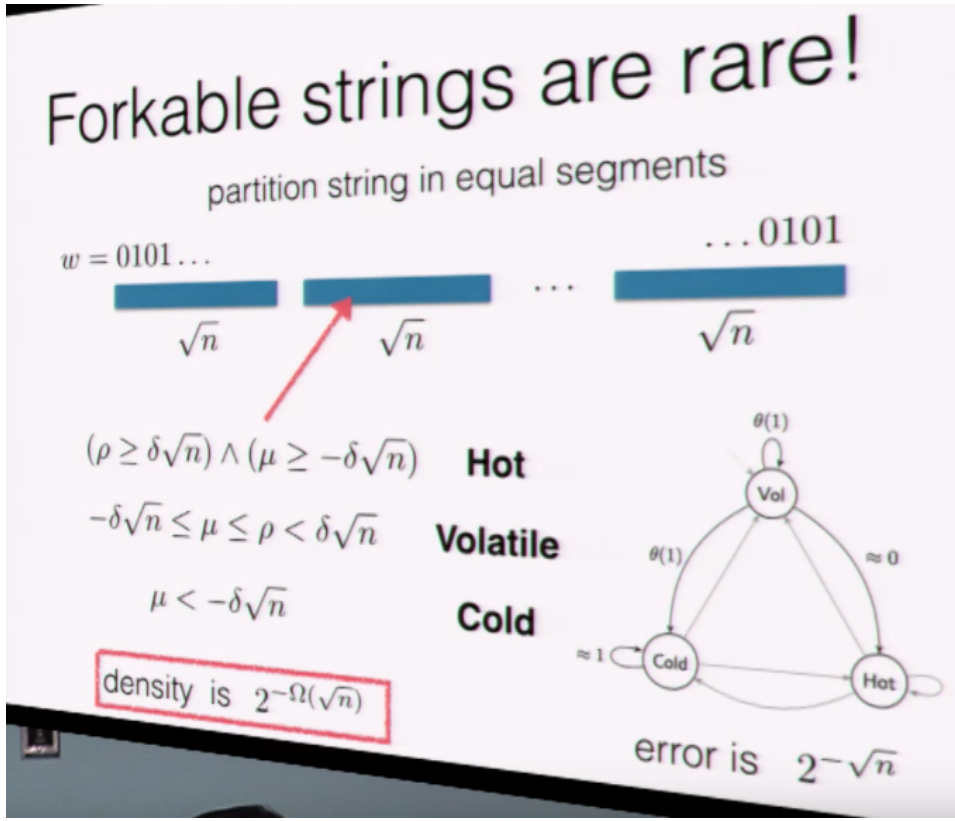
- A way more energy efficient: there are no computational resources required.
- More democratization and hence decentralization.
- Security: Purchasing more than half of the coins is likely more costly than acquiring 51% of PoW hashing power.

Several proposals have been presented, studied and even implemented but PoS still faces some challenges that must be addressed.

Proof of Stake

" Not so trivial "





Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

Definition

Turing Completeness

A programming language is said to be Turing Complete (TC) if can be used to simulate a Turing Machine and hence to solve any mathematical/ computational problem.

A TC-language has some important properties:

- conditional branching;
- infinite **looping** ability;
- [...]

First Generation: Bitcoin

Bitcoin was the first implementation of the Blockchain and is considered the first generation of Blockchain.

- Bitcoin has a programming language called **Script** used to "encode" the transactions, and to control how the payee of a TX can access the funds.
- But, Script is not a **TC-language** (has no loops)...
- ...so Bitcoin can be merely used as a store of value and exchange of value network.

For its nature, it is usually called digital gold.

Current implementation presents scalability issues ($\approx$ 7 TPS)

First Generation: Bitcoin

Bitcoin was the first implementation of the Blockchain and is considered the first generation of Blockchain.

- Bitcoin has a programming language called **Script** used to "encode" the transactions, and to control how the payee of a TX can access the funds.
- But, Script is not a **TC-language** (has no loops)...
- ...so Bitcoin can be merely used as a store of value and exchange of value network.

