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

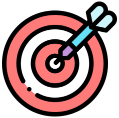
October 19, 2022

Outline

Outline

Goals for this talk

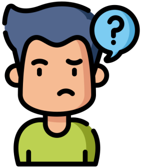
1. Introduce the **blockchain scalability problem**
2. Introduce **existing scalability solutions**
3. Show **major differences** among them



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 Buterin (and other authors) claim that all 3 are **incompatible** at the **same time**
  - **Blockchain Trilemma**

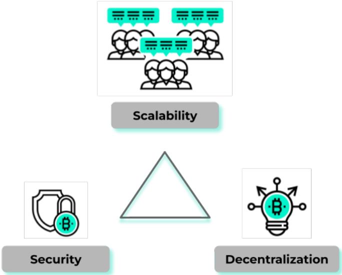
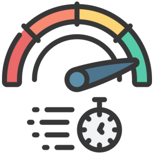


Figure: Diagram of the Blockchain Trilemma

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

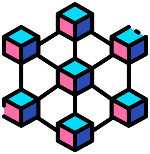
Layer 1 scaling (aka *on-chain* solutions)

Focused on **improvements** in

- Consensus algorithm
- Network
- Data Structure of the Blockchain

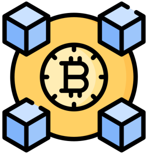
For instance

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



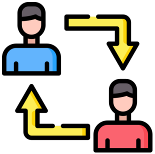
Layer 2 scaling (aka *off-chain* solutions)

- **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



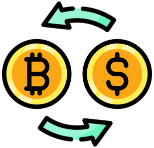
Payment Channel Networks

- 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



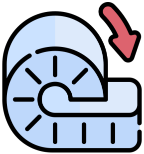
Sidechains

- 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**	Yes, in Zinc	ERC20, Ether (ETH)	No
	Loopring 3.8	No	ERC20, Ether (ETH)	Yes, Loopring (LRC)
	Starknet	Yes, implemented using Cairo	ERC20, Ether (ETH) 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**	**Type of network**
Payment Channels	**Lightning Network**	Inherited from L1 + censorship-resistant within time t + node always online	Hash functions, digital signature	Peer-to-Peer
	Raiden Network	Inherited from L1 + censorship-resistant within time t + node always online	Hash functions, digital signature	Peer-to-Peer
Zero-Knowledge Rollups	**zkSync**	Inherited from L1 + censorship-resistant within time t + CRS always hidden	Pairings, KoE, minimal trusted setup	Centralised
	Loopring 3.8	Inherited from L1 + censorship-resistant within time t + CRS always hidden	Pairings, trusted setup	Centralised
	Starknet	Inherited from L1 + censorship-resistant within time t	Hash functions	Centralised
Optimistic Rollups	**Arbitrum**	Inherited from L1 + censorship-resistant within time t + based on Game Theory	Fraud proofs (Merkle Trees or ZKP)	Centralised
	Optimism	Inherited from L1 + censorship-resistant within time t + based on Game Theory	Fraud proofs (Merkle Trees or ZKP)	Centralised

Cost

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

Outline

Conclusions

- Wide variety of Layer 2 scalability solutions
- Currently it does not seem to be a perfect solution for this problem
- Addition of security assumptions
- Solutions are still in young age, constantly evolving

Future Work

- Add newborn zkRollup solutions
- Extend this article
  - Usability
    - Study 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?

@0xAdriaTorralba

0xAdriaTorralba

atorralbaag@uoc.edu