zkCross: A Novel Architecture for Cross-Chain Privacy-Preserving Auditing

Yihao Guo[1], Minghui Xu[1], Xiuzhen Cheng[1], Dongxiao Yu[1], Wangjie Qiu[2], Gang Qu[3], Weibing Wang[4], Mingming Song[4]

[1]Shandong University

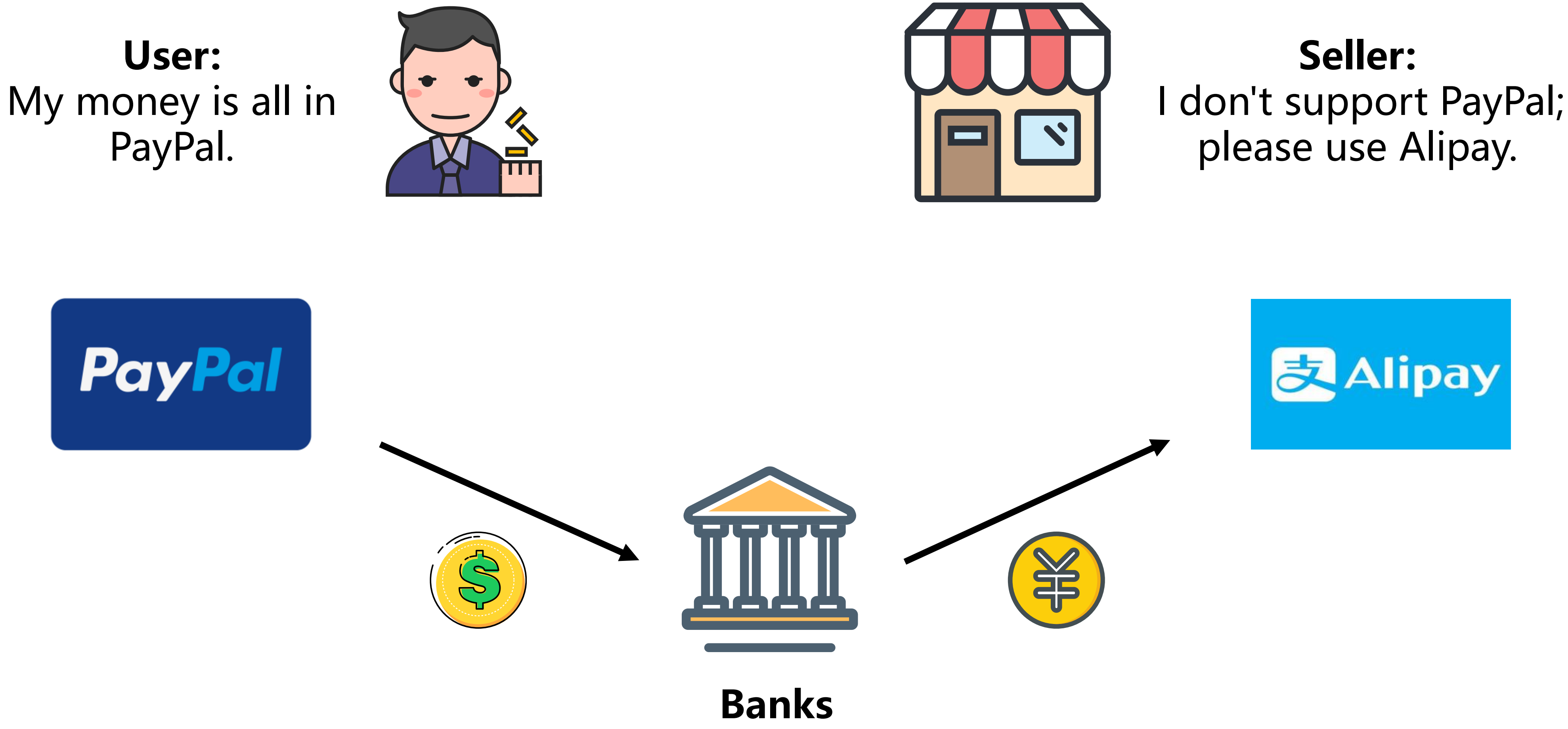
[2]Beihang University

[3]University of Maryland

[4]Cloud Inspur Information Technology Co., Ltd.

Let’s Start with a Simple Question:

- When you travel to another place, how do you spend your money locally?



