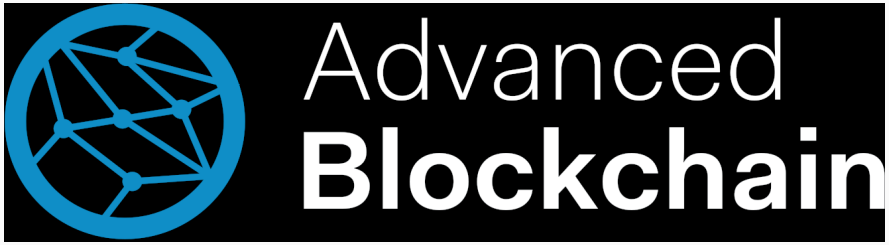


DEFI LAB: Blockchain, DeFi & Friends

Introductory Seminar

Antonio M. Larriba Flor

September 26, 2021

ABAG: Advanced Blockchain

About Advanced Blockchain

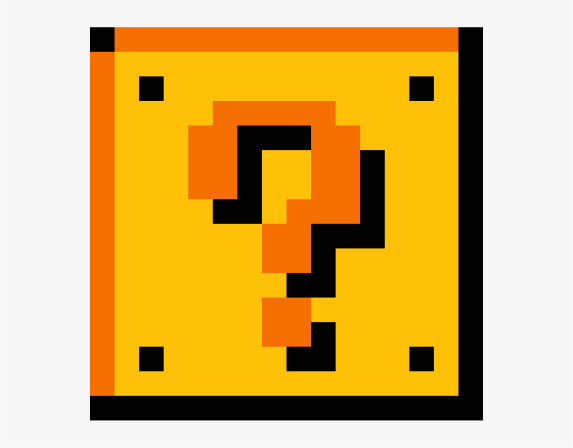
- BaaS: Blockchain As A Service.
- Investing, incubating and consulting on Blockchain projects.
- I am a member of the Research team.
- Read papers, review cryptography, come up with new ideas, etc.

About Me

- Bachelor in Computer Science (2012-2016).
- Master's Degree in Artificial Intelligence, Pattern Recognition and Digital Imaging (2016-2017).
- Getting my PhD (2017-202?).
  - 2017-2019 Neural Machine Translation.
  - 2019-202? Cryptography.

Albarracín 2021.

About this Seminar



What you should expect

- Gentle introduction to blockchain.
- History of cryptocurrencies.
- Basic concepts about cryptography.
- Starting point for later content.

What you shouldn't

- Technical details.
- Low level topics.
- Comprehensive DeFi review.

Index

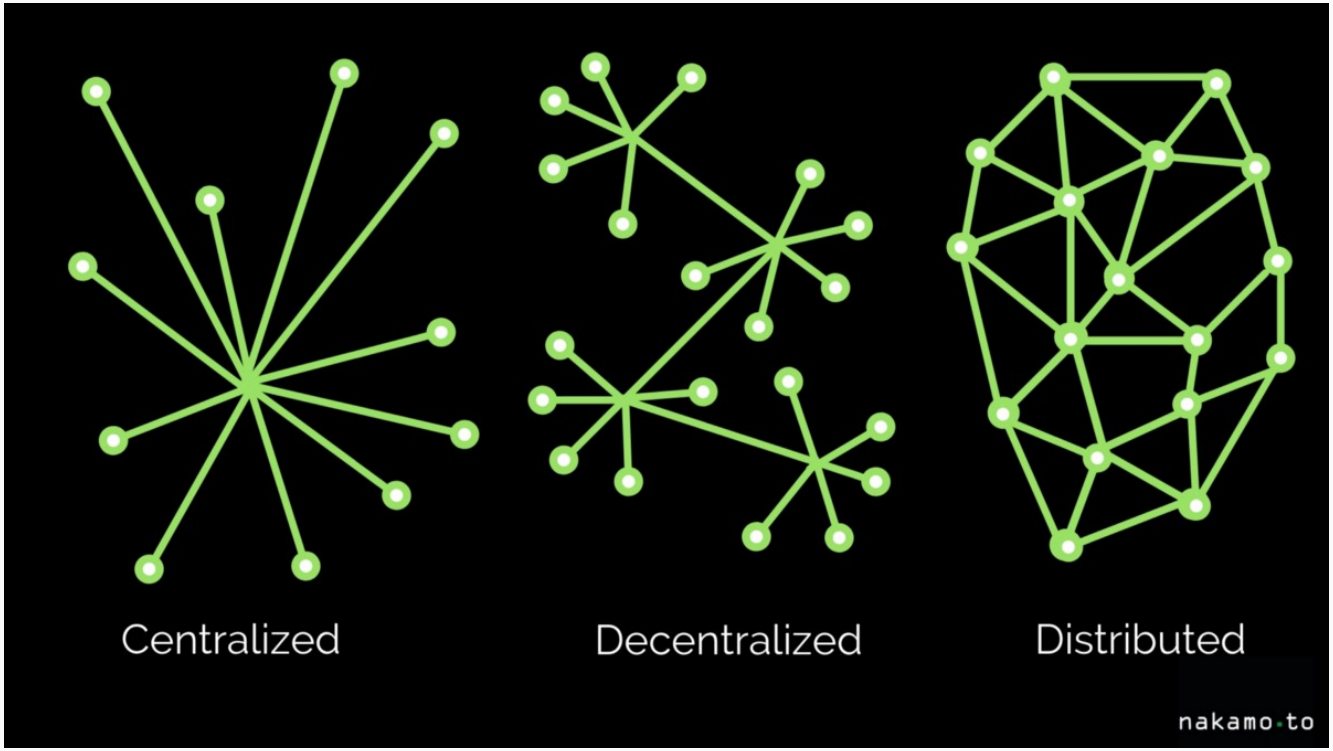
INTRODUCTION

DeFi $\equiv$ Decentralized Finance

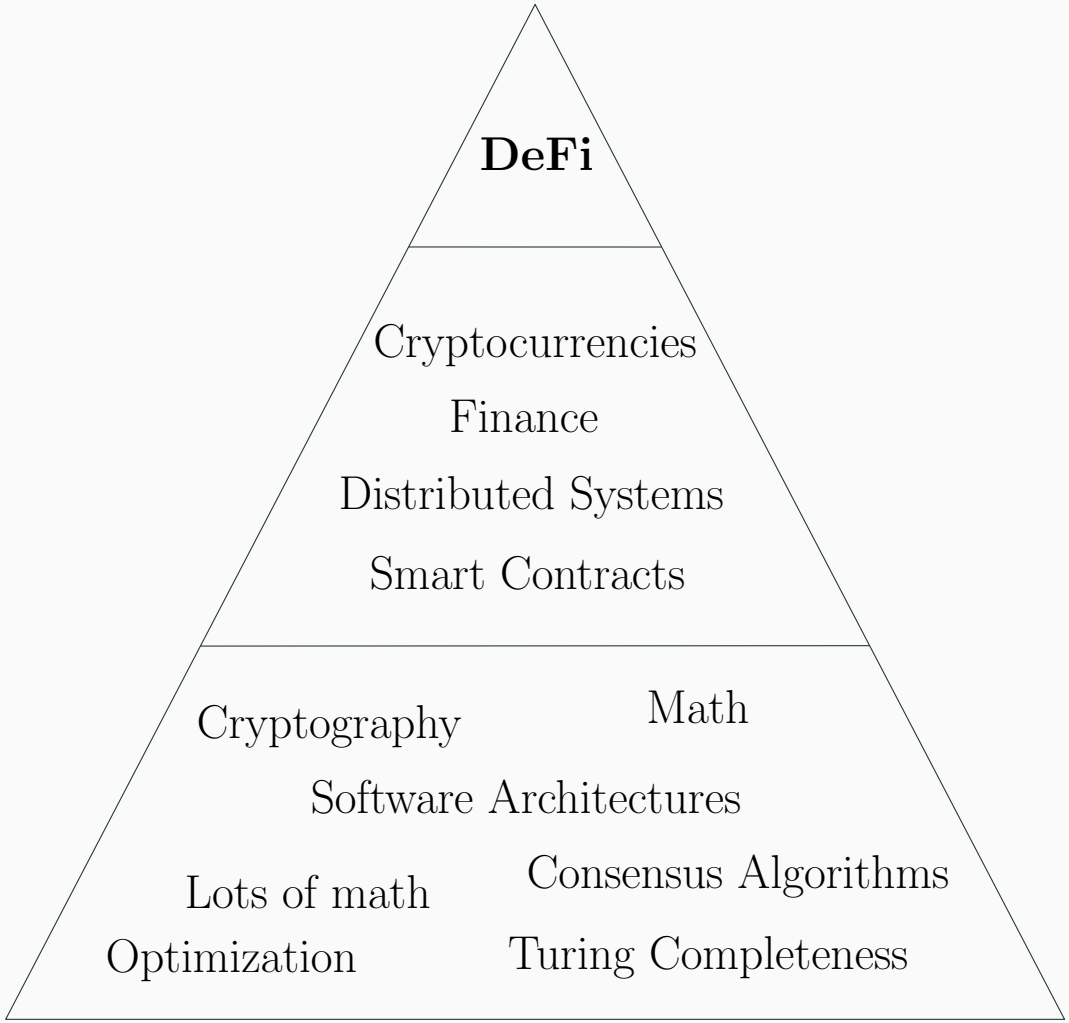
Short definition: Better banking system.

Slightly longer def: Framework where financial products can be built with composable protocols.

Longer definition: It is complicated...



Multidisciplinar area.



Some of the skills in the DeFi Path

- Virtual currency secured by cryptography.
- Usually backed by blockchain technologies that maintain a distributed ledger among a network of computers.
- Distributed and decentralized.

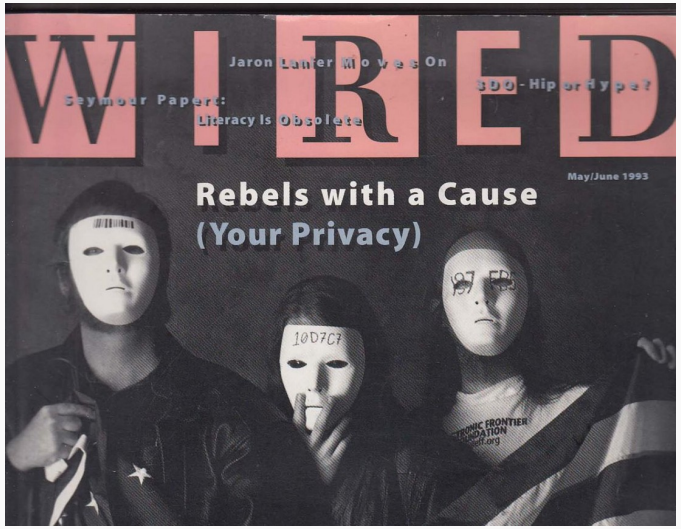
CRYPTO HISTORY

History | Cypherpunks

Cypherpunks Hughes (1993) were a group of mathematicians and cryptographers in the 90s.

> *Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world [...]*
> *[...]The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace. Onward.*

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.



Wired magazine May/June 1993

History | Who?

Non-exhaustive list of cypherpunks:

- Eric Hughes (Founder and admin of the cypherpunk mailing list).
- Timothy C. May (Crypto-anarchist Manifesto).
- John Gilmore (EFF Co-Founder).
- David Chaum (Blind Signatures Chaum (1983), Security without identification Chaum (1985), Digicash Friis (2003), E-cash Camenisch et al. (2005)).
- Adam Back (Hashcash Back et al. (2002)).
- Wei Dai (B-money Dai (1998))
- Hal Finney (Cypherpunk remailer, PGP corp., Early Bitcoin contributor).
- Nick Szabo (Bitgold Szabo (2008)).

History | Why it did not work?

Why did it not succeed?

- Patents.
- Weaker Open Source Community.
- Too early to the party (technology, adoption, widespread).

History | Welcome to the METAVERSE

It planted the seeds for today's Metaverse (Neal Stephenson).
Present and future of Web3:

- Login credentials $\rightarrow$ Digital identity (keys).
- Private payment channels $\rightarrow$ Cryptocurrencies.
- Traditional company $\rightarrow$ Decentralized Autonomous Organization.
- Video games $\rightarrow$ Play to earn.
- Community $\rightarrow$ Tokenized community.
- Ownership $\rightarrow$ NFTs.

BLOCKCHAIN & BITCOIN

Blockchain & Bitcoin | Timeline

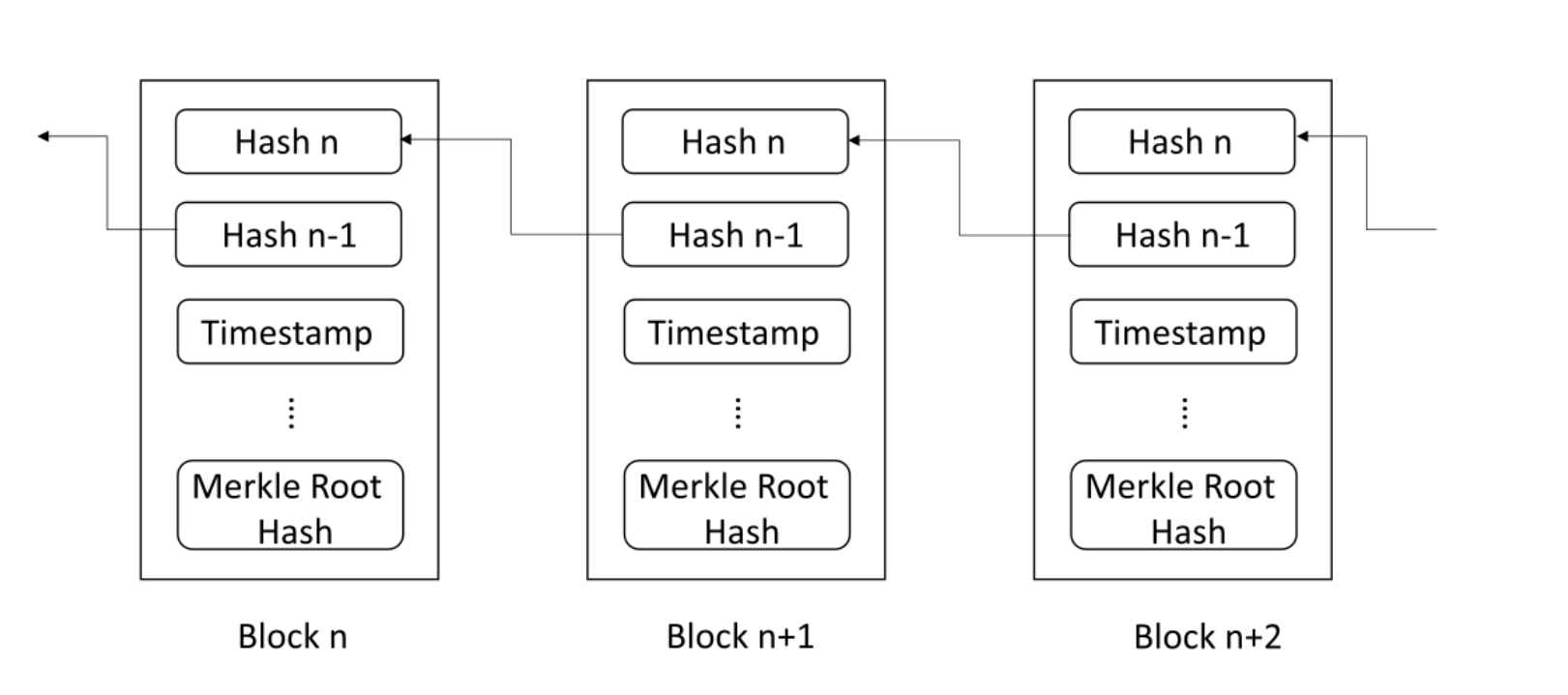
- In 2008, Satoshi Nakamoto publishes the Whitepaper Nakamoto (2008).
- First one to solve the double-spending problem in a decentralized manner.
- In 2009, Bitcoin genesis block is mined.
- Satoshi disappears in 2010.
- May 2010, a guy orders two large pizzas (10,000 BTC).
- 2014, the Mt. Gox fiasco. 70% of global BTC trades.
- In 2015, Ethereum is launched.

A cryptocurrency can be simplified as the sum of the following components:

- A P2P network of participants.
- A consensus algorithm (BFT).
- A chain of cryptographically secure blocks that acts as ledger of the state.
- A currency.

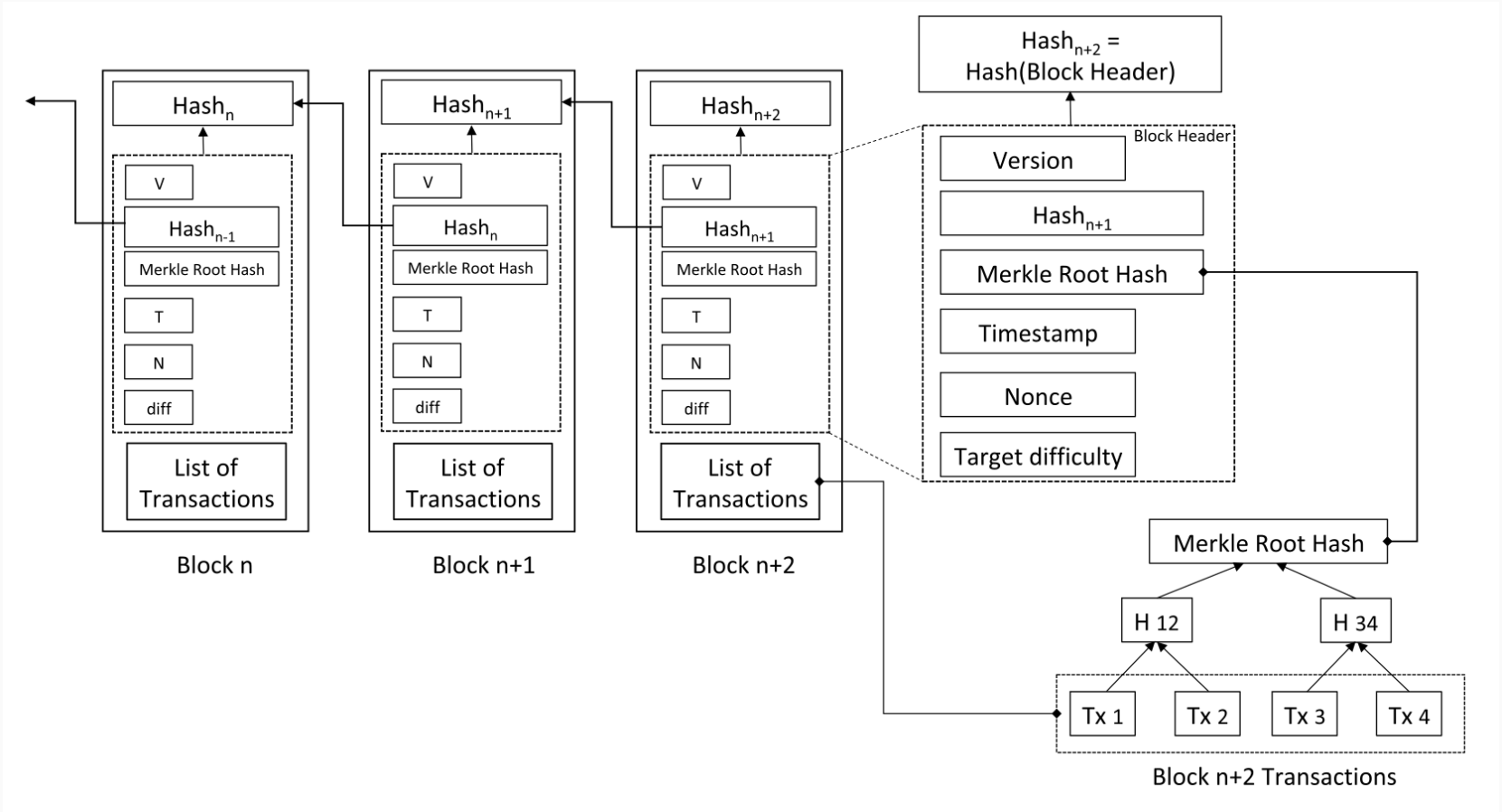
Blockchain & Bitcoin | What is a Blockchain? I

Sequential chain of blocks secured by cryptography.



Blockchain representation. Extracted from Raikwar et al. (2019).

Blockchain & Bitcoin | What is a Blockchain? II



Block header representation. Extracted from Raikwar et al. (2019).

