WHITEPAPER

Permissioned and Permissionless **Blockchains in Tomorrow's Financial System**

Fireblocks

Table of contents

Executive summary

Since the Bitcoin blockchain went live on January 3rd, 2009, permissionless blockchains have significantly influenced various aspects of the financial industry. Data[1] for December 2024 reveals an outstanding total of 180.4 million active user wallets across the top five permissionless blockchain networks, and a remarkable total of $4.526 trillion USD token trading volumes for the top five blockchains. However, these figures are primarily driven by individual and retail traders, with limited participation from traditional financial institutions (FIs).

Over the past year, Fireblocks has witnessed a similar surge in interest and commitment from financial institutions towards the digital assets space. After their initial foray into the digital assets space in 2018, FIs are actively seeking ways to scale and commercialize digital assets within their offerings. However, their primary concerns revolve around ensuring robust security measures, maintaining compliance with regulatory frameworks, and retaining control over their digital asset operations. In many cases, these concerns (as well as regulatory skepticism) have pushed them to experiment with and build on permissioned blockchains.

Choosing between permissionless and permissioned blockchains is a key strategic consideration in the evolving digital finance landscape. This dichotomy represents contrasting philosophies of openness versus control, each catering to specific needs in the digital age. Permissionless blockchains, epitomized by pioneers like Bitcoin and Ethereum, offer transparent and secure decentralized platforms, but face challenges like privacy and settlement finality. On the other hand, permissioned alternatives, such as R3's Corda, Digital Asset's Canton Network, and the Hyperledger consortium, provide a controlled environment that prioritizes security and operational efficiency, ideal for enterprises seeking to harness distributed ledger technology while mitigating associated risks.

Amidst market upheavals, the need for a nuanced approach to blockchain adoption has never been more apparent, as prospective blockchain users look to find the right balance between the allure of innovation and the paramount importance of security and stability.

This paper examines permissioned and permissionless blockchains in depth, exploring how distinct systems are designed to support specific use cases. We explore the crucial role of interoperability in connecting these blockchain types, which is critical to forming a cohesive and integrated ecosystem. Moreover, we delve into the importance of composability—the ability to compile logic and program assets across different networks. Evaluating platforms like the Ethereum Virtual Machine (EVM) and various interoperability protocols, we consider how these solutions facilitate cross-chain interactions, which are vital for a unified financial system.

Finally, to highlight the importance of composability across networks, we present a use case where a wholesale CBDC interacts with other digital assets in order to orchestrate a payment flow from one permissionless blockchain to another via a highly permissioned central bank operated blockchain.

The timing for financial institutions to consider permissionless blockchains has never been more critical. As the digital finance ecosystem matures, we're witnessing a convergence of factors that make this an opportune moment for traditional players to enter the space.

VARUN PAUL
Senior Director, Financial Markets

OREN GOLDBERG
Technical Solutions Principal

AMP BURAPACHAISRI
Business Solutions Associate

[1] As seen on https://tokenterminal.com/terminal

Why Now?

Recent developments underscore the growing legitimacy and integration of crypto assets:

2025

December 2024
The European Union finalizes its comprehensive crypto regulation framework, MiCA 2.0, setting a global standard for digital asset governance.

December 2024
Ripple launches RLUSD, an enterprise-grade stablecoin, available on global exchanges from December 17, expanding the stablecoin ecosystem.

November 2024
Revolut expands its standalone crypto exchange platform, Revolut X, to 30 new markets.

October 2024
Stripe acquires stablecoin infrastructure provider Bridge for $1.1 billion, marking a significant consolidation in the crypto payments sector.

July 2024
Spot ETH ETFs begin trading, with the first day of trading seeing a record of over $1.1 billion in trading volume.

June 2024
VanEck files for the first Solana ETF, signaling Wall Street's expanding interest in diverse crypto assets beyond Bitcoin and Ethereum.

April 2024
Stripe re-enters crypto payments, integrating USDC stablecoins on Solana, demonstrating renewed confidence in digital assets' stability and utility.

March 2024
BlackRock launches the BUIDL (BlackRock USD Institutional Digital Liquidity Fund) fund, offering qualified institutional investors access to tokenized US dollar yields on the Ethereum blockchain and reaching $500m by August 2024.

January 2024
SEC approves multiple Bitcoin ETFs, including offerings from Grayscale, BlackRock, and Fidelity, marking a watershed moment for crypto's mainstream adoption.

November 2023
J.P. Morgan and Apollo deliver “Project Guardian,” showcasing cross-chain portfolio management for tokenized assets.

October 2023
The Bank for International Settlements (BIS) and central banks of France, Singapore, and Switzerland successfully test cross-border wholesale CBDCs through Project Mariana, showcasing the potential of DeFi for global FX markets.

September 2023
Visa expands stablecoin settlement capabilities to merchant acquirers on Solana.

August 2023
PayPal launches PYUSD, a regulated stablecoin, bridging traditional finance and DeFi.

April 2023
Franklin Templeton launches the Franklin OnChain U.S. Government Money Fund (FOBXX), the first U.S.-registered mutual fund on a permissionless blockchain (Polygon).

July 2022
BNP Paribas launches ESG tokenized bonds on a permissionless blockchain.

2022

In this comprehensive examination, we delve into the evolving landscape of blockchain technology, recognizing the critical roles of permissionless and permissioned blockchains. This coexistence underscores the importance of interoperability in seamlessly connecting public and private markets. Our analysis advocates for financial institutions to adopt a proactive stance towards digital assets and blockchain technology, emphasizing interoperability as a cornerstone of future success.

Interoperability, in this context, extends far beyond basic asset transfers. It encompasses full programmability and composability across diverse blockchain ecosystems, enabling a new paradigm of financial innovation. By embracing these principles, institutions can ensure long-term viability, keep pace with rapid technological advancements, and harness the unique strengths of both permissioned and permissionless blockchains.

Established standards, such as the Ethereum Virtual Machine (EVM), offer a solid foundation for achieving this level of interoperability.

EVM, with its widespread adoption and robust developer ecosystem, has the potential to serve as the critical bridge between private and public markets. This approach allows institutions to maintain control over sensitive operations while tapping into the innovation and liquidity of permissionless blockchain ecosystems, creating new, composable financial products that span both domains.

By embracing this forward-thinking strategy, financial institutions can future-proof operations in an increasingly interconnected landscape. As traditional finance and blockchain technologies converge, those prioritizing interoperability will be best positioned to thrive in tomorrow's digital asset economy. Institutions that focus on seamlessly integrating permissioned and permissionless systems will shape the future of finance, unlocking new opportunities and driving innovation across the sector.

The future of permissionless blockchains in tomorrow's financial ecosystems

The rise of permissionless blockchains

Bitcoin's launch in January 2009 marked a pivotal moment, igniting the era of permissionless blockchains. Under Satoshi Nakamoto's pseudonym, Bitcoin introduced the world to a "peer-to-peer electronic cash system," a novel concept that quickly gained traction. While we can think of this as the "big bang" moment of blockchain technology, marking the inception of a revolutionary idea, the subsequent evolution and developments are equally significant. What began as a niche technology for digital currency enthusiasts soon became a global phenomenon, spawning the concept of decentralized finance (DeFi) and laying the groundwork for countless innovations and transformative advancements in the blockchain ecosystem.

The evolution of permissionless blockchains

The evolution of permissionless blockchains – decentralized, publicly accessible networks where anyone can participate without needing approval from a central authority or entity – can roughly be grouped into the following phases, each representing a significant leap in technological advancements and approaches.

- **Phase 1 (2009-2015): The Advent of Digital Currency - Bitcoin and Proof of Work**

  Bitcoin epitomizes the first phase of permissionless blockchains. Launched in 2009, Bitcoin was the first decentralized cryptocurrency designed to function as a digital ledger. Its success laid the foundation for blockchain technology, demonstrating its potential to create a secure, transparent, and immutable record of transactions. By September 2015, Bitcoin's market capitalization had grown to $3.4 billion, with approximately 14.5 million bitcoins in circulation.

  Bitcoin's initial achievements were impeded by high transaction fees and limited scalability, which stems from a design that prioritizes security and decentralization over scalability.

  This shortcoming allowed Ethereum to take the lead, which capitalized on its programmability to dominate the development of decentralized applications (dApps) in NFTs, DeFi, and other use cases.

- **Phase 2 (2015-2021): Smart Contracts, Decentralized Applications, and Proof of Stake**

  Ethereum's innovative approach to using smart contracts allowed developers to create decentralized applications (dApps) and execute programmable transactions on its blockchain. This marked a significant shift from Bitcoin's basic transaction ledger to a more versatile and functional platform. Furthermore, its Turing-complete programming language, Solidity, spurred the creation of new token standards, which led to robust and innovative experiments in DeFi, non-fungible tokens (NFTs), and decentralized autonomous organizations (DAOs). While this unprecedented level of innovation and flexibility outpaced anything seen in the Bitcoin ecosystem, it also exposed Ethereum's critical issues with scalability and throughput, manifesting in high gas fees and network congestion during periods of high activity.

- **Phase 3 (2021 - Now): Scalability, Interoperability, and Composability**

  The third phase focuses on addressing the scalability issues faced by earlier blockchains. Layer 2 solutions, such as Optimism, Arbitrum, Base, and zkSync, emerged to enhance transaction throughput and reduce Ethereum costs while still inheriting Ethereum's robust security designs. Alternative Layer 1 blockchains, like Solana, Avalanche, and TON, introduced innovative consensus mechanisms for higher performance and lower latency. Interoperability has also become a key focus, with protocols like Wormhole, Axelar, LayerZero, Ownera Fin P2P, Chainlink CCIP, and others enabling different blockchain networks to communicate and interact seamlessly. These advancements allow diverse networks to communicate and transact, fostering a more cohesive, efficient, and scalable ecosystem.