For its nature, it is usually called digital gold.

Current implementation presents scalability issues ($\approx$ 7 TPS)

First Generation: Bitcoin

Bitcoin was the first implementation of the Blockchain and is considered the first generation of Blockchain.

- Bitcoin has a programming language called **Script** used to "encode" the transactions, and to control how the payee of a TX can access the funds.
- But, Script is not a **TC-language** (has no loops)...
- ...so Bitcoin can be merely used as a store of value and exchange of value network.

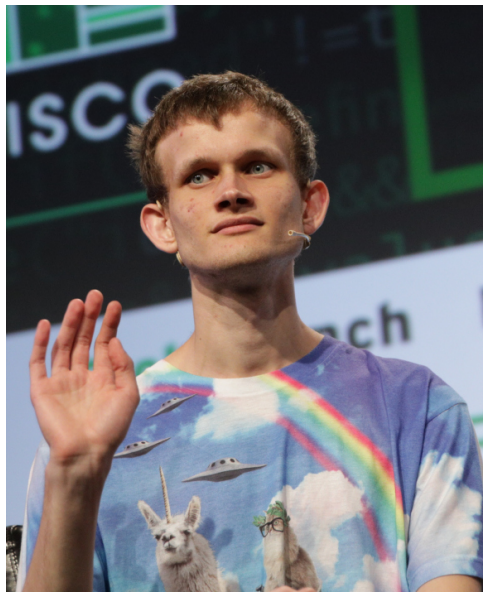
For its nature, it is usually called digital gold.

Current implementation presents scalability issues ($\approx$ 7 TPS)

Second Generation: Ethereum

Ethereum, which is considered a second generation Blockchain, was released in 2015 after two years of research and development.

- Co-founded by Vitalik Buterin, a young cryptocurrency researcher/programmer.
- Features a **TC-complete** programming language called **Solidity** (and experimental Vyper).
- An abstraction of the 1st gen. that allows not only exchange "money" but the execution of any program.
- These programs are called Smart Contracts.
- Users pay fees for contract (program) execution.



Vitalik Buterin

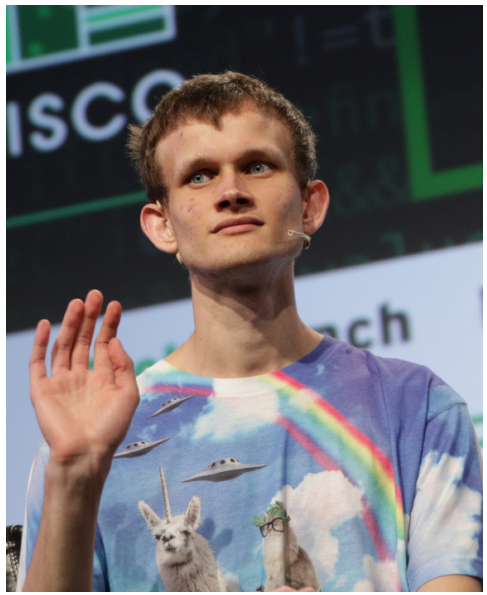
Ethereum is in essence a decentralized application network

Current implementation presents scalability issues ($\approx$ 15 TPS)

Second Generation: Ethereum

Ethereum, which is considered a second generation Blockchain, was released in 2015 after two years of research and development.

- Co-founded by Vitalik Buterin, a young cryptocurrency researcher/programmer.
- Features a **TC-complete** programming language called **Solidity** (and experimental Vyper).
- An abstraction of the 1st gen. that allows not only exchange "money" but the execution of any program.
- These programs are called Smart Contracts.
- Users pay fees for contract (program) execution.



