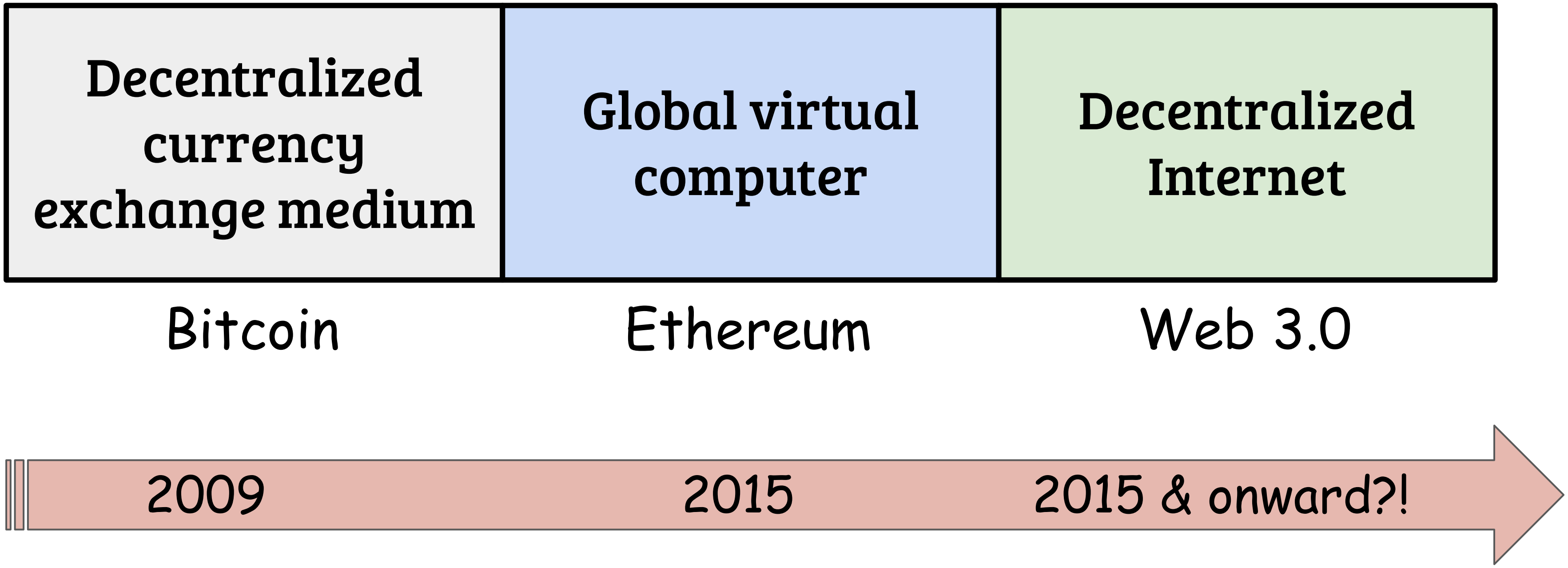
# chainBoost: A Secure Performance Booster for Blockchain-based Resource Markets

Zahra Motaqy, Mohamed Najd, **Ghada Almashaqbeh**

University of Connecticut

EuroS&P 2024

# The Decentralized Internet—Web 3.0



Decentralized currency exchange medium

Bitcoin

2009

Global virtual computer

Ethereum

2015

Decentralized Internet

Web 3.0

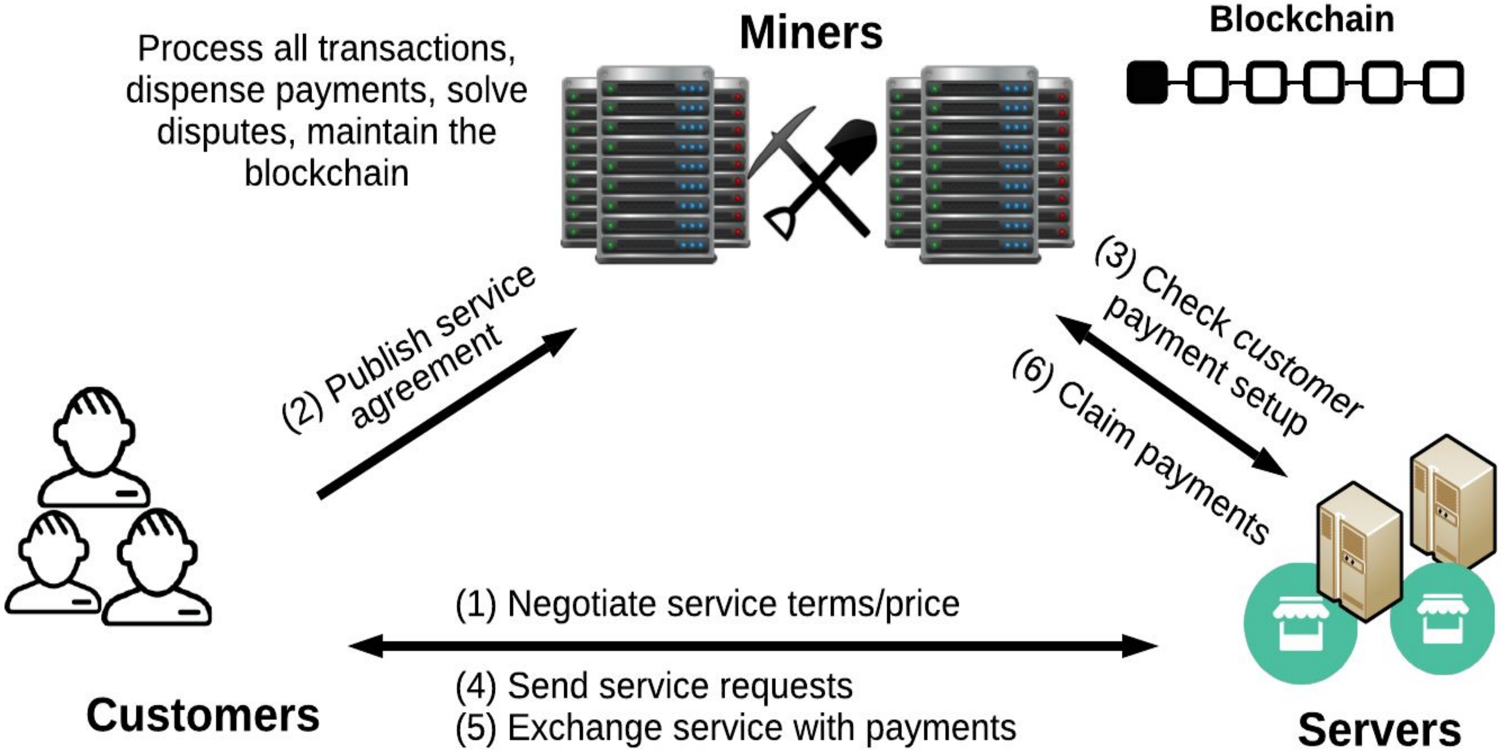
2015 & onward?!

Our focus

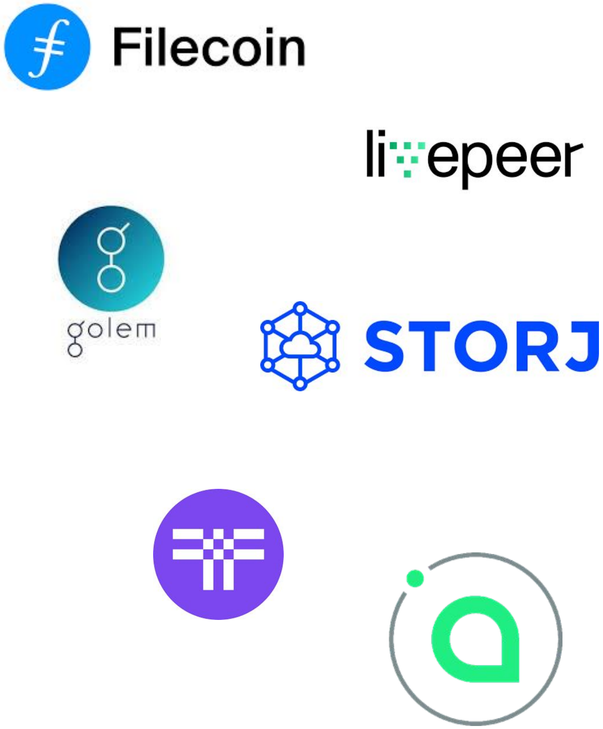
# Decentralized Resource Markets

- Provide distributed services on top of the currency exchange medium.
    - E.g., computation outsourcing, file storage and retrieval, video transcoding, etc.
- They create open-access markets for trading resources.

