CBW3B
Powered by LACChain

Privacy Analysis for CBWeb3

CBWeb3

Version 0.1– 25/04/2025

System/Service	RG-T4567 Phase I (Take-Off): A Regional Solution for Accelerating the Deployment of Central Bank Digital Currencies (CBDC's) for Inclusion in Latin America and the Caribbean		
Status	DRAFT		
Approved by owner			
Authors	CV	Carolina Velasquez	LACChain: Blockchain Solutions Architect
Contributors	NY	Nayam Hanashiro	LACChain Coordinator of Strategic Projects.

Version history

Version	Date	Author	Description
0.1	25/04/2025	CV	First Draft.
	28/04/2025	NH	Content review.

CB W3B
Powered by LACChain

Content

Introduction 4
Case Studies and Examples 4
DREX (Brazil) 5
European Central Bank (ECB) Digital Euro: 6
Bank of Canada: 6
China's Digital Yuan (e-CNY): 6
CBDC Privacy Mechanisms 6
1. Zero-Knowledge Proofs (ZKP) 7
2. Blind Signatures 7
3. Homomorphic Encryption (HE) 8
4. End-to-End Encryption (E2EE) 8
5. Selective Disclosure 9
6. Privacy by Design 9
7. Offline Functionality 8
Modern Privacy Alternatives (Post-Orion/Tessera) 9
Considerations 10
Regulatory Compliance 10
Features and limitations of LACNet/Besu for solving CBWeb3 use cases 11
Capabilities for Wholesale Payments: 11
Challenges and Limitations: 12
Relevant Examples: 12
Conclusions 12
Wholesale Transactions as an Immediate Focus 12
Strategic Recommendations for Enhancing Wholesale Privacy 13

CB W3B
Powered by LACChain

Introduction

CBWeb3 is a IDB Lab project that seeks to enable a regional test-network (Test Net) for Latin America and the Caribbean that will allow for the issuance of CBDCs and the tokenization of financial assets, with a focus on cross-regional interoperability between central banks and financial institutions. The Test Net will build upon the technological capabilities and infrastructure of IDB Lab's initiative LACChain[1] and LACNet[2] the Alliance for the Development of the Blockchain Ecosystem in Latin America and the Caribbean, and capitalize on the Korean experience on the topic including Korean entities from the public, private and academic sectors such as the Bank of Korea (BOK), Korea Exchange (KRX), KAIST Network Security and Privacy Lab and Sungkyunkwan University (SKKU).

There are many challenges to consider in developing this project, and perhaps the most important of these is maintaining the balance between ensuring the highest levels of privacy and security in the handling of data and transactions, while maintaining regulatory compliance. This is why this analysis of the global state of the art of CBDCs has been conducted, seeking to gain an overview of relevant developments and implementations.

A CBDC is a digital form of fiat currency issued by a central bank, designed to complement or replace physical cash in digital transactions. While CBDCs offer efficiency and financial inclusion, they raise significant privacy concerns due to their digital nature, which inherently allows for traceability. The challenge is to design a CBDC that provides strong privacy levels, while adhering to regulatory requirements such as anti-money laundering (AML), know-your-customer (KYC), and data protection laws like the General Data Protection Regulation (GDPR).

This analysis aims to identify the current state of privacy mechanisms for CBDCs, explore viable technological options, and highlight potential implementation challenges specific to Hyperledger Besu as used in the LACNet ecosystem. It provides a foundation for understanding where the ecosystem stands today, what privacy-preserving tools are available or emerging, and what technical or operational barriers must be addressed to enable effective integration. Case studies most notably Brazil's DREX project, the most advanced CBDC initiative in the region alongside others like the European Central Bank's digital euro, help contextualize these considerations through real-world examples.

