Layer-1 and Layer-2 Blockchains for Wholesales CBDCs and Tokenization

Krzysztof Gogol[1,3⋆], Claudio Tessone[1,2], and Benjamin Livshits[3]

[1] University of Zurich
[2] UZH Blockchain Center
[3] Imperial College London

Abstract. Central Bank Digital Currencies (CBDCs) are transforming the financial sector, offering an innovative approach for atomic and decentralized settlement of financial services. This paper focuses on wholesale CBDCs (wCBDCs), available only to institutions with central bank accounts and evaluates blockchain architectures, including Layer-1 (L1) and Layer-2 (L2) networks. We incorporate governance considerations, both for pubic and private networks, including the roles and responsibilities of the network operators. By systematically analyzing functional and technical prerequisites, we highlight the scalability-security trade-offs and present actionable recommendations for the deployment of wCBDCs on the blockchain networks.

Keywords: Wholesale CBDC · Blockchain · ZK-Rollup · Validium

1 Introduction

Central Bank Digital Currencies (CBDCs) can be categorized into retail and wholesale, each requiring distinct design considerations [5,18]. Unlike retail CBDCs, which are intended for public use, wholesale CBDCs (wCBDCs) are exclusively available to entities with accounts at central banks, facilitating interbank settlements and cross-border transactions. While CBDCs share similarities to stablecoins in Decentralized Finance (DeFi), the major difference is the fact that the issuer and guarantor of CBDC is a central bank.

While CBDC does have to be implemented using Distributed Ledger Technology (DLT) [7], the application of blockchain allows for the fundamental transformation of the financial system [13]. Blockchain ensures atomic transaction execution with almost instantaneous finality, resolving challenges related to Delivery vs Payment (DvP) settlement. Moreover, smart contracts — computer programs hosted and executed within the blockchain — can offer compliance assurance and further value-added services, such as trading and lending [20,16,10].

Smart contracts, introduced by Ethereum in 2013 [6], underpin DeFi and gained popularity thanks to their effectiveness and immutability. There are a number of initiatives that pilot the application of smart contracts for wCBDCs.

⋆ Corresponding Author: gogol@ifi.uzh.ch

In Project Mariana [2], smart contracts were applied for cross-border exchanges of wCBDC with the goal of increasing the efficiency of the FX market. In Project Guardian [3], smart contracts facilitated the trading and borrowing of tokenized government bonds and deposits. The tokenization of real-world assets (RWAs), especially debts, further extends the utility of smart contracts and wCBDCs. These initiatives utilize smart contracts that have already demonstrated their effectiveness in DeFi on Ethereum.

The expanding scope of wCBDC applications prompts questions regarding the implementation of wCBDCs, including cross-chain interoperability and availability. This work classifies wCBDCs into *native*, issued directly on the given blockchain, and *bridged*, minted on a domestic blockchain and bridged to other networks. Additionally, consideration is required for the selection of the blockchain for wCBDC issuance. This study compares layer-1 (L1) and layer-2 (L2) blockchain solutions. Rollups, a novel scalability solution, are gaining traction in DeFi [1], serving as L2 networks built atop existing layer-1 (L1) networks, predominantly Ethereum [17,9]. Unlike L1 chains, rollups do have consensus mechanism nor network of validators. They post compressed data into the underlying L1 blockchain. Depending on the validity prove mechanism, rollups can be classified into optimistic and Zero-Knowledge (ZK) based. We evaluate the applicability of optimistic and Zero-Knowledge (ZK) rollups, compared to private (permissioned) L1 blockchains. By fractal scaling rollups, the wCBDCs network can offer infinite Transaction Per Second (TPS) throughput.

Related Work. Existing surveys on DLT and L2 scaling [17,9,12] provide valuable insights. Guo, Kreitem & Moser (2024) [13] review public and private blockchains for CBDCs, emphasizing Byzantine Fault Tolerance, immediate block finality, and smart contract support as major prerequisites to consider by central banks. Rollup-based CBDC issuance is proposed in [14], and cross-border CBDC exchange is simulated in [11].

Contribution. This works contributes to the ongoing research on CBDCs by providing new insights into the implementation of CDBCs on rollups - a novel layer-2 blockchain solution. It compares L1 and L2 blockchains and evaluates their capacity to fulfill the prerequisites for wCBDCs issuance. It scrutinies the governance aspects of L1 and L2s, and analyzes the related risks related to security, scalability, and interoperability. Our contributions can be summarized as follows:

- We formulated and systematized the blockchain prerequisites necessary to support wCBDCs, categorizing them into functional and technical requirements.
- We analyze blockchain solutions, including L1 and L2 networks (rollups), in relation to these criteria and scrutinized the risks associated with centralization and governance.
- We present the approaches for CBDC interoperability and introduce wCBDC design options, including native and bridged tokens.

Paper Organization. The structure of this paper is as follows: Section 2 provides background information on blockchain and unifies terminology. Section 3 formulates the prerequisites for blockchain networks to accommodate wCBDCs. Section 4 assesses alternative blockchain solutions with respect to the established prerequisites. Section 5 examines wCBDC design options to address the cross-chain interoperability.

2 Blockchain Preliminaries

Blockchain networks enable atomic transaction settlement without intermediary institutions. Once recorded in the blockchain ledger, transactions are immutable—they cannot be altered or deleted. Second-generation blockchains, or referred to as programmable-blockchains, initiated by Ethereum in 2013, introduced smart contracts—self-executing computer programs hosted and executed on the ledger-extending the DLT application beyond payments. The recent innovation, introduced to increase the scalability of Ethereum, are rollups, layer-2 blockchains, which are gaining increasing popularity. This section briefly summarizes the key blockchain terminology, and introduce the concept of layer-2 scaling solutions.

2.1 Terminology

Blockchain networks are often categorized based on access and visibility. They can be permissioned or public, depending on access rights, and private or public, depending on data visibility. As these terms are sometimes used interchangeably, this section standardizes the terminology used throughout this work.

- *Public blockchain* - permissionless DLT network, e.g., Bitcoin or Ethereum. Any party can use the network (initiate transactions, read history) or participate in its maintenance (consensus, node).
- *Private (permissioned) blockchain* - permissioned DLT network, e.g., Corda, Hyperledger. Only invited parties are allowed to use or operate the network.
- *Privacy-preserving blockchain* - DLT network, in which transaction details are visible only to the parties involved in the transaction.
- *L1 blockchain* - DLT network with its own consensus mechanism and infrastructure of nodes and validators responsible for maintaining the network security and integrity, e.g. Ethereum, Corda, Hyperledger.
- *L2 blockchain* - DLT network that relies on security - consensus mechanism and infrastructure - and infrastructure of the underlying L1 network, e.g., Bitcoin Lightening Network.
- *Rollup* - noncustodial L2 DLT network, e.g., Arbitrum, Optimism, zkSync Era on Ethereum.
- *ZK rollup* - rollup that use on zero-knowledge (ZK) proofs to compress transactions into L1, e.g., ZKsync and StarkNet with Ethereum as L1.

– *Validium* - ZK rollup that posts in the underlying L1 only ZK proves of transaction state change, guaranteeing that any L1 user can examine the validity o L2 transaction without having access to any transaction data.
– *EVM-compatible blockchain* - DLT network that supports the execution of smart contracts developed for Ethereum Virtual Machine (EVM).

2.2 Layer-2 Blockchain and Rollup

There are two approaches that address the blockchain scalability challenges and the related spikes in gas prices: Layer-1 (L1) and Layer-2 (L2) scaling. The L1 scaling involves the creation of an entirely new blockchain, with new consensus mechanisms and distinct physical infrastructure that maintains the network. L2 scaling adopts an alternative strategy: computations are executed outside of the main blockchain, but their results are saved in the underlying chain. The major types of L2 include state (payment) channels, plasma, and rollups. While plasma and state channels represent L2s aiming to move both data and computation off-chain, rollups are non-custodial: they move computation and state storage off-chain but retain compressed transaction data or their validity proofs on the underlying chain. Consequently, rollups require fewer trust assumptions than state channels, plasma chains, or new L1 networks.