# Decentralized Resource Markets


Miners
Blockchain
Process all transactions, dispense payments, solve disputes, maintain the blockchain
(2) Publish service agreement
(3) Check customer payment setup
(6) Claim payments
(1) Negotiate service terms/price
(4) Send service requests
(5) Exchange service with payments
Customers
Servers

# They are a Large Industry …

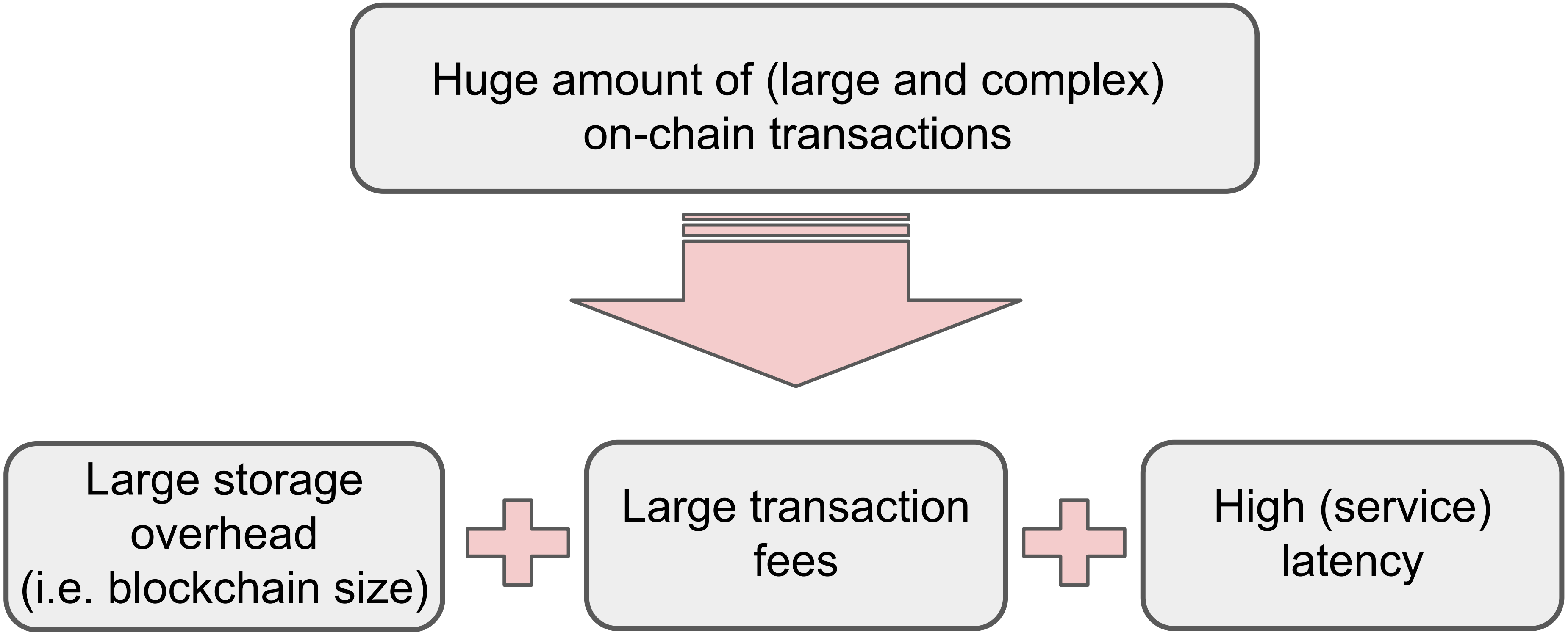


**Interesting Topics**

- Market matching strategies
- Fair exchange protocols
- Proof of service delivery
- Collateral management policies
- Dispute solving
- Privacy
- …

Our focus

# … and a Huge Scalability Problem!



Huge amount of (large and complex) on-chain transactions

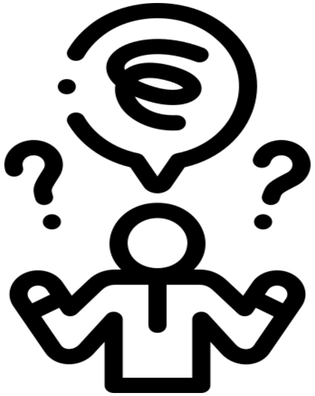
Large storage overhead (i.e. blockchain size)

Large transaction fees

High (service) latency

***Can we build a generic and secure efficiency solution for decentralized resource markets that***

1. has a unified architecture and interfaces, and
2. allows for service-specific semantics, while
3. preserving the public verifiability, decentralization, transparency, etc., that are expected of a Web 3.0 protocol?



# Limitations of Existing Solutions

# Limitations of Existing Solutions

- *Sharding ⇒ High volume of cross-shard transactions!*

# Limitations of Existing Solutions

- *Sharding ⇒ High volume of cross-shard transactions!*
- *Zero-knowledge (ZK) rollups ⇒ ZK proofs are expensive!*
- *Optimistic rollups ⇒ Long contestation periods + incentive compatibility issues!*

# Limitations of Existing Solutions

- *Sharding ⇒ High volume of cross-shard transactions!*
- *Zero-knowledge (ZK) rollups ⇒ ZK proofs are expensive!*
- *Optimistic rollups ⇒ Long contestation periods + incentive compatibility issues!*
- *Sidechains ⇒ Mainly focused on two-way peg and independent sidechains!*

Still, sidechains have potential to solve the problem!