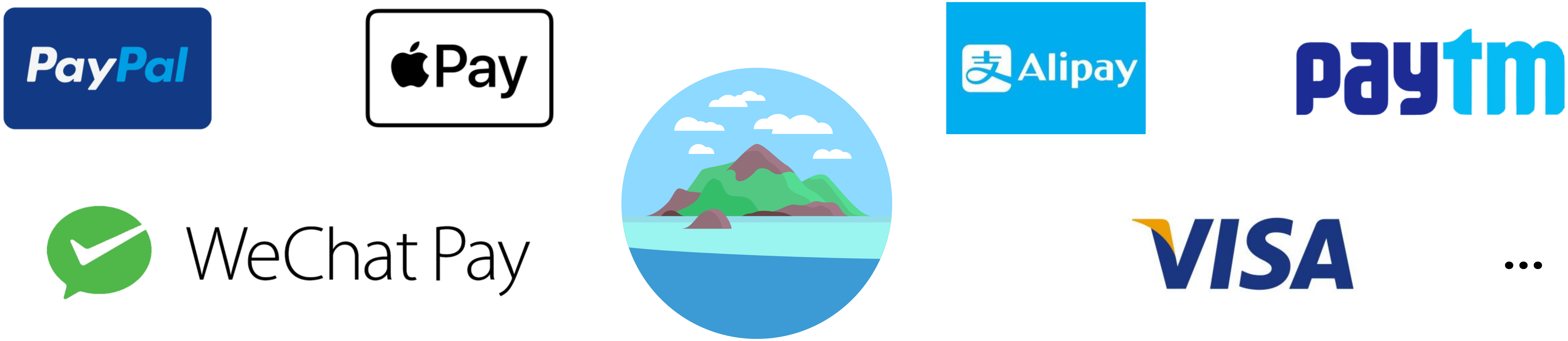
User:
My money is all in PayPal.

Seller:
I don't support PayPal; please use Alipay.

Banks

Background

- ➢ There are various payment tools worldwide, each limited to specific applications, leading to **isolated island problems**.



- ➢ Similarly, **blockchain** encounters **isolated island issues** due to varying application requirements.

Background

- As of July 2024, there are **10k+** active cryptocurrencies listed on Coin Market Cap[1], with each having a substantial market capitalization.

Bitcoin
$1187 billion

Tether
$113 billion

BNB
$80 billion

USDC
$34 billion

Ethereum
$386 billion

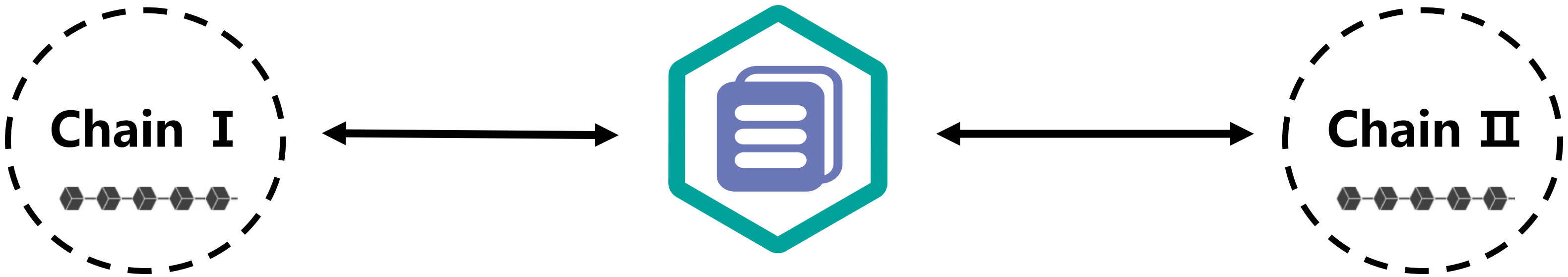
Solana
$68 billion

…

[1] https://coinmarketcap.com/

Background

- **Cross-chain technology** offers an effective solution, acting as a bridge for interactions among isolated blockchain systems[1].



Cross-chain protocols

COSMOS

Interledger

Chainlink

Polkadot

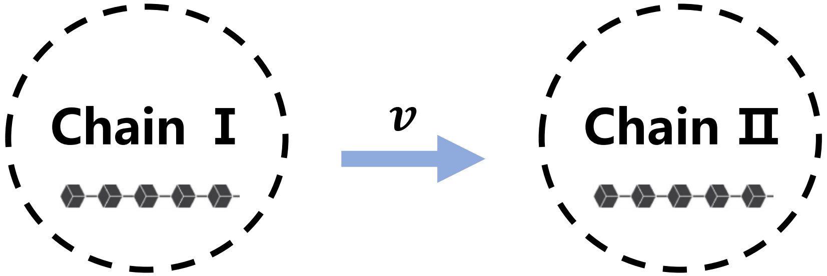
polygon

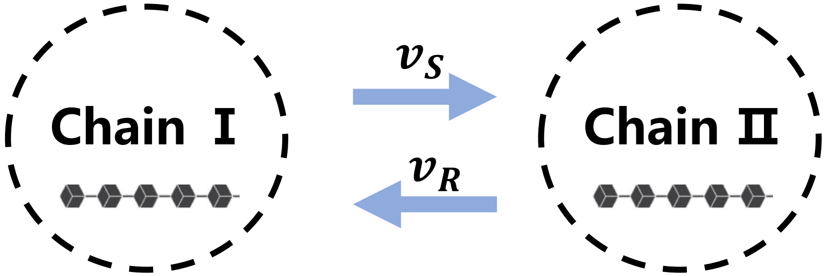
...