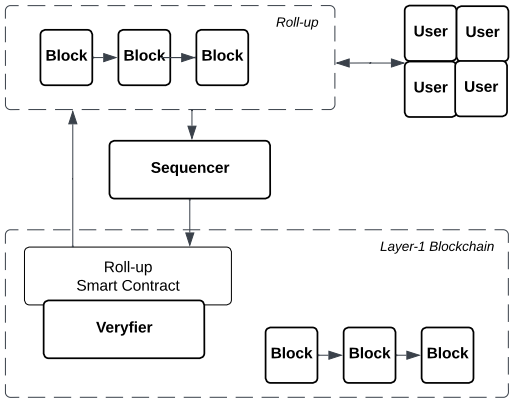

Fig. 1. Architecture of the roll-up - non-custodial L2 blockchain scaling solution.

Rollup A rollup functions as a blockchain: it produces blocks and snapshots those blocks to the main chain. However, it operates in an environment where operators are not trusted, implying that operators can potentially act adversarially by stopping block production, producing invalid blocks, withholding data, or attempting other malicious behaviors. There are two approaches to assure the correctness of the state at rollups: optimistic and zero-knowledge (ZK) proofs [17,9].

Figure 1 illustrates the roll-up architecture with its key components: sequencers and verifiers. Sequencers compress - roll up - transactions to the L1 chain and, by bundling such transactions, they generate great savings on gas fees. Verifiers are smart contracts that operate on L1 and verify the transactions stored by the sequencer, and they ensure the correctness of the transactions [17,22].

Soft and Hard Finality Transaction finality reflects the point in time at which a transaction state in the blockchain's ledger becomes irreversible. In rollups, there are two major types of finality: soft and hard. The *soft finality* indicates when the transaction is irreversible in L2, whereas *hard finality* refers to the point of time, when a batch with this L2 transaction cannot be reverted from the L1 chain [22].

Fractal Scaling Fractal scaling is the construction of multi-layer blockchain networks, with each new layer nested in the previous one. Thanks the transaction compression, fractal scaling increases the transaction throughput and reduces the gas costs of higher blockchain layers. At the cost of increased transaction finality, this approach is capable of processing an infinite number of transactions per second (TPS).

3 Blockchain Prerequisites for CBDCs

This section systematizes the criteria central banks should consider when issuing wCBDC on the blockchain. We categorize these prerequisites into two main groups: functional requirements of wCBDC design and technical network requirements.

3.1 Functional Requirements

Functional requirements of wCBDC design include the features and functionalities that are necessary for blockchain to effectively support the issuance and operation of wCBDCs. These requirements are derived from the four key design principles that central banks should consider:

1. Central banks should be the sole entities authorized to mint CBDCs.
2. Full visibility of issued wCBDCs should be ensured for central banks.
3. Access to wCBDCs should be restricted to eligible participants, reinforcing regulatory compliance.
4. Central banks should have constant access to and possession of a copy of the blockchain's ledger.

The first principle implies that central banks should oversee the issuance of wCBDCs: operate smart contacts and oracles that mint the native wCBDCs, and operate bridges that transfer wCBDC from the domestic to the destination blockchain. Full visibility and control over access to wCBDCs can be

achieved with smart contracts. Centralized stablecoins in DeFi on Ethereum and other blockchains have already implemented such mechanisms with blacklisting of sanctioned wallet addresses [**?**]. In general, achieving regulatory compliance can be realized through one of three approaches:

1. *Blacklisting*: In this approach, all blockchain users have the freedom to use wCBDC unless they are specifically listed on the sanctioned list.
2. *Whitelisting*: This method restricts the usage of wCBDCs solely to blockchain users included on the approved user list.
3. *Credential-based*: Under this approach, access to wCBDCs is granted exclusively to blockchain users possessing the requisite credentials. This approach is implemented with identifiers such as deID and digital signatures that cab be based on Zero-Knowledge Proofs (ZKPs).