Vitalik Buterin

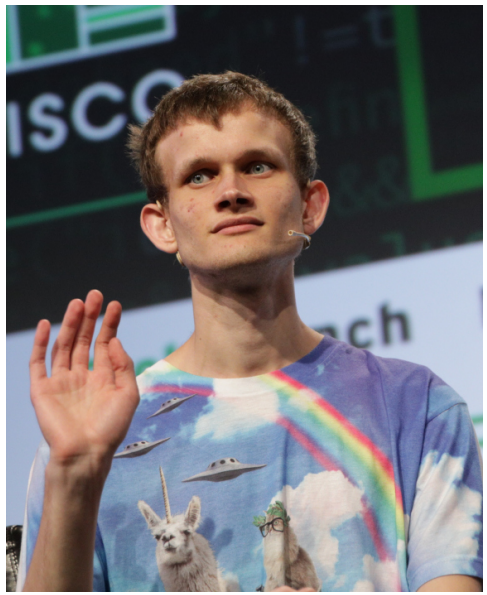
Ethereum is in essence a decentralized application network

Current implementation presents scalability issues ($\approx$ 15 TPS)

Second Generation: Ethereum

Ethereum, which is considered a second generation Blockchain, was released in 2015 after two years of research and development.

- Co-founded by Vitalik Buterin, a young cryptocurrency researcher/programmer.
- Features a **TC-complete** programming language called **Solidity** (and experimental Vyper).
- An abstraction of the 1st gen. that allows not only exchange "money" but the execution of any program.
- These programs are called Smart Contracts.
- Users pay fees for contract (program) execution.



Vitalik Buterin

Ethereum is in essence a decentralized application network

Current implementation presents scalability issues ($\approx$ 15 TPS)

Smart Contracts

> *"A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises."*
>
> *Nick Szabo, 1996*

Example: ICO

When participating in an Initial Coin Offer (ICO) a user sends funds (an investment) to a Smart Contract.

The contract encodes the rules of the agreement: usually a number of tokens proportional to the investment will be sent back to the user (which represents his investment in the project).

No third party is involved.

Smart Contracts

> *"A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises."*
>
> *Nick Szabo, 1996*

Example: ICO

When participating in an Initial Coin Offer (ICO) a user sends funds (an investment) to a Smart Contract.

The contract encodes the rules of the agreement: usually a number of tokens proportional to the investment will be sent back to the user (which represents his investment in the project).

No third party is involved.

Third Generation

The 3rd generation of Blockchain is mainly focused to address two of the main issues of the 2nd generation:

- Scalability
- Security

Scalability

A 3rd generation of Blockchain should be able to scale to several thousands of TPS.

Network usage (bandwidth) and data storage should scale efficiently.

Security

Smart contracts should be able to be verified using Formal Verification.

Third Generation

The 3rd generation of Blockchain is mainly focused to address two of the main issues of the 2nd generation:

- Scalability
- Security

Scalability

A 3rd generation of Blockchain should be able to scale to several thousands of TPS.

Network usage (bandwidth) and data storage should scale efficiently.

Security

Smart contracts should be able to be verified using Formal Verification.

Third Generation

The 3rd generation of Blockchain is mainly focused to address two of the main issues of the 2nd generation:

- Scalability
- Security

Scalability

A 3rd generation of Blockchain should be able to scale to several thousands of TPS.

Network usage (bandwidth) and data storage should scale efficiently.

Security

Smart contracts should be able to be verified using Formal Verification.

Third Generation

The 3rd generation of Blockchain is mainly focused to address two of the main issues of the 2nd generation:

Cardano

is a 3rd generation Blockchain focused to address limitations of 2nd generation Blockchains.

Charles Hoskinson,
co-founder of Cardano
and former co-founder of Ethereum

Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

Cardano

- Born in 2015 as an effort to change the way cryptocurrencies are designed and developed.
- Developed together by IOHK company and several universities.
- Scientific research model and peer review.
- The Blockchain for ADA cryptocurrency.
- Considered a 3rd generation Blockchain.
- Different approach: How to scale instead of how many TPS.
- Current development roadmap planned at least until 2020.
- ADA was launched to trade in October 2017.