[1] Guo, Y., Xu, M., Yu, D., Yu, Y., Ranjan, R., & Cheng, X. (2023). Cross-Channel: Scalable Off-Chain Channels Supporting Fair and Atomic Cross-Chain Operations. IEEE Transactions on Computers.

Background

- There are two types of cross-chain activities: **cross-chain transfer** and **cross-chain exchange**.



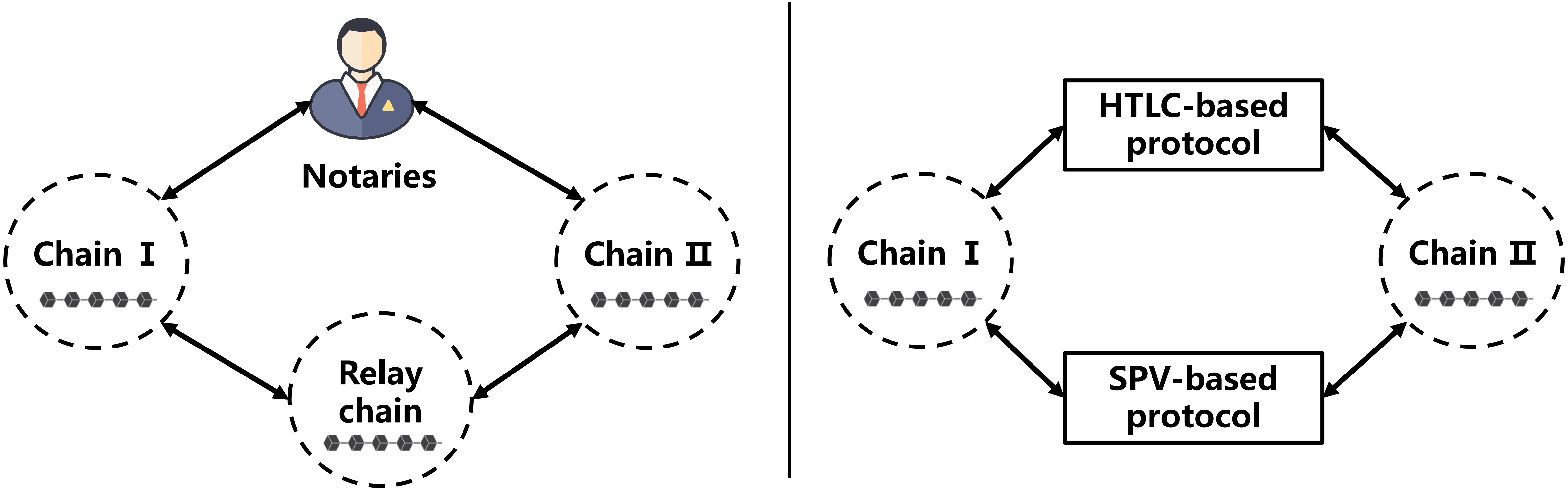


- **Cross-chain transfer** refers to the process of moving digital assets from one blockchain to another blockchain.

- **Cross-chain exchange**, also known as cross-chain swapping, is the process of exchanging digital assets between different blockchains.

Background

- Existing cross-chain protocols can be categorized into **centralized (left)** and **decentralized (right)** types based on whether a third party is introduced.



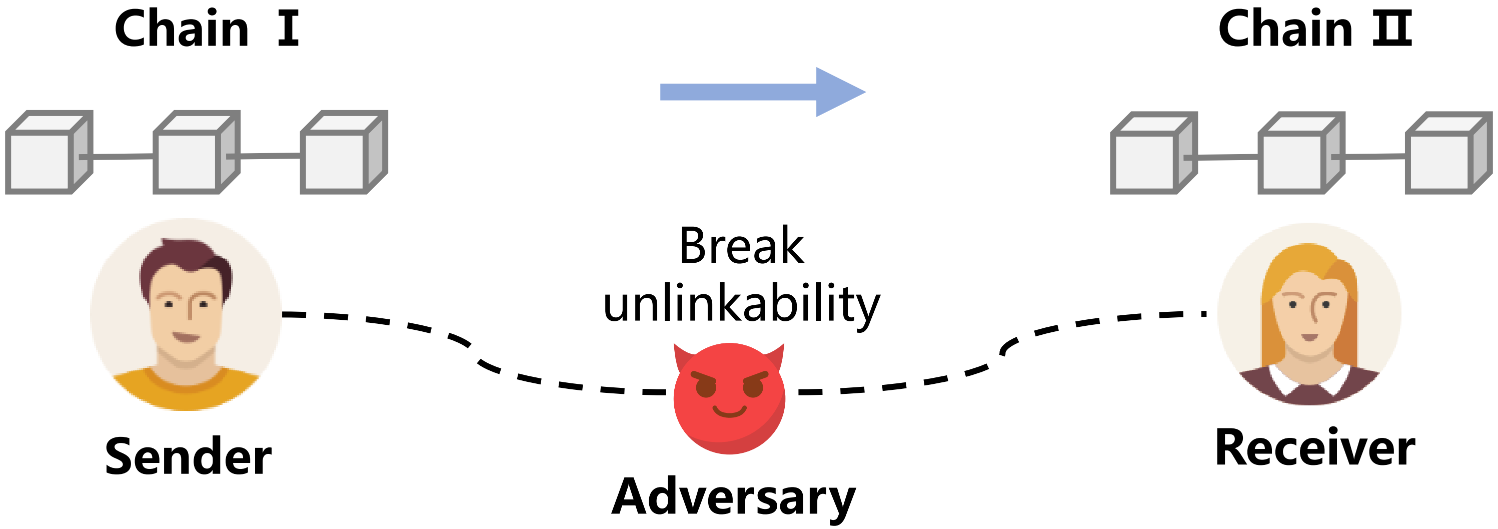
- Neglect privacy and auditing challenges in cross-chain domains.

Challenge Statement

➢ Challenge 1: Cross-chain Linkability Exposure problem (CLE)

- The compromise of unlinkability can result in the leakage of user data. According to IBM, the global average cost of a data breach in 2023 was USD **4.45 million**, a 15% increase over 3 years[1].

- **Unlinkability:** An adversary is unable to link the receiver's account from the transactions initiated by the sender, or conversely.



[1] https://www.ibm.com/reports/data-breach

Challenge Statement

➢ Challenge 2: The Incompatibility of Privacy and Auditing (IPA)

- **Privacy protection** and **auditing** often exist concurrently in a system and have conflicting ultimate goals.

- Privacy protection requires data **confidentiality**, while auditing necessitates data **transparency**. D

Confidentiality
&
Minimize data exposure

Privacy

Auditing

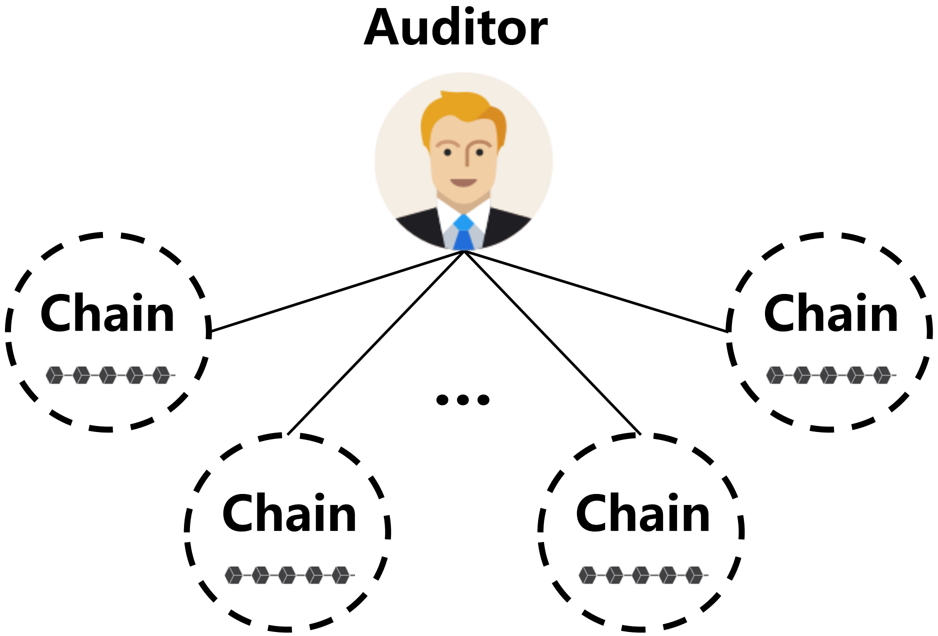
Transparency
&
Access to data

Challenge Statement

➢ Challenge 3: Full Auditing Inefficiency (FAI)

- Multiple chains with low auditing efficiency.

- The ledger sizes of Bitcoin and Ethereum have reached **500** and **700** GB[1], respectively. This implies that when auditing Bitcoin and Ethereum, an auditor requires at least **terabyte-level** storage space.