This work

chainBoost—a new dependent sidechain architecture

# Contributions

A formalization of decentralized resource market setting.

# Contributions

A formalization of decentralized resource market setting.

chainBoost framework: the first sidechain architecture that allow mutual-dependency relation with the mainchain!

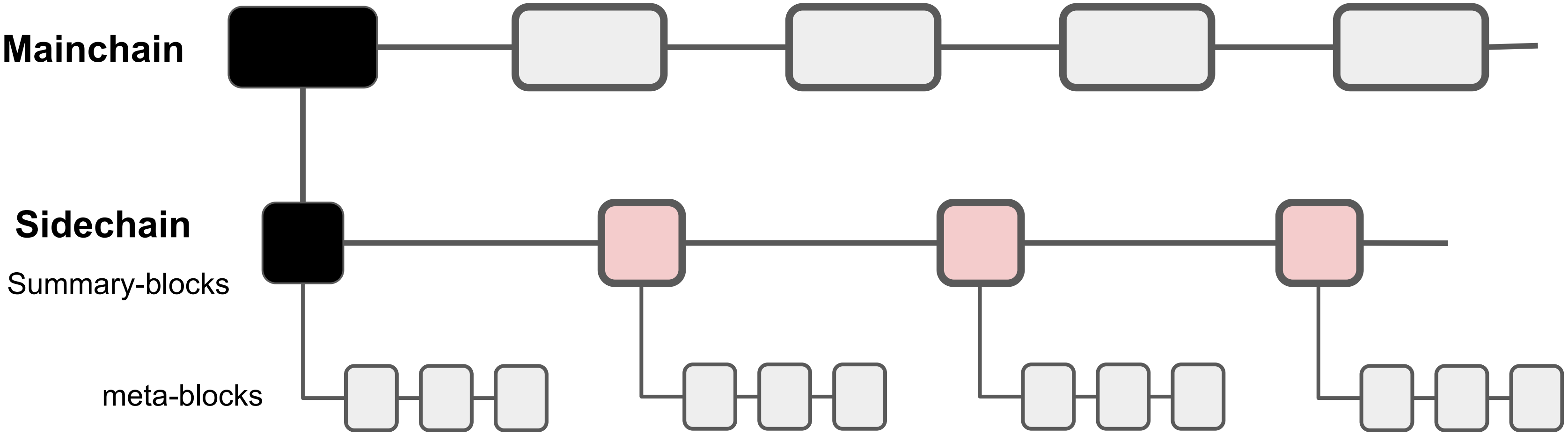
# Contributions

A formalization of decentralized resource market setting.

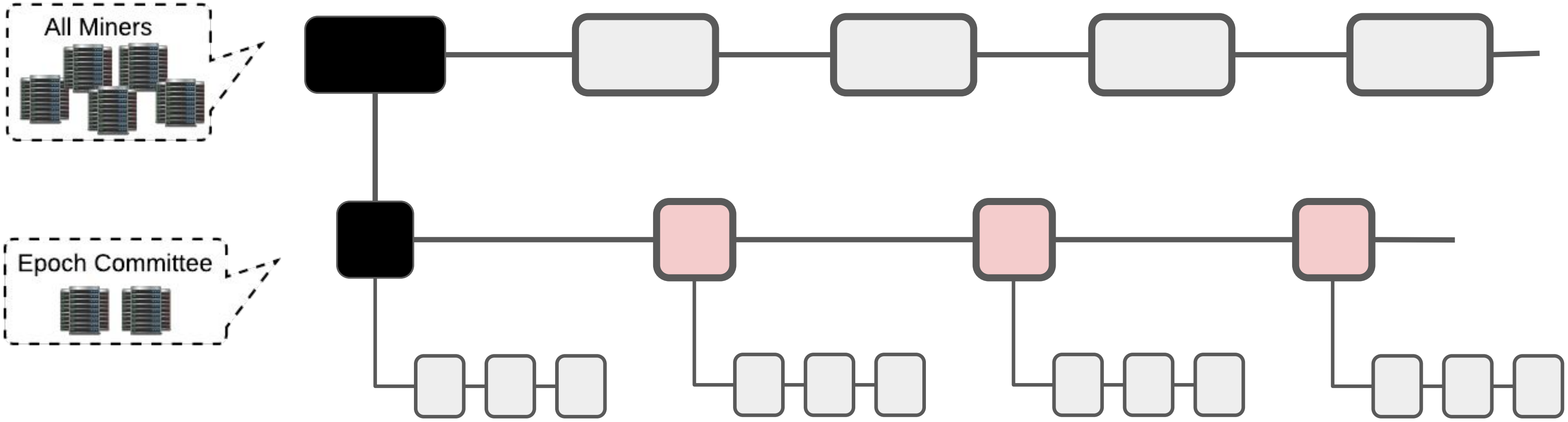
chainBoost framework: the first sidechain architecture that allow mutual-dependency relation with the mainchain!

Security analysis and end-to-end implementation/testing.

# chainBoost Framework



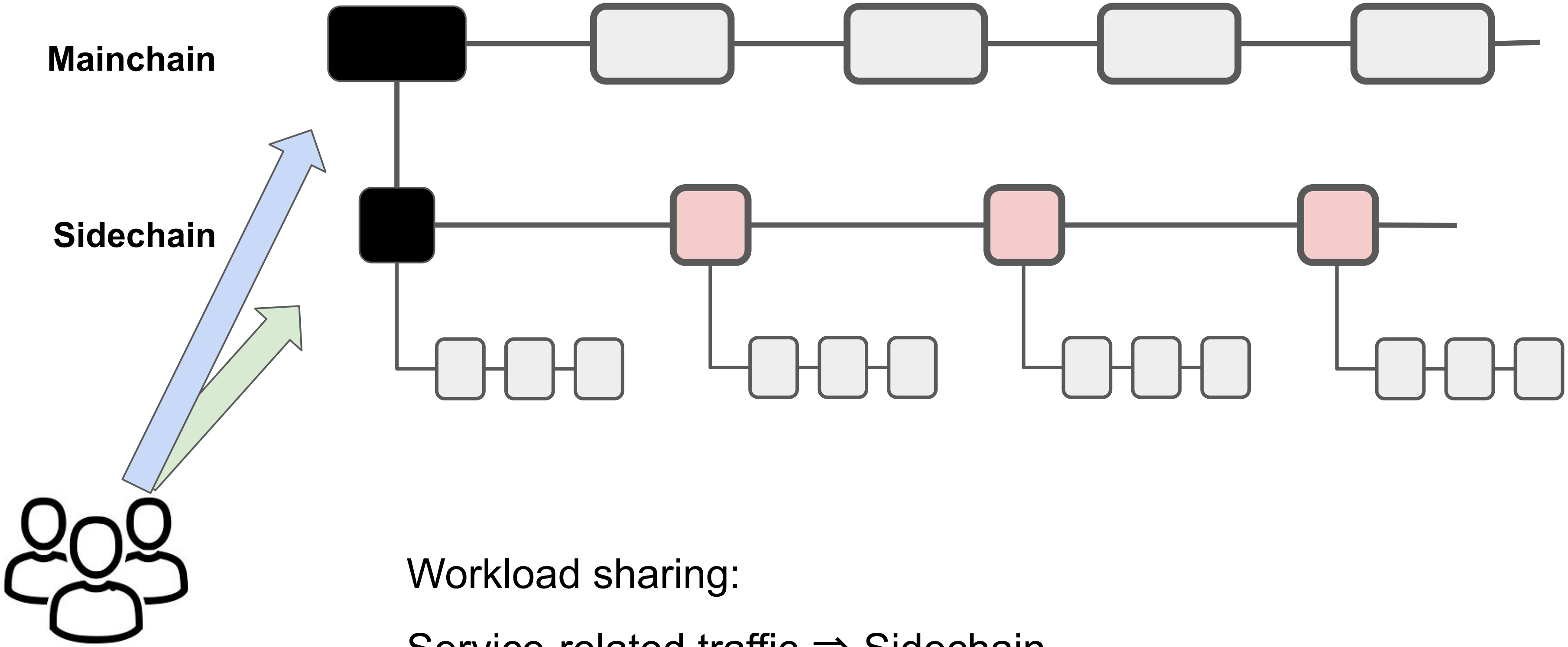
# chainBoost Framework



Works in epochs and rounds

