Regulation-Friendly Privacy-Preserving Blockchain Based on zk-SNARK

Lei Xu, Yuewei Zhang, and Liehuang Zhu
School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China

TOC

Introduction

- A blockchain is a **distributed ledger** technology consisting of a growing list of records, called blocks, that are securely linked together using cryptography.
- Blockchain has the characteristics of **decentralization, tamper proofing, and traceability.**
- Blockchain can establish a trust relationship among different parties and has played an important role in the fields of **finance, insurance, medical care, and supply chain security.**

Introduction

Privacy

- Blockchain users in fields such as finance and medical care **do not** want their sensitive data stored on the blockchain ledger to be fully openly accessed.
- Internal data of enterprises and institutions **should not** be accessible to other collaborators without authorization.

Regulation

- Internal auditors in most companies **should** always have information about how the business is doing.
- Industries such as telecommunications and banking **must** provide information such as communication records and transaction details to the court when they receive a legal request.

Related Work

Privacy

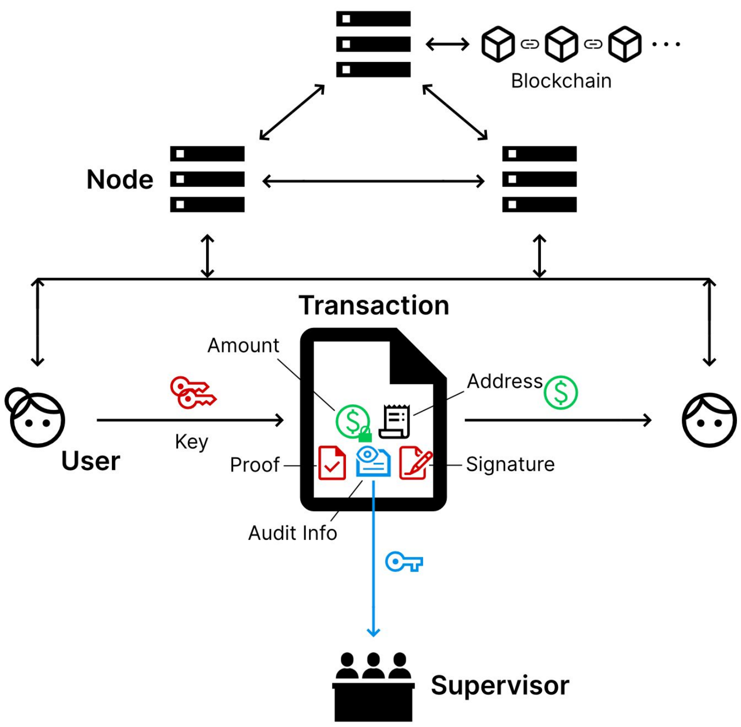
- Ring Signature
  - Monero
- Stealth Address
  - Monero
- Zero-Knowledge Proof
  - Zcash
  - Zether
- Mixing
  - Dash

Regulation

- Zero-Knowledge Proof
  - DAP
  - PAChain
  - RDAP
- Group Signature
  - PPChain
- Verifiable Encryption

Overview

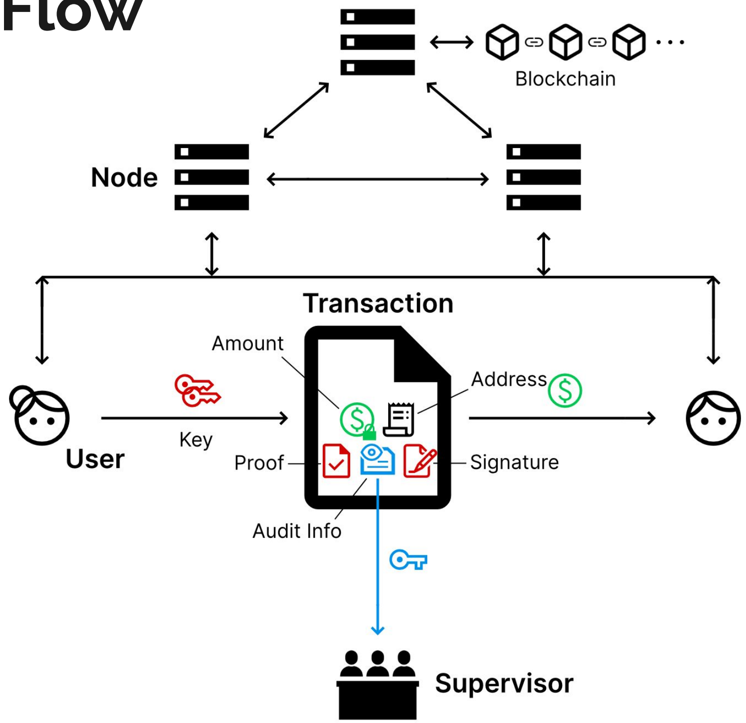
- **Account model** instead of UTXO model
- **Homomorphic encryption** to hide the transaction amounts and account balances of sender and receiver
- **Address obfuscation** to hide the identity information of both parties
- **Zero-knowledge proof** to ensure the validity of the transaction
- Supervisors can decrypt transaction details for **regulatory audit** purposes



