qedit

ZKPROOF

Privacy and Compliance? From Solana to Zcash to a Win with ZKP

March 2025

Arseni Kalma
Software Engineering

QEDIT Succeeded getting Privacy & Compliance at the same time

- Combine Privacy (Zero-Knowledge) & Compliance (KYC/AML)
- Implementations in Stable coins
- Zero-Knowledge Cryptography (Bulletproofs, Plonk)
- Verifiable on Zcash, Solana and other blockchains

Confidential Transfers on Solana were finally activated on Mainnet

- Confidential Transfers are part of Token-2022 contract
- Conceals the transaction amounts using ZKP
- Prepared for large-scale use
- **QEDIT & Bits Of Gold launched the first stablecoin using Confidential Transfers**

Confidential Transfers uses battle-tested encryption and straight-forward ZK

- ElGamal encryption to encrypt token balances
- ZK Proofs via Bulletproofs
- Requires off-chain encryption support
- Not completely private (Pseudo Anonymous)

Solana hides the amounts, transfers still linkable

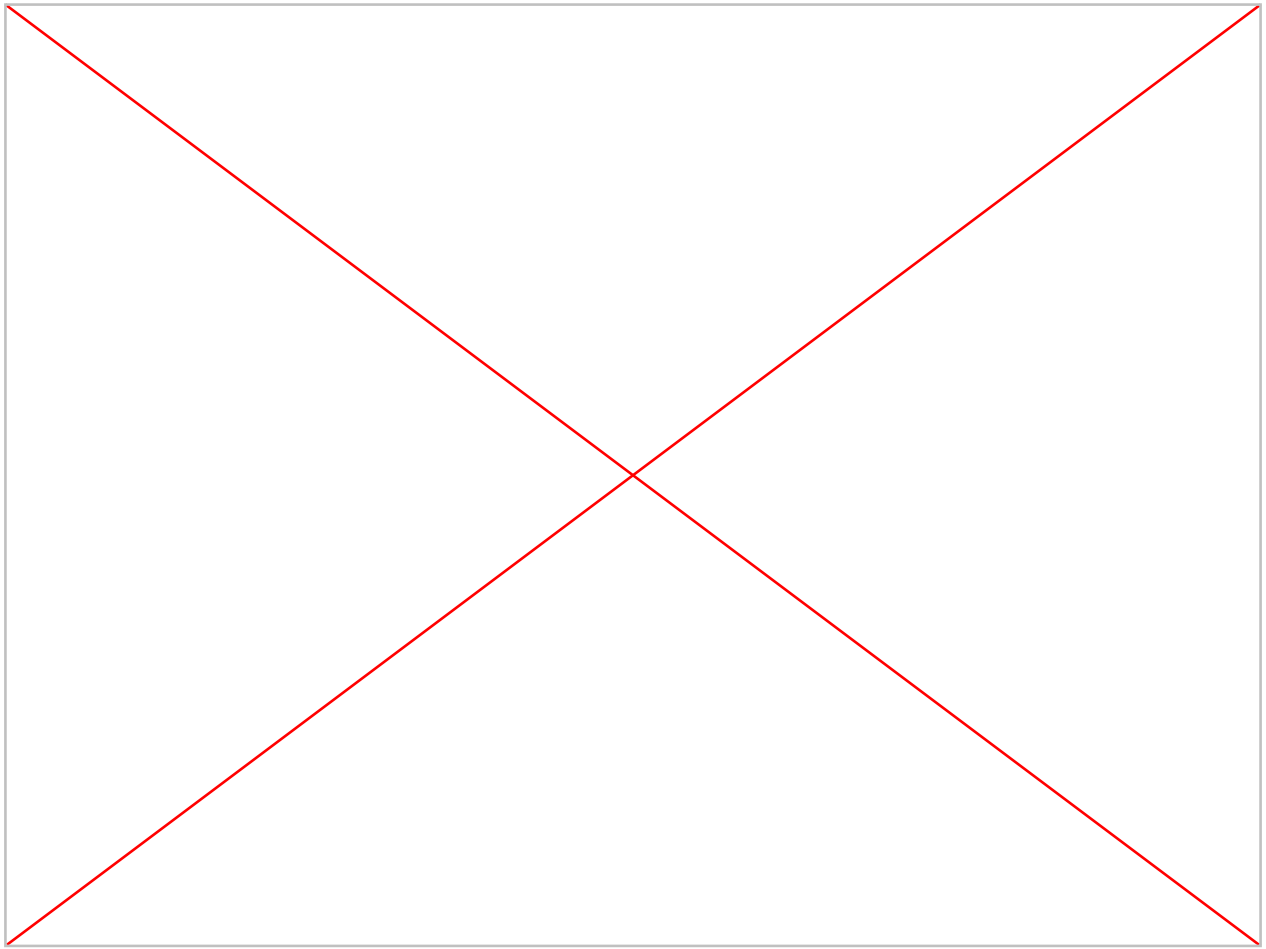
- Privacy vs. Compliance
  - Issuers and authorized parties can select which accounts have privacy features, and 'freeze' any miss-behaving account
  - Transfers are linkable, amounts are hidden