A new sidechain committee is elected for each epoch

# chainBoost Framework

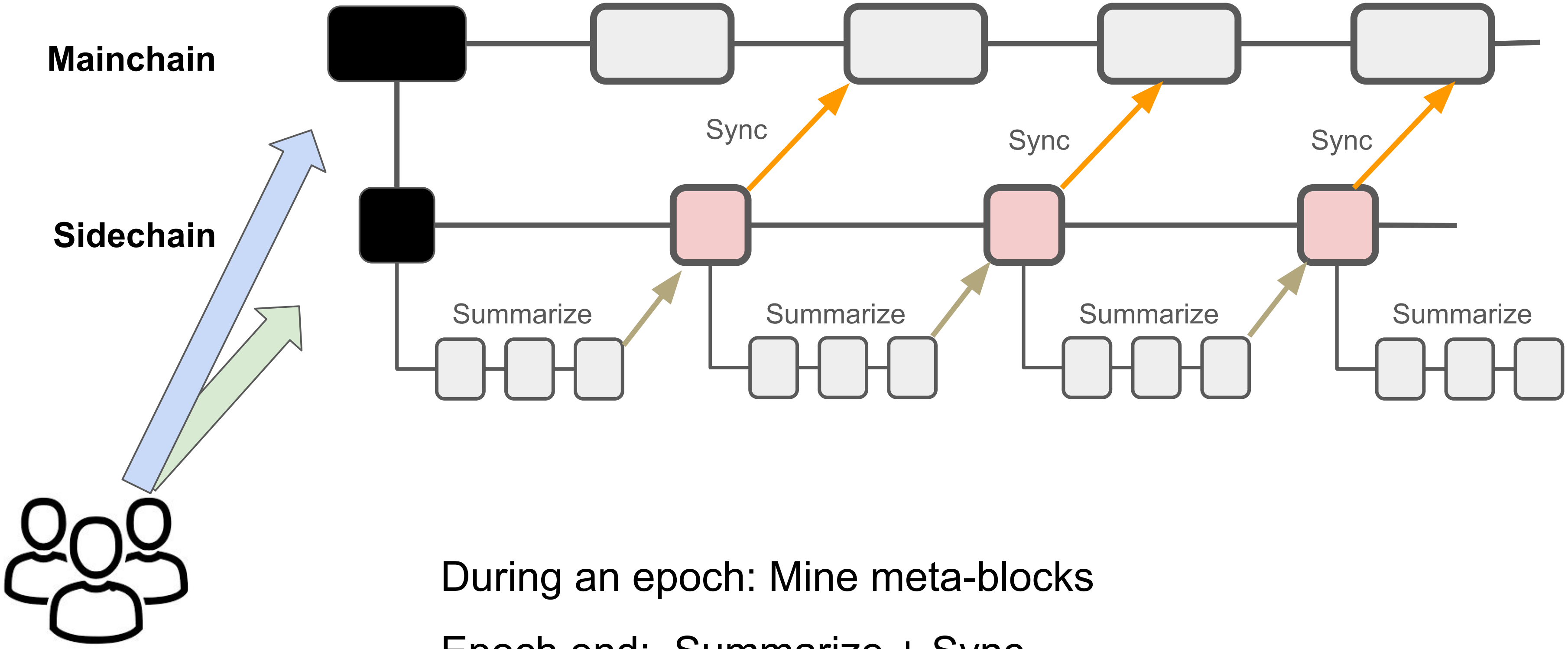


Workload sharing:

Service-related traffic ⇒ Sidechain

Rest of traffic ⇒ Mainchain

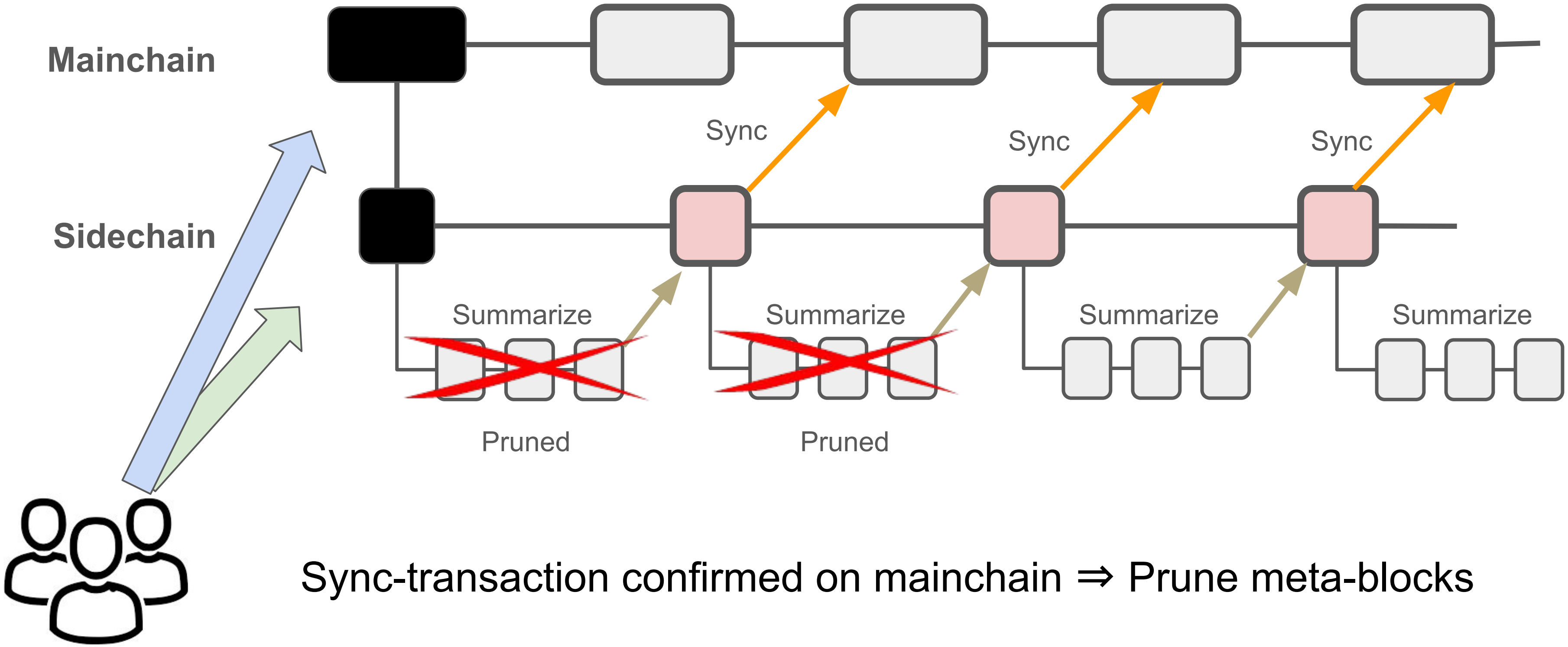
# chainBoost Framework



During an epoch: Mine meta-blocks

Epoch end:  Summarize + Sync

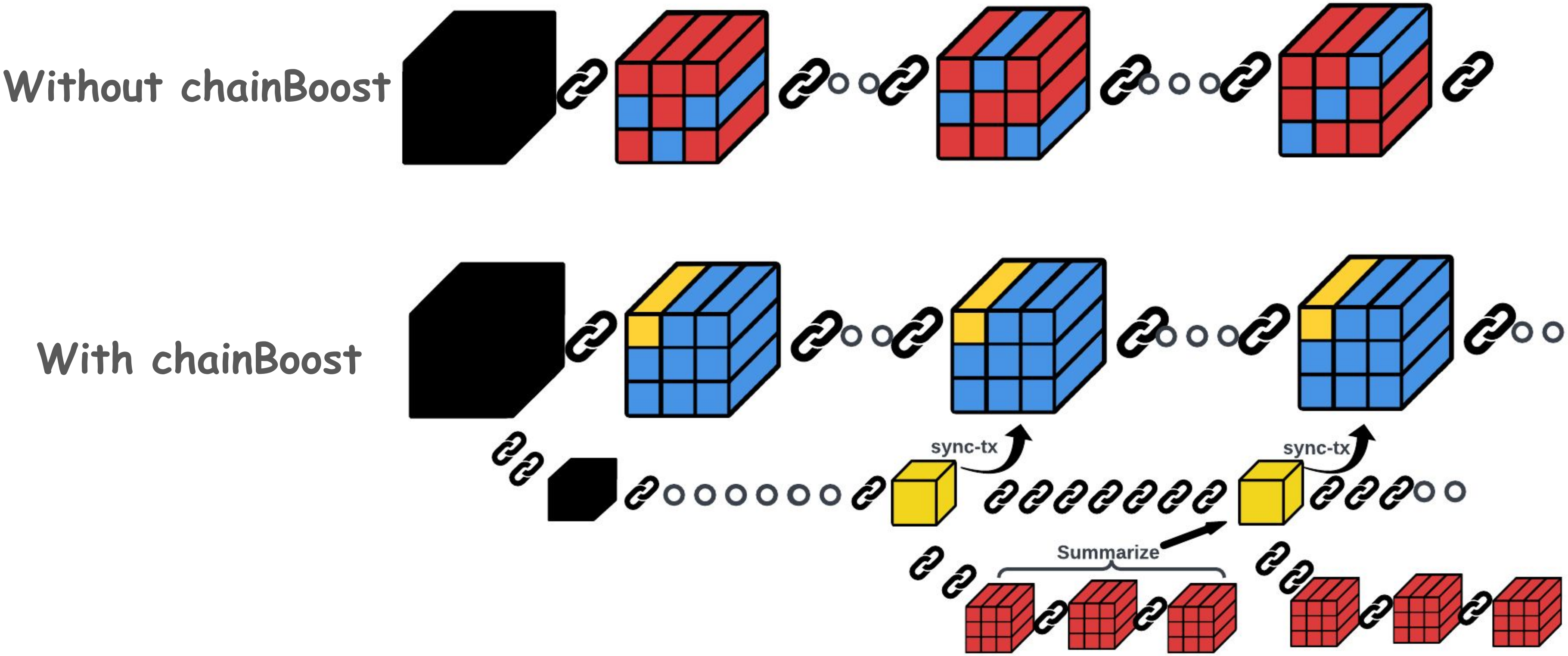
# chainBoost Framework



Sync-transaction confirmed on mainchain ⇒ Prune meta-blocks

Blockchain size
Throughput
Latency

# Performance Boosting



Service transactions are in red, others are in blue.

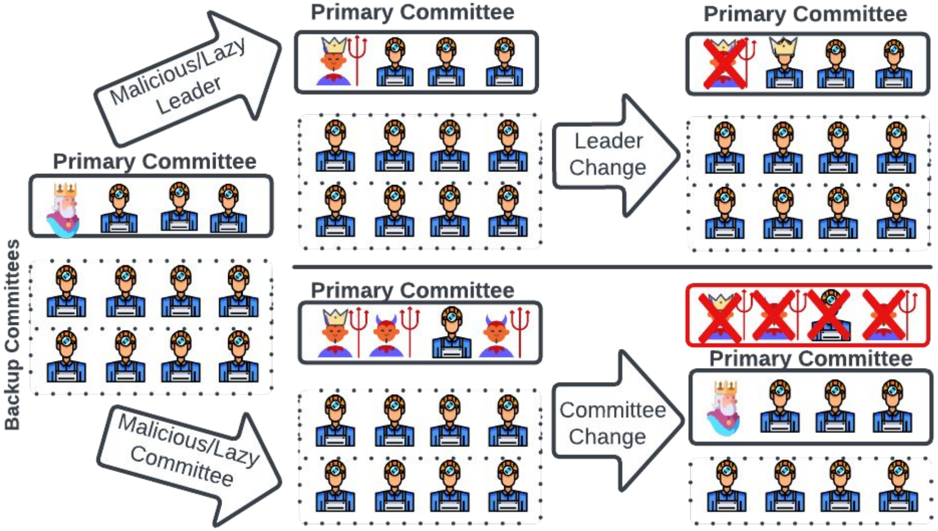
Summary-blocks and sync-transactions are in yellow.

# Summary Rules

- Generic summary rules that can be customized based on the service type.
  - Service delivery proofs ⇒ their count per server
  - Market matching ⇒ finalized contracts
  - Disputes ⇒ incident summary + result/penalty

# Robustness and Resilience

- Handling (mainchain) rollbacks.
  - Mass-syncing approach.
- Autorecovery protocol.
  - Leader change
  - Backup committees.



# Security and Performance

- **Security:**
    - We prove that chainBoost preserves safety and liveness of the underlying resource market.
- **Performance evaluation:**
    - A Filecoin-inspired use case.
    - Proof-of-concept implementation and extensive experiments.

# Implementation

- Sidechain:
  - Implemented our architecture in Go.
  - A collective signature (CoSi)-based PBFT (the BLSCoSi one from Cothority).
  - Onet for communication between miners
  - The sliding window approach from Byzcoin for committee election.
- Underlying storage market:
  - Mimic Filecoin but with compact proof-of-retrievability as proof-of-storage.
  - Traffic generation follows the traffic distribution of Filecoin.
  - Mining power on the mainchain depends on the amount of service the miners (aka storage servers) provide.
- To compare with another layer-two solution, we implemented optimistic rollups (inspired by Optimism).

# Results

- We report throughput, confirmation time, and blockchain size.
- Studied the impact of various parameters (file storage market with/without chainBoost):
  - **Network load (no. of storage contracts):** 4 - 11x throughput, ~60 - 90% reduction in latency, and up to ~90% blockchain size reduction.
  - **Block size and no. of sidechain rounds per epoch:** larger values are better.
  - **Traffic distribution:** chainBoost has utility for systems that have large workload of service-related transactions.
- Comparison with optimistic rollups:
  - Mainly it is about transaction finality (and the verifier issue).

# Conclusion and Future Work

- **This work**
  - A secure, sidechain-based scalability framework for resource markets.
  - Formal modeling.
  - Implementation/testing.
- **Future work**
  - Look into storage pricing/transaction fees.
  - Show how chainBoost can be used for other blockchain system types, e.g. tokens on top of Ethereum.

# Thank you!

# Questions?

ghada@uconn.edu
https://ghadaalmashaqbeh.github.io/

Preprint version: https://eprint.iacr.org/2024/1020