VerusID

VerusIDs are a fully functional blockchain protocol, not just an ID system. There is no corporation involved in the protocol, unlike most blockchain ID implementations. **VerusIDs** provide plenty of opportunity for identity applications. Specifically, **VerusID** provides:

Quantum-ready friendly crypto-addresses on the worldwide Verus network

VerusIDs can be used to receive and send funds, which are controlled by the single or multi-sig addresses specified in the identity itself. If these controlling addresses or the single or multi-sig properties are changed, which can be done by the controller of the identity, all future spends of UTXOs sent to that identity follow the updated spend conditions and are subject to the updated keys. Although Verus 0.6.2 does not include quantum resistant signatures for transactions, Verus IDs are themselves resistant to quantum attack with known algorithms, and we have already started to integrate a quantum secure signature scheme, which we expect to activate on mainnet early next year. When that is available, it will be possible to change an ID and have all of the funds sent to it made retroactively quantum resistant. Verus IDs can also be used to publish ID->destination address mappings on other blockchains, but only the Verus ecosystem has the ability to revoke, recover, inherit, funds in existing UTXOs.

Fully Decentralized Protocol

Anyone can create one and have complete, self sovereign control over it without permission to do so. All costs to create an ID go to miners, stakers, and ID referrers. Verus IDs are:

- Revocable -- each ID includes a revocation authority, which defaults to the identity self. If another ID is specified as the revocation authority it can be used to revoke the identity, which creates a valid transaction that, once mined into a block, prevents the identity from being used to spend or sign until it is recovered, effectively freezing all of its funds, for example, in the case of key theft or turnover in an organization.
- Recoverable -- each ID also includes a separate recovery authority, which also defaults to self. If another ID is specified as the recovery authority it can be used to recover the ID from its revoked state, with the option to alter the primary authorities used to spend and sign.
- Private - Each ID contains a set of zero-knowledge private addresses, which can be used as messaging, financial, or voting endpoints, and each ID also contains a content map of key-value hashes, intended to be used alongside applications and various identity policies to provide everything from private yet selectively provable claims and attestations to selectively provable components of a strong identity, attested to with a quantum secure signature when that is available.
- Powerful - Multiple addresses or other IDs can be defined as primary addresses, and any number of those may be required to spend, sign, or alter the identity (N of M). The revocation authority may only be altered by the revocation authority, and the same applies to the recovery authority, either of which may be another identity with its own N of M multisig controls for its primary addresses.