3.2 Technical Requirements

Technical network requirements refer to the technical specifications and capabilities of the blockchain network, which are crucial for the secure and efficient functioning of wCBDCs.

1. *Integrity and Security* Byzantine Fault Tolerance (BFT) of the blockchain network is essential to mitigate the risk of attacks and vulnerabilities resulting from the centralization risk. This includes security concerns, such as resistance to 51% attacks in PoW blockchains and 67% attacks in PoS ones. While BFT guarantees the security and integrity of blockchain data, it is not the only factor. For ZK-rollups and validium, data integrity is additionally secured with ZKP, and the transaction validity proofs are stored in the L1 network, mitigating the centralization risk of the single sequencer.
2. *Transactions Per Second (TPS)* Transactions Per Second (TPS) refers to the throughput of the blockchain network in terms of transactions that can be processed per second. The European Central Bank's publications propose 150 000 TPS (with 3-4s finality) as a network requirement for retail CBDCs. Given the lower expected trading volume, the requirements for wCBDCs should be lower.
3. *Finality* Finality refers to the speed at which transactions are processed and become irreversible from the blockchain's ledger. It varies between blockchain protocols, with Bitcoin taking 12 minutes and Ethereum taking 12 seconds. In rollups, *hard finality* refers to irreversibility from the L1 chain, whereas *soft finality* from L2 chain [22].
4. *Strong Privacy* Strong privacy of blockchain transactions ensures that the transaction and its details are only visible to involved parties. However, in the context of central banks issuing wCBDCs, the strong privacy rule needs to be relaxed to allow central banks to access transaction details. This adjustment is essential to ensure compliance with regulatory requirements.
5. *EVM-Compatibility* In order to host and execute smart contracts, the blockchain network must have a virtual machine. Most DeFi smart contracts operate today on Ethereum, and EVM-compatible blockchains support smart contracts initially developed for the Ethereum blockchain.

4 Blockchain Review

There are various approaches to guarantee blockchain security and scalability. In this section, we analyze how various blockchains can fulfill the requirements for wCBDC deployment. In particular, we assess public L1 and L2 blockchains in various settings: public and private, permissioned and permissionless.

4.1 Assessment

Public L1 Blockchains Ethereum was the first programmable blockchain, and over half of DeFi's total value is locked there. Its advantages include the Ethereum Virtual Machine (support of smart contracts) and a high level of decentralization, which ensures security and Byzantine fault tolerance. Being PoS-based, malicious actors would need to control over 66% of staked Ethereum to alter Ethereum's ledger history. Challenges include the lack of transaction privacy, as all transactions on the Ethereum blockchain are public, and scalability concerns, such as high gas costs during network congestion and low TPS.

Public L1 Blockchains with Strong Privacy While some of the public L1 blockchains preserve the privacy of transactions, their user adoption remains low. Other concerns include the security model - consensus mechanism and the economic security for PoS networks - and EVM compatibility.

Private L1 Blockchains Hyperledger is a notable example of a private L1 blockchain provider. Advantages include high TPS and strong privacy of transaction data. Regulation can be enforced using ZK-based checks that are performed off-chain. Drawbacks include high infrastructure investments required for decentralization (and BFT) and a lack of support for smart contracts (VM).

Public Rollups As non-custodial layer-2 blockchains, rollups inherit security from the underlying L1 blockchains. Once hard finality is reached, altering the ledger of the underlying L1 blockchain becomes necessary to modify the rollup history. Consequently, rollups on Ethereum exhibit a security level that surpasses that of other L1 networks. Additionally, rollups offer enhanced scalability compared to their underlying L1 counterparts, with increased throughput and faster (soft) finality. While optimistic rollups achieve EVM compatibility more easily than ZK rollups, the hard finality of optimistic rollups typically takes around 7 days, compared to hours for ZK rollups. Today's rollups often lack the strong privacy feature.

Validium Validiums represent permissioned rollups, restricting participation solely to invited parties. Moreover, only invited parties have access to transaction data and history. Despite transaction states being stored on L1, typically the public Ethereum network, they remain encrypted, protecting them from Ethereum user visibility. Many Validium implementations are EVM compatible, utilizing both optimistic and ZK rollup technology. While achieving hard finality may pose

a concern, particularly for optimistic rollups, soft finality, especially when the sequencer can be considered trustworthy, is reliable. To operate a validium; a central bank would need to oversee i) a sequencer that aggregates transactions into blocks, ii) a prover that provides validity proofs for transactions, and iii) a verifier's smart contracts on the underlying L1 networks.

4.2 Blockchain Providers

Table 1 and fig 2 compares the features of the major L1 blockchain and rollup providers.

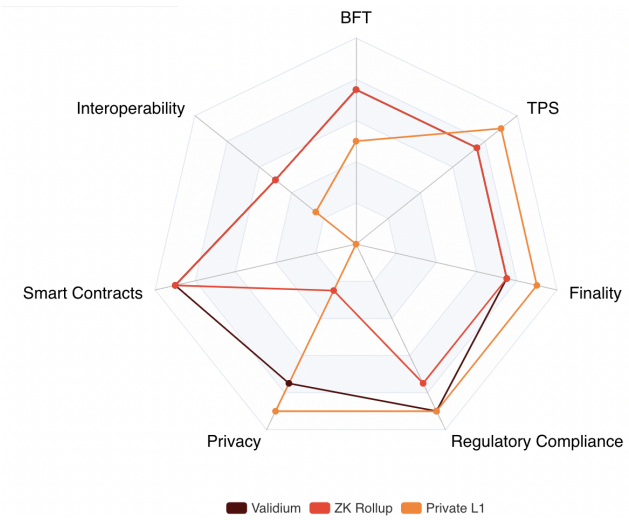

Fig. 2. Comparison between validium, ZK rollup and private L1 blockchain.

Table 1. Comparison of major L1 and L2 blockchain solution provider

	L1 Decent.	TPS	Finality	Privacy	VM	EVM
Ethereum	L1 High	12	12s	No	Yes	Yes
Hyperledger Fabric	L1 Low	100k	High	Yes	No	No
zkSync Era	L2 High	150	High/Low	No	Yes	Yes
zkEVM	L2 High	150	High/Low	No	Yes	Yes
StarkNet	L2 High	150	High/Low	No	Yes	No
Miden	L2 High	150	High/Low	Yes	Yes	No
Validium	L2 High	150	High/Low	No	Yes	Yes
Validium Fractal Scaling	L2 High	150k	High/Low	No	Yes	Yes
Polkadot Parachain	L2 Medium	-			Yes	
Cosmos Chain	L1 Low	-			Yes	

Based on the analysis of the available options, those closest to meeting the eligibility criteria for wCBDC implementation would be:

1. *Validium* solutions provide robust privacy features and compatibility with the Ethereum Virtual Machine (EVM).
2. *Private L1* blockchain with strong privacy features and support for the Ethereum Virtual Machine (EVM).
3. *Public ZK rollup with strong privacy* protections and compatibility with the Ethereum Virtual Machine (EVM).

These options offer a balance between security, privacy, scalability, and compatibility with existing Ethereum-based infrastructure, making them promising candidates for central banks considering wCBDC deployment. Nevertheless, the commercially available validium does not support strong privacy, whereas permissioned L1 and ZK rollups with strong privacy are not compatible with EVM.