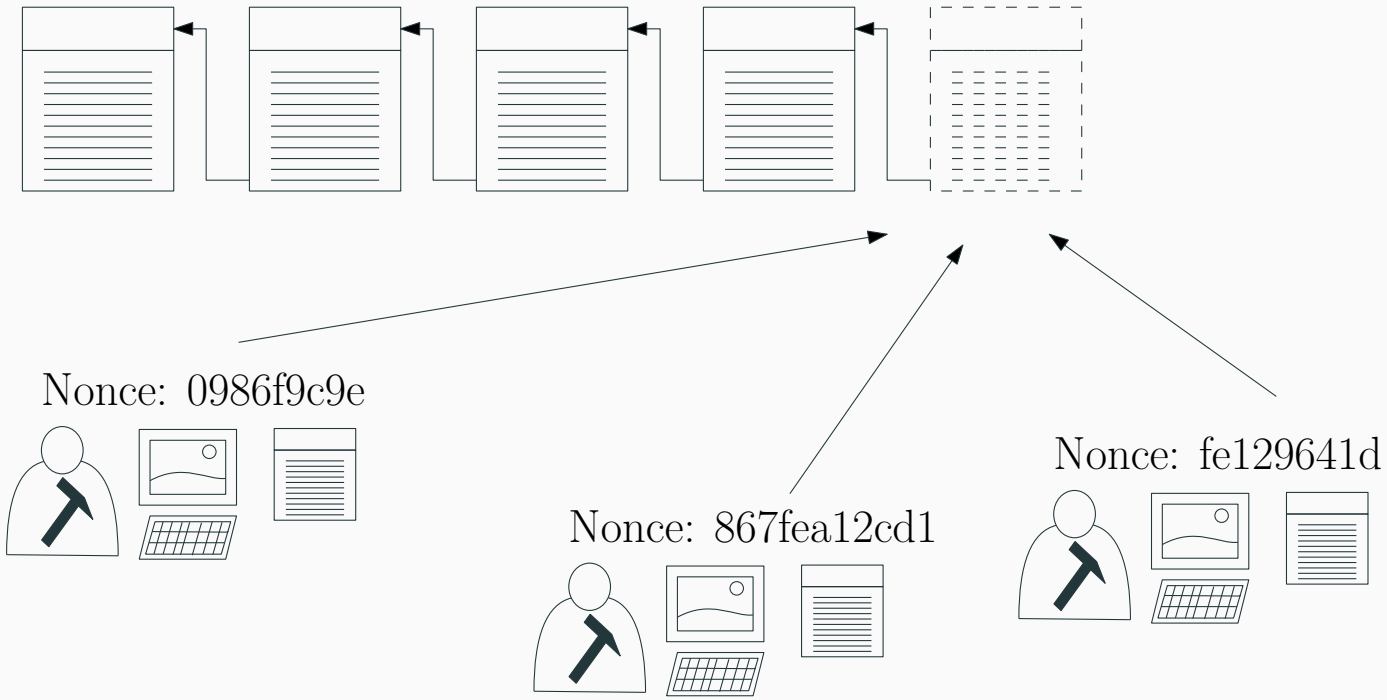
CAP theorem states that a distributed service cannot provide Gilbert and Lynch (2002); Brewer (2012) these three properties at the same time:

- Strong Consensus (C). Well...
- High Availability (A). Yes/No
- Partition Tolerance (P). Yes/No

Multiple consistency models Muñoz-Escoí et al. (2019).

Bitcoin uses Proof-Of-Work to reach implicit consensus. Based on Hascash Back et al. (2002) and Time-lock puzzles Rivest et al. (1996). If you solve the puzzle first, your block is added to the chain.

$$SHA256(Version||PrevHash||...||Nonce) \leq T$$



PoW competition.

Blockchain & Bitcoin | Possibles and impossibles

Can be done

- Distributed ledger.
- Decentralized cryptocurrency.
- Payment system.

Cannot

- Limited scripting language.
- No complex products.
- Scalability.

ETHEREUM & SMART CONTRACTS

Ethereum & Smart Contracts | A new hope I

- A young Bitcoin enthusiast starts thinking about expanding Bitcoin.
- In 2013, Vitalik Buterin, proposed an improvement to the Mastercoin team.
- Vitalik decided to start a new chain, Ethereum.

Vitalik Buterin. Blockchain visionary and fashion God.

Ethereum & Smart Contracts | A new hope II

- Dr.Gavin Wood and many others joined the project.
- Ethereum is announced in 2014.
- In 2015, Ethereum's beta (Olympic) is launched.
- DAO hack in 2016. A hard fork resulted in two chains.
- Today Ethereum is the 2nd biggest crypto and the first smart contract platform.

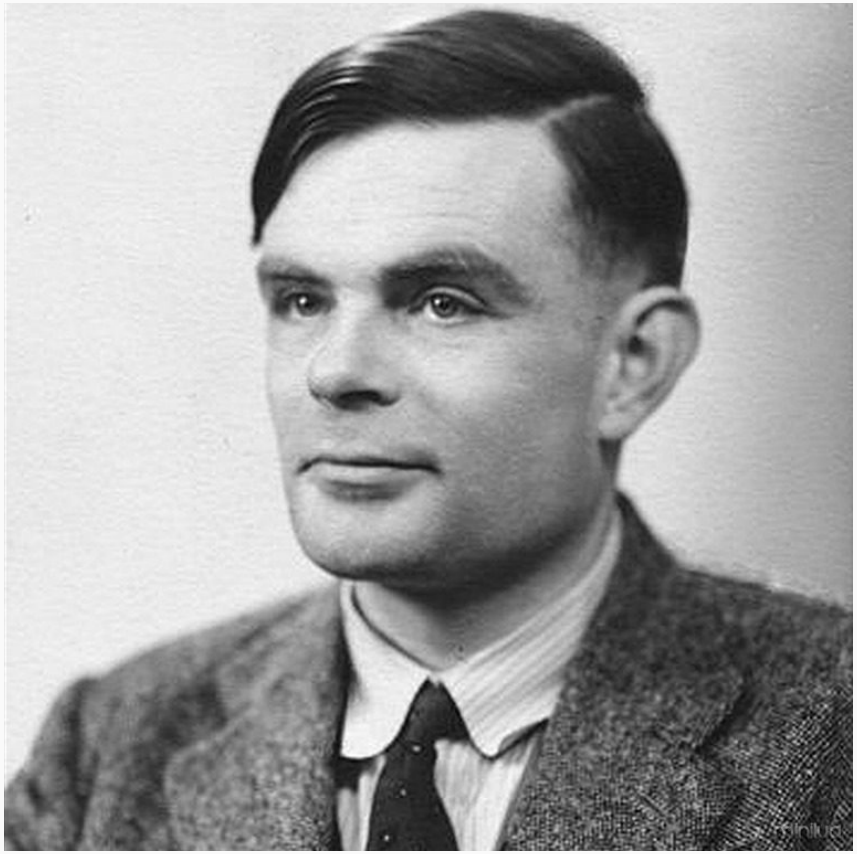
How is Ethereum different from Bitcoin?
Ethereum will transition (est. Q4 2021) to Proof-of-Stake (PoS), a different consensus mechanism.