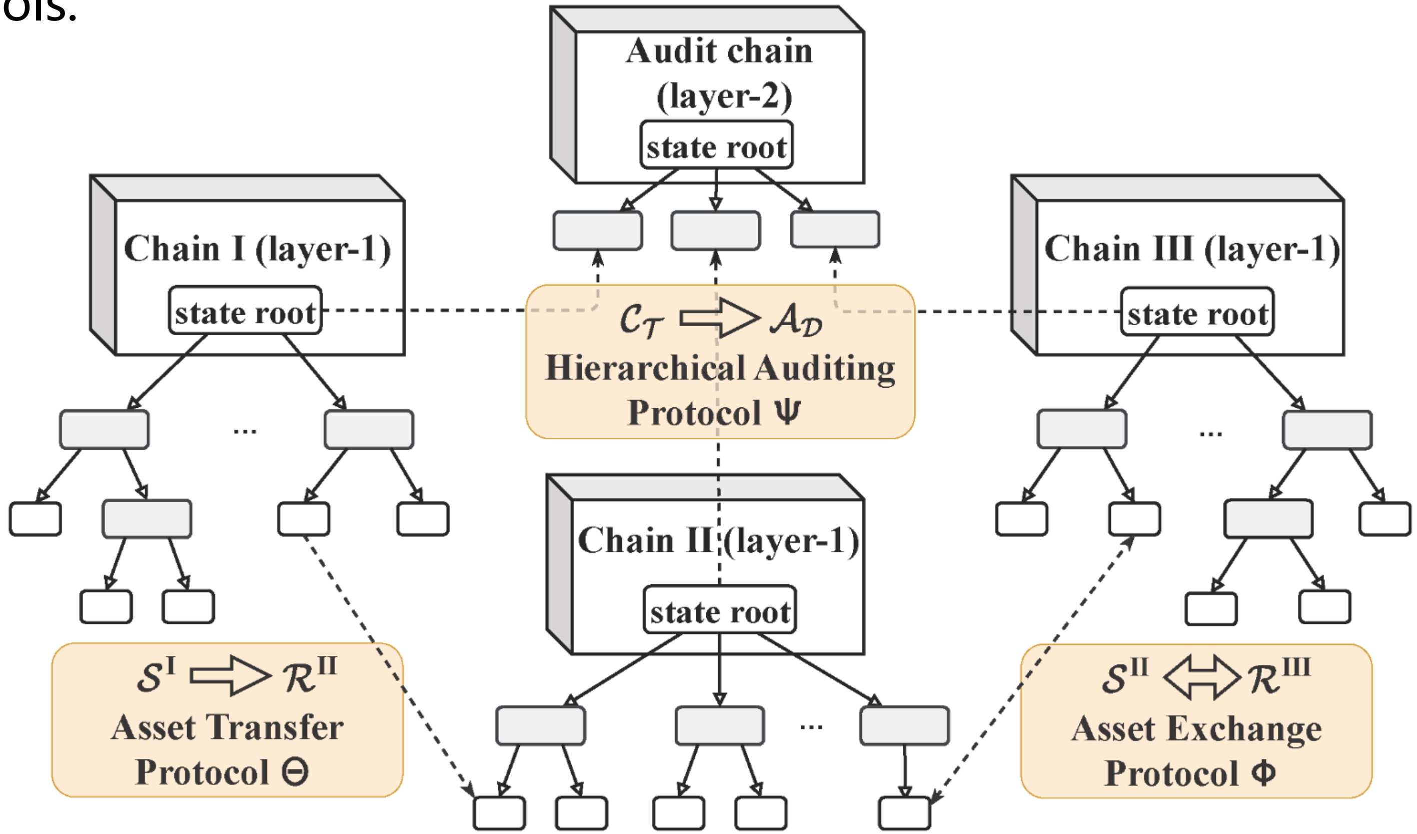


[1] Heo, J. W., Ramachandran, G. S., Dorri, A., & Jurdak, R. (2024). Blockchain data storage optimisations: a comprehensive survey. *ACM Computing Surveys*, *56*(7), 1-27.

zkCross

➢ Overview

- zkCross addresses the existing issues of CLE, IPA and FAI. It includes a two-layer architecture and three key protocols.


Audit chain (layer-2)
state root
Chain I (layer-1)
state root
Chain III (layer-1)
state root
$\mathcal{C}_\mathcal{T} \Rightarrow \mathcal{A}_\mathcal{D}$
Hierarchical Auditing Protocol Ψ
Chain II (layer-1)
state root
$\mathcal{S}^{\mathrm{I}} \Rightarrow \mathcal{R}^{\mathrm{II}}$
Asset Transfer Protocol Θ
$\mathcal{S}^{\mathrm{II}} \Leftrightarrow \mathcal{R}^{\mathrm{III}}$
Asset Exchange Protocol Φ
...