5 Wholesale CBDCs Design Options

As demand for CBDCs across multiple blockchain networks is expected to emerge, addressing interoperability challenges becomes essential. This section preents two design paradigms for every blockchain tokens - native and bridged - and applied them for wCBDCs. *Native CBDCs* are issued by a central bank directly on multiple blokchains, each operated by different parties for specific wCBDC use cases, as depicted in fig 3. In the second approach, the central bank issues the wCBDC on its domestic blockchain platform and bridges wCBDCs to other blockchains - fig 4. Consequently, each *bridged CBDCs* corresponds to native or bridged CBDCs locked on another blockchain.

This design mirrors stablecoin designs on public blockchains, such as USDC from Circle or USDT from Tether. These stablecoins are issued as native or bridged tokens, depending on the blockchain. Initially, users may not notice any differences, as both native and bridged USDT and USDC maintain a 1:1 peg with the USD. However, disparities emerge in the underlying risks and costs associated with inter-blockchain transfers. Native stablecoins incur lower transfer costs when transferred between blockchains and are not prone to potential hacking attacks on bridges. Contrarily, bridged stablecoins offer a simpler and swifter setup process, with less complex maintenance compared to their native counterparts. Given the growing demand for stablecoins across multiple blockchains, bridged stablecoins often precede native issuance.

Likewise, central banks should consider strategies for simultaneously supporting wCBDCs across multiple blockchain platforms. Anticipating the growing demand for wCBDC across various DLT platforms —each managed by distinct entities, serving distinct objectives, and operating within diverse jurisdictions— is imperative. For instance, some blockchain platforms may solely leverage wCBDCs for settlement functions, while others facilitate asset tokenization exchanges or cross-border transactions. Such operations can be automated through the application of smart contracts.

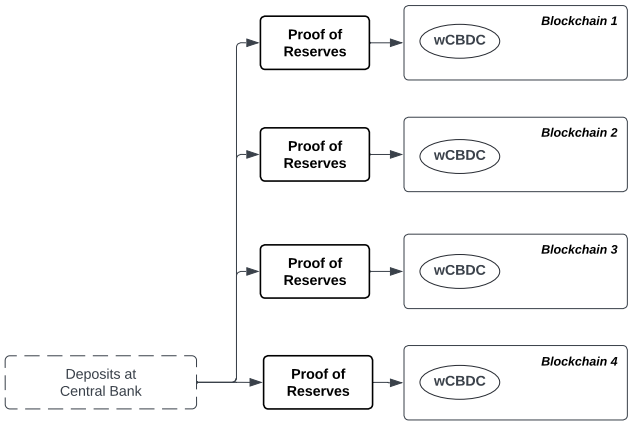

Fig. 3. Architecture of native wCBDC setup. Central bank issues wCBDCs directly on destination blockchain

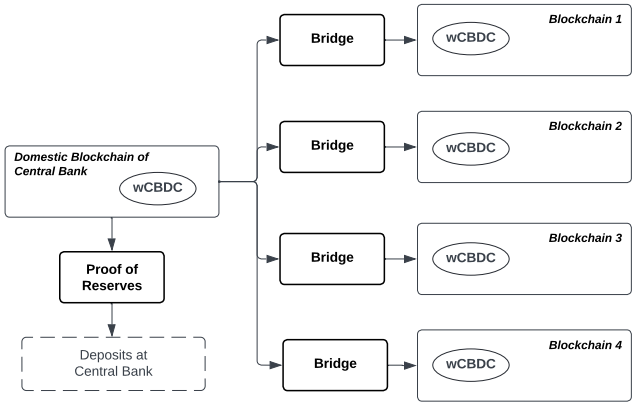

Fig. 4. Architecture of bridged wCBDCs. Central bank issues wCBDCs on the domestic blockchain and bridges to the destination blockchains

5.1 Native wCBDC

Native wCBDC is issued by the central bank directly on each blockchain operated by the regulated institution, e.g., the Swiss National Bank issued the native digital CHF (wCBDC) on the SDX platform in the pilot project Helvetia [4]. This approach does not impose any technological limitation on the financial institutions' blockchains. Each institution can decide on the technology of its

DLT network. Another advantage is the support of competition between DLT platform operators in order to lower fees and boost innovation. However, this approach requires the central bank to maintain the native wCBDCs on multiple networks and poses interoperability challenges in cross-DLT platform transfers.