Cardano

Key features

- Proof of Stake (Ouroboros consensus algorithm)
- Sustainable ecosystem
- Strongly focused on scalability
- Interoperability with other Blockchains
- Smart contracts
- Treasury
- Based on epochs and quorums
- Parallelize transactions amongst quorums will allow to scale
- Reduces network pressure by using RINA

Cardano

Aims to solve 3 main problems of current cryptocurrencies:

- Scalability
- Interoperability
- Sustainability

Cardano

Aims to solve 3 main problems of current cryptocurrencies:

- Scalability
- Interoperability
- Sustainability

Scalability

PoS and parallelization of epochs	$\longrightarrow$	Δ TPS (Transactions per second)
Split network in subnets (RINA)	$\longrightarrow$	∇ Bandwidth
Pruning, compression, partitioning	$\longrightarrow$	∇ Storage

Cardano

Aims to solve 3 main problems of current cryptocurrencies:

- Scalability
- Interoperability
- Sustainability

Interoperability

Allow different cryptocurrencies to talk each other.

Allows metadata into TX $\longrightarrow$ Better integration with banks/governments.

Cardano

Aims to solve 3 main problems of current cryptocurrencies:

- Scalability
- Interoperability
- Sustainability

Sustainability (Treasury)

The treasury is a special wallet not controlled by anyone that receives a small percentage of every transaction.

It promotes continuous improvement of the system by funding the most voted improvement proposals.

It will keep Cardano sustainable.

Powered by smart contracts.

Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

What is a cryptocurrency?

What is a cryptocurrency?

Cryptocurrency

A **digital asset** (or currency) that relies on cryptography to work and runs over a decentralized network, typically backed by a Blockchain.

Crypto in crypto-currency does **not** mean that all information in the Blockchain is encrypted and secret...

- Bitcoin Blockchain is not confidential at all as transaction details are public.
- ...But can be challenging to trace and relate transactions.

What is a cryptocurrency?

Cryptocurrency

A **digital asset** (or currency) that relies on cryptography to work and runs over a decentralized network, typically backed by a Blockchain.

Crypto comes from the use of cryptographic techniques used by the protocol such as:

- Public-key (asymmetrical) cryptography
- Cryptographic hashes (e.g. SHA-256 Bitcoin)
- . . . *(probably more)*

What is a cryptocurrency wallet?

What is a cryptocurrency wallet?

What is not a wallet...

A software or physical device where your coins are **stored inside**.

What is a wallet indeed...

The term wallet can refer to 2 things:

A. a software that allows to interact with a Blockchain (a light client);

B. a store for your addresses and its private keys;

where usually $A \supset B$.

What is a cryptocurrency wallet?

What is not a wallet...

A software or physical device where your coins are **stored inside**.

What is a wallet indeed...

The term wallet can refer to 2 things:

A. a software that allows to interact with a Blockchain (a light client);

B. a store for your addresses and its private keys;

where usually $A \supset B$.

Type of wallets

Some different kind of wallets exist:

By type

Type	Example
Software wallets	Electrum
Hardware wallets	Ledger
Paper wallets	walletgenerator.net
Brain wallets	keybase.io/warp

By storage mode

- Hot storage
- Cold storage

Hierarchical Deterministic Wallets (HD)

- Introduced by BIP32 (2012), provides a way to generate several addresses from a single master key using key-derivation-functions.
- The whole wallet is generated from a seed (12 words) and is the only thing the user needs to back up.

Type of wallets

Some different kind of wallets exist:

By type

Type	Example
Software wallets	Electrum
Hardware wallets	Ledger
Paper wallets	walletgenerator.net
Brain wallets	keybase.io/warp

By storage mode

- Hot storage
- Cold storage

Hierarchical Deterministic Wallets (HD)

- Introduced by BIP32 (2012), provides a way to generate several addresses from a single master key using key-derivation-functions.
- The whole wallet is generated from a seed (12 words) and is the only thing the user needs to back up.

