Privacy and CBDC

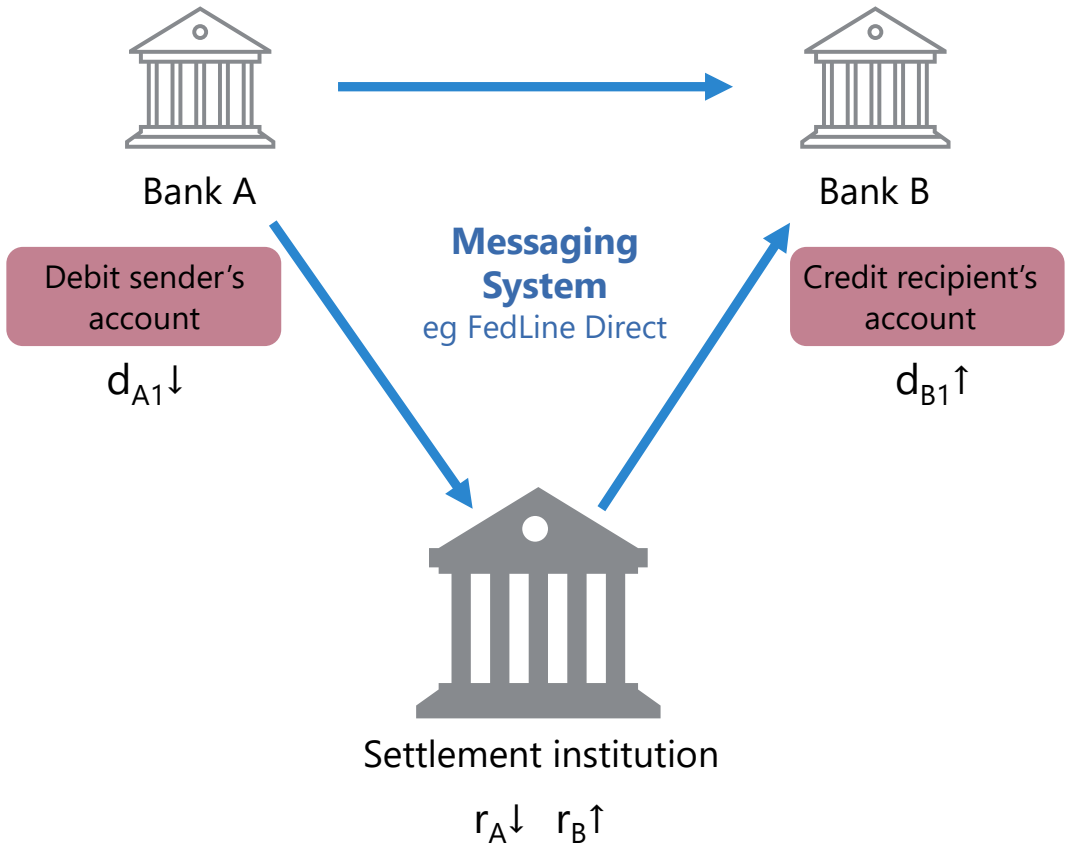
Rod Garratt, Senior Adviser

Bank for International Settlements

DC ^{3} Conference: from Cryptocurrencies to Central Bank Digital Currencies, January 26, 2023

Making a payment through Fedwire

Proprietary data sets and messaging system

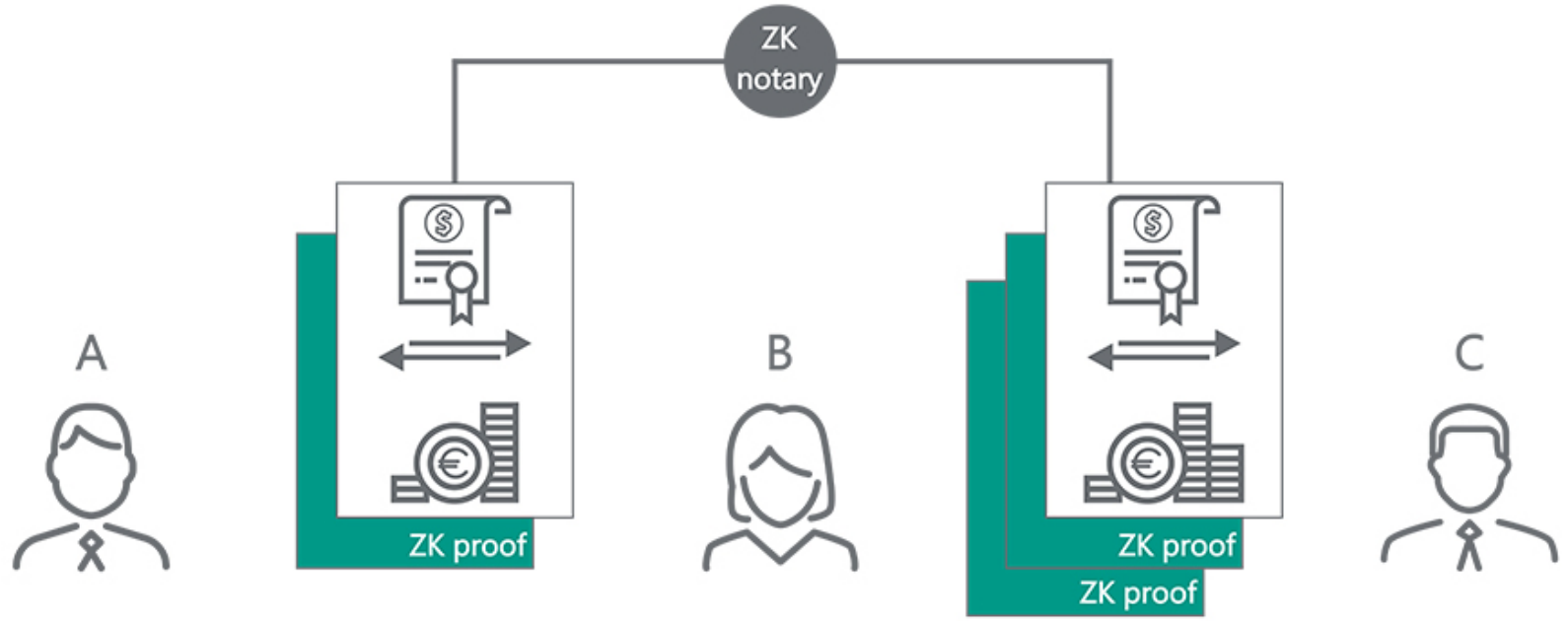


- Existing wholesale payment systems are centralized.
- Banks initiate payments to each other by sending messages to the central infrastructure with instructions specifying the amount, the recipient and other required details.
- Only the payor, the payee and infrastructure operator know the payment details.
- This arrangement meets the privacy requirements of all participants.

Project Jasper

- Phase 1 was built on the Ethereum platform, which uses a PoW consensus protocol.
  - A key advantage was no single point of failure, but this implementation was rejected on the grounds that transactions were not private and in a closed, private network, like a wholesale payment system, PoW protocols are neither necessary nor desired.
- Phase 2 was built on the Corda platform.
  - In Corda platform, updates to the ledger are achieved through a verification function and a uniqueness function.
  - The verification function, performed by the parties involved in the transaction, ensures that all details of the transaction are correct, and that the sender has the required funds.
  - The uniqueness function (which replaces PoW) is performed by a trusted notary.

Backchain problem and proposed solution with ZKPs



ZK = zero-knowledge.

Sources: Adapted from Annerie Vreugdenhil, ING Bank, CordaCon 2021.

- Information required to verify each past transaction is replaced by a ZKP.
- The current recipient sees only the current transaction details and the sequence of past ZPKs.

Need to build in privacy; it's not a trade-off

- Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada articulated the foundational principles of "Privacy by Design"**:**

1. Proactive not reactive; preventive not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric