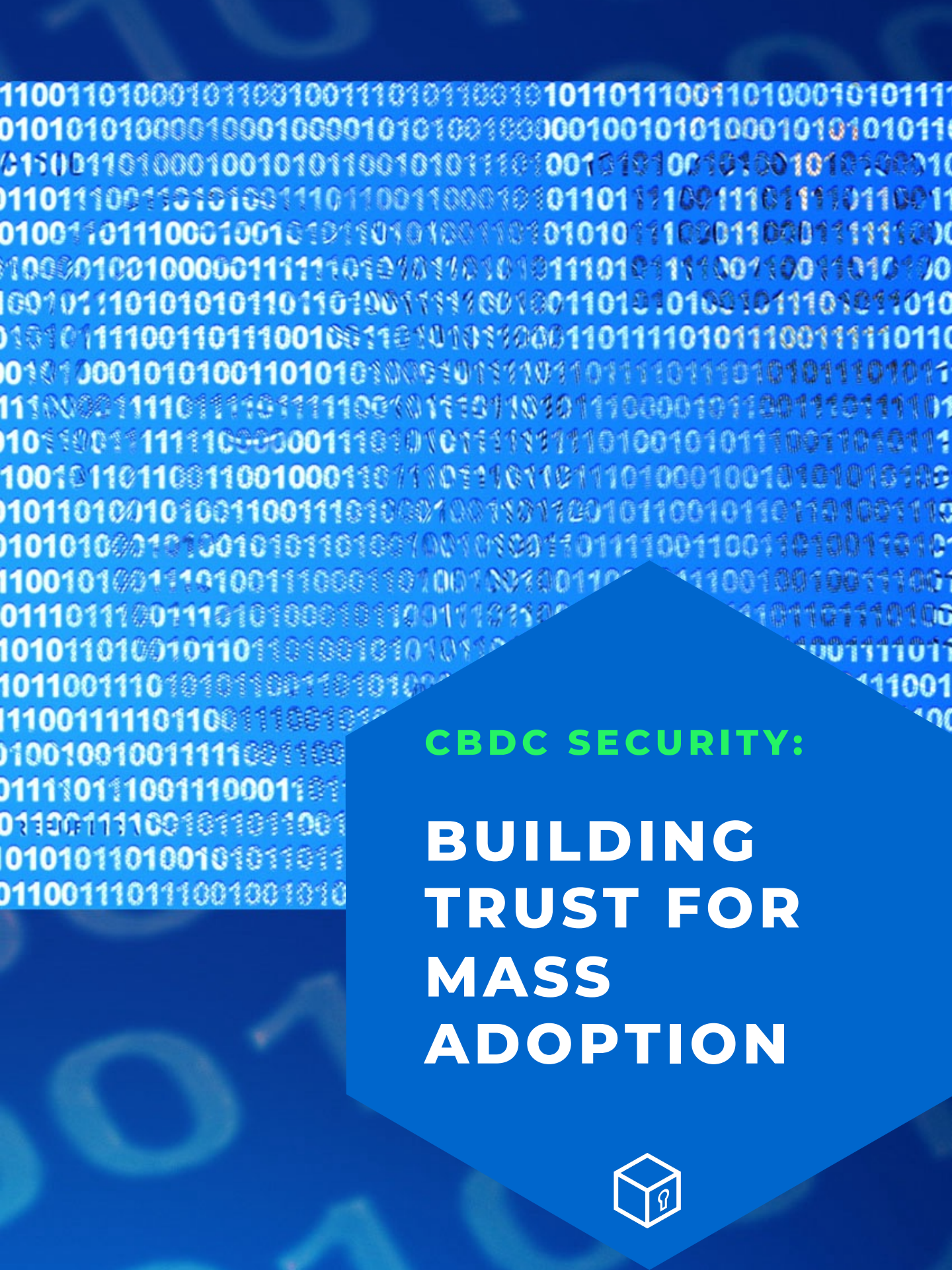


CBDC SECURITY:

BUILDING TRUST FOR MASS ADOPTION

For Central Bank Digital Currencies (CBDCs) to gain widespread acceptance, the "man on the street" needs confidence in their security.

Public trust in CBDCs hinges on addressing their security risks. A secure CBDC is crucial because it directly impacts financial well-being and is more vulnerable to cyberattacks than traditional systems. People are already hesitant to move away from familiar systems like cash due to perceived risks associated with new technologies and the fear of cryptocurrencies generated by adverse publicity.

If a CBDC system were to be compromised, it could lead to a permanent loss of funds, privacy violations, and a significant erosion of trust in the entire financial system. It doesn't matter where the security issue arises, at Central Bank level, at Payment Provider level, or in the customer's wallet, focusing on the security of the private key and secrets that secure these systems is paramount. If the private key or password, that grants access to a CBDC wallet, is not secure, then the entire system becomes vulnerable.

The security challenges for retail (consumer) CBDC's and wholesale (such as interbank and settlements) are different and the Lokblok solution addresses both domains.

"As the interest in cryptocurrency has increased, this has not gone unnoticed by cybercriminals and threat actors."

BIS Project Polaris Framework

LOKBLOK: SOLVING CBDC SECURITY CHALLENGES

There are several security challenges central banks face when implementing CBDCs. Lokblok offers solutions to these challenges through its Phantom Secrets technology and its broader Zero Trust Ecosystem.

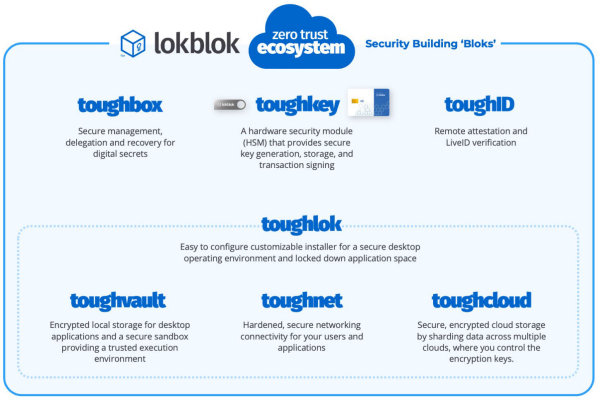
CBDC Security Challenges as summarised by the BIS

1. **Cyberattacks:** CBDC systems, as critical national infrastructure, are potential targets for various cyberattacks, ranging from simple malware to sophisticated APT attacks.
2. **New & Unproven Technologies:** Utilizing new and unproven technologies like DLT and smart contracts introduces new security and operational risks that need to be thoroughly understood and mitigated.
3. **Large Attack Surface:** The complexity of a CBDC ecosystem, involving numerous participants and integration points, creates a large attack surface and multiple points of failure for potential exploitation.
4. **Insider Threats:** Malicious insiders with privileged access can pose a significant threat by exploiting their knowledge of CBDC system logic to commit fraud.
5. **Human Error:** Unintentional mistakes by developers, operators, or administrators, such as using vulnerable software, delaying security patches, or misconfigurations, can compromise system security.
6. **Technology Failures:** Software and hardware bugs, storage failures, and untested software updates can disrupt CBDC systems, particularly in complex technology stacks.
7. **Concentration Risk:** Reliance on a single service provider by multiple ecosystem participants increases operational complexity and risk for the central bank.
8. **Quantum Computing:** Advances in quantum computing pose a threat to current cryptographic algorithms, requiring CBDC systems to be crypto-agile to adapt to future-proof encryption, signature, and key agreement methods.

Understanding Lokblok's Solutions

Lokblok's Zero Trust Ecosystem, which utilizes Phantom Secrets technology to address these challenges. How? Lokblok ensures private keys and secrets such as passwords that are crucial for CBDC operations, exist only within a secure hardware wallet at the point of transaction signing, and are destroyed immediately afterwards. This:

- **Eliminates Persistent Key Risks:** Mitigates the risk of key theft or compromise by removing keys from persistent storage.
- **Provides Hardware-Level Security:** Secures key operations within FIPS 140 and Common Criteria certified tamper-resistant hardware modules.
- **Additional Security Features:** Lokblok offers features such as customizable key signing thresholds and multiparty computation requirements for governance and compliance. These address the need for wholesale CBDC wallets to provide capabilities to support segregation of duties and signing limits.
- **Creates a Secure Terminal:** When combined, the components of the Lokblok Zero Trust Ecosystem turn an ordinary computing device into a secure terminal, where operations can happen in a secure and trusted environment. This can be particularly useful in the wholesale CBDC environment where high value transactions need to be conducted with superior end-to-end security.
- **Seamless Integration and Scalability:** Lokblok is designed to integrate seamlessly with existing financial software systems and acts as security middleware. This addresses a key concern in retail CBDC's where payment intermediary providers will wish to maintain a familiar look and feel to their banking apps/wallets without introducing further complexity for consumers.



Lokblok Zero Trust Ecosystem

Addressing CBDC Security Challenges

1. **Cyber Attacks:** Lokblok's Zero Trust Ecosystem where all cryptographic operations are authorized in hardware create secure cyber-resistant enclaves.
2. **New & Unproven Technologies:** Lokblok is a novel and unique implementation of well understood and well tested technologies, minimising unproven technology risk.
3. **Reduces Attack Surface:** Makes the system less attractive to hackers by eliminating storage vulnerabilities.
4. **Insider Threats and Human Error:** By eliminating persistent keys and utilizing secure hardware, Lokblok minimizes the impact of insider threats and human error because there are no stored keys to be stolen or mishandled. Any reconstitution of keys or secrets requires multiple recovery agents (the number required is predetermined when the secret is enrolled) to authorize.
5. **Technology Failures:** The on-demand key regeneration and their immediate destruction minimize the window of vulnerability to technology failures.
6. **Concentration Risk:** By turning secrets into shards and public data, the risk of honey pots of data is mitigated. The distributed nature of Lokblok means it's designed to be 'Zero Trust' or 'Trustless' in blockchain parlance, and not reliant on any single point of failure.
7. **Quantum Computing:** With a focus on hardware-level security and by distributing cryptographic functions across multiple , the system becomes more resilient to emerging quantum computing capabilities.
8. **Estate Planning:** Banks have procedures to transfer funds upon notification of a customer's demise. These do not take into consideration the additional complexity of transferring digital assets which use private keys. Lokblok also provides a mechanism to support digital inheritance but in a non-custodial way, so no one person or organization can co-opt the digital assets without the cryptographic consent of the other parties.

SUMMARY

Lokblok's emphasis on securing secrets through Phantom Secrets, and the wider Zero Trust Ecosystem directly addresses security concerns of deploying digital wallets. By ensuring that keys only exist when they are needed and that they are then immediately destroyed, Lokblok mitigates the risks associated with key theft or compromise, offering a potential solution to allay the concerns of the average citizen and help pave the way for mass CBDC adoption.