UCoin An Efficient Privacy Preserving Scheme for Cryptocurrencies

ABSTRACT

In cryptocurrencies, privacy of users is preserved using pseudonymity. However, it has been shown that pseudonymity does not result in anonymity if a user’s transactions are linkable. This makes cryptocurrencies vulnerable to deanonymization attacks. The current solutions proposed in the literature suffer from at least one of the following issues: (1) requiring a trusted third–party entity, (2) poor performance, and (3) incompatible with the standard structure of cryptocurrencies. In this paper, we propose Unlinkable Coin (UCoin), a secure mix–based approach to address these issues. In UCoin, the link between the input (payer) and output (payee) addresses in a transaction is broken. This is done by mixing the transactions of multiple users into a single aggregated transaction in which the output addresses have been secretly shuffled. In our protocol design, we first develop HDC–net, a secure shuffling protocol that enables a group of users to anonymously publish their data. Then, we deploy the proposed HDC–net protocol in the UCoin architecture (as a mixing unit) to generate the aggregate transactions. We show that UCoin (1) does not rely on a trusted third–party, (2) can mix 50 transactions in 6.3 seconds that is 18% faster than the current solutions, and (3) is fully compatible with the architecture of

cryptocurrencies.

**EXISTING SYSTEM**

In this section, we present a brief literature review of anonymity and privacy in cryptocurrencies. We review the related research work in three main categories.

**(1) Cryptocurrencies that provide anonymity by design**: A number of cryptocurrencies have been proposed in the literature that inherently provide anonymity for users, i.e. privacy preserving issues have been considered in their design. In CryptoNote [13], ring signatures are used to group the users’ addresses. The users in the group employ non–interactive zero–knowledge proofs to generate a ring signature. To verify this ring signature, all the public keys of the users in the group are required. Thus, it is not feasible to determine which address belongs to a specific user. However, in CryptoNote, a larger group size results in a transaction with a larger size [8], [16].

In Zerocoin [14], the link between transactions are hidden using non–interactive zero–knowledge Proofs. It works based on a decentralized setting, thus, it does not require any trusted party. The Schnorr [29] technique is used for the zero–knowledge proofs. However, Zerocoin does not hide amounts and destinations of payments [10]. To address these issues, Ben-Sasson et al. [10] proposed Zerocash, a fully-developed ledger–based cryptocurrency. In Zerocash, Zero Knowledge Succinct Non–interactive ARguments of Knowledge (zk–SNARK) [30] is employed to hide not only inputs but also outputs and amount of a transaction. Due to the use of zkSNARKS, Zerocash needs a one–time parameter setup performed by a trusted party. This makes it dependant on a trusted party [16], [8].

**(2) Privacy–preserving protocols developed for Bitcoin**: These protocols are added as an extension to the Bitcoin architecture to provide anonymity for the users. CoinShuffle++ proposed by Ruffing et al. [16] is a decentralized mixing protocol designed for Bitcoin users specifically. Coin- Shuffle++ works based on DiceMix, a peer–to–peer mixing protocol proposed in the same paper. In fact, DiceMix is

applied on Bitcoin to make transactions unlinkable. Coin- Shuffle++ is simpler and more efficient than its predecessor, CoinShuffle [15]. In CoinParty [17, 18], a number of peers are selected to perform as mixing peers to provide unlinkability for the Bitcoin transactions. It uses threshold variant of the Elliptic Curve Digital Signature Algorithm (ECDSA) to aggregate coins by a threshold transaction in the commitment phase before the final address shuffling is performed. SecureCoin [19] is another privacy preserving protocol that is fully compatible with Bitcoin. It shuffles the destination addresses of Bitcoin transactions using public key encryption. The employed technique is similar to the onion routing [25] protocol. Unlike CoinParty, SecureCoin does not require any mixing peer. Thus, it is not vulnerable to disruptions that may be conducted by mixing peers. However, SecureCoin needs its users to trust the protocol since it requires the peers to deposit their coins in a temporary aggregation bitcoin address before the main stage of the protocol is performed.

**(3) Mixing Services**: A number of centralized mixing services [20] have been proposed to provide anonymity for Bitcoin users. By using these services, users can send their coins to a trusted mixing service and receive them back at a new address. In fact, a mixing service removes the link between a bitcoin address used in a transaction from the owner of the transaction. However, users must fully trust the mixing service provider. These services provide limited anonymity because the mixing service provider is still able to link the new addresses to the real addresses [32].

Mixcoin proposed by Bonneau et al. [21] is a centralized mixing service that tries to address the first issue by using an accountable mechanism. It makes the mixing service provider accountable and ensures that any dishonest mixing operation results in poor reputation. However, it does not guarantee that the mix service always performs the protocol honestly. To enhance the Mixcoin protocol, Valenta et al. proposed Blindcoin [22]. It uses a blind signature scheme [33] to prevent the mixing server from accessing the output addresses of transactions. Thus, the link between input and output addresses is removed for the mixing server. However, the risk of coin theft is still present.

**Disadvantages**

In Bitcoin, every block didn't include a SHA–256 cryptographic hash of the previous block. This links every block to its previous block and hence creates the whole blockchain.

Proposed System

\_ We develop solutions to address the security drawbacks of the original DC–net protocol. These drawbacks make it feasible for an adversary to deanonymize the sender of each message.

\_ We propose HDC–net, a decentralized and self– organizing anonymous mixing protocol that does not require any trusted–third party. It enables a group of peers to anonymously and securely mix their messages such that it is not feasible to determine which message belongs to which peer.

\_ Further, we develop UCoin by deploying the proposed HDC–net protocol as the mix approach to provide anonymous Bitcoin payments. UCoin is simpler and faster than the current solutions. Moreover, it is fully compatible with the Bitcoin protocol.

**Advantages**

In the proposed system, UCoin is developed by applying the HDC–net mixing protocol to the Bitcoin setting. It ensures that the input and output accounts in a jointly created mixing transaction are unlinkable. Note that the links between input and output addresses in an aggregated transaction are unknown to not only an external observer (an adversary who monitors the transactions to deanonymize users), but also to the peers who have created that transaction, i.e., among all the shuffled output addresses, they are able to recognize only the output addresses that have been added

by themselves. In other words, the only difference between the deanonimizing power of an adversary from outside the group and the peers in the group is that the peers can recognize the output addresses added by themselves. Thus, the anonymity set is smaller for them.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL