"Put your thinking caps on for short and long term privacy technologies that defend fungibility... homomorphic encrypted value, committed (hidden) transactions... If your business depends on the success of bitcoin, it depends on the fungibility of bitcoin. You can quote me on that."

- Adam Back, HashCash inventor, bitcointalk 11/14/13

"To stop this nonsense [coin validation efforts] we have to make it impractical to pull off by changing the default behavior in the bitcoin ecosystem. We consider the lack of a central authority to be an essential virtue, which means that we can't be protected by one either. We must protect ourselves. This means things like avoiding address reuse, avoiding centralized infrastructure, adopting— and funding!— privacy enhancing technology."

- Gregory Maxwell, Core Developer, bitcointalk

SUMMARY

The goal of OZcoin (OZRS) is to create freedom through fungibility. What does it mean for a currency to be fungible? Inherently, any unit of OZRS is freely exchangeable and interchangeable with another unit of OZRS. Bitcoin, for example, is not inherently fungible and relies on privacy preserving measures to protect it. OZRS has fungibility built in. In order to create OZRS, we had to tackle two distinct problems that allow a party to discriminate against a transaction or against some set of coins: linkability and visibility. We utilized existing architectures and cryptography found in CryptoNote, Coinjoin, Monero, ZeroCash, and Confidential Transactions and added OZRS, short for "One-time Zero-sum Ring Signatures".

FEASIBILITY

Scalability and feasibility are paramount to the architecture of any cryptocurrency. OZcoin has additional security features in order to ensure privacy and anonymity. As such, there is additional overhead (time and space cost) per transaction, but there's no price for fungibility and freedom from discrimination.

UNIQUENESS

OZcoin is unique in that it requires uniformity amongst all transactions, so that de-anonymizing transactions is not possible. Although it builds upon existing architectures like Monero, CT, etc. OZcoin offers a unique combination of the security features of each with a new ring signature.

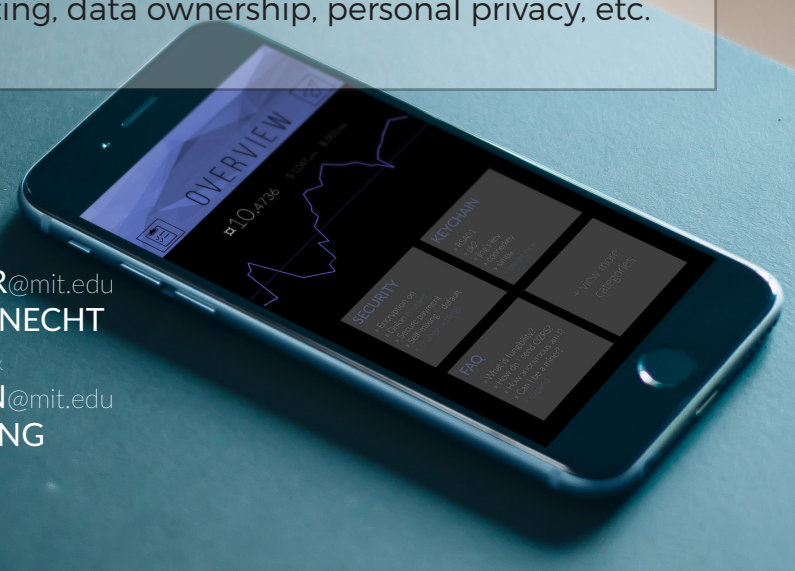
IMPLEMENTATION AND EXECUTION

Scalability and feasibility are paramount to the architecture of any cryptocurrency. OZcoin has additional security features in order to ensure privacy and anonymity. As such, there is additional overhead (time and space cost) per transaction, but there's no price for fungibility and freedom from discrimination.

NEED

OZcoin fulfills unmet needs as both a currency and as a platform technology. When money is not fungible, it introduces itself to and creates political and regulatory hurdles that vary across jurisdictions. How can global, borderless cryptocurrency truly be both those things if networks are laced with jurisdictional traps?

Fungibility makes discrimination impossible - this paves the path for other tools of democracy to be built, like anonymous voting, data ownership, personal privacy, etc.



CONNER@mit.edu
FROMKNECHT
&
JINGLAN@mit.edu
WANG