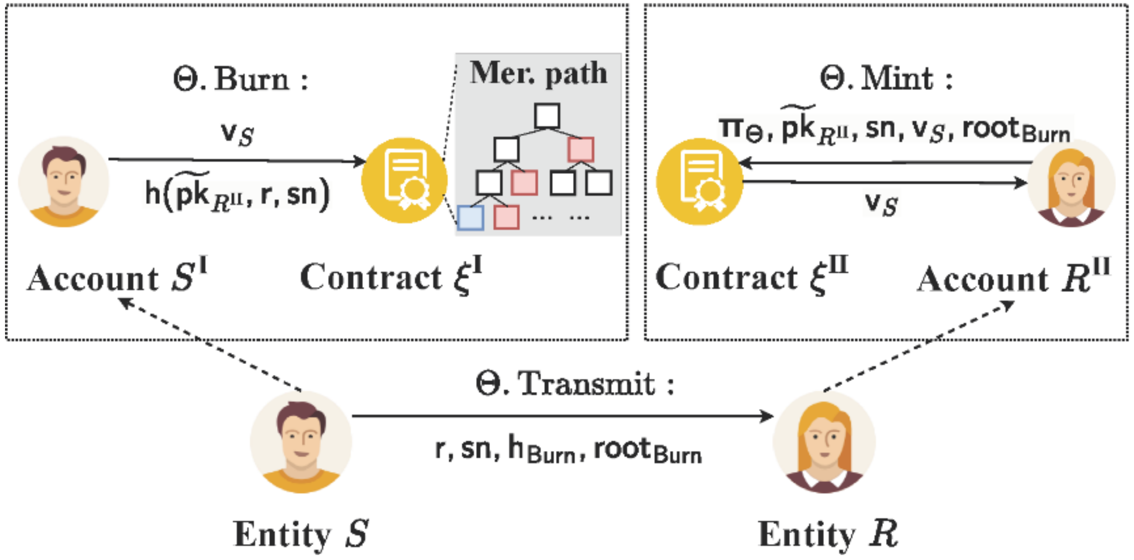
zkCross

- Technique 1: A privacy-preserving protocol for transfers
  - **Burn-S:** burn the transfer amount (a fixed denomination) and hash R's address.

    hide R's address
  - **Transmit-S:** send critical information to R in an off-chain manner.

    no on-chain information
  - **Mint-R:** generate a zero-knowledge proof based on a circuit to mint the transfer amount.

    hide S's address



Θ. Burn :
v_S
$\mathsf{h}(\widetilde{\mathsf{pk}}_{R^{\mathrm{II}}}, \mathsf{r}, \mathsf{sn})$
Mer. path
... ...
Account S^{I}
Contract ξ^{I}
Θ. Mint :
$\pi_\Theta, \widetilde{\mathsf{pk}}_{R^{\mathrm{II}}}, \mathsf{sn}, \mathsf{v}_S, \mathsf{root}_{\mathsf{Burn}}$
v_S
Contract ξ^{II}
Account R^{II}
Θ. Transmit :
$\mathsf{r}, \mathsf{sn}, \mathsf{h}_{\mathsf{Burn}}, \mathsf{root}_{\mathsf{Burn}}$
Entity S
Entity R

zkCross

➢ Technique 2: A privacy-preserving protocol for exchanges

- **Prepare-S:** generate a zero-knowledge proof based on the circuit and send it to R in an off-chain manner.

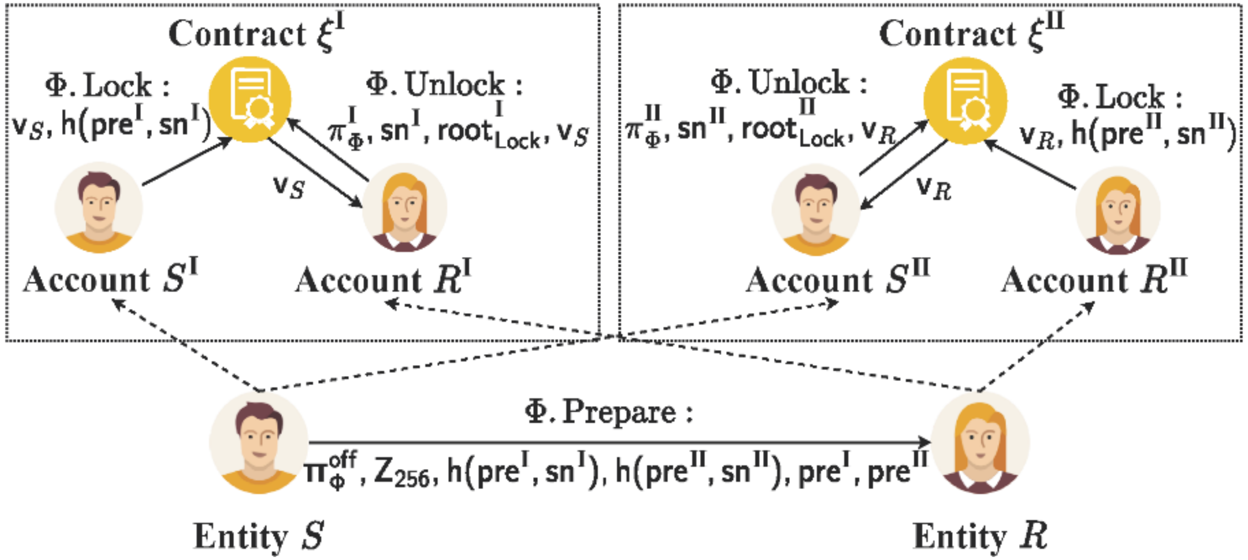
→ **no on-chain information**

- **Lock-S/R:** use independent hash locks to lock the exchange amounts (a fixed denomination).

→ **hide hash locks**

- **Unlock-S/R:** generate a proof to unlock the exchange amounts.