Key notes

- Address **reuse** is discouraged as compromises privacy and security $\Rightarrow$ HD wallets allow zero-address reuse.
- The user does not need to trust anyone but himself to safely store his funds.
- But the lost of the key/seed results in the inability to access the funds (unlike traditional banking).

Bitkey

Bitkey is a Linux live distribution that includes a set of tools and wallets for some of the most popular cryptocurrencies.

It can run in 2 modes:

- Hot online: Interact with the Blockchain from a secure environment.
- Cold offline: This is the most secure way of operating as it starts as an air-gapped system where private key is never exposed.

As a side project has not received updates in a while, but a recent fork provided by @estevaocm on GitHub includes many interesting tools such as:

- QR-code scanning through webcam :) – A very convenient way to import and export TX and addresses.
- Support for several other cryptocurrency wallets other than Bitcoin (Ethereum, Litecoin,...) —more are being constantly added.

Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

The future will be decentralized

Since its creation, Internet has been **mostly** centralized[1], which implies that it is:

- Easy to watch/monitor
- Easy to censor
- Easy to attack
- Fragile to failure

During the years more distributed and P2P protocols has been deployed, although client-server model is the most common yet.

[1] ARPANET hosts file is a great example.

The future will be decentralized

Since its creation, Internet has been **mostly** centralized[1], which implies that it is:

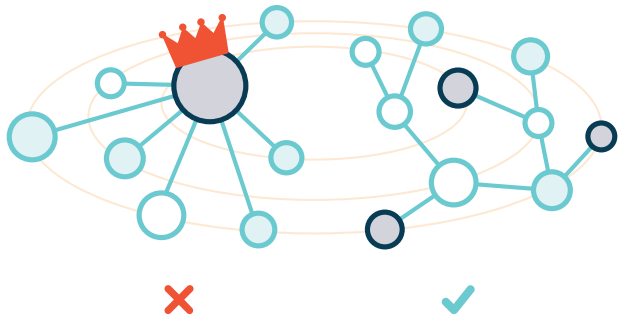
- Easy to watch/monitor
- Easy to censor
- Easy to attack
- Fragile to failure

During the years more distributed and P2P protocols has been deployed, although client-server model is the most common yet.

But the appearance of new P2P systems can drive Internet to a new state

[1] ARPANET hosts file is a great example.

The future will be decentralized



A nice example

IPFS (Inter Planetary File System)

Another example

Steemit is a blogging/social media website built on top of a Blockchain.

Steemit has proven to be able to run an entire social network in a Blockchain.

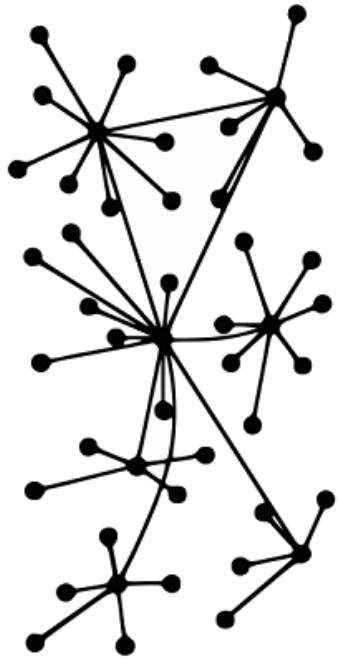
All blog entries are stored in the Blockchain.

The future will be decentralized

The future of the Internet?