- The probability of validating a block depends the stake of each validator.
- Validators collect fees from the transactions.
- Better energy efficiency.
- Lower hardware requirements.

Ethereum & Smart Contracts | Turing complete

Ethereum includes Solidity, a Turing complete language.

Includes the concept of Gas to avoid vicious cycles.



Alan Turing, he is back!

Turing completeness means we can do everything a regular computer does.

Solidity code is run on-chain.

The code is also deployed on-chain (Dapps).

That means...

Ethereum's purpose is not primarily to be a digital currency payment network. While the digital currency ether is both integral to and necessary for the operation of Ethereum, ether is intended as a utility currency to pay for use of the Ethereum platform as the world computer. (Mastering Ethereum Book)

This opened the door to infinite possibilities.

- Games.
- Finances.
- Ownership.
- Identity.
- Oracles.

-

We only talked about Bitcoin and Ethereum.

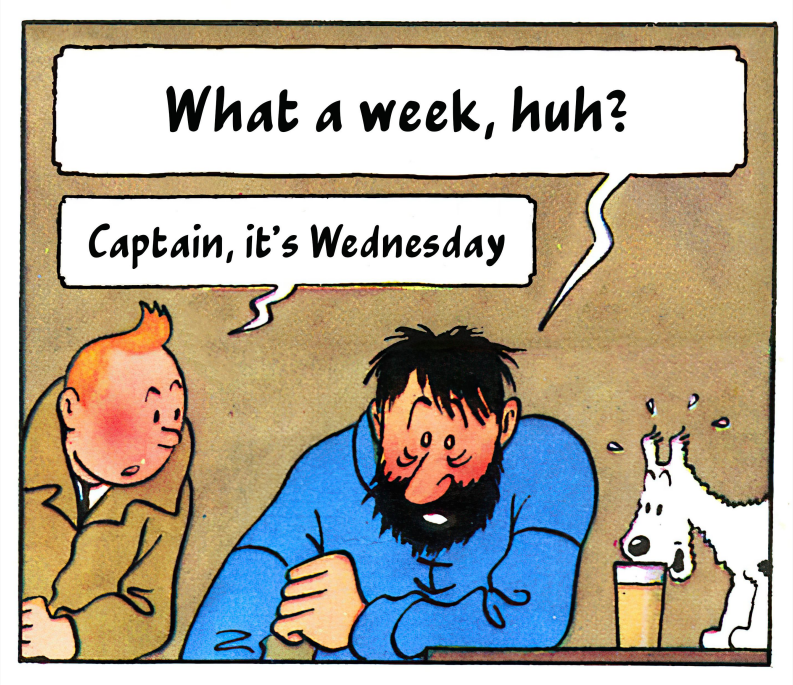
Multichain future

Monero, Polkadot, Chainlink, Cosmos, Cardano, Solana, Algorand, Avalanche, Fantom, Helium, Filecoin...

PROBLEMS

Problems | Scalability

Many blockchain technologies present limited throughput. The number of Transactions Per Second (TPS) is limited when compared to other traditional and centralized networks (e.g: VISA). There is always a trade-off between security and scalability.



There are always some problems...

- Sharding.
- New Consensus protocols.
- Layer 2s
  - Sidechains.
  - State Channels.
  - Rollups.

But we can always try to find a solution.

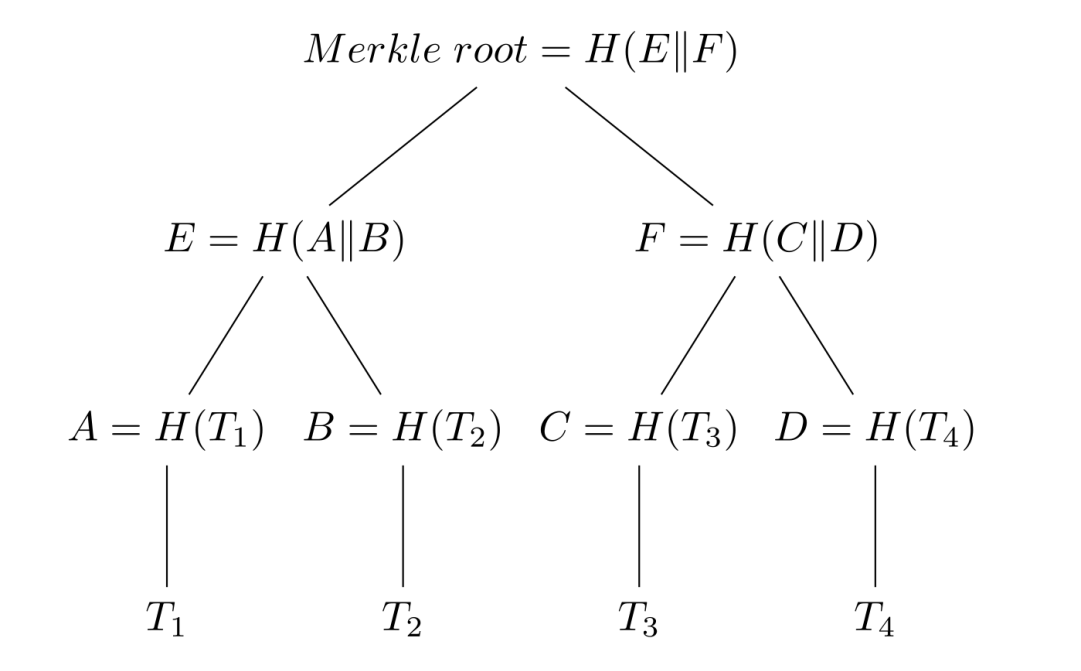
CRYPTOGRAPHY BASICS

Functions that map any arbitrary length input to a random fixed-size output.

- Collision Resistance. Difficult to find a, b such that $H(a) = H(b)$.
- Preimage Resistance. Given y, it is difficult to find a such that $H(a) = y$.
- Second Preimage Resistance. Given a and y such that $H(a) = y$, it is difficult to find a second input b such that $H(b) = y$.

```
Hash("Hello") = 0x185F8D...381969
```

Merkle trees are a kind of trees in which the leafs are the hash of a data block.