The Bitcoin community has not been idle in the face of these challenges either. They have been addressing these issues head-on through several key contributions. Layer 2 solutions, including the Lightning Network, Stacks, and Rootstock, significantly improve Bitcoin's scalability and efficiency by handling transactions off the main blockchain. Additionally, innovations such as Ordinals and BRC20 tokens facilitate the creation of NFTs and fungible tokens directly on Bitcoin. Proposals like OP_CAT aim to bring more advanced smart contract functionalities to the network. These collective efforts instill hope for the future, showing that Bitcoin's efficiency and versatility can be enhanced while staying true to its core values of decentralization and security.

The strengths of permissionless blockchains

Bitcoin's launch in 2009 was the genesis of permissionless blockchains, sparking a wave of innovation that evolved through distinct technological leaps and laid the foundation for today's decentralized financial ecosystem. Each phase introduced new capabilities that expanded the technology's appeal, moving from digital currency to programmable smart contracts and, more recently, to highly scalable and interoperable ecosystems. Beyond these advancements, the themes of openness, accessibility, and trust underpin permissionless blockchains and have positioned them as essential infrastructure for Web3 and the future of finance.

- **2021's Layer 1 Token Surge: a catalyst for ecosystem growth**

  The 2021 surge in Layer 1 token prices — Bitcoin up 62%, Ethereum 404%, Solana 11,366%, and Avalanche 3,346% — sparked a wave of interest across the tech and finance sectors. This price rally drew unprecedented venture capital and accelerated development iin blockchain ecosystems, creating a "flywheel effect" of funding, talent, and innovation. With over $104 billion invested in crypto since 2014, much of it directed to infrastructure, CeFi, and DeFi, Layer 1 ecosystems saw transformative growth. Developer activity skyrocketed, as seen in Electric Capital's 300% quarter-over-quarter increase in smart contract deployments on EVM chains, highlighting the increasing appeal for builders and investors alike.

  This token-driven momentum established Layer 1 platforms as a new foundation for financial systems, drawing continuous investment and positioning blockchain for broader adoption and real-world applications.

- **Trust and Decentralization**

  The decentralized structure of permissionless blockchains, a defining feature from Bitcoin's inception, fosters trust in a unique way. By distributing control across a global network of nodes, these blockchains remove the need for centralized authorities and intermediaries, instead relying on consensus mechanisms to secure the network. Each subsequent phase, from Bitcoin's Proof of Work to Ethereum's Proof of Stake and other consensus mechanisms, has reinforced this decentralization. It is this trust-by-design approach that not only enhances security but also aligns with the values of transparency and accountability, enabling a new level of assurance for participants.

- **Accessibility and Permissionless Participation**

  Permissionless blockchains provide unparalleled accessibility by removing entry barriers and allowing anyone with internet access to interact onchain. This theme of inclusivity has been strengthened over time with developments like Ethereum's dApp ecosystem, which expanded blockchain use cases to a diverse range of applications including DeFi, NFTs, and DAOs. By eliminating the need for centralized gatekeepers, these open networks democratize access to financial services, making it possible for individuals worldwide to participate in and benefit from the digital economy.

- **Innovation and Programmability**

  This confluence of factors has supercharged innovation within public, permissionless chains, far outpacing progress in private and permissioned networks. The synergy between a burgeoning developer community, substantial venture funding, and active retail participation has fostered unprecedented creativity and technological advancement.

Ethereum's successful implementation of the Merge, Shapella, and Dencun upgrades is a testament to permissionless blockchains' resilience. These transitions, notably the shift from Proof of Work to Proof of Stake consensus mechanisms, have significantly enhanced energy efficiency while maintaining operational continuity. Ethereum's ability to avoid outages during high-volume periods and critical upgrades demonstrates the robustness required to support an expanding decentralized ecosystem.

- **The future of blockchain: parallels with internet evolution**

  The trajectory of blockchain development bears striking similarities to the evolution of the Internet, where network effects are crucial. Permissionless blockchains are well-positioned to leverage this dynamic, having already secured critical components such as venture funding, a vibrant developer ecosystem, and broad retail engagement.

  Drawing a parallel to the development of the Internet versus Intranets, builders on the public Internet had to learn specific languages and protocols that were different from those used in private Intranets. Similarly, developers working with Ethereum or permissioned blockchains face the challenge of mastering specific languages and frameworks unique to each platform. This learning curve can be a significant barrier to entry, affecting the developer adoption rate and, consequently, the ecosystem's growth.

  Permissionless blockchains are primed to outpace their private and permissioned counterparts, echoing how the open Internet eventually triumphed over closed Intranets. Decentralized by design, these networks dismantle traditional entry barriers, empowering global participation without the need for centralized intermediaries.

  This democratization is a crucial driver of innovation and efficiency, as seen in the rapid growth and development of blockchain infrastructure and applications.

  Furthermore, permissionless blockchains benefit from network effects; as more users and developers engage, the ecosystem becomes more robust and valuable.

  This dynamic is evident in the expanding user base and increasing number of applications built on networks like Ethereum, TON, and Solana.

Challenges faced by financial institutions in adopting permissionless blockchains

Despite the transformative potential of permissionless blockchain technology, financial institutions face a gauntlet of challenges in their adoption journey. The issue of regulatory compliance is at the forefront of these obstacles; it is a non-negotiable requirement for entities operating in the traditional financial sector.

- **Regulatory hurdles: a compliance conundrum**

  Across the globe, regulatory requirements for risk-managing financial services delivered via permissionless ledger technology are often inconsistent or disproportionate, or both. This is usually for three reasons.

  Firstly, the decentralised non-intermediary nature of permissionless ledgers creates a different operational risk profile from other types of financial technologies. This has not been addressed clearly in operational resilience / material outsourcing frameworks. We note that workable policy precedents do already exist. A number of critical technologies deeply integrated into regulated financial services, for instance cloud computing, rely on open-source frameworks, and do so in safe and compliant ways. Open source frameworks, from an operational risk management perspective, are analogous to permissionless ledgers.

  Secondly, tokens issued on permissionless blockchains, unlike equities, have multiple uses which are not, and cannot be, pre-determined by the issuer. For instance, an ETH token can be used for investment, perhaps for payment, and often to allow the transfer of a tokenized fund. To date, rules applicable to ETH tokens address one, or two of these use cases, but as a result, make the infrastructure use prohibitively expensive. Prudential regulators should be aware of all uses of permissionless ledgers and tokens in order to regulate them proportionately.

Thirdly, because permissionless ledgers change the operational risk profile of services delivered through them, the paradigm of same risk/same rules does not hold. In addition to operational, and financial stability risks, tax frameworks, settlement finality rules, and AML rules need to be adapted. Reporting, data and privacy frameworks also can be clearer, as, for instance, node operations must navigate varying data privacy and financial reporting requirements, adding complexity for financial institutions hoping to leverage blockchain technology. Further, staking is an activity over which financial regulation might get extended. This creates more questions around the classification of staking rewards and the responsibilities of validator nodes.

- **Scalability: the throughput dilemma**

  While Layer 2 solutions have made strides in addressing scalability, many permissionless blockchains still struggle to match the transaction throughput required by large financial institutions. The specter of high transaction fees during network congestion further erodes the economic viability of using permissionless blockchains for high-volume operations. This scalability challenge is not just a technical issue, but a fundamental barrier to the widespread adoption of permissionless blockchains in institutional finance. Until these networks can consistently handle the transaction volumes typical in traditional finance without prohibitive fees, many institutions will remain on the sidelines.

- **The double-edged sword of transparency**

  Transparency, often touted as a key benefit of permissionless blockchains, presents challenges for financial institutions. When combined with other data sources, the public nature of blockchain transactions can inadvertently expose sensitive client information.

  This level of transparency can be a liability for financial institutions, potentially compromising client privacy and exposing individuals to risks such as identity theft and financial fraud. Balancing the benefits of blockchain transparency with the need for client data protection remains a significant challenge for institutions considering permissionless blockchain adoption.

  As financial institutions continue to explore the potential of permissionless blockchains, addressing these regulatory, scalability, and privacy concerns will be crucial. The future of institutional involvement in permissionless blockchains hinges on finding innovative solutions to these persistent challenges.

A spectrum of blockchains, from permissionless to permissioned

As FIs navigate these challenges, it's crucial to understand the full spectrum of blockchain technologies available and how they might interact in the future financial ecosystem.

Permissioned blockchains are a type of blockchain where access to the network is restricted and controlled through a governance model. Within this type of blockchain, only certain users have the right to participate in the network with actions such as creating transactions, writing data, or reading information from the blockchain. Its key distinction from permissionless blockchain is the ability to regulate who can participate in the network and under what conditions, allowing for a customizable level of security, privacy, and governance that suits the needs of an organization.

An example of a permissioned blockchain is Hyperledger Besu, part of the broader Hyperledger project hosted by the Linux Foundation. Its permissioned structure distinguishes it from permissionless blockchains, where anyone can join and participate without restrictions. This setup enables organizations to create a distributed ledger technology (DLT) environment that meets privacy, compliance, and scalability requirements.

Another example worth highlighting is the Canton Network, which takes a hybrid approach in the form of a public, permissioned blockchain. Developed by Digital Asset, Canton Network uniquely blends privacy and control typical of permissioned networks with elements of permissionless blockchain openness. It offers granular privacy and data control at the sub-transaction level. Additionally, it is designed to meet financial institutions' regulatory and operational requirements while offering a level of decentralization through its public synchronization by a network of independent companies.