Decentralization provides

- censorship resistance
- freedom of Internet
- democratization
- more privacy



Worldwide financial services

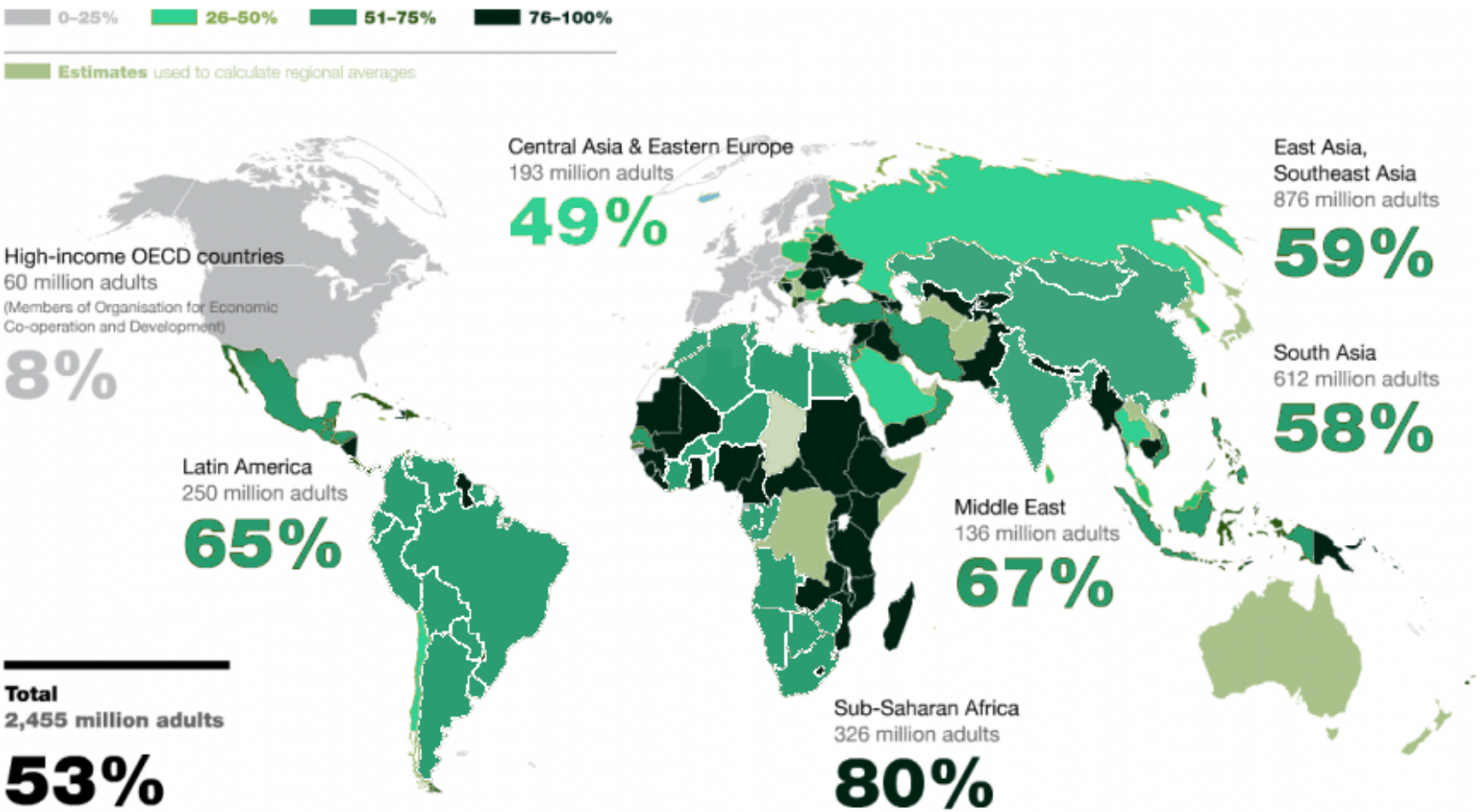
- >50% of world's population (2-3 billion people) does not have access to formal, or any kind of financial services at all.
- People sending money to their families in developing or third world countries pay very high fees.
- Access to loans for those unbanked collectives is difficult and they pay extraordinary high interests (>100% in some cases).

Worldwide financial services

- >50% of world's population (2-3 billion people) does not have access to formal, or any kind of financial services at all.
- People sending money to their families in developing or third world countries pay very high fees.
- Access to loans for those unbanked collectives is difficult and they pay extraordinary high interests (>100% in some cases).