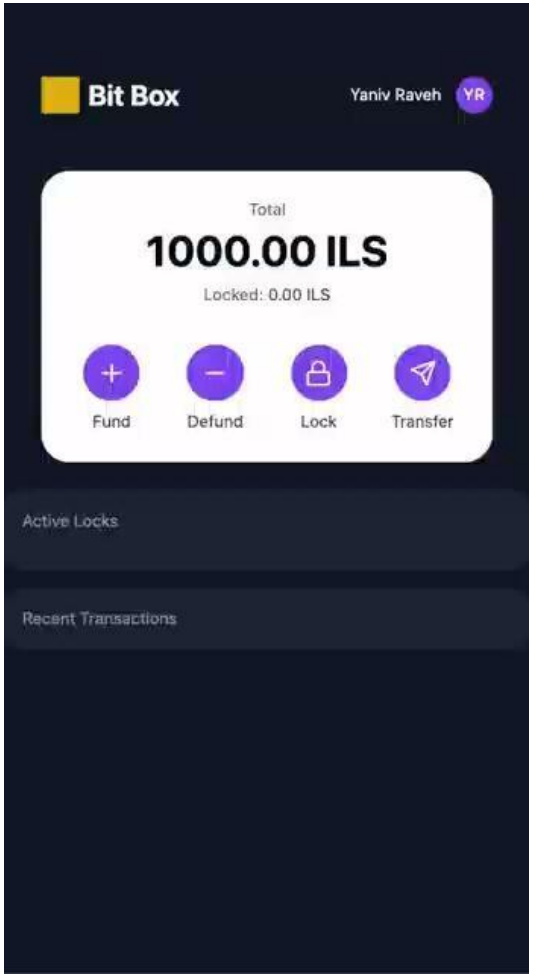
Zcash Shielded Assets will provide full privacy and unlinkability

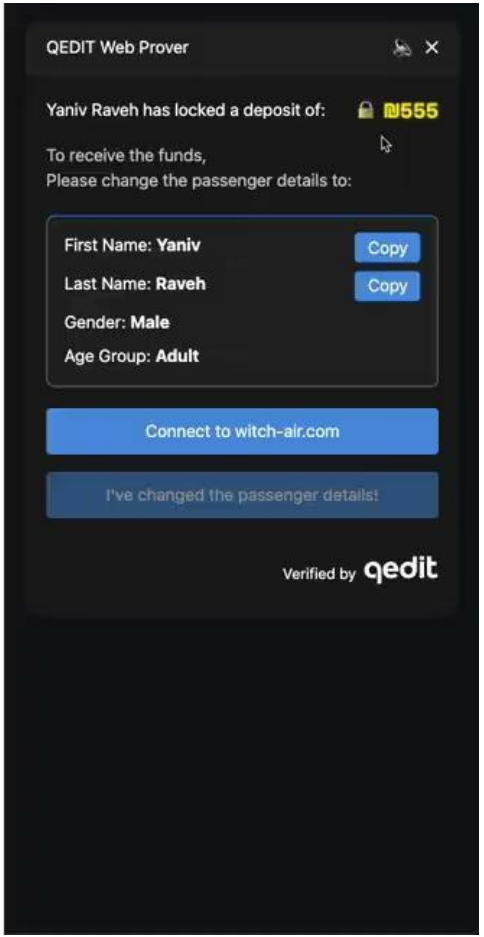
- **Deeper Privacy with ZSA**
- Zcash hides the **amounts** and the **transaction graph**, enabling even higher level of privacy
- Conditional transaction disclosure using "viewing keys"
- Custom assets inherit Zcash level privacy