Design Details of Transaction Flow

Transfer

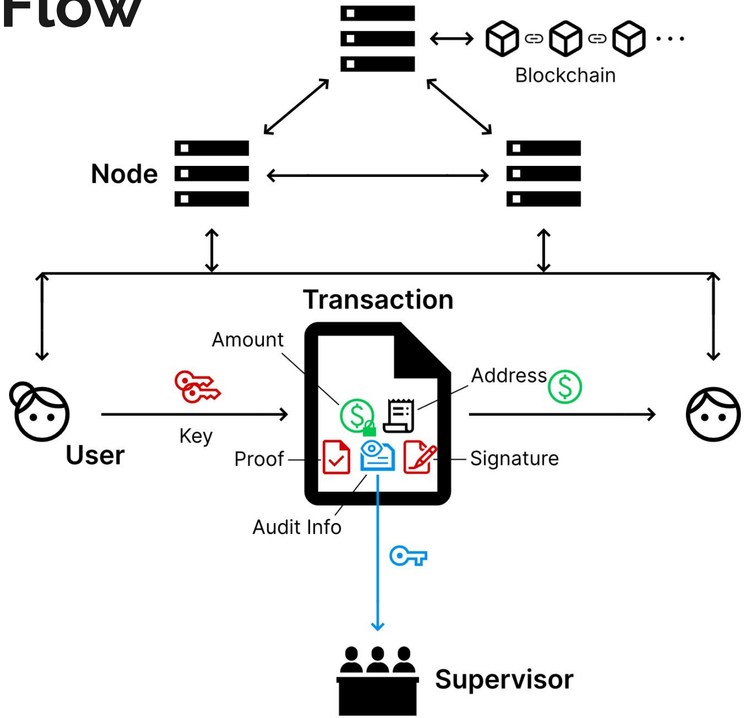
- The sender uses the private key to generate **one-time keys** and encrypts the amount with the public key
- Create **obfuscated addresses,** mixed with sender and receiver addresses
- The sender encrypts the amount, balance, its public key, and the receiver's public key with the supervisor's public key as **audit information**
- The sender uses the **zk-SNARK protocol** to prove that the transaction is valid and contains audit information, and uses a **one-time** signing key to generate a signature
- The sender constructs the transaction to call the smart contract, and the smart contract verifies the signature and zero-knowledge proof
- The smart contract uses the **homomorphic** property to update the balance of both parties and the balance of the obfuscated addresses



Design Details of Transaction Flow

Audit

- The supervisor obtains the encrypted audit information from the transaction
- Decrypts it using its private key
- Checks whether the transaction complies with regulatory rules



Design Details of Transaction Flow - ZKP

- The transfer amount a and balance b' of the transaction sender are **non-negative**
- All a-related ciphertexts are well-formed and encrypt the same value **a**
- All -a-related ciphertexts are well-formed and encrypt the same value **-a**
- All v-related ciphertexts are well-formed and encrypt the same value **0**
- **Audit information** is properly encrypted with the supervisor public key

$$\pi : \{(\mathsf{pk}, \overline{\mathsf{pk}}, \mathsf{sv}, \mathsf{pk_k}, C_L, C_R, C, D, \overline{C},$$

$$C'_L, C'_R, C', D', \overline{C'}, C_{L,k}, C_{R,k}, C_k, D_k, \overline{C_k},$$