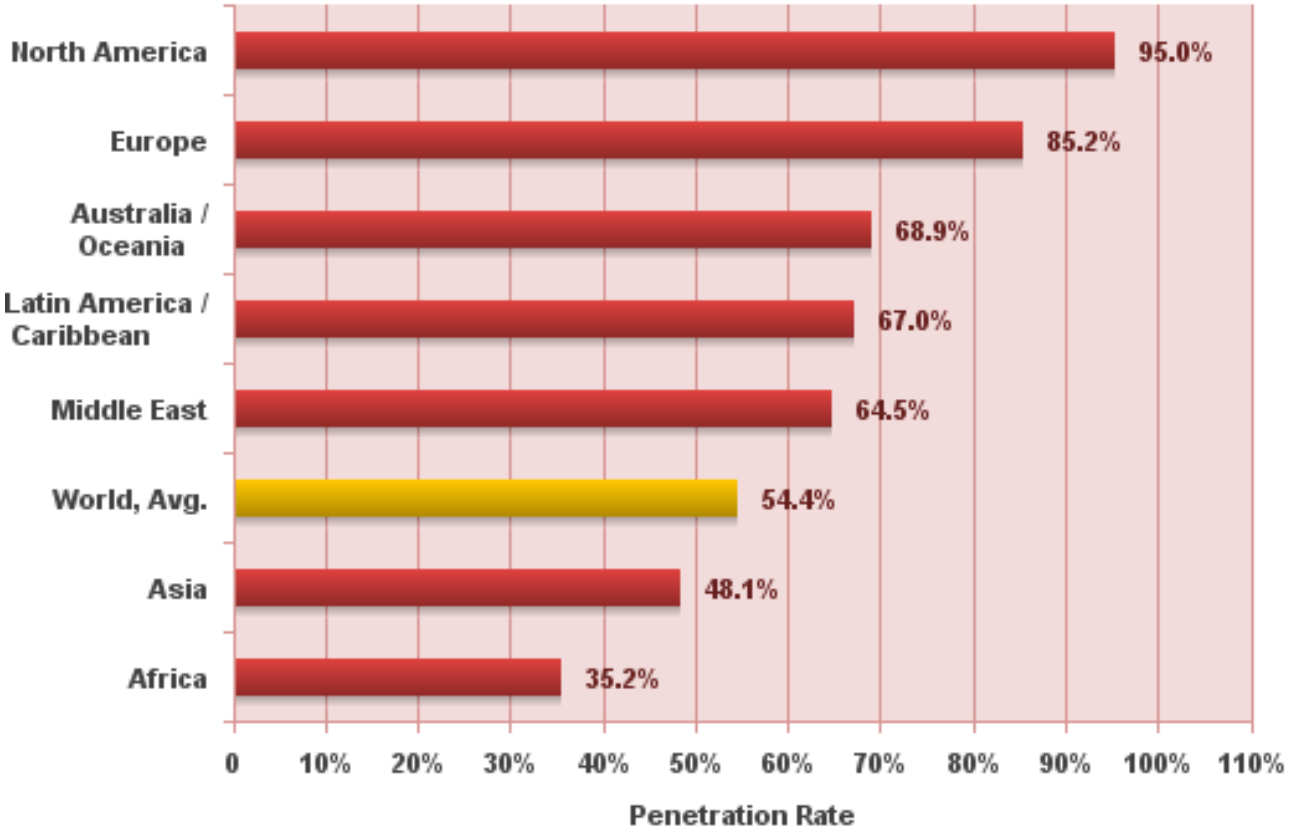
Blockchain and Smart Contracts could provide the infrastructure to **tackle** such a serious problem.

Worldwide financial services



Percentage of unbanked people (Source: ethichub.com)

Worldwide financial services



But...

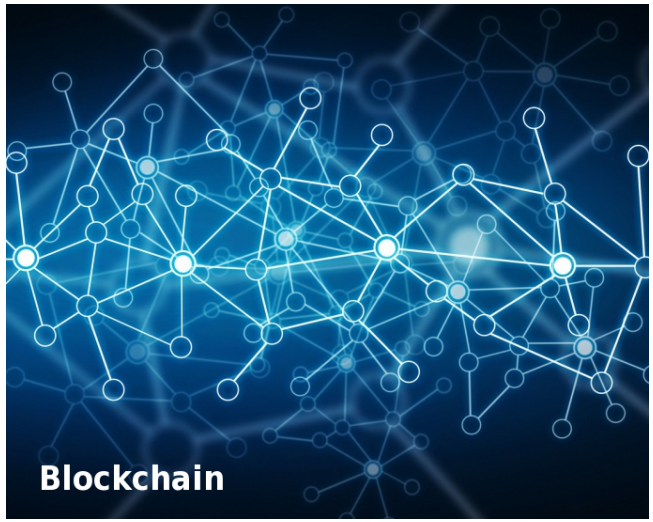
only 54.4% of world's population have access to Internet

(Source: Internet World Stats 2018)

Technology to the rescue again

- **Starlink** is a project of SpaceX and co-financed by Google that aims to provide a global Internet connection using a constellation of satellites.
- Recently the first two satellites of what aims to conform a worldwide-available hi-speed Internet network have been launched.
- In near future, it could potentially provide Internet access to hundreds of millions of people that are offline nowadays.

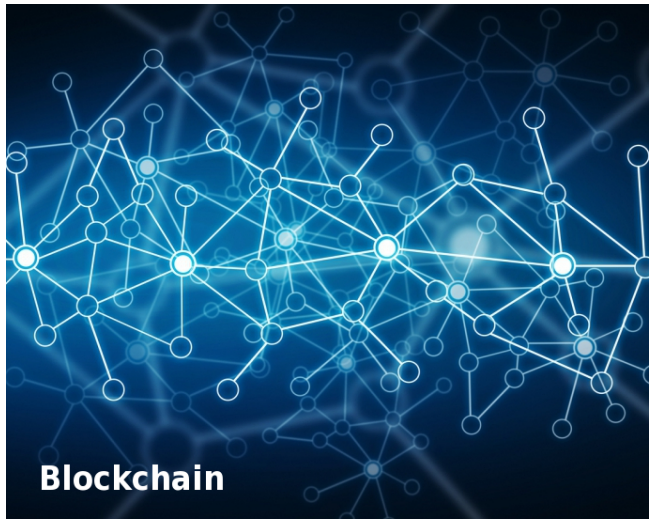
+



Technology to the rescue again

- The combination of all these could empower people, bringing financial services everywhere.
- Everyone could become its own bank.
- Think about yourself being able to crediting third world population.
- It could flip the whole system.

+



Outline

1. Preliminary concepts
2. How does it work?
   - Consensus
   - Proof of Work
   - Proof of Stake
3. Blockchain by generations
   - Preliminaries
   - First Generation
   - Second Generation
   - Third Generation
4. Cardano: A scientific research-driven Blockchain
5. Cryptocurrency wallets
6. Why is it revolutionary?
   - The future will be decentralized
   - Worldwide financial services
7. Some conclusions

Some conclusions

As a result of all these, one can think:

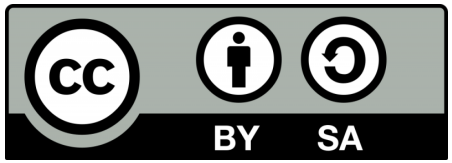
- Wow! Technology is always awesome and has power to change the world.
- Traditional financial model is becoming out-dated...
- ...but for now, Blockchain ecosystem is probably not yet mature enough to drive world's economy.
- The future is going to be more decentralized.
- Awesome things could happen, but only time will tell.

Thanks for your time!

Questions?

License

These slides are licensed under Creative Commons CC-BY-SA.



Slides code available on GitHub:

github.com/gerardbosch/blockchain-presentation

Updated PDF available online:

blockchain-presentation.gerardbosch.xyz