**INTRODUCTION**

Since their emergence in the last decade, cryptocurrencies (e.g., Bitcoin) have attracted a lot of attention from both academia and industry. According to the latest records, 2224 different cryptocurrencies have been listed in CryptoCurrency Market Capitalizations web site with $250 billion total market cap [1]. The main characteristic of cryptocurrencies that makes them popular is that unlike e–cash systems [2–3], they do not require any trusted central party to work. Instead, cryptocurrencies store users’ transactions in a distributed ledger known as the blockchain which is publicly accessible. Use of the blockchain technology also enables cryptocurrencies to guarantee data integrity which is absolutely critical for financial databases. The reason is that blockchains are inherently immutable and completely resistant to data modification, i.e., once data is added to the ledger, it cannot be changed or deleted [4–6]. Although there is a common perception that cryptocurrencies provide anonymous transactions, the majority of cryptocurrencies still struggle to guarantee anonymity for their users [7–8]. In cryptocurrencies, users may use many different pseudonyms (e.g., Bitcoin addresses) to preserve their privacy. Thus, they believe that their transac-tions are anonymous. However, this is not correct because pseudonymity does not always result in anonymity. The results of some research studies show that since users’ transactions are generally linkable, they can be deanonymized by using information available in the public ledger [9–12]. This may make cryptocurrencies vulnerable to deanonymization attacks.

To address this issue, a number of privacy protection schemes have been proposed in the literature. In some of these proposals, a new cryptocurrency has been proposed that provides anonymity by design [10], [13–14]. In other proposed solutions, privacy–preserving protocols have been developed specially for Bitcoin to provide anonymity for its users [15–19]. There are also some centralized mixing services that have been implemented to provide anonymity for Bitcoin users [20–22]. They receive Bitcoin transactions from different users and mix them together into an aggregated transaction in such a way that it is infeasible to link each bitcoin address (pseudonym) in the aggregated transaction to its owner.

However, these solutions suffer from at least one of the following issues: (1) requiring a trusted third-party entity [17], [18], [21], [22], (2) poor performance (in terms of speed or storage) [13], [15], [22], and (3) lack of compatibility with the standard structure of cryptocurrencies [5]. Moreover, some of these proposals are vulnerable to DoS attacks [16], [19] or do not support blockchain pruning [10], [13], [14]. The latest approach (mixing services) also needs relying on a third party that is not always secure [7–8], [23]. Motivated by this, we present UCoin, an efficient protocol for anonymous payment in cryptocurrencies. Our protocol design consists of two phases, i.e. (1) development of a mixing protocol, and (2) integration of the mixing protocol into the architecture of cryptocurrencies. In the first phase, we modify the Dining Cryptographers Network protocol (DC–net) [26] and propose Harmonized DC–net (HDC–net) as a new decentralized and self–organizing mixing protocol.

The original DC–net protocol suffers from two drawbacks that make it impractical, (1) collision possibility, and (2) security issues. We propose a solution for each drawback and develop the final HDC–net mixing protocol. HDC–net is a distributed and non–interactive mixing protocol. It enables N peers to mix their messages in such a way that an attacker who monitors the peers’ traffic cannot determine which message belongs to which peer (note that message here refers to any sort of information, not necessarily payment information. In other words, HDC– net can work with non–monetary applications as well). The main characteristic of HDC–net protocol is that it does not require any trusted third party for mixing, such as a mix server or an onion router [24], [25]. In other solutions for anonymous communication (e.g. Tor [24] and onion routing [25]), a number of trusted mixing servers are needed, otherwise, the protocols become vulnerable against traffic analysis attacks [16].

In the next phase, we employ the proposed HDC– net protocol as the core module of UCoin and use it to mix the individual transactions of a group of users into a single aggregated transaction in such a way that the link between the payers and payees is unknown to any observer. We apply the proposed mechanism on Bitcoin [27] as the most popular cryptocurrency [4], [6], [8] to provide anonymous Bitcoin payments. The same approach can be used for other cryptocurrencies since our HDC–net protocol is fully–independent of the applied cryptocurrency settings. Using the UCoin protocol, N peers can non–interactively mix their transactions into a single aggregated transaction (without using a third–party mixing server) to ensure that the input and output accounts in the aggregated transaction are unlinkable (see fig. 1).