qedit

Privacy & Security Considerations of CBDC and Stablecoins

Daniel Benarroch
Director of Research at QEDIT, ZKProof.org

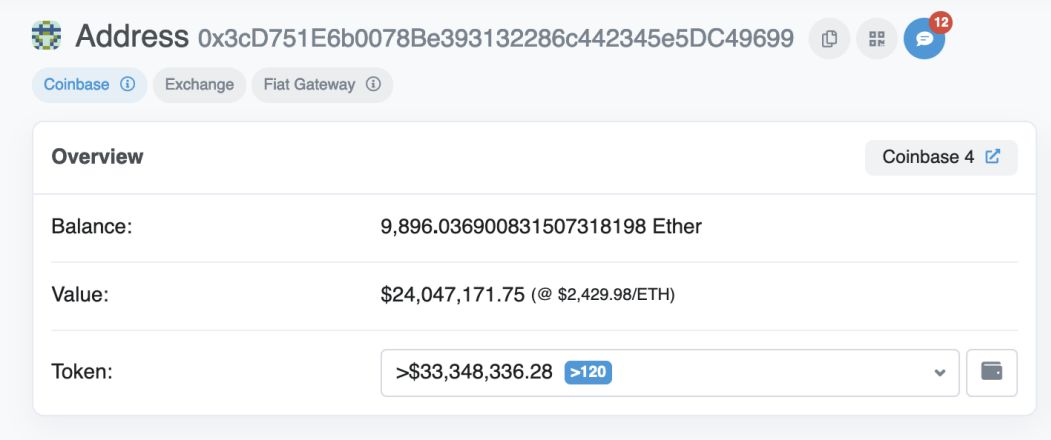
January 2022

The Importance of Privacy on Blockchain

Blockchains are NOT private by default.

Transactions can be read and linked by anyone.

Tools exist to inspect the data stored on blockchains (e.g.: Ethereum)



Most users are not aware of the non-private nature of blockchains & DLs

Pros

- More difficult to hide criminal activity and fraudulent behaviour
- Governments can audit blockchains to track the wellbeing of the system

Cons

- People can take advantage of public data to identify users and monetize on private data
- Validators of blockchains can front-run the transactions by adding theirs before

WHAT IF THERE EXISTED A TOOL THAT PROVIDES THE BEST OF BOTH WORLDS?

- Cryptography can unlock all the value of applications while maintaining the privacy of the data and the individual, and ensuring that trust is not needed in interactions
- Cryptography can also enable checks on usage to ensure proper behavior of individuals and prevent fraud and criminal activity. Furthermore, authorities can audit

State-of-the-art of Privacy-Enhancing Techniques

1. Zero-Knowledge Proofs

➔ enables integrity of computation and privacy of data
➔ used today on blockchains for scalability and to preserve privacy of transactions, can unlock auditability
➔ in CBDC can be used for gov to audit financial behavior

1. Multi-Party Computations

➔ enables computation on private distributed data
➔ used today for private key management (multi-signature, key recovery, ...)
➔ in CBDC can be also used to enhance future apps

3. Homomorphic Encryption

➔ enables cloud computations on private data
➔ used today for basic statistical aggregation, future use includes machine learning on private data
➔ in CBDC can be used for credit score computation

4. Differential Privacy

➔ enables private analysis of data, deriving macro results
➔ used today to aggregate data from users without revealing individual users(US census, mozilla firefox)
➔ in CBDC can be used for macro-usage of financial sys.

Unlocking the Full Value of CBDC and Stablecoins

For CBDC to succeed we need

- Censorship resistant system
- Trustless interactions
- Privacy of transactions and data
- Unique user identification
- Integrity of the system, prevent fraud
- Auditability of behavior and taxes

In fact, IDENTITY is core aspect

- Single identity onboarded
- Transactions are not linkable
- Anonymous interactions
- Privacy of transactions and data
- Authority can deanonymize behavior only when fraudulent triggers happen

THANK YOU

