Poster: An Offline Delegatable Cryptocurrency System

Rujia Li *†, Qin Wang ‡§, Xinrui Zhang ¶, Qi Wang *, David Galindo †, Yang Xiang ‡
* *Southern University of Science and Technology*, Shenzhen, 518055, Guangdong, China.
† *University of Birmingham*, Edgbaston, B15 2TT, Birmingham, United Kingdom.
‡ *Swinburne University of Technology*, Melbourne, VIC 3122, Australia.
§ *CSIRO Data61*, Sydney, NSW 2015, Australia.
¶ *Nankai University*, Tianjin, 300350, China.

***Abstract*—In this poster, we propose an offline delegatable cryptocurrency system. We exploit the trusted execution environments (TEEs) as the decentralized "virtual agents" to prevent malicious delegation. In our scheme, an owner can delegate his coins through offline-transactions without interacting with the blockchain network. The implementation and preliminary evaluation demonstrate that our scheme is practically feasible.**

***Index Terms*—Cryptocurrency, TEEs, Offline Delegation**

I. Introduction

Blockchain-based cryptocurrencies significantly facilitate the convenience of payment by providing a decentralized online solution for customers. However, merely online processing of transactions confronts the problem of low performance and high congestion. Offline delegation provides an alternative way to mitigate the issue by enabling users to exchange the coin [1]. Unfortunately, offline delegations still have risks caused by unreliable participants. The misbehaviors may easily happen due to the absence of effective supervision. As an example, let us start from a real scenario: imagine that Bob, a nine-year-old wild teenager, wants some digital currency (*e.g.*, BTC) to buy a film ticket from his father, Alex. According to current decentralized cryptocurrency payment technologies [2][3], Alex has two delegation approaches: (1) *coin-transfer,* Alex asks for Bob's BTC address, and then Alex transfers a specific amount of coins to Bob's address. (2) *ownership-transfer,* Alex directly gives his own private key to Bob.

We observe that both approaches suffer drawbacks. For the first approach, coin-transfer requires a global consensus of the blockchain, which makes it time-consuming. Moreover, moving the coins through the blockchain network will be charged with certain fees [2][3]. For the second approach, ownership-transfer highly relies on the honesty of the delegatee. The promise between the delegator and delegatee depends on their trust or relationship, which is vulnerable and weak. The delegatee may spend all the coins in the address, or spend the coins for other purposes. Back to the example, Alex's original intention is to give Bob $ 10 to buy a film ticket, but Bob may spend all the coins to purchase his favourite toys. These two types of approaches represent most of the mainstream schemes ever aiming to achieve a secure delegation, but none of them provides a satisfactory solution.

In this poster, we propose *DelegaCoin*, an offline delegatable electronic cash system. We utilize the trusted execution environments (TEEs) to play the role of decentralized "virtual agents". TEEs prevent malicious delegation of the coins (*e.g.* double-delegation on the same coins). As shown in Figure 1, the proposed system allows the owner to share their coins without interacting with the blockchain or any trusted third parties. The owner is able to directly delegate specific amounts of coins to others by sending them through a secure channel.

II. DelegaCoin

In DelegaCoin, three types of entities are involved: coin owner (delegator) $\mathcal{O}$, coin delegatee $\mathcal{D}$, and blockchain $\mathcal{B}$. The main idea behind DelegaCoin is to exploit the TEEs as decentralized agents between the owner and delegatee.

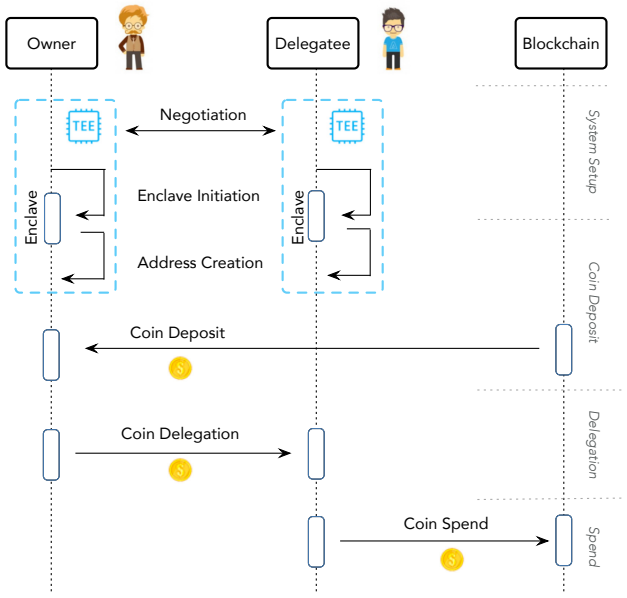


Figure 1. DelegaCoin Overview

Firstly, both $\mathcal{O}$ and $\mathcal{D}$ initialize and run their enclaves, and $\mathcal{O}'s$ enclave generates an address addr with a private key maintained internally. Next, $\mathcal{O}$ deploys delegation policies into the owner $\mathcal{O}'s$ enclave and deposits the coins to the address addr. Then, $\mathcal{O}$ delegates the coins to $\mathcal{D}$ by triggering

the execution of delegation policies inside the enclave. After that, $\mathcal{D}$ spends the delegated coins through broadcasting the decrypted transaction to the blockchain network $\mathcal{B}$. Detailed descriptions are shown as follows.