QEDIT provides a compliance solution for stablecoin issuers on Zcash

- **Amounts** and the **transaction graph** are hidden from the public
- If required, the **amounts** and the **transaction graph** can be inspected by an auditor
- Extends Zcash privacy to custom assets
- Still in development; QEDIT is prepared to integrate




Bit Box
Yaniv Raveh
YR
Total
1000.00 ILS
Locked: 0.00 ILS
Fund
Defund
Lock
Transfer
Active Locks
Recent Transactions


QEDIT Web Prover
Yaniv Raveh has locked a deposit of:
₪555
To receive the funds,
Please change the passenger details to:
First Name: Yaniv
Copy
Last Name: Raveh
Copy
Gender: Male
Age Group: Adult
Connect to witch-air.com
I've changed the passenger details!
Verified by qedit

QEDIT Won CBDCs competition with its ZKP solution

QEDIT showcased itself in a national competition and won

- Solves 'ticket sale race condition'
- Involves advanced cryptography
- Won Bank of Israel award
- Easy to use

TLS Notarization moment? We showcased a simple use, and people got it

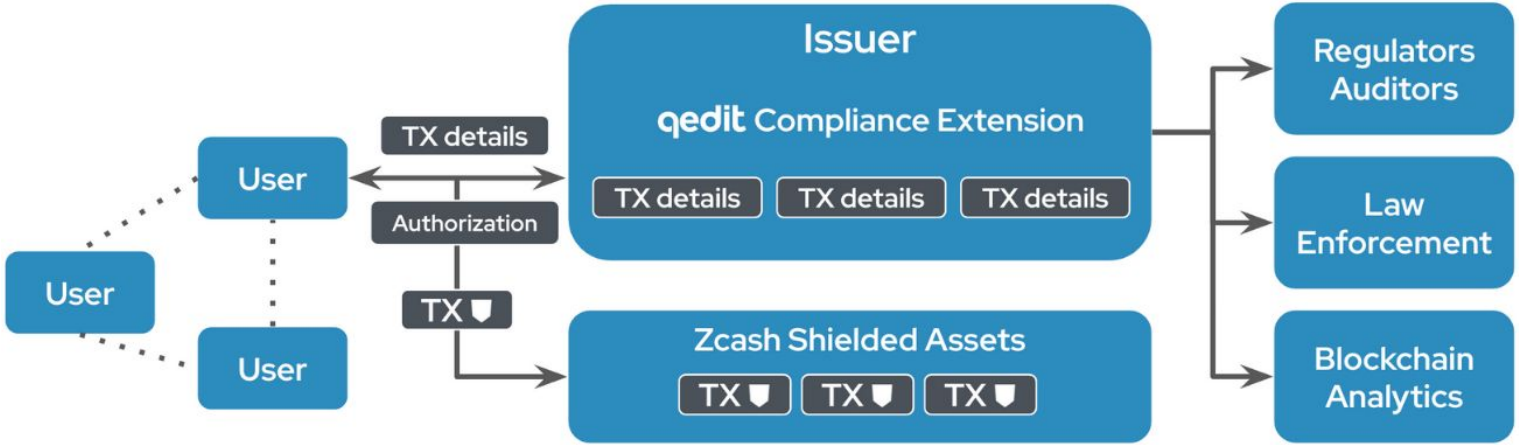
- A cryptographic method to create a "snapshot" of a webpage, certifying its content without revealing unnecessary data
- Allows partial redaction (e.g., hiding cookies or personal info), while still proving authenticity of the page **without** exposing full user details.

Thank you!

QEDIT – Privacy & Compliance Solutions

Questions?

arseni@qed-it.com



- User Sends Shielded Transactions to Zcash
- Others can't see Details

- Issuer Authorizes Transactions
- Issuer Receives Transactions Details
- Issuer Controls Disclosure

Compliance Operates on Full Transaction Details

