A Comparison of Layer 2 Techniques for Scaling Blockchains

Adrià Torralba-Agell[1, 2]
atorralbaag@uoc.edu

Cristina Pérez-Solà[1, 2]
cperezsola@uoc.edu

[1]Universitat Oberta de Catalunya - KISON Research Group

[2]Cybercat - Center for Cybersecurity Research of Catalonia

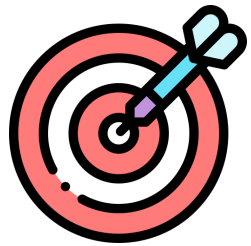
July 5, 2022

Outline

Outline

Goals for this talk

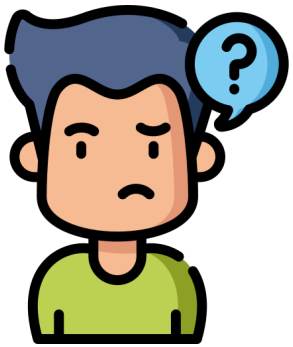
1. Introduce the **blockchain scalability problem**.
2. Introduce **existing scalability solutions**.
3. Show **major differences** among them.



Outline

Why is this happening?

- Rise in **popularity** of **blockchain** techlonology.
  - dAPPS,
  - DeFi,
  - NFTs,
  - Blockchain games,
  - etc.
- Heavy **congestion**
  - **Poor** performance,
  - **High** transaction **fees**.



Blockchain Trilemma

- 3 desirables properties
  - Scalability,
  - Security,
  - Decentralization.
- Vitalik (and others) believe that all 3 are **incompatible** at the **same time**.
  - **Blockchain Trilemma**.

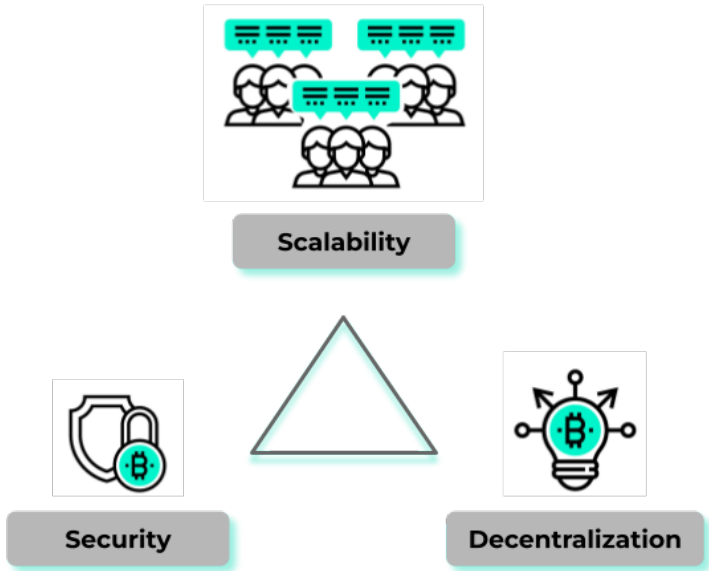
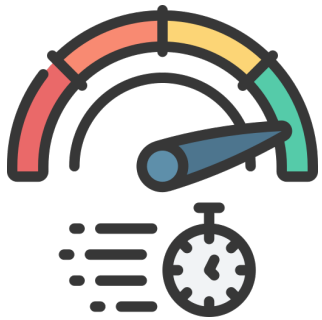


Figure: Diagram of the Blockchain Trilemma.

Performance Metrics

- Transaction throughput (**Transactions per Second**, TPS).
- Latency.
- Bootstrap time.
- Cost per **confirmed transaction**, in terms of computation, network and storage resources.
- Cost to **maintain a full node** also in terms of computation, network and storage.
- ...



Outline

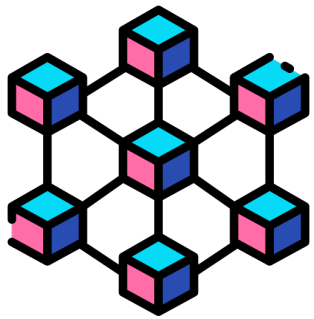
Layer 1 scaling (aka *on-chain* solutions)

Focused on **improvements** in

- Consensus algorithm,
- Network,
- Data Structure of the Blockchain.

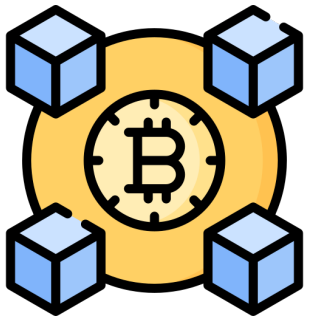
For instance

- Changes to the **size** of the **block**,
- Implement techniques to **split the work of building a block across many participants** (*sharding*).



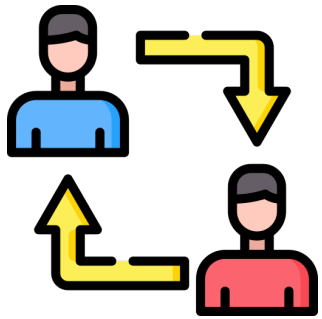
Layer 2 scaling (aka *off-chain* solutions)

- **Withdraw computation** from the *main network* (Layer 1) and **perform this work off-chain** (Layer 2).
- We consider here three different approaches
  - Payment Channel Networks,
  - Sidechains,
  - Rollups.



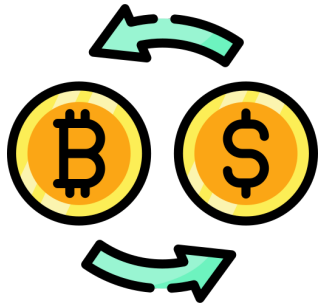
Payment Channel Networks

- A **Peer-to-Peer** network on top of the main blockchain.
- Can perform **many transactions** without the **restrictions** imposed by the main network.
- Come with the **cost** of security and reliability.
- Examples
  - **Lightning Network** for Bitcoin Blockchain,
  - **Raiden Network** for Ethereum Blockchain.



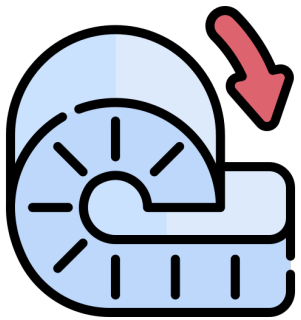
Sidechains

- A **whole new blockchain** in parallel of the main blockchain.
- Tokens can **flow** between main network and sidechain.
- Have to deal with
  - Consensus mechanism,
  - Tokens,
  - Security.



Rollups

- Group a **batch of transactions**, "roll-up" them and publish to Blockchain, providing a *proof* for its **correctness**.
- There are **two main flavours** for this technique
  - **zkRollups** based on **validity proofs.**
  - **Optimistic Rollups** based on **fraud proofs.**



Outline

Considered technologies

- Payment Channels
  - **Lightning Network,**
  - **Raiden Network.**
- Rollups
  - Zero-Knowledge Rollups
    - ★ **zkSync,**
    - ★ **Loopring,**
    - ★ **StarkNet.**
  - Optimistic Rollups
    - ★ **Arbitrum,**
    - ★ **Optimism.**

Usability

		Usability		
Scalability Solution Type	**Technology Name**	**General-purpose Script / Turing Complete Machine**	**Supported tokens**	**Native proprietary token?**
Payment Channels	**Lightning Network**	No	Bitcoin (BTC)	No
	Raiden Network	Yes, native	ERC20	Yes, Raiden Network Token (RDN)
Zero-Knowledge Rollups	**zkSync 2.0**	Yes, in Zinc	Ether (ETH), ERC20	No
	Loopring 3.8	No	Ether (ETH), ERC20	Yes, Loopring (LRC)
	Starknet	Yes, implemented using Cairo	Ether (ETH), ERC20, ERC721	No
Optimistic Rollups	**Arbitrum**	Yes, through ArbOS (EVM compatible)	ERC20, ERC721	No
	Optimism	Yes, supports Solidity and Vyper	ERC20, ERC721	Yes, Optimism (OP)

Security

		Security				
Scalability Solution Type	**Technology Name**	**Security Model**	**Cryptographic primitives**	**Zero-Knowledge technique**	**Post-quantum resistant**	**Type of network**
Payment Channels	**Lightning Network**	Inherited from L1 + node always online + censorship resistant within time t	Hash functions, digital signature	NA	No	Peer-to-Peer
	Raiden Network	Inherited from L1 + node always online + censorship resistant within time t	Hash functions, digital signature	NA	No	Peer-to-Peer
Zero-Knowledge Rollups	**zkSync 2.0**	Inherited from L1 + CRS always hidden + censorship resistant within time t	Pairings, KoE, minimal trusted setup	PLONK	No	Centralised
	Loopring 3.8	Inherited from L1 + CRS always hidden + censorship resistant within time t	Pairings and trusted setup	zkSNARK	No	Centralised
	Starknet	Inherited from L1 + censorship resistant within time t	Hash functions	zkSTARK	Yes	Centralised
Optimistic Rollups	**Arbitrum**	Inherited from L1 + Based on Game Theory + censorship resistant within time t	Fraud proofs (Merkle Trees or ZKP)	NA	No	Centralised
	Optimism	Inherited from L1 + Based on Game Theory + censorship resistant within time t	Fraud proofs (Merkle Trees or ZKP)	NA	No	Centralised

Cost

		Cost		
Scalability solution type	**Technology name**	**Fees**	**Processing time**	**Withdrawal time**
Payment Channels	**Lightning Network**	Funding transaction + (possible hops +) closing transaction	Near instant	1 hour to several days
	Raiden Network	Similar to Lightning Network fee system	Near instant	Up to 3 hours
Zero-Knowledge Rollups	**zkSync**	≈100 times cheaper for ERC20 ≈ 30 times cheaper for ETH	Near instant	10 minutes to 7 hours
	Loopring 3.8	30 to 100 times cheaper for ERC20 and ETH	Near instant	6 minutes to 2 hours
	Starknet	L1 Fees (in the future also L2 fees)	Near instant	Not specified
Optimistic Rollups	**Arbitrum**	Up to 10 times cheaper	Near instant	Around 7 days
	Optimism	L2 execution fee + L1 security fee	Near instant	Around 7 days

Outline

Conclusions

- Wide variety of Layer 2 scalability solutions.
- Currently does not seem to be a perfect solution for this problem.
- Addition of security assumptions.
- Solutions are still in young age. Constantly evolving.
- Concerns about centralised approaches?

Future Work

- Work in progress.
- Extension of this article.
  - Usability
    - ★ Capabilities of smarts contracts.
    - ★ Rate ease of use.
  - Security
    - ★ Review Zero-Knowledge requirements.
  - Cost
    - ★ Perform experiments deploying the solutions to benchmark different properties (fees, processing time, withdrawal time, computational resources...)

Thank you for your attention!

Questions?