[1] LACChain is a global alliance for the development of the blockchain ecosystem in LAC by IDB Lab.
[2] LACNet is the executing agency that will sign the agreement with the Bank for this project. This executing agency is a non-profit foundation based in Uruguay. LACChain Networks are blockchain networks developed by the LACChain Alliance and orchestrated by LACNet. Under the framework of LACChain, LACNet plays a pivotal role in not only facilitating the institutional consolidation and sustainability of the LACChain operations, but also in harnessing the collective strength of the LACChain Alliance community.

Case Studies and Examples

For this inform more than 25 CBDC projects analyzed, of which several projects provide insights into privacy implementations:

DREX (Brazil)

DREX, Brazil's CBDC, developed by the Central Bank of Brazil (BCB), like LACChain, uses Hyperledger Besu. The first phase of the pilot began in 2023, testing transactions with tokenized assets, such as government bonds, demonstrating technical feasibility. The second phase, beginning in 2024, will expand testing to 13 topics, including trade finance and real estate transactions, with a focus on smart contracts developed by third parties. DREX is also exploring elements of DeFi and asset tokenization, integrating with technologies like Chainlink's CCIP[3] for cross-border interoperability, and leverages partners like Microsoft and Banco Inter for privacy and cloud computing solutions.

The project faces challenges in balancing decentralization, privacy, and programmability. Privacy is a critical hurdle, with solutions such as Microsoft's ZKP Nova and Consensys' Anonymous Zether under evaluation until 2025 to comply with Brazil's LGPD (Brazilian General Data Protection Law). Furthermore, BCB seeks to prevent bank disintermediation through tokenized deposits and limits public access to DREX through financial institutions. The system is designed to replace the current real-time gross settlement (STR) system, described as STR 2.0.

The Drex pilot is currently in its second phase and has presented significant technical challenges that have led to schedule adjustments. Originally, a commercial launch was planned for late 2024, but the BCB itself postponed this date. In October 2024, the central bank's president (Roberto Campos Neto) estimated that Drex would require "two more years" of development before its official launch.[4]

In February 2025, the BCB confirmed that the pilot faces technological limitations that require more time and intensive oversight, so new use cases will not be incorporated until the current ones are resolved. The three test focuses (wholesale Drex, retail Drex via tokenized deposits, and tokenized federal bonds) will continue to be refined throughout 2025, prioritizing security, data privacy, and platform robustness before expanding their reach.

The central bank has been clear that it will only advance to production once Drex fully guarantees data protection and transaction reliability. While there is no official launch date, current estimates place a potential general rollout around 2025-2026, depending on the results of the ongoing pilot.

---

[3] Chainlink's Cross-Chain Interoperability Protocol (CCIP) allows secure interaction and value transfer between blockchain networks.

[4] https://www.tradingkey.com/news/cryptocurrencies/250407959-reuters#:~:text=Initially%20planned%20for%20late%202024%2C,its%20instant%20payment%20system%2C%20Pix

European Central Bank (ECB) Digital euro:

The ECB is developing a digital euro with a strong emphasis on privacy, aiming to offer the highest privacy levels of any electronic payment option. It includes offline functionality for cash-like privacy, where transaction details are only known to the payer and recipient[5].

The ECB has committed to ensuring that the Eurosystem cannot directly link users to their payments, aligning with GDPR. The European Data Protection Board (EDPB) has recommended further enhancements to ensure high data protection standards[6].

Bank of Canada:

The Bank of Canada has published research on privacy in CBDC technology, outlining different technical choices for privacy models and emphasizing the need for consultation with external parties to define privacy requirements[7]. This includes exploring blind signatures and off-chain transactions.

China's Digital Yuan (e-CNY):

China's e-CNY, one of the most advanced CBDC implementations, incorporates some privacy features, such as allowing users to conduct transactions without revealing their identity in certain cases. However, it has been criticized for potential surveillance capabilities, highlighting the balance between privacy and control[8].