5.2 Bridged wCBDC

In this approach, the central bank issues wCBDC on the domestic blockchain platform. The interested parties interact directly within the central bank platform or bridge wCBDCs to their DLT networks. For example, in Project Mariana [2], wCBDCs of Swiss Franc, Euro, and Singapore Dollar were bridged from the domestic blockchains of central banks to the blockchain of Project Mariana. This approach requires the central bank to maintain its own DLT network and introduce additional security and trust assumptions related to the maintenance of bridges to other blockchains. It creates challenges related to enforcing regulations on the blockchains operated by external parties.

The design of wCBDC should envisage efficient settlement of transactions as well as the support of other applications that might become possible thanks to smart contracts.

6 CBDCs in DeFi

The application of wCBDCs extends beyond atomic payments and settlements, when applied in DeFi smart contracts. As most DeFi smart contracts are developed and operated on Ethereum, DLT networks that aim to operate them should be EVM-compatible. DeFi protocols can be applied for multiple use cases ranging from trading, lending, and borrowing to asset management [19,15,10].

As it was initially not feasible to implement an order book on the blockchains due to costs and security reasons [**?**], decentralized exchanges - DeFi smart contacts that facilitate trading - introduced Automated Market Makers (AMMs) [21]. AMMs determine the exchange price of tokens based on the token reserves in the liquidity pool. AMMs can enable the atomic exchange of various wCBDCs or the exchange of wCBDCs for the tokenized assets. Protocols For Loanable Funds, or short Lending Protocols [8] facilitate lending and borrowing of tokens with the interest-rates formula implemented within the smart contract. Thanks to lending protocols, wCBDCs can be atomically borrowed with tokenized assets as collateral.

The potential applications of wholesale CBDCs (wCBDCs) in conjunction with DeFi protocols and tokenized real-world assets (RWAs), such as tokenized bonds, include the following:

- **Trading:** Smart contracts, particularly Automated Market Makers (AMMs), act as trading counterparties for tokenized RWAs or facilitate transactions in the foreign exchange (FX) markets.

- **Forex Market:** AMMs provide efficient FX trading by acting as decentralized counterparties, enabling seamless cross-border currency exchanges with wCBDCs.
- **Lending:** Cross-bank repurchase agreements (repos) leverage tokenized RWAs, such as bonds, as collateral to borrow wCBDCs, enhancing liquidity and minimizing settlement risks in interbank markets.

These use cases demonstrate the versatility of wCBDCs in bridging traditional finance and decentralized financial infrastructure, unlocking new efficiencies and opportunities.

7 Discussion

Interoperability Both approaches - native and bridged CBDCs - present challenges for central banks. Native CBDCs require the support of various blockchains and bridged CBDCs of multiple bridges. While native CBDCs are direct liabilities of central banks, bridge CBDCs can be viewed as indirect liabilities. Bridged CBDCs are backed by other CBDCs, which ultimately represent direct liabilities of central banks. Furthermore, if the bridge from the domestic central bank blockchain to the destination one is not operated by the central bank, the bridge CBDCs can be considered private money.

Scalability vs Smart Contracts Most of private L1 blockchains operate the UTXO-bases model rather than an account-based model. While the UTXO-based network optimize TPS capacity and transaction privacy, they do not sufficiently support smart contract execution, including DeFi protocols. The ability to seamless operate DeFi protocols, originated on Ethereum, should be considered a precondition for the wCBDCs deployment. Rollups 0 L2 blockchains - rollups - as account-based networks, support smart contracts and offer EVM-compatibility.

Security and Decentralization Permissioned L1 blockchains require for its operation the entire network of node operators. Otherwise, the network does not achieve decentralization and sufficient resistance to attacks (Byzantine Fault Tolerance) and, consequently. Conversly, permissioned L2 blockchains can inherit the security grantees from the underlying public L1, mitigating the centralization risk.

