# CONCLUSION

This paper proposed Unlinkable Coin (UCoin), a secure and efficient mixing approach to protect cryptocurrencies against deanonymization attacks. It enables users to make anonymous payments by generating unlinkable transactions. To develop the UCoin protocol, we first proposed HDC–net a decentralized mixing protocol that enables a group of peers to anonymously mix their messages. Then, we added HDC–net as an extension to the Bitcoin architecture to provide anonymous Bitcoin payments. The main strengths of the proposed scheme are: (1) no dependency on a trusted third–party entity, (2) fully compatible with architecture of the current cryptocurrencies, and (3) simpler and faster than the current solutions. Our prototype implementation shows that UCoin is a practical protocol that provides anonymity for Bitcoin users.

An interesting direction for future work is to apply our HDC–net mixing protocol to other applications in which lack of anonymity is a concern. This results in developing different applications that provide anonymity as a feature for their users.