CBDC Privacy Mechanisms

The following mechanisms are identified as critical for achieving near-absolute privacy in CBDCs. The analysis explores how privacy mechanisms integrate with Besu, their performance implications, and their suitability for LACNet's regional context.

[5] Digital euro and privacy

[6] Digital euro: ensuring highest data protection

[7] Privacy in CBDC technology

[8] Theories and Practice of exploring China's e-CNY

1. Zero-Knowledge Proofs (ZKP)

Description: ZKPs (e.g., zk-SNARKs, zk-STARKs[9]) enable transaction validation without disclosing sensitive data, ideal for CBDC anonymity.

- **Implementation**: Deployable via Ethereum smart contracts in Solidity or precompiled contracts. Off-chain proof generation (e.g., using ZoKrates[10]) with on-chain verification is practical.
- **Performance**: Proof generation is resource-intensive (O(n log n)), but verification is lightweight (O(1))[11].
- **Pros**: Robust privacy; efficient verification.
- **Cons**: High setup cost (trusted setup for zk-SNARKs); proof generation latency (~seconds).
- **Viability**: High with optimizations (e.g., zk-STARKs for scalability). DREX's exploration of ZKP validates feasibility.

2. Blind Signatures

Description: Blind signatures anonymize transactions by allowing signing without revealing content.

- **Implementation**: Implementable through smart contracts using elliptic curve cryptography (e.g., secp256k1[12]).
- **Performance**: Signing/verification is O(1), with minimal overhead (~ms latency). LACNet's writer nodes can manage this efficiently.
- **Pros**: Simple and effective anonymity.
- **Cons**: Key management complexity.
- **Viability**: High, easily integrated into LACNet's architecture.

---

[9] zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs (Scalable Transparent Arguments of Knowledge) are cryptographic methods that allow one party to prove knowledge of a value without revealing it.

[10] ZoKrates is a toolbox for zk-SNARKs on Ethereum that facilitates the creation of zero-knowledge proofs via high-level programming and integration with smart contracts.

[11] These are time complexity notations: O(n log n) represents proof generation time in ZKPs (grows with input size), while O(1) indicates constant-time verification regardless of input size.

[12] secp256k1 is a widely used elliptic curve in cryptography, notably used in Bitcoin and Ethereum for key generation and digital signatures.

3. Homomorphic Encryption (HE)

Description: HE allows computations on encrypted data, supporting operations like addition (PHE) or full computation (FHE)[13]. Libraries like Microsoft SEAL[14] implement schemes like CKKS or BFV[15].

- **Implementation**: HE can be integrated off-chain, with results verified on-chain via Besu smart contracts. FHE is impractical due to high overhead; PHE (e.g., Paillier) is more suitable for simple analytics (e.g., balance checks).
- **Performance**: PHE operations (e.g., addition) have ~O(n) complexity but are ~10^2 slower than plaintext; FHE is ~10^5 slower. LACNet's permissioned nature reduces throughput demands, but latency remains a bottleneck.
- **Pros**: Enables private computation (e.g., aggregated CBDC analytics).
- **Cons**: Significant latency; large ciphertext sizes (~MBs).
- **Viability**: Low for real-time transactions; medium for batch analytics. Off-chain computation clusters are recommended.

4. End-to-End Encryption (E2EE)

Description: E2EE ensures data is encrypted between endpoints, using AES-256 for symmetric encryption and ECIES[16] for key exchange.

- **Implementation**: LACNet already uses RLPx with ECIES for node communication. E2EE can extend to transaction payloads via smart contract logic.
- **Performance**: AES-256 encryption/decryption is O(n), with negligible latency (~µs). LACNet's validator nodes can handle this seamlessly.
- **Pros**: Mature; aligns with LACNet's existing security stack.
- **Cons**: Limited to communication privacy; does not obscure metadata.
- **Viability**: Very high, leveraging LACNet's built-in protocols.

---

[13] PHE (Partially Homomorphic Encryption) allows specific operations (e.g., addition) on encrypted data, while FHE (Fully Homomorphic Encryption) allows arbitrary computation but with high computational cost.
[14] Microsoft SEAL (Simple Encrypted Arithmetic Library) is an open-source library implementing homomorphic encryption schemes for secure data analysis.
[15] CKKS supports approximate arithmetic (e.g., for real numbers), while BFV supports exact arithmetic on integers both are common schemes in homomorphic encryption.
[16] Elliptic Curve Integrated Encryption Scheme (ECIES) is a hybrid encryption system combining asymmetric and symmetric cryptography for secure message transmission.

5. Selective Disclosure

Description: Uses cryptographic commitments (e.g., Pedersen[17]) or verifiable credentials to reveal only necessary data.

- **Implementation**: Besu smart contracts can implement Pedersen commitments, with off-chain computation for credential issuance. LACNet's LACChain ID framework supports this natively.
- **Performance**: Commitment generation/verification is O(1), with low overhead. LACNet's writer nodes can manage efficiently.
- **Pros**: Balances privacy and regulatory needs.
- **Cons**: Requires trusted issuers for credentials.
- **Viability**: High, enhanced by LACChain's identity stack.

6. Privacy by Design

Description: Embeds privacy into the system architecture via data minimization and pseudonymization

- **Implementation**: LACNet can adopt PETs[18] (e.g., anonymized node identities via enodeID hashing) and enforce minimal data collection in smart contracts.
- **Performance**: Negligible overhead; design-time cost.
- **Pros**: Proactive privacy protection.
- **Cons**: Requires upfront expertise.
- **Viability**: Medium-high, depending on developer capabilities.

Modern Privacy Alternatives (Post-Orion/Tessera)

Since Orion and Tessera are deprecated, LACNet must adopt newer privacy solutions for Hyperledger Besu:

1. **Besu Private Transactions with Enclaves**
   - Description: Uses secure enclaves (e.g., Intel SGX[19]) to process private transactions, replacing Orion.
   - Feasibility on LACNet: Medium; requires enclave-capable hardware on validator nodes, which may not be universal in LAC.

[17] Pedersen commitments are cryptographic primitives that allow values to be hidden while still enabling verification of certain properties, such as correctness or ranges.
[18] Privacy-Enhancing Technologies (PETs) are techniques and tools designed to protect personal data and user privacy in digital systems.
[19] Intel Software Guard Extensions (SGX) provide hardware-based isolation for sensitive computations, enabling secure enclaves for private transaction processing.

- Pros: Strong isolation; native Besu integration.
- Cons: Hardware dependency; enclave vulnerabilities.

2. **ZK-Rollups**
   - Description: Aggregates transactions off-chain using ZKPs, settling on-chain.
   - Feasibility on LACNet: High; Besu supports rollup integration via EVM extensions.
   - Pros: Scalability and privacy; reduces on-chain load.
   - Cons: Off-chain infrastructure setup.
   - Recommendation: ZK-Rollups are preferable for LACNet, offering both privacy and scalability without hardware constraints.

Considerations

ZKP, Blind Signatures, and Selective Disclosure are highly feasible on LACNet, leveraging Besu's EVM and smart contract capabilities. HE is viable for batch analytics but impractical for real-time use due to latency and computational overhead. ZK-Rollups offer a modern, scalable privacy solution, fitting LACNet's architecture. Addressing performance, connectivity, and expertise gaps is critical for successful deployment.

Regulatory Compliance

While these mechanisms enhance privacy, they must be carefully balanced with regulatory requirements. These are the regulatory frameworks to consider.