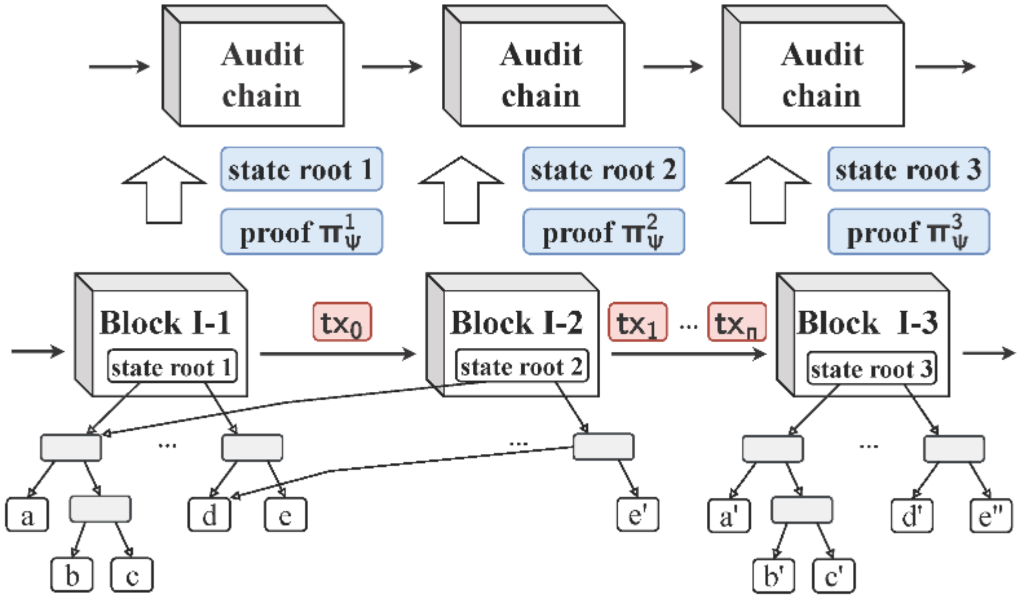
→ **hide preimages**



Contract ξ^{I}
$\Phi.\mathrm{Lock}$:
$\mathsf{v}_S, \mathsf{h}(\mathsf{pre}^{\mathrm{I}}, \mathsf{sn}^{\mathrm{I}})$
$\Phi.\mathrm{Unlock}$:
$\pi_{\Phi}^{\mathrm{I}}, \mathsf{sn}^{\mathrm{I}}, \mathsf{root}_{\mathsf{Lock}}^{\mathrm{I}}, \mathsf{v}_S$
v_S
Account S^{I}
Account R^{I}
Contract ξ^{II}
$\Phi.\mathrm{Unlock}$:
$\pi_{\Phi}^{\mathrm{II}}, \mathsf{sn}^{\mathrm{II}}, \mathsf{root}_{\mathsf{Lock}}^{\mathrm{II}}, \mathsf{v}_R$
$\Phi.\mathrm{Lock}$:
$\mathsf{v}_R, \mathsf{h}(\mathsf{pre}^{\mathrm{II}}, \mathsf{sn}^{\mathrm{II}})$
v_R
Account S^{II}
Account R^{II}
$\Phi.\mathrm{Prepare}$:
$\pi_{\Phi}^{\mathsf{off}}, \mathsf{Z}_{256}, \mathsf{h}(\mathsf{pre}^{\mathrm{I}}, \mathsf{sn}^{\mathrm{I}}), \mathsf{h}(\mathsf{pre}^{\mathrm{II}}, \mathsf{sn}^{\mathrm{II}}), \mathsf{pre}^{\mathrm{I}}, \mathsf{pre}^{\mathrm{II}}$
Entity S
Entity R

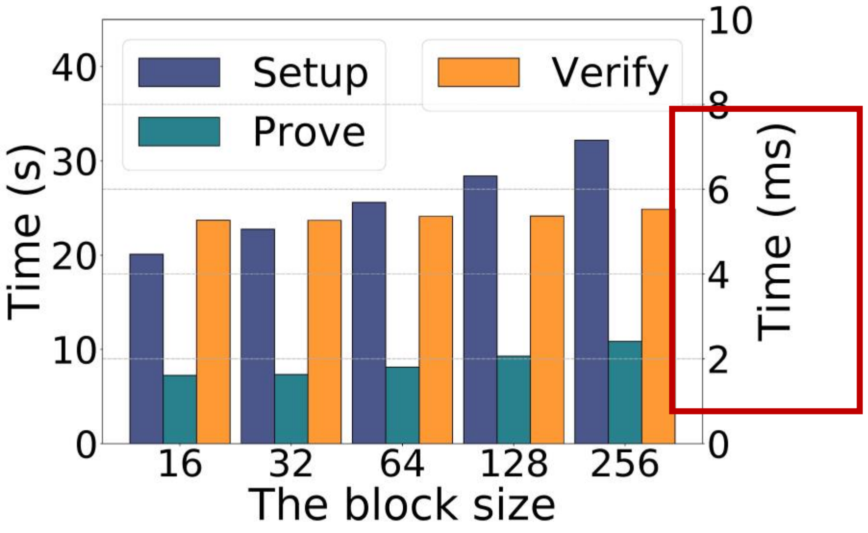
zkCross

- Technique 3: An efficient auditing protocol for auditing
  - **Initialize-C_t:** generate key parameters based on the circuit, such as the proving keys, and verification keys.
  - **Commit-C_t:** generate a proof to aggregate verification and auditing.
  - **Audit-A_d:** verify the proof uploaded by the committer.

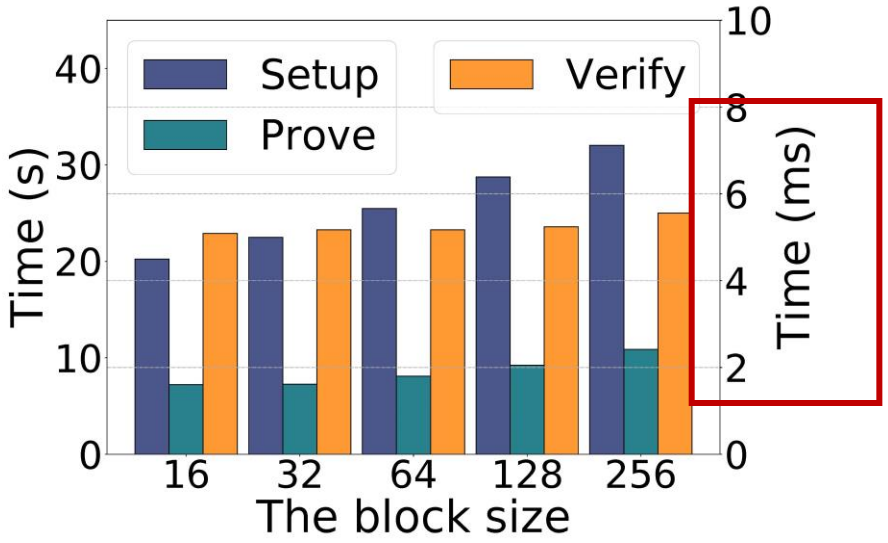


zkCross

- ➢ The performance of cross-chain transfers and exchanges
  - Run time for the initialization (Setup), generation (Prove), and verification (Verify) of proofs.



(a) The proof used for cross-chain transfers.



(b) The proof used for the Prepare phrase of cross-chain exchanges.

Setup (s)	Prove (s)	Verify (ms)
6.96	1.91	5.16

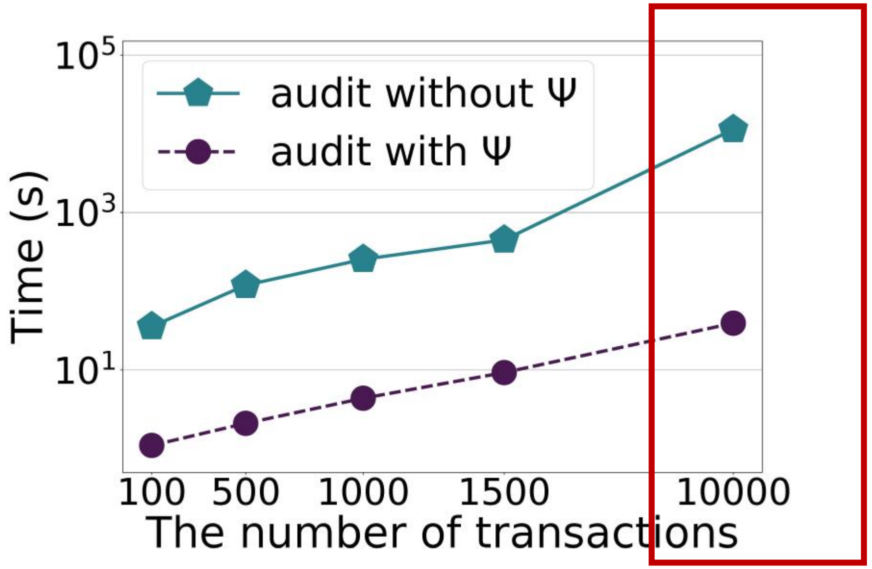
(c) The proof used for the Unlock phrase of cross-chain exchanges.

- Only the **Verify** process needs to be executed on-chain, which takes only **milliseconds**.

zkCross

➢ The performance of cross-chain auditing

- A comparative experiment on the audit efficiency: One experiment used our protocol Ψ, and the other did not.



- When the number of transactions is **10,000**, the audit time to be around **3.15 hours** without Ψ. With Ψ, the audit time is decreased to about **40 seconds** under the same condition.

zkCross

Conclusion and future work

- Conclusion
  - Identify three challenges, namely Cross-chain Linkability Exposure (CLE), Incompatibility of Privacy and Auditing (IPA), and Full Auditing Inefficiency (FAI).
  - Design two privacy-preserving protocols to solve CLE issue.
  - Introduce a efficient auditing protocol to solve IPA and FAI problems.
- Future work
  - Enhance the system's resilience against attacks while maintaining privacy.
  - Extend zkCross to support multi-layer (more than 2) auditing, thereby expanding its application scenarios.

Thank you!