Quali-Sign

Mobile apps for eID & SCA

Sharing technical, regulatory and business expertise for multipurpose eWallets

eWALLET NETWORK

CBDC Models follow-up: Account vs. Token vs. Hybrid

24th January 2022

Michael Adams
+44 7808 203856

michael_adams@quali-sign.com

CBDC Key Requirements

1	CBDC balances are protected by the central bank	◆ A user’s balance can be restored: ◆ If they lose or damage their smartphone. ◆ Their PIP’s data/systems are totally wiped out.
2	Funds can be received (and re-spent) while offline	◆ Aim is to implement digital cash not digital cheques. ◆ A digital replacement for physical cash (i.e. notes & coins). ◆ Resilience and inclusion are fundamental. Must not assume network availability or data plan. ◆ Assumes offline irrevocability and finality.
3	User privacy is of utmost importance	◆ As the user moves from shop to shop, their CBDC transactions must not be capable of being linked. ◆ Otherwise we put the user at risk of being tracked, profiled and their true identity derived.

Compromising on these requirements would weaken user adoption.

Account vs. Token vs Hybrid : A Comparison

Model	Definition	1. Balance protected by BoE	2. Funds re-spent offline	3. Prevents tracking
Account	◆ The user balance is maintained (increased and decreased) on the central bank core ledger. ◆ User account is represented by a constant value, e.g. IBAN or fixed public/private key pair.	YES	NO	NO
Token	◆ Bearer instrument (UTXO). ◆ Units of value are moved directly between different owners.	NO	YES	NO

Neither Account nor Token models meet the requirements!

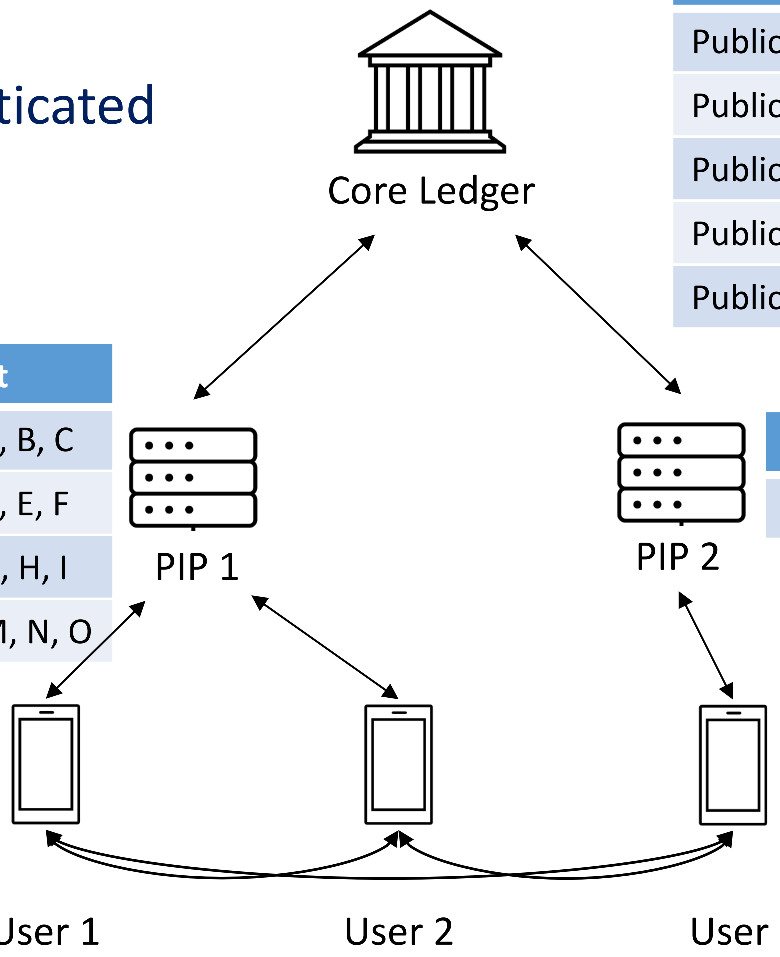
Hybrid	◆ A model that blends aspects of the Account (balance protection) and Token (offline) models and improves privacy.	YES	YES	YES

The following slides will outline a proposal for the Hybrid model…

Hybrid: Tracking Prevention

A simple approach that does not rely on sophisticated cryptographic privacy enhancing techniques

- A CBDC account is represented by a set of [1 + n] public/private key pairs.
- The wallet can randomly rotate between key pairs when transacting (incl. while offline).
- This prevents the user from being tracked and profiled.
- Key sets can be renewed on a regular basis while the wallet is online.



CBDC Account	Ledger Balance
Public Keys: A, B, C	£10
Public Keys: D, E, F	£40
Public Keys: G, H, I	£10
Public Keys: J, K, L	£30
Public Keys: M, N, O	£10

User	CBDC Account
User 1	Public Keys: A, B, C
User 2	Public Keys: D, E, F
User 2	Public Keys: G, H, I
User 1	Public Keys: M, N, O

User	CBDC Account
User 3	Public Keys: J, K, L

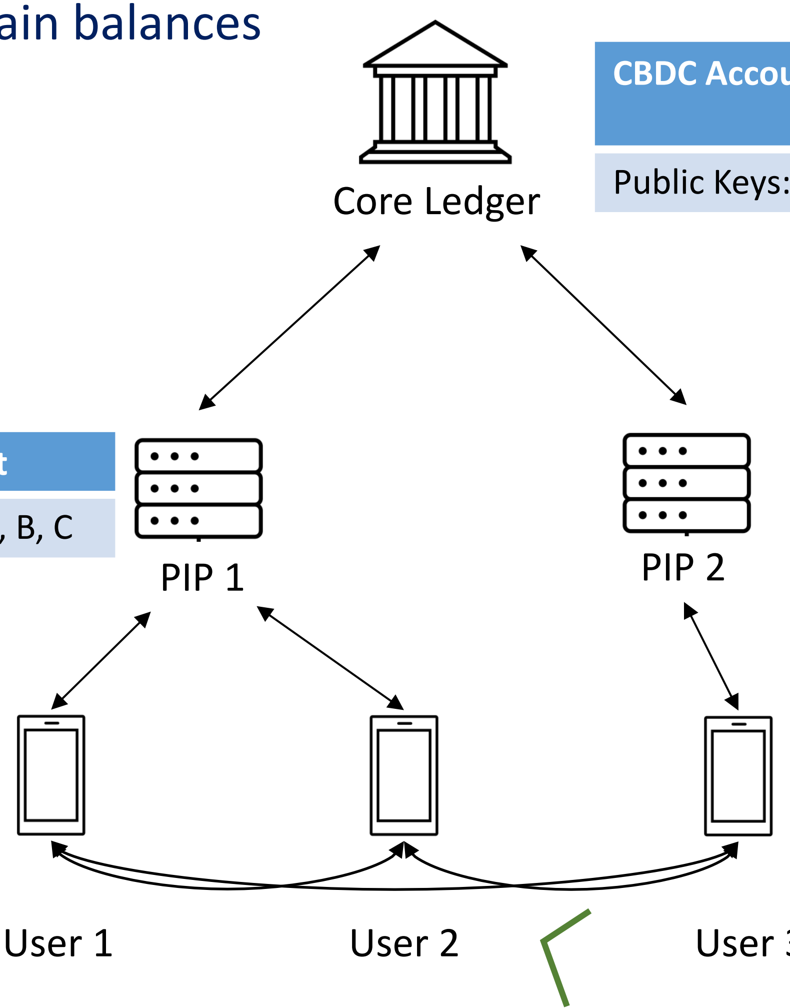
CBDC Account
Public/Private Keys: A, B, C
Public/Private Keys: M, N, O

CBDC Account
Public/Private Keys: D, E, F
Public/Private Keys: G, H, I

CBDC Account
Public/Private Keys: J, K, L

Hybrid: Offline Spending & Funds Recovery [1..2]

Both the central ledger and the smartphone need to maintain balances



CBDC Account	Ledger Balance
Public Keys: A, B, C	£10

1. Central ledger maintains the user account balance.

User	CBDC Account
User 1	Public Keys: A, B, C

User 1: Account – Offline Transactions

Tx.	Offline Credits	Offline Debits	Local Balance
Starting balance (from central ledger)			£10
1	£20		£30
2		£10	£20
3		£5	£15

2. The wallet also maintains a local balance, whilst offline.

3. Funds are exchanged via proximity connections (e.g. BLE).

Hybrid: Offline Spending & Funds Recovery [2..2]

Similar to UTXO, Account based CBDC transactions will need to include previous (offline) transaction history

Timeline

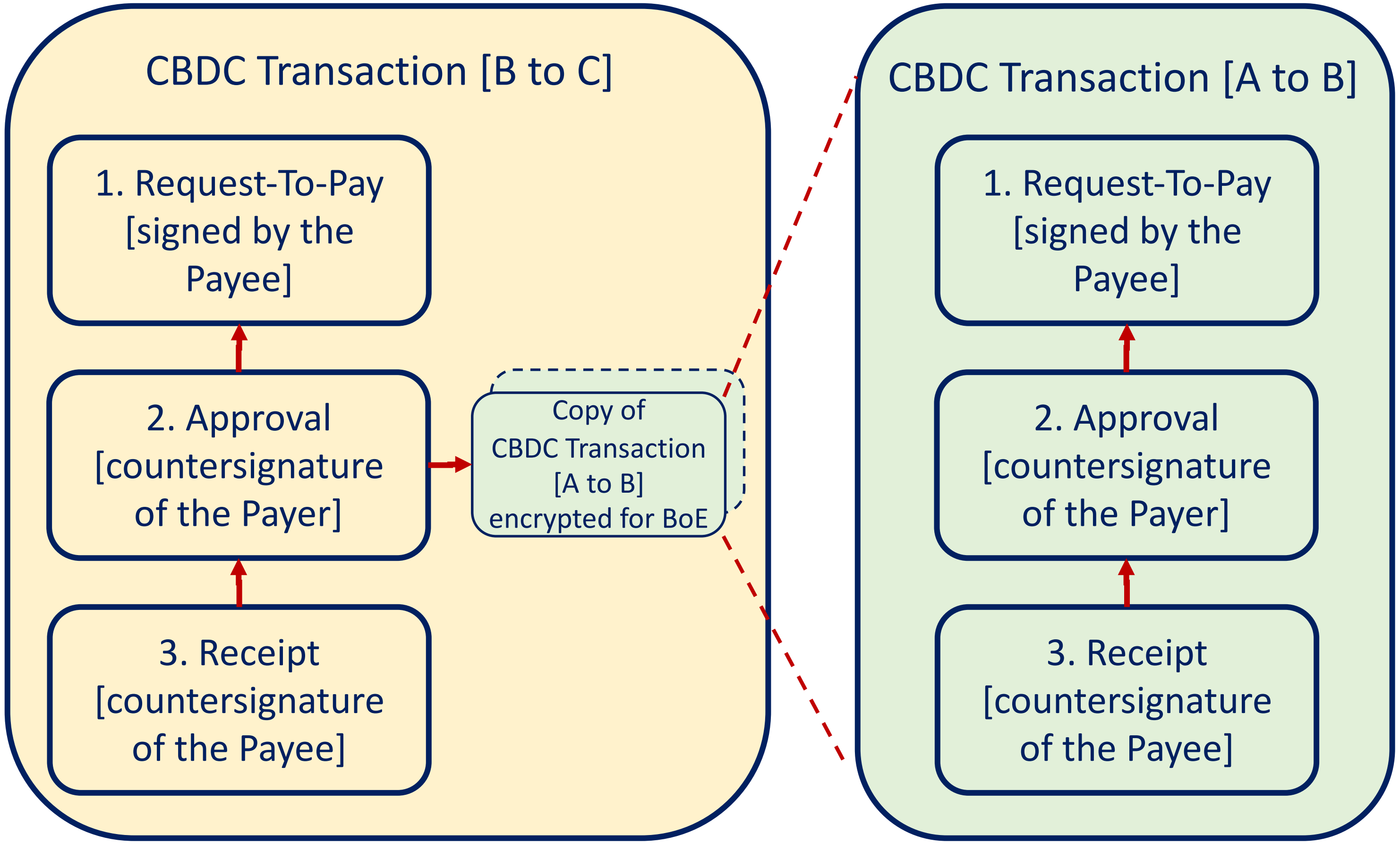
	Person A	Person B	Person C
Central Ledger Balance	£100	£0	£0
	Goes offline	Goes offline	Goes offline
Transfer [A to B]	£80 →		
Offline Balance	£20	£80	£0
	Destroys smartphone		
Transfer [B to C]		£60 →	
Offline Balance		£20	£60
		Loses smartphone	
			Goes online
Central Ledger Balance	£20	£20	£60
	Replaces smartphone	Replaces smartphone	

The only way the [A to B] transaction can reach the central bank is via person C.

Hybrid: Potential CBDC Transaction Structure

Analogous to Russian Dolls

- One option would be for a CBDC transaction to be represented by a chain of (payee and payer) signatures.
- The payer's offline transaction history can be included in this package.
- The payer wallet would encrypt the payer transaction history so that only the central bank can decrypt it.
- The payer would also sign the encrypted payer history.
- This concept is analogous to Russian Dolls
- This approach is already supported in the ETSI Electronic Signature standards
- The ETSI Associated Signature Container (ASiC) is a ZIP structure which can include multiple elements.


CBDC Transaction [B to C]
1. Request-To-Pay [signed by the Payee]
2. Approval [countersignature of the Payer]
3. Receipt [countersignature of the Payee]
Copy of CBDC Transaction [A to B] encrypted for BoE
CBDC Transaction [A to B]
1. Request-To-Pay [signed by the Payee]
2. Approval [countersignature of the Payer]
3. Receipt [countersignature of the Payee]

Conclusion

Model	Definition	1. Balance protected by BoE	2. Funds re-spent offline	3. Prevents tracking
Account	◆ The user balance is maintained (increased and decreased) on the central bank core ledger. ◆ User account is represented by a constant value, e.g. IBAN or fixed public/private key pair.	YES	NO	NO
Token	◆ Bearer instrument (UTXO). ◆ Units of value are moved directly between different owners.	NO	YES	NO
Hybrid	◆ A model that blends aspects of the Account (balance protection) and Token (offline) models and improves privacy.	YES	YES	YES

A practical study to prove the Hybrid model would be highly beneficial!