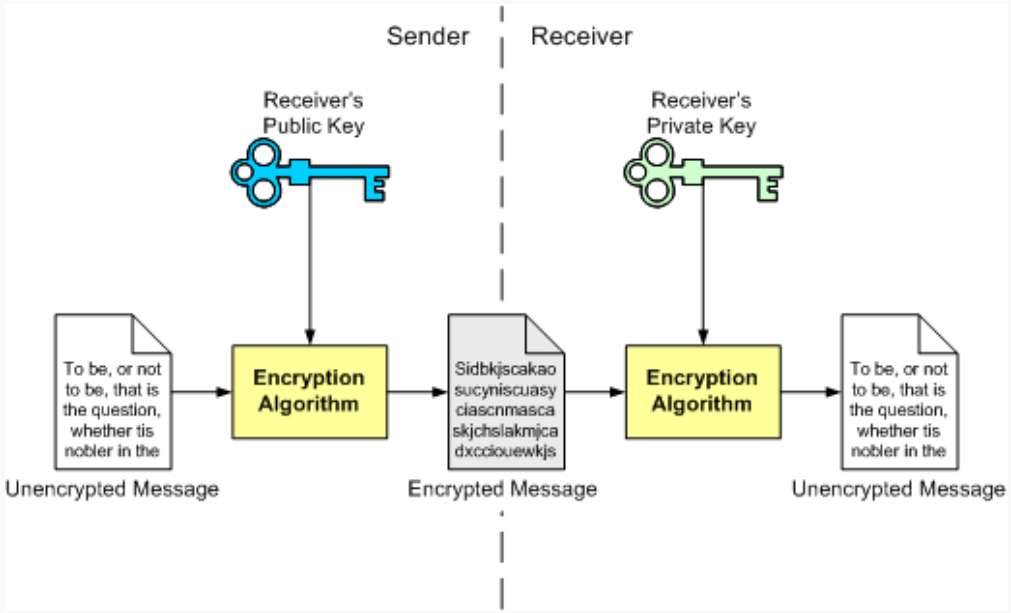
Merkle Tree Structure.

Its root is used as an accumulator of the data it contains. Can be used as Proof-Of-Membership.

Public (or asymmetric) key cryptography presents 2 keys.

- A public key v
- A private key s

Different functions (Enc, Dec) for encrypting and decrypting. They are invertible. $Dec(Enc(M, v), s) \equiv Enc(Dec(M, s), v)$.



Public Key Cryptography Scheme.

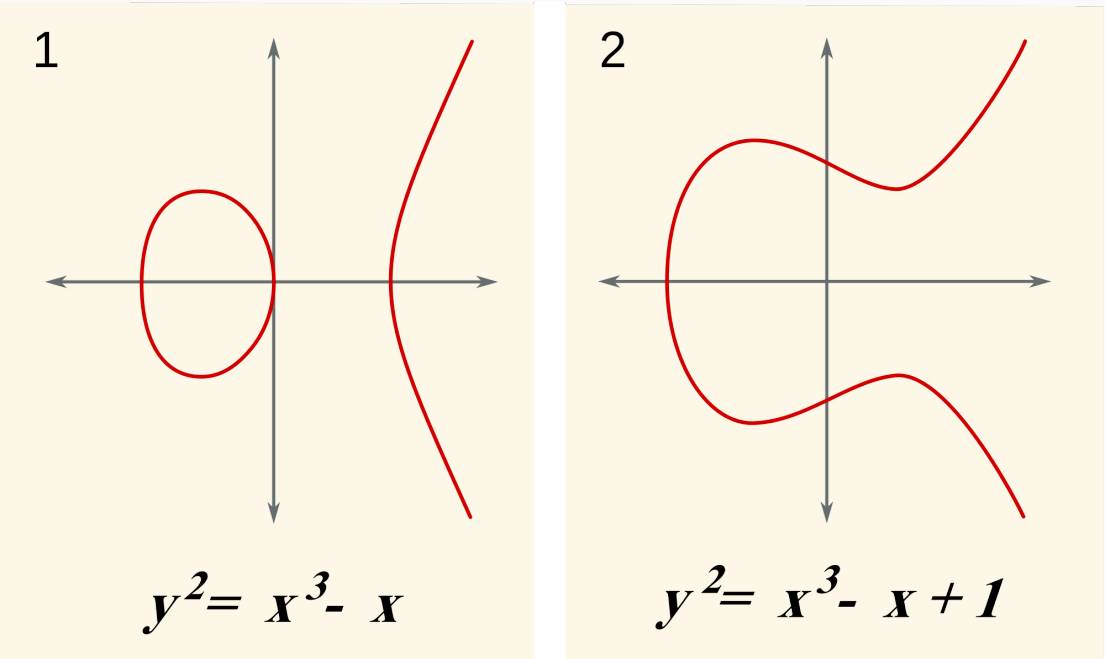
Digital signatures are based on public key cryptography. They provide verifiable codes that ensure:

- Data integrity.
- Identification of the signer.
- Non-repudiatibility.

Elliptic curves are a special kind of polynomials. When defined over a finite field of order p (prime), they have interesting properties.

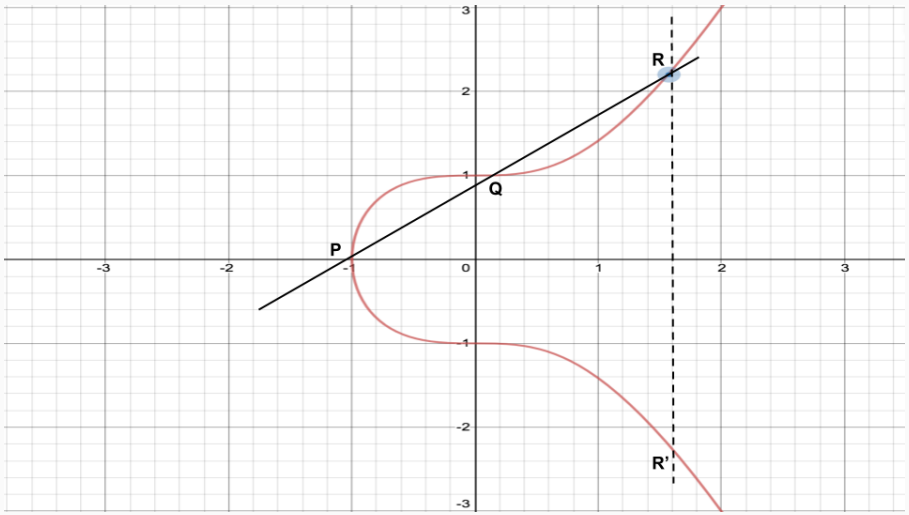
$$y^2 = x^3 + ax + b \pmod{p}$$

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}$$



Elliptic curves.

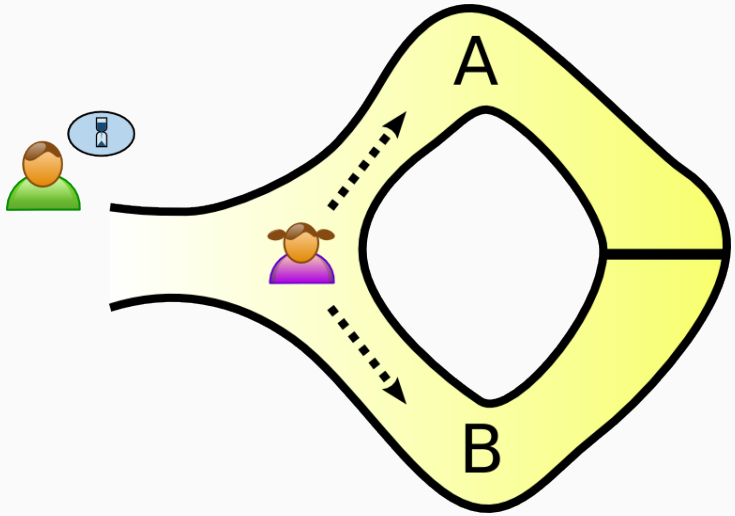
Elliptic Curve Cryptography (ECC) is based on the Elliptic Curve Discrete Logarithm Problem.



Sum on Elliptic Curves.

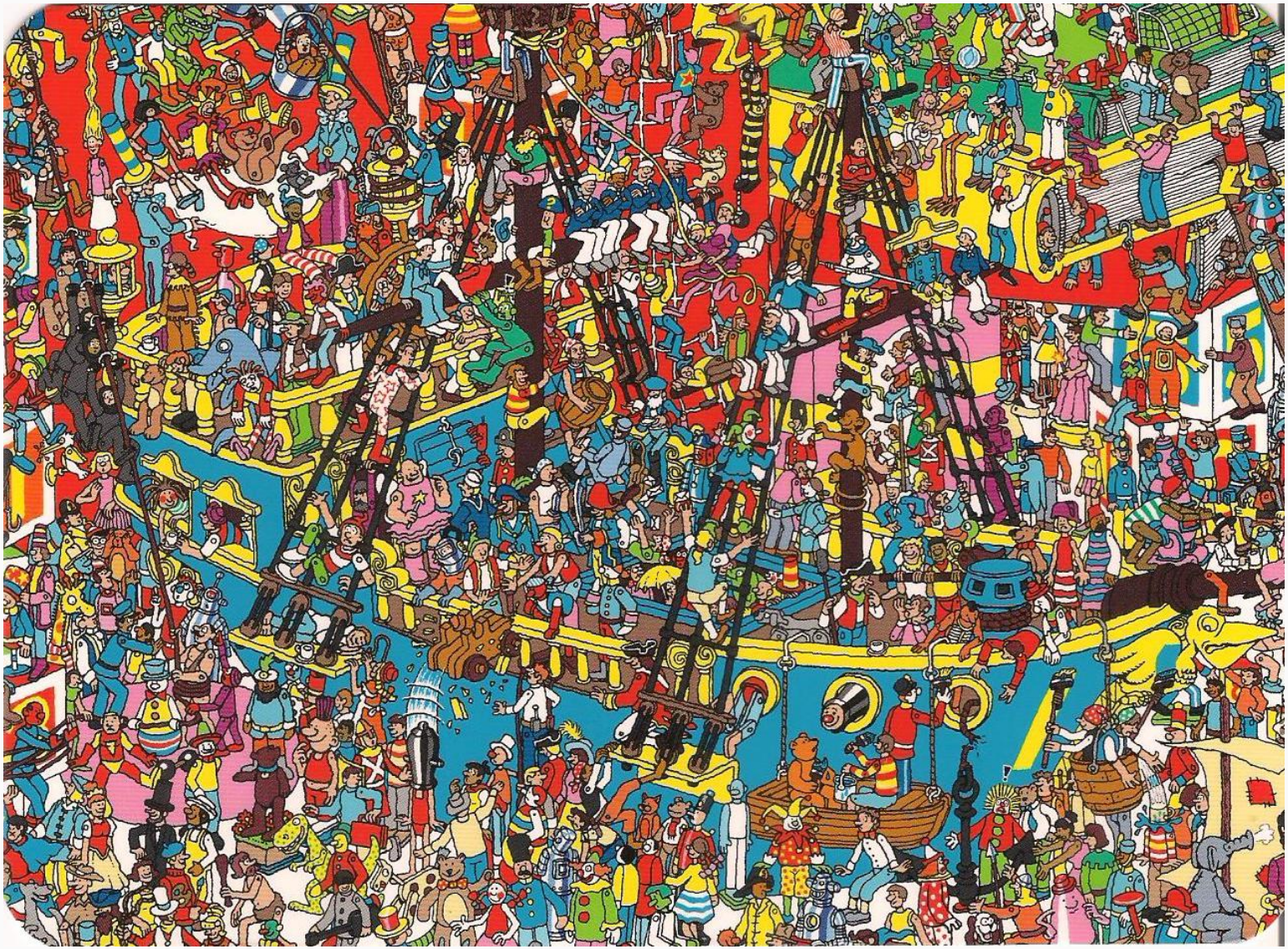
Given a random number $r \in Z_q$ it is easy to compute its associated point on the curve $R = rG$. But given R, computing r is a hard problem with no efficient solution (ECDLP). You can check Andrea Corbellini tutorial for EC.

Scheme that allows a Prover (P) to convince a Verifier (V) about the validity of a statement, without revealing any other information. Quisquater et al. (1989).



ZK-Proof concept idea.

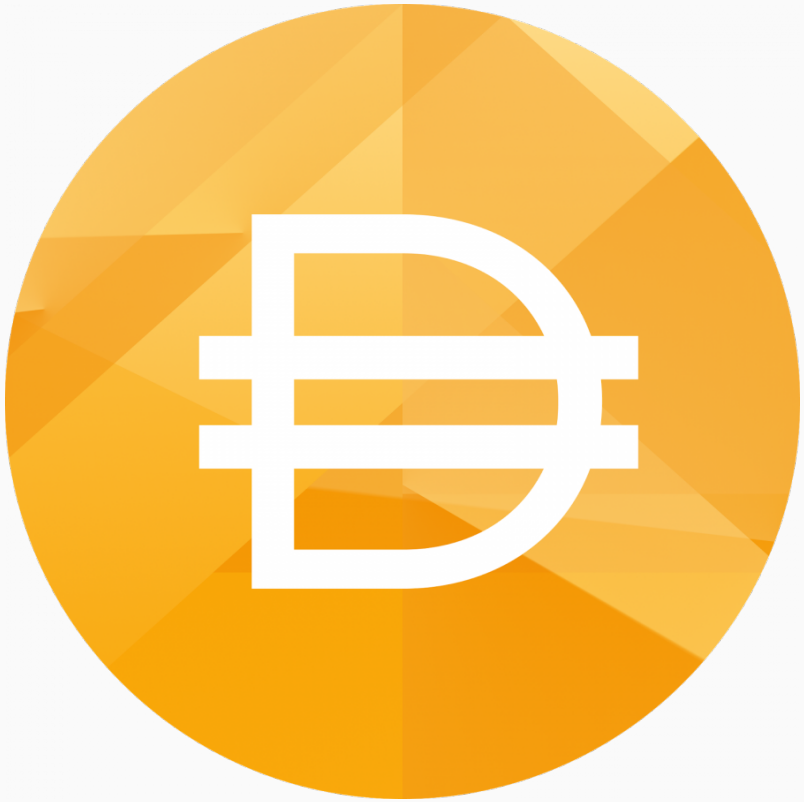
Highly technical area. Many different concepts:
Proof-Of-Knowledge, ZK-Proofs, ZK-Proofs of Knowledge, ZK-Proof-Of-Range, zkS**N**ARKs, zkS**T**ARKs, Bulletproofs, ...



DEFI

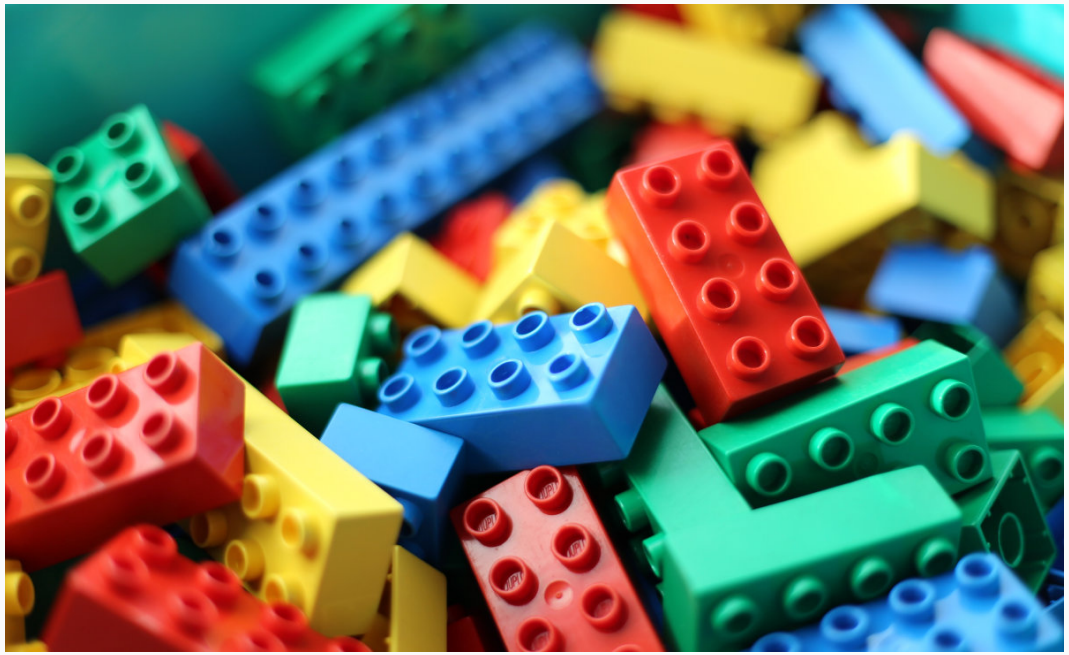
DeFi | Why not before?

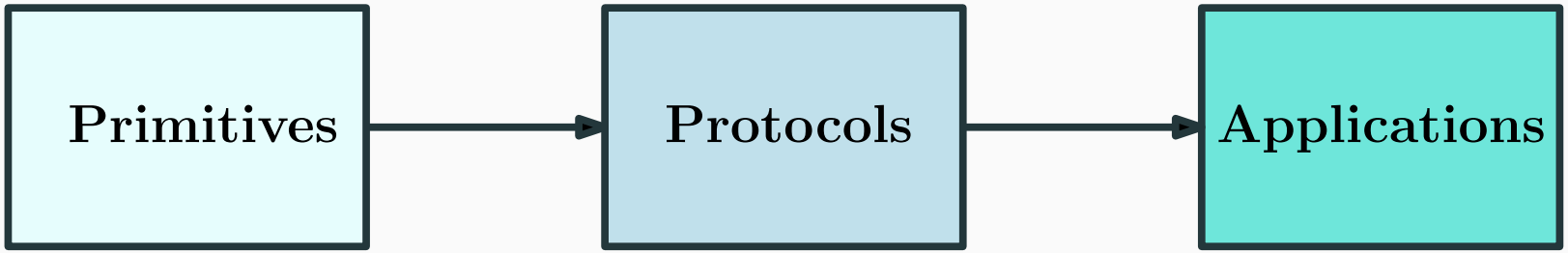
If Bitcoin has been around since 2010 and Ethereum has been since 2015. Why didn't we have Decentralized Finances until 2019? **Volatility**.



DAI is a stablecoin from MakerDAO

DeFi | Composability





DeFi Apps are also called Money Legos

DeFi | Examples

- Stablecoins.
- Savings.
- Decentralized Exchanges (DEX).
- Collateralized Loans.
- NFTs.
- Lending Protocols.

You can check the biggest DeFi projects on: DeFi Pulse.

DeFi | ICOs & Utility Tokens

Utility tokens enable access to a product or service. They are usually launched through Initial Coin Offerings (ICOs) in an effort to make the fundraising more democratic.

- Avoid regulation from the SEC (Security vs. Utility).
- They provide access to a service or a platform.
- ICO fever.

DeFi | DeFi Summer 2020

- Compound launched its own governance token (COMP) on June 2020.
- Yield farming was rewarded with extra tokens.
- Everybody was launching governance tokens. Memes included.
- Uniswap vs. Sushiswap Vampiric War.

CONCLUSIONS

Conclusions

Alea Iacta Est

- We covered the basics.
- It's time to work!
- You can come later and explore the references.

Q & A

BIBLIOGRAPHY

References

Back, A. et al. (2002). Hashcash-a denial of service counter-measure.

Brewer, E. (2012). CAP twelve years later: How the "rules" have changed. *Computer*, 45(2):23–29.

Camenisch, J., Hohenberger, S., and Lysyanskaya, A. (2005). Compact e-cash. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 302–321. Springer.

Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044.

Dai, W. (1998). B-money. *Consulted*, 1:2012.

Bibliography ii

Friis, J. B. (2003). "digicash implementation. *University of Aarhus*.

Gilbert, S. and Lynch, N. A. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News*, 33(2):51–59.

Hughes, E. (1993). A cypherpunk's manifesto. *Crypto anarchy, cyberstates, and pirate utopias*, pages 81–83.

Muñoz-Escoí, F. D., de Juan-Marín, R., García-Escrivá, J.-R., González de Mendívil, J., and Bernabéu-Aubán, J. M. (2019). Cap theorem: revision of its related consistency models. *The Computer Journal*, 62(6):943–960.

Nakamoto, S. (2008). Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*.

Quisquater, J.-J., Quisquater, M., Quisquater, M., Quisquater, M., Guillou, L., Guillou, M. A., Guillou, G., Guillou, A., Guillou, G., and Guillou, S. (1989). How to explain zero-knowledge protocols to your children. In *Conference on the Theory and Application of Cryptology*, pages 628–631. Springer.

Bibliography iii

Raikwar, M., Gligoroski, D., and Kralevska, K. (2019). Sok of used cryptography in blockchain. *IEEE Access*, 7:148550–148575.

Rivest, R. L., Shamir, A., and Wagner, D. A. (1996). Time-lock puzzles and timed-release crypto.

Szabo, N. (2008). Bit gold proposal. *Decentralized Business Review*, page 21449.