System Setup. $\mathcal{O}$ and $\mathcal{D}$ initialize their TEEs to provide environments for the operations with respect to the delegation.

Negotiation. $\mathcal{O}$ negotiates with $\mathcal{D}$ for initial setup.

Enclave Initiation. $\mathcal{O}$ and $\mathcal{D}$ initialize the enclave $E_{\mathcal{O}}$ and $E_{\mathcal{D}}$. Then, $E_{\mathcal{O}}$ and $E_{\mathcal{D}}$ create their internal keys.

State Retrieve. The encrypted states are read back to $E_{\mathcal{O}}$ under the sealing key.

Coin Deposit. $E_{\mathcal{O}}$ generates an address addr and corresponding private key. The private key is stored inside TEEs memory. After that, $\mathcal{O}$ deposits addr.

Address Creation. $\mathcal{O}$ calls $E_{\mathcal{O}}$ to generate a transaction address addr. The corresponding private key is secretly stored and is generated by an internal pseudo-random number.

Coin Deposit. $\mathcal{O}$ generates an arbitrary transaction and transfers coins to addr as the fund deposits. This step is executed through online blockchain transactions.

Coin Delegation. Neither $\mathcal{O}$ nor $\mathcal{D}$ needs to interact with blockchain. $\mathcal{O}$ can instantly complete the coin delegation through an offline transaction.

Transaction Generation. Once receiving a delegation request from $\mathcal{O}$, $E_{\mathcal{O}}$ creates a transaction Tx with a valid signature.

Balance Update. $E_{\mathcal{O}}$ checks current balance to ensure that it is enough for deduction. Then, $E_{\mathcal{O}}$ updates the balance.

Coin Delegation. $E_{\mathcal{O}}$ encrypts Tx, and sends the encrypted transaction C_{Tx} to $\mathcal{D}$ through a secure channel created by remote attestation.

State Seal. Once completing the delegation, the delegated records are required to permanently stored outside the enclave. If any aborts or halts happen, a re-initiated enclave starts to reload the missing information.

Coin Spend. $\mathcal{D}$ decrypts C_{Tx}, and forwards the decrypted transaction Tx to the blockchain network.

III. Security Discussion.

DelegaCoin aims to employ TEEs to provide a secure delegatable cryptocurrency system. In brief, TEEs prevent malicious delegation in three aspects: (1) The private key of a delegated transaction and the delegated transaction itself are protected against the public. If an adversary learns any knowledge about the private key or the delegated transaction, she may spend the coin before the delegatee uses it; (2) The local trusted environments and strict measurements ensure correct execution of delegation protocol. In particular, the spendable amounts of delegated coins must be less than (or equal to) original coins; (3) The sealing technologies guarantee the consistency of the delegation, which prevents fund loss or theft caused by the accidental TEEs failure.

IV. Implementation & Evaluation

We implement a prototype with three types of entities: the owner node, the delegatee node, and the blockchain system. The owner node and the delegatee node are separately running on two computers. The codes are developed in C++ using the Intel® SGX SDK 1.6 under the operating system of Ubuntu 20.04.1 LTS. For the blockchain network, we adopt the Bitcoin testnet [4] as the prototype platform.

We test the main functionalities including *system setup*, *coin deposit*, *coin delegation* and *coin spend*. We observe that the enclave initiation spends much more time than (transactions) key pair generations. Fortunately, the time used on enclave initiation can be omitted since the enclave each time launches only once (one-time operation). The operations of transaction generation and remote attestation takes about 6.8 and 19.5 seconds, respectively. This is much more efficient than the time consumed in BTC. The operations of coin deposit and transaction confirmation depend on the configuration of the Bitcoin testnet, varying from 10+ seconds to several minutes. We omit them in our local testing environment.

Table I
THE AVERAGE TIME OF VARIOUS OPERATIONS

Phase	Operation	Average Time / ms
System setup	Enclave initiation	13.18940
	Public key generation (Tx)	0.34223
	Private key generation (Tx)	0.01119
Coin deposit	Address creation	0.00690
	Coin deposit	–
Coin delegation	Transaction generation	6.88361
	Remote attestation	19.50990
	State update	0.00366
	State seal	5.43957
Coin spend	Transaction decryption	3.98275
	Transaction confirmation	–

V. Conclusion

In this poster, we provide a secure and practical way to realize an offline delegatable cryptocurrency system. In our design, The TEEs are used as the primitive tools to establish secure delegation channels and offer better storage protections of metadata (keys and policies). An owner can delegate the coin through an offline-transaction asynchronously with blockchain. Furthermore, we present an implementation with the help of Intel® SGX and Bitcoin testnet. The preliminary evaluation demonstrates that our scheme is practically feasible.

References

[1] Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. Sok: Layer-two blockchain protocols. In International Conference on Financial Cryptography and Data Security, pages 201–226. Springer, 2020.

[2] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[3] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. In Ethereum Project Yellow Paper, 2014.

[4] Bitcoin testnet. In https://coinfaucet.eu/en/btc-testnet/, 2020.

Poster: An Offline Delegatable Cryptocurrency System

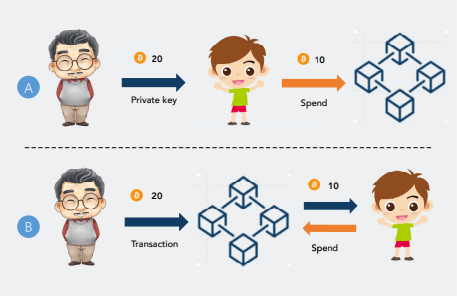
Rujia Li[1,2], Qin Wang[3,4], Xinrui Zhang[5], Qi Wang[1], David Galindo[2], Yang Xiang[3]

1.*Southern University of Science and Technology*; 2.*University of Birmingham*; 3.*Swinburne University of Technology*; 4.*CSIRO Data61*; 5.*Nankai University*

Research Problem

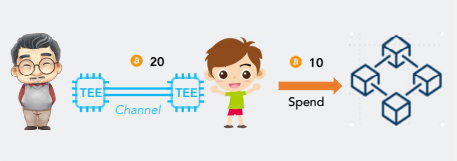
Cryptocurrencies delegation:

- **A. ownership transfer:** Coin owner loses control of the rest of coins.
- **B. coin transfer:** Time-consuming and costly (transaction fee [1]).



Our Solution

An offline delegatable cryptocurrency system exploiting TEEs [2].

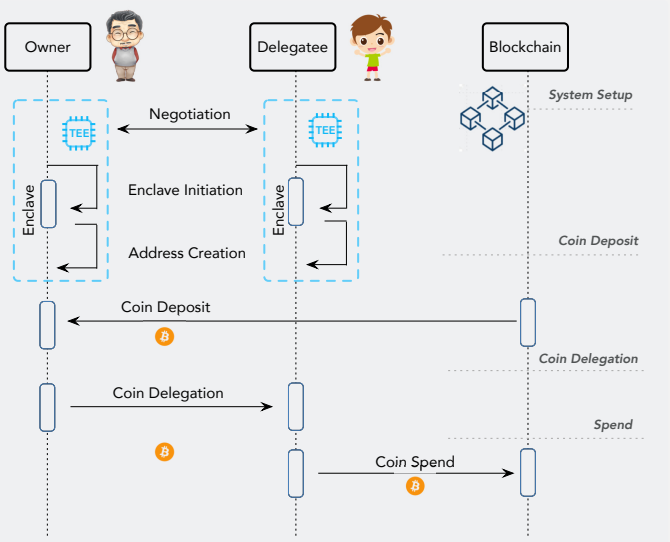


Properties

- Offline-transferable;
- Owner auditable;
- Double-spending prevented;
- Efficient and costless.

Protocol

TEEs are employed as decentralized agents between coin owner and coin delegatee.



- **System setup.** The coin owner and the delegatee initialize their TEEs.
  - Negotiation. The owner negotiates with the delegatee for delegation policies.
  - Enclave Initiation. The owner and delegatee create their enclaves $E_{\mathcal{O}}$ and $E_{\mathcal{D}}$.
  - State Retrieve. The owner calls $E_{\mathcal{O}}$ to retrieve the sealed state.
- **Coin Deposit.** The coin owner deposits coins through a standard online transaction.
  - Address Creation. The owner calls $E_{\mathcal{O}}$ to generate a transaction address.
  - Coin Deposit. The owner transfers some coins to the address.
- **Coin Delegation.** The coin owner completes the coin delegation.
  - Transaction Generation. The owner calls $E_{\mathcal{O}}$ to create a delegation transaction Tx.
  - Balance Update. The enclave $E_{\mathcal{O}}$ updates the new balance.
  - Coin Delegation. The enclave $E_{\mathcal{O}}$ sends Tx to the delegatee (remote attestation).
  - State Seal. The enclave $E_{\mathcal{O}}$ stores the delegated records into the disk.
- **Coin Spend.** The delegatee forwards Tx to the blockchain network.

Performance Evaluation

The performance of various operations.

Operation	Average Time / ms
Enclave initiation	13.18940
Public key generation (Tx)	0.34223
Private key generation (Tx)	0.01119
Address creation	0.00690
Coin deposit	—
Transaction generation	6.88361
Remote attestation	19.50990
State update	0.00366
State seal	5.43957
Transaction decryption	3.98275
Transaction confirmation	—

Security Analysis

TEEs prevent the delegated coin from

- double-spending attack;
- man-in-middle attack;
- adversary's replay attack.

References

[1]. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[2]. McKeen, Frank, Ilya Alexandrovich, Alex Berenzon, Carlos V. Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Savagaonkar. "Innovative instructions and software model for isolated execution." Hasp@ isca 10, no. 1 (2013).