8 Conclusions

This study established key principles for wholesale CBDC (wCBDC) design, and presents a clear taxonomy of Layer-1 (L1) and Layer-2 (L2) blockchain architectures. The taxonomy highlights their respective capabilities and risks, including the transparency challenges of public chains, control issues in private chains, and vulnerabilities of centralized sequencers in Layer-2 solutions, such as data withholding and censorship.

By addressing scalability, security, and governance challenges, this study provides a structured framework to guide central banks in selecting blockchain solutions that meet the unique demands of wCBDCs while mitigating key risks.

Acknowledgements

This research article is a work of scholarship and reflects the authors' own views and opinions. It does not necessarily reflect the views or opinions of any other person or organization, including the authors' employer. Readers should not rely on this article for making strategic or commercial decisions, and the authors are not responsible for any losses that may result from such use.

References

1. DeFi Llama (12 2022), https://defillama.com/
2. Cross-border exchange of wholesale cbdcs using automated market-makers (2023), https://www.bis.org/about/bisih/topics/cbdc/mariana.htm
3. Project guardian - open and interoperable networks (2023), https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-guardian-open-interoperable-networks
4. Project helvetia (2023), https://www.bis.org/about/bisih/topics/cbdc/helvetia.htm
5. Auer, R., Frost, J., Gambacorta, L., Monnet, C., Rice, T., Shin, H.S.: Central bank digital currencies: motives, economic implications and the research frontier (2021), https://www.bis.org/publ/work976.pdf
6. Buterin, V.: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. (2014)
7. Chaum, D., Grothoff, C., Moser, T.: How to issue a central bank digital currency (2021)
8. Chiu, J., Ozdenoren, E., Yuan, K., Zhang, S.: On the Fragility of DeFi Lending (2022), https://g20.org/wp-content/uploads/2022/02/FSB-Report-on-Assessment-of-Risks-to-Financial-
9. Gangwal, A., Gangavalli, H.R., Thirupathi, A.: A survey of layer-two blockchain protocols (2022)
10. Gogol, K., Killer, C., Schlosser, M., Boeck, T., Stiller, B.: SoK: Decentralized Finance (DeFi) - Fundamentals, Taxonomy and Risks. vol. 2022-March. IEEE Computer Society (2023)
11. Gogol, K., Messias, J., Schlosser, M., Kraner, B., Tessone, C.: Cross-border exchange of cbdcs using layer-2 blockchain (2024)
12. Gorzny, J., Derka, M.: A rollup comparison framework (2024)
13. Guo, S., Kreitem, J., Moser, T.: Dlt options for cbdc. Journal of Central Banking Theory and Practice **13**(1), 57–88 (2022)
14. Nyffenegger, R.: A proposal for a layer-2 cbdc on a rollup (2023)
15. Schär, F.: Decentralized finance: on blockchain-and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review **103**(2), 153–174 (2021). https://doi.org/10.20955/r.103.153-74

16. Schär, F.: Decentralized finance: On blockchain- and smart contract-based financial markets (2020), https://ssrn.com/abstract=3571335orhttp://dx.doi.org/10.2139/ssrn.3571335
17. Sguanci, C., Spatafora, R., Vergani, A.M.: Layer 2 blockchain scaling: A survey. arXiv preprint arXiv:2107.10881 (2021)
18. Ward, O., Rochemont, S.: Understanding central bank digital currencies (cbdc). Institute and Faculty of Actuaries pp. 1–52 (2019)
19. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.: SoK: Decentralized Finance (DeFi) (1 2021), http://arxiv.org/abs/2101.08778
20. Werner, S.M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., Knottenbelt, W.J.: Sok: Decentralized finance (defi) (2022)
21. Xu, J., Paruch, K., Cousaert, S., Feng, Y.: SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols (3 2021), http://arxiv.org/abs/2103.12732
22. Yee, B., Song, D., McCorry, P., Buckland, C.: Shades of finality and layer 2 scaling (2022)