Pseudonymity is not enough: Why Monero is ‘missing out’ on decentralised identity.

Ben Biedermann
Islands and Small States Institute
University of Malta
Msida MSD 2080, Malta
ben.biedermann.20@um.edu.mt

June 2023

Abstract

Since the advent of cryptocurrencies, governments globally have set out to regulate them as new means for storing, exchanging, and accounting value. The European Union has produced multiple legal frameworks to legislate a characterisation of cryptocurrencies, regulate their circulation, and identify holders of decentralised wallets. While the EU’s *‘Directive on markets in crypto-assets’* or its *‘Regulation on information accompanying transfers of funds and certain crypto-assets’* are notable, they appear to be pretext for more regulation in Europe. Thus, it must be investigated which actions on EU-level are taken to deepen user identification for controlling digital money flows. Ironically, the cryptocurrency and the underlying cryptographic research are currently delivering the answer to the EU’s ambitious goal of reclaiming its monopoly over monetary policy. The turing-complete nature of Ethereum’s native programming language Solidity allows complex computations to be performed on-chain. Subsequently, applications form an ecosystem on Ethereum as layer one, which today is known as Web3. Like the EU’s objective to control money currents from and to unhosted wallets, Web3 faces the issue of authenticating users when they are accessing information stored in auxiliary backends. Actors in Web3 responded by coining the notion of decentralised identity, or self-sovereign identity in today’s terminology. The exploration of data formats and communication protocols used in SSI and Web3 is interesting and relevant. Yet, the relationship between identifiers and referenced identity data is crucial to illuminate the reasons for Monero missing out on SSI. Within the paradigm of SSI, identifiers and identity data are associated through a decentralised identifier (DID) document. Hence, a verifiable connection between public keys and metadata forms the foundation for SSI.

For example, to create a self-sovereign identity with a DID-method based on Bitcoin the actor has to create two Bitcoin compliant key pairs and post a transaction to the Bitcoin network. The transaction identifier then is stored in a DID registry and links the key pair used to post a transaction with an entity, which uses the private key to sign the credentials it issues. Although Monero prevents double spending, like Bitcoin through proof-of-work, its confidentiality preserving features for the transactor have rendered the creation of Monero-based DID-methods prohibitively complex. Thus, currently no Monero-based DID-method exists. Meanwhile, the narrative of trustable and verified identities used for issuing credentials pertains primarily to institutional SSI-actors. Natural persons’ identifiable information, however, should not be subjected to the immutability and persistence that are used for institutions. While some SSI-solutions did not fully acknowledge their infringing nature on a person’s right to be forgotten, they do so to the end of enabling users to continuously present their credentials. In other words, privacy preserving key rotation for users, who are natural persons, remains unaddressed by existing SSI-solutions. Thus, this contribution explores whether Monero rightfully misses out on decentralised identity, whereas it can offer privacy-preserving DID-anchoring to facilitate key rotation for natural persons.

Keywords Decentralized Identifier · Digital Identity · Monero · Blockchain