$$C_a, C_{b'}, g; \mathsf{sk}, a, b', r) :$$

$$a \in [0, \mathsf{Max}] \wedge b' \in [0, \mathsf{Max}] \wedge$$

$$C = g^a \mathsf{pk}^r \wedge \overline{C} = g^a \overline{\mathsf{pk}}^r \wedge D = g^r \wedge$$

$$C_L / C = g^{b'} (C_R / D)^{\mathsf{sk}} \wedge$$

$$C' = g^{-a} \mathsf{pk}^r \wedge \overline{C'} = g^{-a} \overline{\mathsf{pk}}^r \wedge D' = g^r \wedge$$

$$C'_L / C' = g^{b'} (C'_R / D')^{\mathsf{sk}} \wedge$$

$$C_k = g^v \mathsf{pk_k}^r \wedge \overline{C_k} = g^v \overline{\mathsf{pk_k}}^r \wedge D_k = g^r \wedge$$

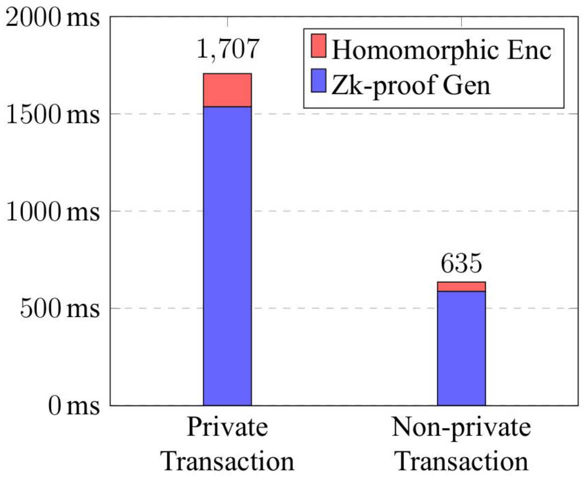
$$C_{L,k} / C_k = g^{b'} (C_{R,k} / D_k)^{\mathsf{sk}} \wedge$$

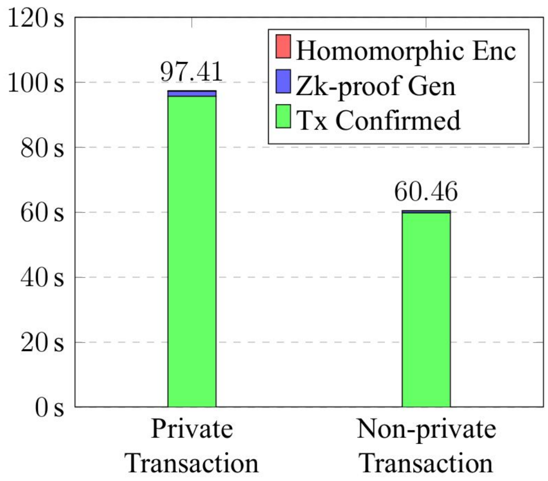
$$v = 0 \wedge \mathsf{pk} = g^{\mathsf{sk}} \wedge$$

$$C_a = g^a \mathsf{sv}^r \wedge C_{b'} = g^{b'} \mathsf{sv}^r \wedge$$

$$C_{\mathsf{pk}} = g^{\mathsf{pk}} \mathsf{sv}^r \wedge C_{\overline{\mathsf{pk}}} = g^{\overline{\mathsf{pk}}} \mathsf{sv}^r\}, \forall k \in [0, n]$$

Performance Analysis





- The time consumed by cryptographic operations such as homomorphic encryption and zero-knowledge proof is short enough, and the performance of private transactions is acceptable.
- Compared with non-private transactions, the additional computation required by private transactions is not time-consuming and will not become a significant bottleneck.

Conclusion

- The innovation of the proposed system lies in the use of the account model and zk-SNARK protocol, the regulatory process is efficient and easy to use, taking into account the needs of privacy protection and regulatory support, and the time overhead is low.
- The proposed system can further expand the application scenarios of blockchain and play a role in industries with strict regulatory requirements and high privacy protection requirements.

Thanks

Lei Xu, Yuewei Zhang, and Liehuang Zhu

School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China