1. **Data Protection and Privacy**: Comply with laws such as Brazil's LGPD, Colombia's Law 1581, and GDPR-inspired regulations to guarantee user privacy, especially in cross-border transactions (Digital Privacy EU).
2. **AML/KYC (Anti-Money Laundering and Know Your Customer)**: Follow FATF[20] recommendations to prevent illicit activities, adapting traceability mechanisms that balance privacy and compliance (FATF Recommendations).
3. **Financial and Monetary Stability**: Align with IMF and BIS guidelines to avoid banking disintermediation and systemic risks, such as those described in the BIS Innovation Hub (BIS CBDC Framework).
4. **Foreign Exchange (FX) Regulations**: Review local FX regulations for cross-border payments, such as in Brazil with the BCB or in Mexico with Banxico, ensuring interoperability (WEF CBDC Interoperability).
5. **Interoperability and International Standards**: Adopt standards such as ISO 20022[21] and BIS principles to facilitate interoperability with other CBDCs, such as DREX (ISO 20022 for CBDCs).

[20] The Financial Action Task Force (FATF) is an intergovernmental body that sets international standards for combating money laundering and terrorist financing.
[21] ISO 20022 is a global standard for financial messaging. Its adoption in CBDCs ensures compatibility with existing banking infrastructure and cross-border interoperability.

6. **Financial Inclusion**: Design frameworks that promote access to unbanked populations, aligned with IDB objectives (IDB Financial Inclusion).
7. **Cybersecurity and Operational Resilience**: Implement regulations based on NIST[22] or ISO 27001[23] standards to protect against cyberattacks (NIST Cybersecurity Framework).

Features and limitations of Besu for solving CBWeb3 use cases

Use Case Context:

CBWeb3 targets two main scenarios in a wholesale context:

- Domestic (DvP[24]): Transfer and settlement of digital assets (e.g., tokenized bonds) and CBDCs, where financial privacy is critical.
- International (PvP[25]): Cross-border payments for FX settlement between interoperable networks, such as CBWeb3 and DREX, requiring privacy and regulatory compliance.

Capabilities for Wholesale Payments:

In wholesale environments (interbank, high-value transactions), privacy, traceability, and compliance are essential. Hyperledger Besu, as a permissioned Ethereum network, supports smart contracts and EVM extensions, allowing for the implementation of modern privacy mechanisms such as zero-knowledge proofs (ZKP), blind signatures, and selective disclosure.

With ZKPs (e.g., zk-SNARKs or zk-STARKs), transactions can be validated without revealing sensitive data. These proofs can be generated off-chain and verified on-chain in Besu with minimal computational cost, making them viable for financial privacy in CBDC systems. Likewise, ZK-Rollups provide a scalable solution by aggregating transactions off-chain and verifying them collectively on-chain, reducing network load while preserving confidentiality.

Besu also supports selective disclosure mechanisms (e.g., Pedersen commitments), allowing only the necessary data to be revealed to regulators while maintaining broader transaction privacy. This can be reinforced with frameworks like LACChain ID and verifiable credentials.

---

[22] The NIST Cybersecurity Framework provides voluntary guidelines based on existing standards to help organizations manage and reduce cybersecurity risks.
[23] ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a framework for establishing, implementing, maintaining, and continually improving an ISMS to ensure the confidentiality, integrity, and availability of information assets.
[24] Delivery versus Payment (DvP) is a settlement mechanism that ensures securities are delivered only if payment is made simultaneously, reducing counterparty risk.
[25] Payment versus Payment (PvP) is a settlement mechanism used in foreign exchange transactions where each payment is conditional on the other, eliminating principal risk.

Besu's IBFT consensus provides immediate finality, which is critical for irrevocable payments. Its permissioned nature, combined with encrypted communication channels (e.g., ECIES), ensures secure and confidential data exchange among authorized nodes. Additionally, blind signature schemes can anonymize content prior to validation—an effective and lightweight technique compatible with LACNet's existing cryptographic stack.

Challenges and Limitations:

While these advanced cryptographic tools offer promising privacy capabilities, their implementation presents challenges. ZKPs involve high proof-generation costs and require specialized expertise, though they are efficient to verify. More advanced methods like homomorphic encryption are only practical for aggregated analytics due to their significant computational overhead, making them unsuitable for real-time payments.

Adopting ZK-Rollups and similar off-chain privacy solutions requires complementary infrastructure beyond Besu, including coordination of new components and ensuring appropriate hardware availability. Secure enclave-based solutions (e.g., Intel SGX) are technically feasible but limited in practicality due to hardware requirements that are not yet widespread in the region.

Maintaining compatibility with legacy banking systems also adds complexity, requiring middleware to synchronize blockchain transactions with internal ledgers. Traditional RTGS features such as queuing or liquidity-saving mechanisms would need to be implemented via custom smart contracts or second-layer solutions.

Relevant Examples:

Pilots like Project Khokha (South Africa) and Project Ubin (Singapore) have demonstrated the feasibility of Ethereum-based permissioned networks for wholesale payments, incorporating privacy and transaction control. In Latin America, Brazil's DREX project is actively exploring ZKPs to strengthen transaction confidentiality, with several consortia proposing rollup-based and advanced cryptographic architectures in their pilots.

Conclusions

Following the analysis of privacy options for the CBWeb3 project on LACNet/Besu, the following conclusions emphasize the relevant and viable privacy mechanisms for wholesale transactions in Latin America and the Caribbean (LAC).

Wholesale Transactions as an Immediate Focus

Given the architectural maturity and current constraints of LACNet/Besu, CBWeb3 should prioritize wholesale transactions, such as interbank transfers and high-value settlements where privacy, auditability, and regulatory compliance are critical. Instead of relying on deprecated solutions like Tessera, the project should now incorporate modern privacy-preserving technologies supported by Besu's smart contract environment, including:

- **Zero-Knowledge Proofs (ZKPs):** Allow transaction validation without revealing sensitive information, resolving the confidentiality-verifiability trade-off.
- **Selective Disclosure**: Enables controlled access to transaction data for regulators under predefined conditions, aligning with compliance requirements.
- **Blind Signatures**: Offer participant anonymity without revealing transaction details, preserving competitive confidentiality.

Hyperledger Besu permissioned network ensures all entities are pre-identified and authorized, which supports regulatory alignment with frameworks like the FATF recommendations and national data protection laws (e.g., Brazil's LGPD). These privacy techniques, implemented at the smart contract level, allow configurable transaction visibility rules that protect data from peer institutions while maintaining transparency for designated authorities.

Despite these advantages, wholesale privacy implementation still faces technical challenges. While mechanisms like ZKPs and Pedersen commitments with range proofs can validate transactions without exposing values, they add cryptographic and computational complexity, requiring external proof generation and robust infrastructure. Additionally, metadata leakage remains a risk: even if transaction content is private, observable patterns in hashes or node activity can reveal transactional behavior. Countermeasures such as padding and decoy transactions can obscure these patterns but increase system complexity.

Strategic Recommendations for Enhancing Wholesale Privacy

1. **Enhance Privacy and Verifiability:** Integrate ZKP-based validation and Pedersen commitments to ensure wholesale transactions are private yet verifiable by validator nodes. This approach has been validated in pilots like Project Khokha, demonstrating the ability to support high-throughput, confidential transactions with immediate finality.

2. **Mitigate Metadata Leakage:** Apply obfuscation techniques, such as padded or decoy transactions, to conceal transaction frequency and volume patterns. This protects sensitive operational data from competitors within the network.

3. **Adopt Scalable Cryptographic Architectures:** Evaluate ZK-Rollups and other Layer 2 solutions as future extensions to enhance privacy and scalability, reducing on-chain load while preserving auditability and confidentiality.

4. **Promote Ecosystem Collaboration:** Engage with technology partners to develop secure cryptographic infrastructure, privacy-respecting governance models, and monitoring tools that align with LACNet's compliance and performance standards.