Finally, J.P. Morgan's Kinexys Digital Assets platform is a permissioned blockchain designed for trading and settling tokenized financial instruments. It leverages the Ethereum Virtual Machine (EVM) and can interoperate with other non-EVM networks. To date, the platform has processed over $900 billion in tokenized assets, such as U.S. Treasuries, demonstrating its capacity for handling high-value transactions and its significant role in the financial blockchain ecosystem.

Key considerations for FIs when adopting blockchain technology

Control

Financial institutions (FIs) must maintain strict control over their operations and data to comply with regulatory requirements and internal policies. This need for control becomes particularly challenging when adopting blockchain technology. The decentralized nature of permissionless blockchains often conflicts with traditional control mechanisms used by FIs. As a result, these institutions need help to balance the innovative potential of blockchain technology with their regulatory obligations and risk management practices.

To address this challenge, many FIs are exploring permissioned blockchain solutions that offer the benefits of distributed ledger technology while preserving the necessary level of control and oversight. This approach allows FIs to leverage blockchain's advantages in transaction efficiency and data integrity without compromising their ability to meet regulatory standards and manage operational risks effectively.

- **Governance:** FIs require clear governance structures to manage blockchain technology. This includes defining roles and responsibilities for maintaining the blockchain and ensuring compliance with regulatory standards.
- **Data Control:** With permissionless blockchains, data is distributed across multiple nodes, making it difficult to control and manage. FIs need solutions that allow them to maintain control over sensitive information, potentially through hybrid blockchain models that combine public and private elements.
- **Operational Control:** The ability to manage transactions, validate nodes, and oversee smart contracts is a critical aspect of operational control. FIs must ensure that they can effectively enforce rules and standards within the blockchain network to prevent misuse or unauthorized activities.

Privacy and consumer protection

Access and Transparency

While permissionless blockchains foster trust and accountability through their inherent transparency, this very feature can create significant challenges for data privacy and confidentiality. This is particularly concerning when dealing with personal information or metadata that could unintentionally expose an individual's identity, which poses serious risks for financial institutions that are bound by strict legal obligations to maintain confidentiality and safeguard sensitive information. In contrast, permissioned blockchains help mitigate these risks by creating a closed network where data confidentiality is preserved. With access controls in place, only trusted parties are allowed to engage with the network, ensuring a more secure environment for data handling.

Immutability and privacy principles:

The immutable nature of permissionless blockchains directly conflicts with a fundamental principle of data privacy laws, which require that personal data be erased when it is no longer needed (commonly known as "the right to be forgotten"). In contrast, permissioned blockchains allow administrators to modify or delete data, which aligns better with data privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Moreover, the principles of purpose limitation and data minimization are challenged by the potential replication of data across multiple nodes, unnecessary storage of metadata, and excessive transparency.

Accountability

The lack of a clearly defined Data Controller in permissionless blockchains poses a significant challenge for financial institutions when it comes to adhering to privacy laws. In contrast, permissioned structures facilitate easier compliance. With such systems, administrators can enforce privacy policies, set data retention limits, and meet regulatory requirements more effectively.

Privacy and control measures

- **Zero-Knowledge Proofs (ZKPs):** ZKPs, including zk-SNARKs and zk-STARKs, enhance privacy by allowing transactions to be verified without revealing sensitive information. Their implementation addresses privacy concerns while maintaining the benefits of permissionless blockchains. Furthermore, this information can be made more private by utilizing off-chain data storage and data tokenization.
- **Selective Participation:** Access and participation rights are granted based on predefined rules and conditions.
- **Customization:** Ability to customize the blockchain according to the specific needs and policies of the controlling organization.
- **Centralized Control:** Permissioned blockchains feature centralized control, as they are governed and managed by a single organization or a consortium of entities, offering greater authority over the network's operations and participant access.

Operational and cybersecurity risks

Operational and cybersecurity risks are significant concerns for FIs considering blockchain adoption. The immutable and decentralized nature of blockchain technology can introduce new vulnerabilities that need to be managed effectively.

- **Cybersecurity threats:** Malicious actors frequently target DeFi protocols and smart contracts on permissionless blockchains due to the substantial liquidity and user engagement these platforms attract. However, we must distinguish between the security of applications and the underlying blockchain infrastructure. While vulnerabilities can exist in applications, the core blockchain networks like Bitcoin and Ethereum remain secure and highly resistant to direct hacking, except in extreme scenarios such as a 51% attack. The primary threats stem from unaudited smart contracts, private key leakage or theft, and other off-chain vulnerabilities, which constitute a significant portion of attacks in the space. To mitigate these risks, FIs must prioritize rigorous auditing and implement robust security measures to maintain the integrity of their infrastructure and underlying assets. For best practices in this area, the Fireblocks and Ernst & Young LLP (EY) report on key management provides comprehensive guidelines to help maintain the integrity of infrastructure and underlying assets.
- **Operational resilience:** FIs need to ensure that their blockchain systems are resilient to operational disruptions. This includes having a highly available network architecture, rigorous disaster recovery plans, regular security audits, and ensuring system redundancy at all times.
- **Incident response**: Effective incident response strategies are crucial for mitigating the impact of cybersecurity incidents. This involves having predefined protocols for detecting, reporting, and responding to security breaches.

AML / CFT / KYC risks

AML (Anti-Money Laundering), CFT (Countering the Financing of Terrorism), and KYC (Know Your Customer) risks are paramount for FIs, as they must comply with stringent regulations to prevent financial crimes.

- **Transaction monitoring:** While permissionless blockchains are often pseudo-anonymous rather than fully anonymous, they still present challenges for transaction monitoring. Given the privacy features inherent in some blockchain networks, financial institutions must implement sophisticated analytics and monitoring tools to effectively track transactions and identify potential AML/CFT risks across various blockchain ecosystems. This approach allows FIs to maintain regulatory compliance while still leveraging the benefits of blockchain technology, balancing innovation with risk management in an evolving digital asset economy.
- **Identity verification:** Robust KYC processes are essential for verifying the identities of participants in blockchain transactions. This can be challenging on some permissionless blockchains, where user anonymity is a key feature.
- **Regulatory reporting:** FIs must ensure that they can generate accurate and timely reports for regulatory authorities. This requires integrating blockchain data with existing AML/CFT compliance systems to streamline reporting processes.

Legal and policy risks

Legal and policy risks are critical factors for financial institutions (FIs) considering blockchain technology adoption. Ensuring compliance with both global and local regulations is non-negotiable for maintaining legal standing and operational integrity. The choice of permissionless vs. permissioned blockchain is presumably an operational one, but regulation points to further considerations, including potentially materially changing the capital required of the business or mandating privacy-protecting deployment.

Below are some important frameworks for FIs that are participating or operating in the crypto space to consider:

Regulatory frameworks	Description	Key challenge with the use of blockchains	Affected countries & entities
Basel III	Basel III is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision (BCBS), to strengthen the regulation, supervision, and risk management of the banking sector. The BCBS guidelines for the prudential treatment of crypto asset exposures classify crypto assets into two main groups with specific capital requirements and exposure limits.	Very cautious on public blockchains, imposing prohibitively high capital requirements for banks holding any asset on a public blockchain.	Global: Applicable to countries adhering to Basel Committee on Banking Supervision guidelines.
General Data Protection Regulation (GDPR)	A data protection law in the European Union that governs the processing of personal data. It is designed to give individuals more control over their personal information and to standardize data protection laws across the EU. Organizations must collect and process data lawfully and transparently, while also ensuring robust data security measures are in place. GDPR also mandates that data breaches be reported to authorities within 72 hours and requires notifying affected individuals if their rights are at high risk.	Enshrines the "right to be forgotten," which is difficult for blockchains which serve as a permanent and immutable record, and prevents the sharing of personal identifiable data (PII) on blockchains, even in encrypted form. Sets out additional principles in relation to data minimization and purpose limitation, which can be challenging in the blockchain. Provides clearly distinguishable roles that companies play when processing personal data - i.e. the "Data Controller".	Any organization processing personal data of EU Member States, regulated financial institutions, and crypto-asset service providers.
SAB121*	Staff Accounting Bulletin No. 121 (SAB 121), rolled out by the SEC in March 2022, tightens the accounting requirements for entities safeguarding customer crypto assets. These entities are now mandated to report both a corresponding asset on their balance sheets, marked at fair value. The directive applies broadly to entities under US GAAP or IFRS that file with the SEC, particularly those preparing for public offerings.	Requires banks to disclose cryptoasset holdings on balance sheet and hold capital against them, even if they are simply held in custody on behalf of clients, which makes it prohibitively expensive to custody digital assets.	SEC registrants (public companies), entities preparing to go public, FIs and platforms custodial services for crypto assets in the United States.
DORA	The EU's Digital Operational Resilience Act (DORA) seeks to bolster the operational resilience of fi nancial institutions against digital disruptions, particularly cyber threats. It mandates risk management frameworks, business continuity plans, and stringent management of ICT providers.	DORA does not account for reliance on open-source or permissionless technology models. Therefore, these are presumed to either be addressed by industry best practices (see above), or avoided.	EU Member States, regulated financial institutions, and crypto-asset service providers.

Permissionless and permissioned blockchains as complements

Permissionless and permissioned blockchains: unique strengths and applications

Permissionless and permissioned blockchains each bring unique strengths to the evolving landscape of digital finance. Ethereum and its Layer 2 solutions have emerged as the preferred platforms for decentralized applications (dApps). These blockchains are particularly well-suited for secondary markets, where the volume, transparency, and lack of boundaries allow assets to move freely between traders without the constrictions or requirements of primary markets. Moreover, the security of permissionless blockchains is inherently strong due to the large number of nodes and validators in the ecosystem. As the number of participants grows, the network becomes increasingly robust and resistant to attacks, making permissionless blockchains highly secure and resilient against malicious actors.

Use cases for permissionless blockchains

- **DeFi:** Enabling a wide range of financial services like lending, borrowing, and trading.
- **Digital identity:** Providing secure, verifiable identities.
- **Voting systems:** Ensuring transparent and tamper-proof election processes.
- **Content distribution:** Allowing creators to publish content and receive direct compensation.
- **Payments:** Facilitating fast, secure, and low-cost transactions, especially for cross-border settlements, pay-ins, pay-outs, and payroll.

Conversely, permissioned blockchains are specifically designed to meet the rigorous requirements of financial institutions, offering a controlled environment that ensures compliance with regulatory standards and data privacy. Well-suited for applications like interbank settlements, tokenizing repos, and fund distribution, these networks allow known and trusted entities to participate, providing clear accountability for operational risks.

This configuration enables financial institutions to leverage blockchain technology's benefits – such as faster settlement times, reduced counterparty risk, and streamlined processes – without compromising control or regulatory adherence. As a result, permissioned blockchains offer a compelling solution for modernizing legacy systems and enhancing operational efficiency in the financial sector.

Use cases for permissioned blockchains:

- **Interbank settlements:** Streamlining transactions between banks.
- **Tokenizing repurchase agreements (Repos):** Facilitating the digital representation of repurchase agreements.
- **Fund distribution:** Managing the distribution of funds securely and transparently.
- **Supply chain management:** Tracking the provenance of goods and ensuring timely information access.

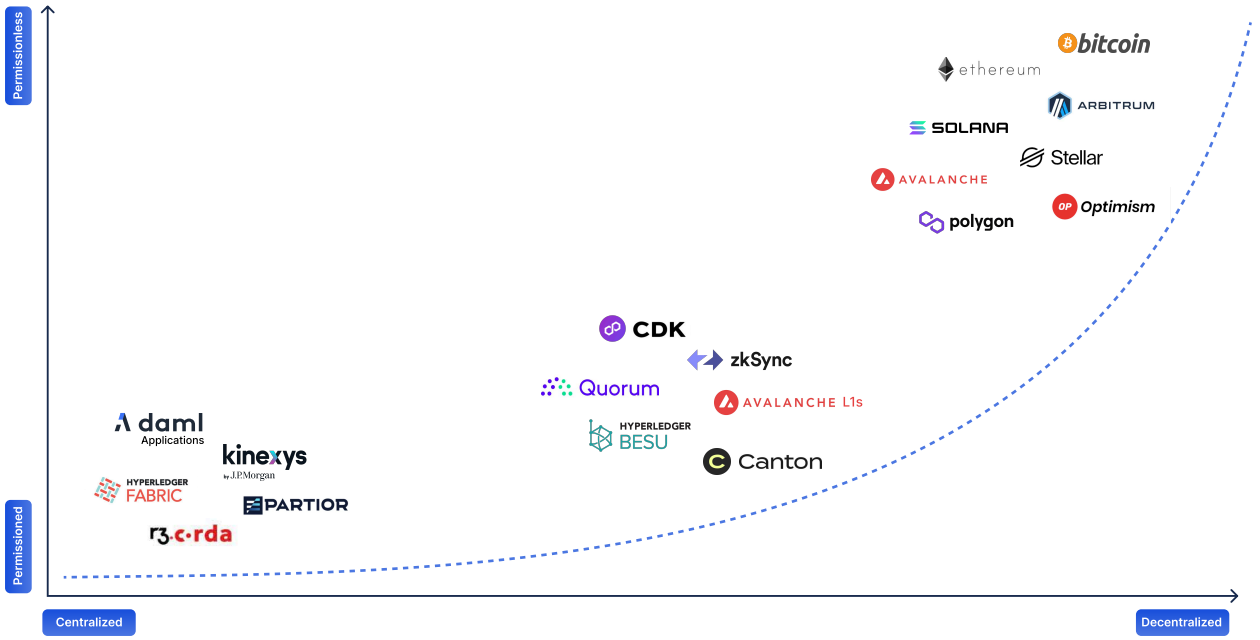
While permissionless blockchains offer transparency and decentralization, private and permissioned blockchains provide the control and privacy that FIs need. Both blockchains have unique strengths and applications, and their symbiotic relationship will shape the future of digital finance. Permissionless blockchains will continue to drive innovation and attract a diverse range of participants, while permissioned blockchains will provide the necessary infrastructure for FIs to operate securely and compliantly within the digital asset space.

The convergence of two worlds

It is crucial to recognize that permissioned blockchains alone cannot fulfill the diverse needs of the evolving digital finance landscape. While they excel in catering to the specific requirements of financial institutions, they lack the open, permissionless nature that has driven the explosive growth and innovation witnessed in the permissionless blockchain space. Permissioned blockchains, by their very design, restrict access to a select group of participants, limiting the potential for network effects and the development of a thriving ecosystem.

The Blockchain Spectrum

This is a stylized representation of distributed ledger technologies selected by financial institutions. It includes protocols, networks, and applications – and presents them as clusters along a spectrum. It is not intended as a linear ranking.



In examining the current landscape of blockchain networks, it becomes evident that these networks predominantly fall into two categories: centralized permissioned networks and decentralized permissionless networks. There are also examples of semi-permissioned and semi-centralized networks positioned between these two extremes.

Notable distributed ledger technologies such as Corda, DAML, Partior, and Hyperledger Fabric align with the permissioned and centralized side of the spectrum. These networks are designed primarily for enterprise-grade applications, emphasizing governance, security, and compliance. Traditionally, they have been favored by highly regulated financial institutions seeking to venture into digital assets and blockchain technologies, but they have hit limits in terms of connectivity. On the opposite end of the spectrum are permissionless and decentralized networks like Bitcoin, Ethereum, Polygon, Avalanche, Stellar, Solana, Optimism, and Arbitrum, which prioritize widespread adoption, open access, and a decentralized governance approach, but have seen only limited adoption from FIs.

Additionally, networks such as Canton and JPM Kinexys (formerly Onyx) facilitate transactions within a closed environment of permissioned participants, employing centralized governance structures. Meanwhile, Hyperledger Besu, Quorum, Avalanche Subnets, zkSync, and Polygon CDK provide a broad range of configurations, spanning from loosely permissioned to strongly permissioned networks and from highly centralized to highly decentralized structures.

As such, the future of digital finance lies in the synergistic coexistence of both permissionless and permissioned blockchains. Each type of blockchain serves a distinct purpose, catering to the unique needs of different stakeholders within the financial ecosystem. Permissionless blockchains will continue to serve as the foundation for decentralized applications, driving innovation and attracting a diverse range of participants, while permissioned blockchains will provide the necessary infrastructure for financial institutions to operate securely and compliantly within the digital asset space.

A limited number of assets, such as wholesale CBDCs and repos, may continue to operate on private and closely permissioned chains due to their specific requirements for control and security. However, the majority of assets, including retail CBDCs, stablecoins, bonds, and real estate, are expected to migrate to permissionless blockchains. The need for broader accessibility and the scalability challenges of permissioned networks will naturally drive this shift. As digital asset adoption grows, the practicality of onboarding millions of users onto a permissioned network diminishes. Thus, it is becoming increasingly improbable to consolidate financial assets on private or permissioned blockchains.

To reach a broader user base, financial institutions must begin bridging their assets to permissionless blockchains. This approach allows them to leverage the benefits of public networks, such as enhanced security, transparency, and interoperability. Consider repurchase agreements (repos): while the assets themselves might continue to be held on private networks, their settlement could be mirrored on public blockchains. This hybrid model allows for transparent ownership and transaction records on public ledgers while ensuring the secure management of assets within private systems.

The interoperability imperative

The key to unlocking the full potential of this symbiotic relationship lies in interoperability. As the blockchain ecosystem matures, the development of robust interoperability solutions will enable seamless communication and interaction between public and permissioned networks. This goes beyond simple lock and unlock mechanisms, minting or burning tokens, or delivery versus payment (DvP). True interoperability requires a comprehensive framework that supports full programmability across chains, enabling a smooth and secure transfer of data and assets.

The current interoperability solutions, such as bridging and messaging layers, are not sufficient to achieve the full potential of blockchain integration. While these mechanisms allow for basic interactions, they fall short of enabling the complex, programmable interactions necessary for a fully integrated financial ecosystem. For example, relying solely on bridges and messaging layers often introduces latency and security risks due to the finality periods and reliance on single points of failure.

Moreover, the concept of cross-chain composability, which refers to the ability to combine and program assets across different networks, will play a pivotal role in the future of digital finance. EVM-based blockchains, Solana, and Cosmos, are already paving the way for cross-chain composability, enabling the creation of complex financial products and services that span multiple blockchain networks. As interoperability and composability solutions continue to evolve, financial institutions will be able to harness the full potential of blockchain technology, creating a more efficient, inclusive, and innovative financial system.

The foundation of tomorrow's financial ecosystems

The initial philosophical disagreement between the two factions on what type of blockchain is superior has evolved into a practical technological challenge of combining compliance, governance, and risk management with the principles of openness, decentralization, transparency, and security.

Advocates of permissionless blockchains argue in favor of a model where all assets are issued, managed, and exchanged on a publicly accessible blockchain network. They assert that the fundamental principles of blockchain technology, rooted in decentralization, are compromised when permissioned blockchains are utilized, thereby deviating from the original intentions of the technology's creators. This debate is further heightened, albeit unfairly, by the comparison of permissioned blockchains with traditional databases and the potential value, if any, they can offer to the broader financial ecosystem, given that both essentially function as centralized data repositories.

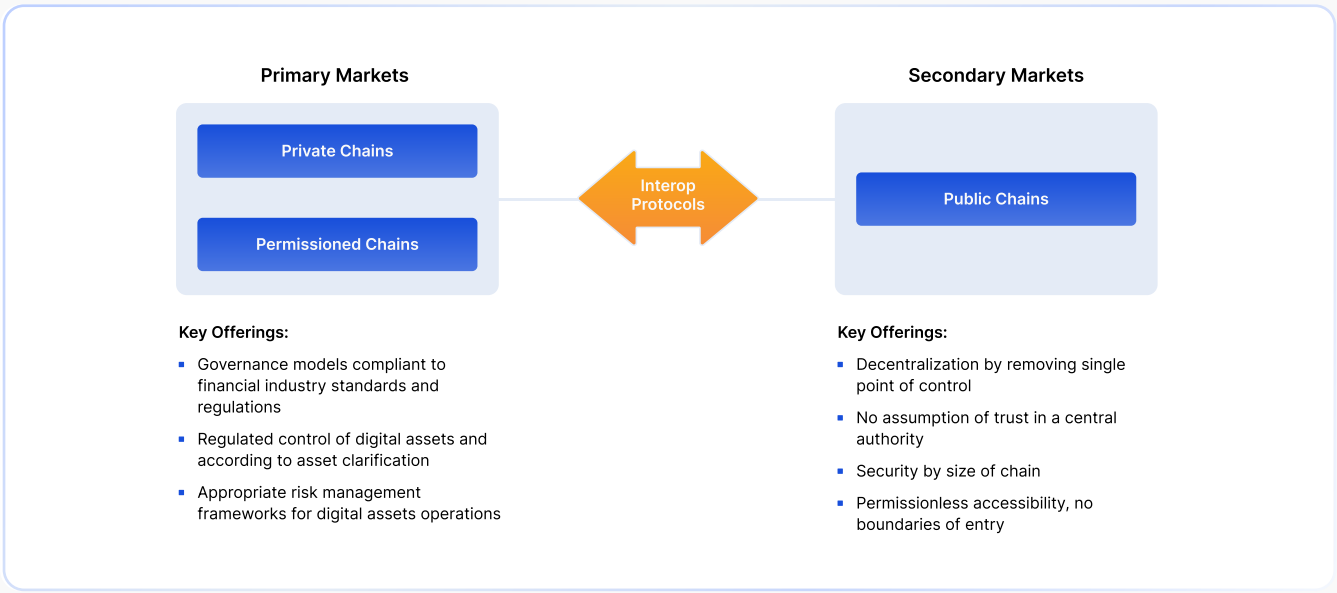
In contrast, conservative stakeholders, prioritizing risk aversion, contend that permissionless networks lack the capacity to establish essential governance frameworks and risk mitigation protocols necessary to progress or even to merely emulate the established workflows and procedures employed by traditional financial institutions. Their primary objections revolve around the decentralized decision-making and responsibility inherent in permissionless networks, as well as the premise that no data remains completely anonymous or confidential on a permissionless blockchain, arguments that were recently echoed officially in Basel III by the BCBS.

In the financial services ecosystem, there is growing recognition of the advantages offered by both permissionless and permissioned blockchains. On one side, permissionless blockchains provide transparency and decentralization, and on the other, permissioned blockchains offer greater control and privacy. Instead of imposing rigid requirements on either permissionless or permissioned blockchains, we propose a framework that seeks to facilitate the coexistence and interaction of both. This approach aims to ensure that all essential functionalities and specific requirements are effectively addressed, allowing for a more balanced and flexible approach to blockchain integration in financial systems.

After extensive consultations with various financial entities, regulators, industry experts, and digital assets trailblazers, it is clear that a more robust framework is needed to facilitate the development of compliant and secure products and use cases in the financial system. The framework set out in this paper may not be universally applicable to all asset classes, but it is crucial for supporting activities such as creation (minting), revocation (burning), trading across diverse asset classes, and managing investor access via KYC processes.

Given the involvement of multiple asset classes with distinct requirements in many financial use cases, relying solely on permissionless or permissioned blockchains may be insufficient.

To illustrate the point, we will assume that all asset classes exist on-chain or are mirrored as digital twins using smart contracts. Although this assumption may not be the current reality, it is expected that, over time, all asset classes will either fully exist on-chain or adopt a mirroring mechanism due to the benefits associated with smart contracts and the programmability of digital assets.



The proposed model can be outlined for example by examining the fundamental architecture of primary and secondary financial markets. This architecture serves as a versatile framework that can effectively represent any two facets of a financial ecosystem. On one side, there exists a segment characterized by a stringent commitment to confidentiality and data privacy. Access to this side is restricted solely to authorized participants, ensuring that sensitive information is safeguarded against unauthorized exposure. In contrast, the other side of the structure emphasizes broader accessibility, welcoming a diverse array of global users. This duality not only highlights the need for protected spaces within the financial system but also underscores the importance of inclusivity and transparency in reaching a wider audience. By balancing these two dimensions, the model aims to establish a secure yet accessible financial environment that meets the needs of different parts of the same ecosystem.

We allocate permissionless and permissioned blockchains in our model based on their alignment with requirements in different markets:

Permissioned blockchains are particularly well-suited for primary markets, as demonstrated in many successful projects in recent years. In these markets, a clearly defined governance framework ensures that digital assets and financial activities conform to industry standards and regulatory obligations.

Market Survey

A notable example is JP Morgan's Kinexys Digital Assets platform, which operates as a permissioned network involving multiple institutional participants such as BNP Paribas[2] and Goldman Sachs[3]. It has reportedly[4] facilitated the processing of assets valued between 1 and 2 billion USD per day, including US treasury bonds, mortgage-backed securities, and cash. The security and governance controls provided by permissioned blockchain networks are essential for enabling large financial institutions to issue and trade assets while upholding compliance with regulatory standards. This has allowed JP Morgan's Kinexys Digital Assets platform to issue over $900 billion USD in assets successfully, and this figure is projected to increase as more institutions transition their processes to operate on-chain.

Citi recently announced[5] its Token Services platform, which operates on a permissioned blockchain owned and operated by Citi. Similar to JP Morgan's Kinexys Digital Assets platform, this platform will offer institutional clients continuous, compliant services in line with Citi's risk and controls framework. Leveraging the 24/7 availability and programmability of blockchain networks, it will enable cost-efficient cross-border payments, liquidity, and automated trade finance products.

[2] https://globalmarkets.cib.bnpparibas/bnp-paribas-trades-intraday-repo-on-j-p-morgans-onyx-digital-assets-platform-2/
[3] https://www.bloomberg.com/news/articles/2021-06-22/goldman-sachs-begins-trading-on-jpmorgan-repo-blockchain-network
[4] https://www.marketsmedia.com/jp-morgans-onyx-digital-assets-processes-up-to-2bn-per-day/
[5] https://www.citigroup.com/global/news/press-release/2023/citi-develops-new-digital-asset-capabilities-for-institutional-clients 4 https://www.marketsmedia.com/jp-morgans-onyx-digital-assets-processes-up-to-2bn-per-day/ 3 https://www.bloomberg.com/news/articles/2021-06-22/goldman-sachs-begins-trading-on-jpmorgan-repo-blockchain-network

This framework ensures the security of sensitive information, such as financial transactions, contracts, and customer data, through permissioned access to the blockchain networks of primary markets. This level of security is essential for primary markets that deal with confidential transactions and manage proprietary data. Moreover, the presence of primary markets in private and permissioned chains enables the establishment and implementation of effective risk management frameworks for digital asset operations. This is accomplished by ensuring that the governing bodies of such networks have the capability to execute mission-critical transactions, including the ability to reverse transactions in the event of errors, fraud, or malicious activities, and the capacity to facilitate dispute resolution among network participants. Equally significantly, these risk management frameworks also facilitate secure data sharing among network participants to mitigate the risk of data tampering and unauthorized disclosure, and incorporate procedures for regulatory compliance and reporting. **In other words, in this ecosystem of known participants, we can clearly define operational responsibilities and operate with trust.**

Permissionless blockchains, however, are particularly well-suited for the facilitation of seamless and cost-effective trading of digital assets in secondary markets due to their decentralized nature. This allows for easy onboarding of participants without enforced entry barriers, powering mass adoption of these networks as clearly demonstrated by crypto markets on permissionless blockchain networks. It is worth noting, however, that compliance requirements for onboarding participants into specific secondary markets still apply. For example, most markets require Know Your Customer (KYC) processes for participant onboarding, utilizing decentralized identifiers and other identity-based authorization methods. Therefore, while creating a wallet or account on a permissionless blockchain may not impose onboarding requirements on participants, individual secondary markets built on these networks can impose their own participation requirements by incorporating them into their smart contracts and compliance logic.

In other words, to achieve widespread engagement, including by previously unknown participants, we need to leverage more of what the technology has to offer to solve the accessibility problems we face in the financial system today.

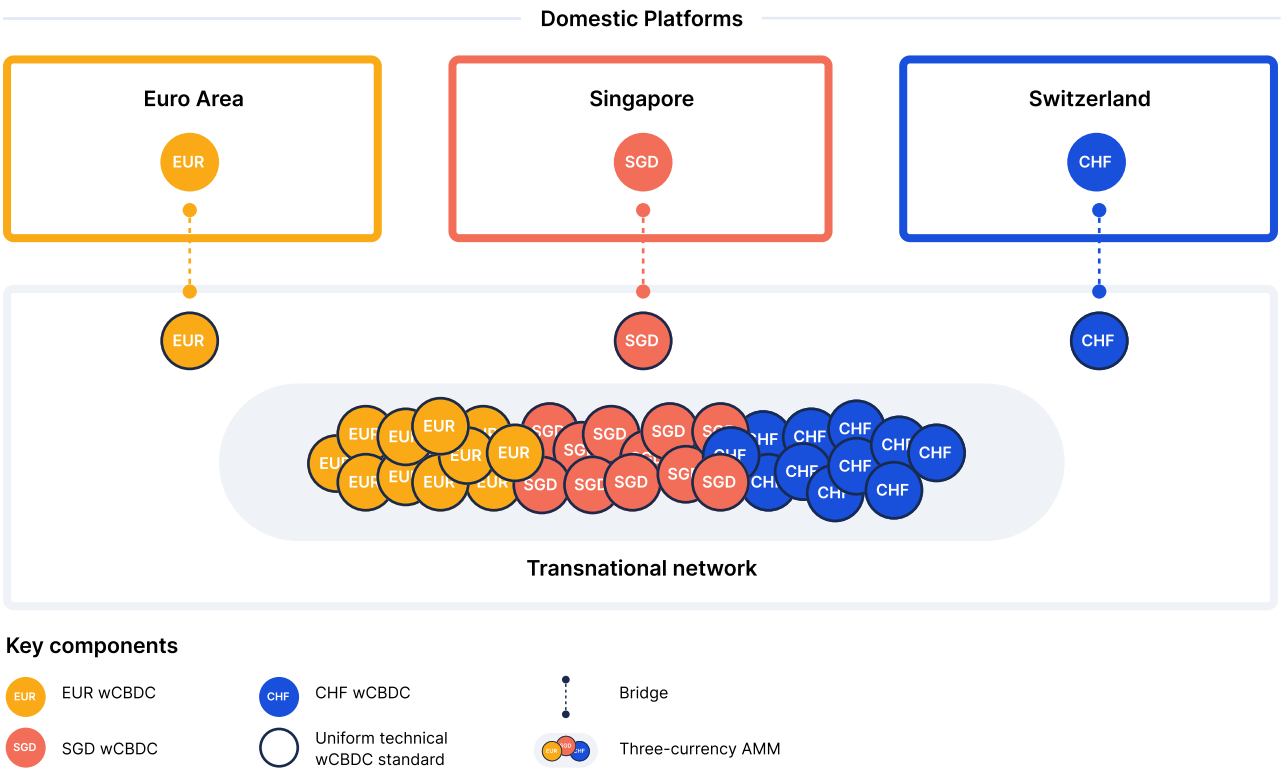
UBS has recently[6] engaged in the tokenization of a money market fund as part of the Monetary Authority of Singapore's Project Guardian-controlled pilots. This initiative involved issuance of an MMF token onto the Ethereum network, with the aim of enhancing liquidity and reducing distribution costs through fractionalization of the MMF.

ABN AMRO, the first Dutch bank to register a digital green bond on a permissionless blockchain[7], provides a prime illustration of a permissionless blockchain application for asset tokenization. In a recent instance, Vesteda secured €5 million from DekaBank by issuing an innovative bond on the Polygon blockchain. ABN AMRO has demonstrated prior expertise with Ethereum and Stellar, as evidenced by its assistance to APOC Aviation in issuing a €450,000 bond via the Stellar blockchain in early 2023.

Last year, BlackRock launched its inaugural digital fund on the Ethereum blockchain called the BlackRock USD Institutional Digital Liquidity Fund (BUIDL). This fund is designed as a money market fund with the goal of maintaining a stable value of $1 for its investors. Recent reports indicate that BlackRock's spot Ether exchange-traded fund (ETF) amassed $109.9 million in inflows on August 6, resulting in a total inflow of $869 million since its introduction on July 23, 2024. This substantial $870 million inflow has positioned BlackRock's spot Ether ETF among the top six best-performing ETFs launched in 2024.[8]

[6] https://www.ubs.com/global/en/media/display-page-ndp/en-20230927-first-blockchain-native.html?caasID=CAAS-ActivityStream
[7] https://www.abnamro.com/en/news/abn-amro-registers-first-digital-green-bond-on-the-public-blockchain
[8] https://cointelegraph.com/news/blackrock-spot-ether-etf-rakes-nearly-900-million-since-launch

Mariana high-level architecture **Graph 1**



The BIS, Banque De France, the Monetary Authority of Singapore, and the Swiss National Bank formulated a noteworthy and comparable framework in Project Mariana.[9]

In this framework, wholesale CBDCs issued on domestic networks are interconnected and transferred to an international network that houses an Automated Market Maker.

Such domestic platforms operate as permissioned networks, facilitating the secure inclusion of financial institutions, regulators, and auditors, allowing for ongoing compliance with all regulations.

On the other hand, the transnational network, while initially appearing as a permissioned network in this proof of concept, could potentially function entirely on a public network while still adhering to all required permission settings. This would offer improved secondary market conditions, liquidity, and accessibility for assets transferred from domestic permissioned networks to investors.

[9] https://www.bis.org/publ/othp75.pdf

Composability at the heart of tomorrow's financial ecosystems

As the use of blockchain technology has become more widespread, it has given rise to a variety of specialized blockchain networks, each tailored to tackle specific issues and fulfill unique objectives. These networks encompass various categories of blockchains, including permissionless L1 networks, L2 networks, supernets, consortium networks, and more. Most of these networks share a common feature, consisting of Turing-complete virtual machines (VMs) that facilitate the implementation of programmable protocols, commonly referred to as smart contracts. Across different blockchains, virtual machines might be labeled differently, yet they perform the critical function of enabling decentralized application development. EVM is used by platforms such as Ethereum, Polygon, Avalanche, Hyperledger Besu, and ConsenSys Quorum. On the other hand, CosmWasm is utilized by Cosmos and Tron, while DAML serves as the foundation for Canton. Despite their different names, these virtual machines play a crucial role in developing and operating applications on decentralized networks.

Digital assets, such as tokenized currencies like USDC and tokenized securities such as corporate bonds, serve as primary examples of decentralized blockchain applications used by financial institutions. Although smart contracts can be applied in various ways across blockchain networks, the focus in recent years has predominantly been on financial institutions testing or implementing tokenized digital assets through blockchain technology. Some financial institutions have started experimenting with smart contracts to digitize and automate their traditional processes, yet the main use of smart contracts in financial services still centers on representing digital assets.

Cross-chain composability, or the capacity to enable applications to be programmed and utilized across various blockchain networks, is an integral component of future financial ecosystems. In practice, the ability to program decentralized applications should not be confined to individual blockchain networks, as this limits the potential to create complex use cases that span multiple networks.

This limitation hinders the seamless flow of events, data, and intent across chains, akin to developing a computer operating system that lacks the ability for processes to interact with each other. While technically feasible, this fragmentation severely restricts the range of applications and workflows that can be developed on the system. Some common problems encountered when working across multiple ecosystems can include different standards for assets, fragmented liquidity, and varying standards of privacy.

The process of bridging, a method of transferring digital assets from one blockchain to another, involves locking and unlocking or burning and minting an asset to remove it from one chain and create it on another. While this facilitates an important part of composability, which is the ability to signal intent between chains, it falls short in providing a robust way of transferring messages across networks, thus allowing for complex workflows that extend beyond simply transferring and creating assets across different chains.

Interoperability protocols are designed to facilitate the transfer of various messages across networks, allowing different applications to work together seamlessly across different blockchains. These messages can convey a wide range of instructions, enabling the development of applications on both permissioned and permissionless networks.

Our proposed framework highlights the importance of interoperability specifically between primary (private) and secondary (public) markets. This merger between permissioned and permissionless networks encompasses a diverse array of digital assets and financial products, necessitating workflows that can vary from simple to highly complex. Interoperability protocols elegantly address these complexities, making it easier to connect digital assets across both permissioned and permissionless networks.

Several pioneering projects like Axelar, Chainlink CCIP, LayerZero, Ownera, and Wormhole are at the forefront of solving these interoperability challenges, offering cutting-edge solutions for cross-chain communication and asset transfer.

Axelar

Axelar is tackling the problem of seamless cross-chain communication and asset transfer between diverse blockchain ecosystems. It employs a decentralized network with Byzantine Fault Tolerant (BFT) consensus, along with the Axelar Gateway, APIs, and Software Development Kits (SDKs) for developers. Axelar's universal interoperability layer simplifies the integration process, making cross-chain interactions more accessible and efficient for developers.

Chainlink CCIP

Chainlink CCIP (Cross-Chain Interoperability Protocol) leverages Chainlink's decentralized oracle network to enable secure cross-chain interactions. Utilizing oracles and smart contracts, it connects smart contracts across different blockchain networks, enhancing the interconnected functionality of decentralized applications for institutions seeking highly secure solutions.

LayerZero

LayerZero addresses the challenge of fast and cost-effective cross-chain transactions. Utilizing ultra-light nodes and relayers, it provides an omnichain interoperability protocol that ensures scalability and efficiency in cross-chain communication. This solution is particularly advantageous for developers needing lightweight and scalable solutions.

Ownera

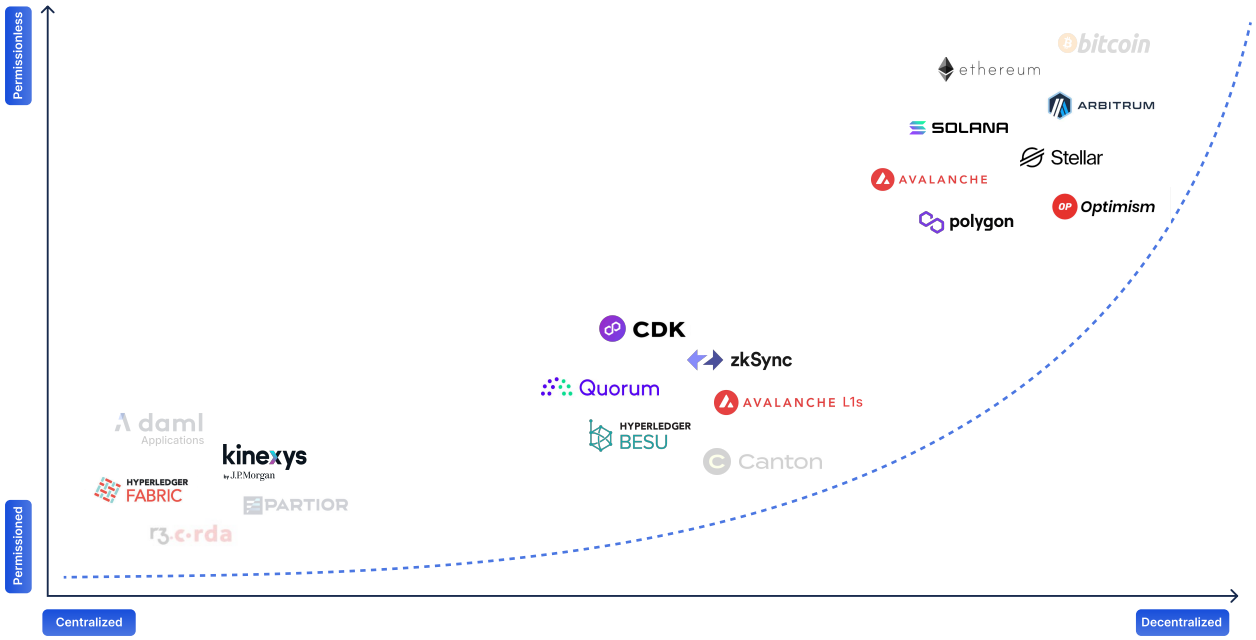
Ownera targets the digital securities market, facilitating seamless asset transfers and ensuring regulatory compliance by connecting various blockchain platforms. Integrating blockchain networks and regulatory frameworks, Ownera bridges traditional finance and blockchain technology, creating a global liquidity network for digital securities.

Wormhole

Wormhole offers a dependable cross-chain messaging protocol that enables asset and information transfer across various blockchain networks. A network of guardians ensures the security and integrity of cross-chain transactions. As a bridging solution, Wormhole's security-focused design provides a versatile solution for various use cases, from DeFi to NFTs.

The EVM-compatible Blockchain Spectrum

This is a stylized representation of distributed ledger technologies selected by financial institutions. It includes protocols, networks, and applications – and presents them as clusters along a spectrum. It is not intended as a linear ranking.



If we revisit our diagram illustrating the convergence of permissioned and permissionless blockchains in financial institutions, it is apparent that the majority of chains currently employed by financial institutions are either EVM-compatible or have previously explored EVM compatibility, such as Hyperledger Fabric. While the diagram does not provide an exhaustive list of chains financial institutions utilize for constructing digital asset products, it does reflect the current state of blockchain adoption within these institutions. Most financial institutions demonstrate a preference for EVM-compatible chains due to the abundance of resources, developers, expertise, supporting frameworks, and widespread adoption. Moreover, EVM-compatible chains are distinguished for offering a wide range of purpose-built networks tailored for low fees, high throughput, configurability, developer focus, centralization, and numerous other use cases.

This preference is further illustrated by the selection of network support by interoperability protocols. The aforementioned interoperability protocols[10] favor EVM-compatible networks, which account for an average of 91% of all supported networks.

Some non-natively EVM-compatible chains offer EVM support via bridges or rollup networks like Cosmos and Polkadot, which are not factored into this average.

Although a multi-chain trend is gaining momentum, with 34% of all developers in 2023 building for multiple chains, a notable 87% of these multi-chain developers work on at least one EVM-compatible chain, underscoring Ethereum's continued dominance in the smart contract landscape. This trend highlights the increasing interconnectedness of blockchain ecosystems and the growing importance of interoperability in the evolving digital asset economy.

Unsurprisingly, this means that EVM stands out as the pre-eminent protocol and developer framework most widely employed in the market for constructing digital asset products. As a result, it has become increasingly evident that the EVM ecosystem is also emerging as a leading candidate for serving as the cornerstone of future composable and interconnected financial ecosystems.

[10] With the exception of Ownera, who as of November 2024 did not publicly publish their list of supported networks

Use cases in the financial sector

FIs are steadily recognizing the transformative potential of blockchain technology and are actively diving into tokenization projects on both permissioned and permissionless blockchains. This transition showcases the practical applications of blockchain in the financial sector, bringing about improvements in efficiency, security, and transparency.

Use cases such as tokenized funds, stablecoins, and corporate bonds reveal the innovative ways FIs are using blockchain technology to streamline their operations. Below, we highlight various successful tokenization initiatives, including those implemented by Fireblocks, as well as other case studies across both permissioned and permissionless blockchains.

HSBC

HSBC

Use case: rCBDC, Hyperledger Besu

In a strategic push to elevate its digital currency capabilities, HSBC partnered with Fireblocks to distribute the eHKD stablecoin on Hyperledger Besu, which is backed by a central bank. Fireblocks provided secure MPC wallets that were used to sign all underlying transactions, including mint/burn/transfer transactions onto the private Besu Hyperledger network of HSBC. This initiative, aimed at transitioning from an NFT pilot to full production within 12 months, hinged on integrating with Hyperledger Besu to meet HSBC's stringent requirements for a secure, compliant wallet infrastructure with a swift go-to-market strategy. This collaboration not only navigated HSBC's privacy and risk concerns effectively but also enabled the minting, burning, and secure distribution of NFTs, ensuring seamless management of token treasury and the implementation of smart contracts for rewards.

Reserve Bank of Australia

RESERVE BANK OF AUSTRALIA

Use case: CBDC, EVM-compatible ConsenSys Quorum blockchain

Fireblocks played a crucial role in the Digital Finance CRC (DFCRC) and the Reserve Bank of Australia's (RBA) central bank digital currency (CBDC) pilot program, providing custody and tokenization technology for nearly half of the pilot use cases. The proof of concept (PoC) involved the secure minting and burning of the new CBDC, named eAUD. Fireblocks also powered the policy-based administration of smart contracts and facilitated transfers to end customers.

The RBA, in collaboration with the DFCRC, has set a significant precedent for central banks worldwide by exploring innovative use cases for a CBDC in Australia with a deliberate and pragmatic approach. The publication of the RBA's CBDC pilot report highlights its commitment to leveraging emerging technologies to provide access to a central-bank-issued version of digital money, positioning itself as a leader in digital asset innovation. Fireblocks is proud to contribute its institutional-grade digital asset operations platform to this landmark pilot project, which will shape the future of payments in Australia.

ABN AMRO

Use case: corporate bond, blockchain: Stellar

In the Dutch financial sector, Fireblocks and ABN AMRO utilized the Stellar blockchain to issue and sell a corporate bond to 10-12 of the bank's commercial clients.

By utilizing Fireblocks' end-to-end tokenization platform, ABN AMRO was able to securely mint and burn tokens, manage digital assets, and simplify treasury processes. The bond issuance, totaling €450,000, marked ABN AMRO as the first bank in the Netherlands to register a digital bond on a permissionless blockchain. The project's goal was ambitious yet focused: to develop a minimum viable product (MVP) that tokenizes a single financial asset for one client, proving the efficacy of the solution in a real-world application.

Fireblocks, in collaboration with Bitbond, played a pivotal role in navigating these complexities, leveraging its robust platform and bespoke tokenization services to meet ABN AMRO's specific needs. Its ability to support the Stellar blockchain was crucial, enabling seamless transactions across the network. Fireblocks' platform facilitated the secure minting, managing, and transferring of tokens, demonstrating unparalleled efficiency and reliability.

Australia and New Zealand Banking Group

Use case: stablecoin, Blockchain: Ethereum

ANZ Bank's introduction of A$DC, a stablecoin pegged to the Australian dollar, represented a significant innovation in the financial sector, drastically reducing transfer times from one to two days to merely 30 minutes and enabling operations around the clock. This move was strategically designed to provide ANZ's institutional clients with an efficient and secure gateway to digital assets, streamlining the process of converting Australian Dollars (AUD) to cryptocurrencies. Central to ANZ's digital asset strategy was the execution of a pioneering transaction: the purchase of tokenized carbon credits (BCAU) from the carbon exchange BetaCarbon.

In navigating the complexities of this initiative, Fireblocks provided indispensable support with its sophisticated tokenization engine and robust wallet infrastructure. This collaboration ensured secure and compliant minting, custody, and transfer of A$DC throughout the project. Leveraging Fireblocks' technology enabled ANZ to automate back-office tasks and achieve almost instantaneous settlements, optimizing cost efficiency and reducing administrative burdens. The partnership also highlighted Fireblocks' capacity to support complex use cases, demonstrating the seamless integration of blockchain technology in banking through ANZ's innovative use of A$DC's ERC-20 based architecture with advanced institutional controls.

BlackRock

Use case: tokenized fund, blockchain: Ethereum

In a notable stride towards integrating traditional finance with the digital asset space, BlackRock has launched its first tokenized fund, the BlackRock USD Institutional Digital Liquidity Fund (BUIDL), on Ethereum. This money market fund enables qualified institutional investors to access U.S. dollar yields via a blockchain-based framework, supported by U.S. Treasury bills, repos, and cash, ensuring both stability and efficiency. Daily dividends are seamlessly delivered as tokens, thanks to a partnership with Securitize, the fund's transfer agent, and BNY Mellon, which oversees custody operations. Fireblocks key management infrastructure secured the smart contracts at Securitize to make it a truly world-leading offering.

Franklin Templeton

Use case: U.S. government money market fund, blockchain: Arbitrum, Base

Following successful launches on Stellar and Polygon, global asset manager Franklin Templeton has expanded its OnChain U.S. Government Money Fund (FOBXX) to the Arbitrum network. The fund, which is represented as BENJI tokens, provides stable U.S. dollar yields, secured by government securities, cash, and repurchase agreements. The Benji Investments platform now includes USDC conversion services through Zero Hash, enabling institutional investors to easily convert USDC to USD for BENJI token purchases. This move is a clear step in Franklin Templeton's broader mission to merge the reliability of traditional finance with the innovative potential of permissionless blockchain networks, making the fund more resilient and accessible in a rapidly changing market.

Tel Aviv Stock Exchange

Use case: Tokenized Bonds, Private EVM-compatible permissioned blockchain infrastructure hosted on AWS

Fireblocks was instrumental in the success of TASE's Project Eden, a pioneering initiative aimed at tokenizing and clearing digital bonds for the State of Israel. By leveraging a TASE self-hosted permissioned EVM blockchain, Fireblocks delivered a comprehensive solution that encompassed the seamless issuance, custody, and atomic settlement of digital assets. The involvement of Fireblocks extended beyond providing the foundational technology; it included the design and development of bespoke smart contracts, dApp development, deployment, and secure custody, all tailored to meet the project's specific technical and regulatory requirements. A key achievement of Fireblocks' contribution was the implementation of atomic settlements, a critical feature that ensured a simultaneous and risk-free exchange of securities and payment tokens between the Ministry of Finance, TASE, and primary dealers. This capability not only enhanced transaction security and reliability but also demonstrated the platform's ability to support sophisticated financial blockchain applications at scale, underscoring Fireblocks' role in advancing the tokenization ecosystem.

Sample use case: cross-chain smart contract composability

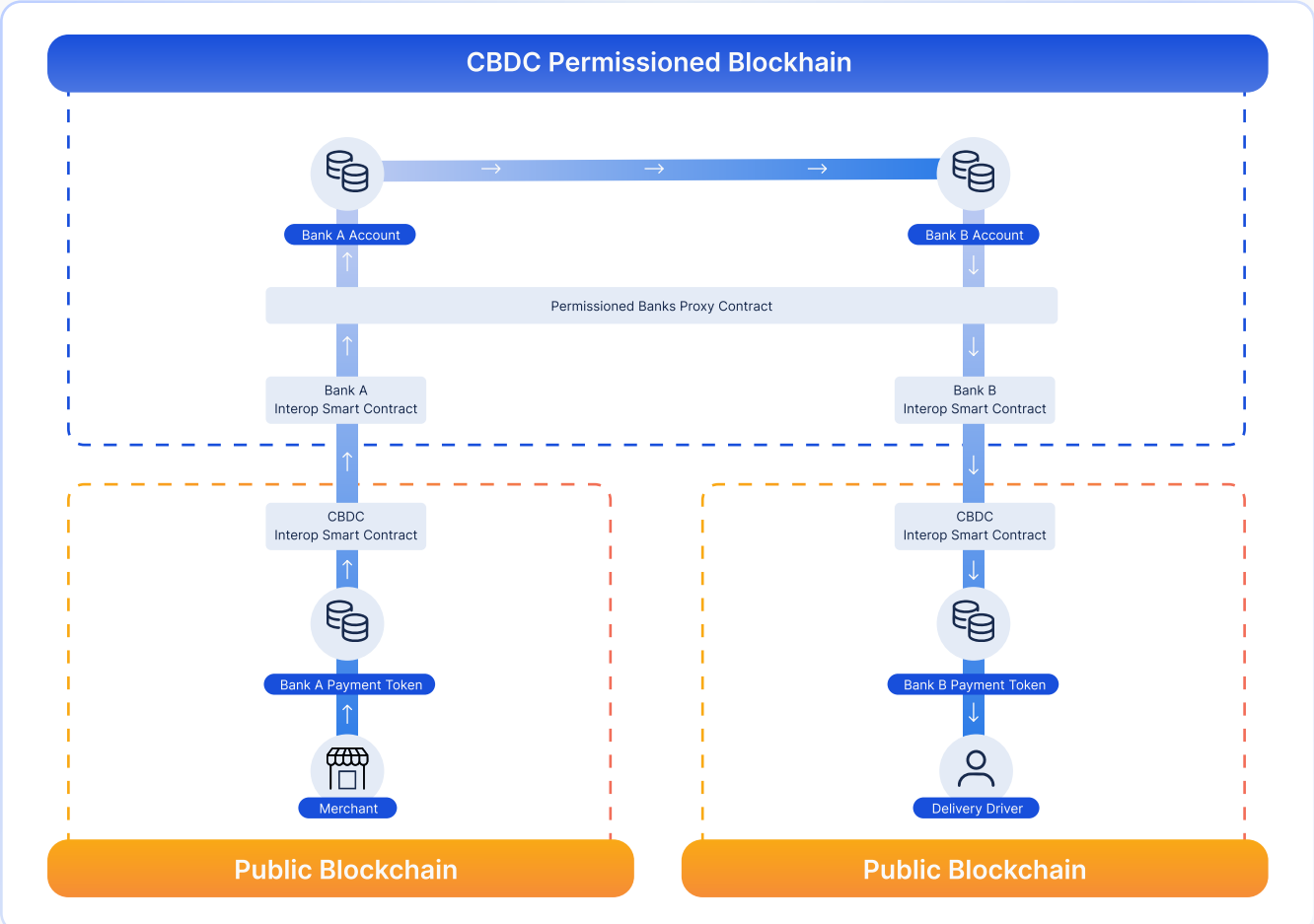
The concept of cross-chain composability allows smart contracts on different blockchains to interact, enabling higher-order functionality without fragmentation. For instance, in the tokenized money ecosystem, various issuers like central bank digital currencies (CBDCs), tokenized deposits, and stablecoins will require different governance and access mechanisms, leading them to choose different blockchains. Interoperability between these blockchains is crucial.

Permissionless blockchains serve a crucial role in facilitating transparency and accessibility, particularly on a large scale. Conversely, permissioned blockchains offer essential governance and control features, which are paramount in certain contexts. Additionally, the need for rapid settlement execution, as will be demonstrated in wholesale CBDC transactions, may prioritize efficiency over decentralization, warranting a closed environment for optimal performance.

Hence, different blockchain architectures cater to diverse requirements, each serving distinct purposes within the technological ecosystem.

For example, a central bank may issue a wholesale CBDC on a highly permissioned blockchain, while a stablecoin issuer may opt for a permissionless option to maximize adoption. An innovative merchant could create smart contracts for "delivery versus payment," where consumers use tokenized deposits to hold funds until goods are received. This system requires confirmation, like a signature or video, to release thefunds directly to the merchant, who can then use them for various payments, including to the delivery driver, for example.

If the delivery driver and the merchant are not customers of the same bank, a set of smart contracts can manage complex transactions, using the wholesale CBDC as a settlement asset and allowing real-time payments using different forms of tokenized money.



To transfer money from Bank A to Bank B, the stablecoin from Bank A must be exchanged for Bank B's stablecoin in the recipient's account. This involves using the Central Bank Digital Currency (CBDC) layer, which manages the transaction. Funds move through CBDC bridges, transferring money between accounts on the CBDC's private ledger.

Both banks connect their smart contracts to the main network, allowing them to operate without needing to understand each other's systems. All conversions between different tokenized currencies happen through this main network. Each bank conducts its actions on a secondary network, with events shared using interoperability protocols and smart contracts.

The CBDC layer offers a flexible framework that can adapt to changes. This allows the central bank to control which banks can join or leave the network, regulating access to the CBDC ledger.

Bank A's smart contract only needs to interact with the CBDC layer when dealing with an external transfer. It does not need to know much about the recipient, only that they are a customer of Bank B. When the funds and payment instructions arrive at Bank B, it is able to identify its customer and it mints its own stablecoin to the delivery driver's wallet. In this way, each FI is responsible for operating its own (blockchain) infrastructure, and cross-chain composability ensures that different types of tokenized money interact seamlessly.

In a second scenario, a wholesale CBDC could be used for real-time tax payments. Merchants could pay sales tax immediately upon receiving consumer payments instead of at the end of the fiscal year. The tax authority would expect these payments in wholesale CBDC rather than privately issued money. Upon payment, the merchant would transfer the tax amount to the tax office via the CBDC, including necessary details like payment source, date, and amount for accurate reconciliation.

The presence of different blockchain models complicates the process, as relying solely on a single permissionless blockchain may not be practical. Settlement procedures might occur on another blockchain or go directly to the tax office, which may resist using permissionless systems. Alternatively, the tax office could create private APIs and an off-chain system for operations, but this could require manual reconciliation. To enhance efficiency and reduce manual work, implementing composable smart contracts can ensure automatic notifications to relevant stakeholders like the tax office and commercial banks for every legitimate transaction.

The first use case describes a Delivery versus Payment (DvP) flow employing the CBDC layer as the settlement platform for diverse currency denominations and payment tokens. This involves the transfer of settlement events between the commercial banks' networks and the top-level CBDC network. The second use case on the other hand involves the transfer of payment information and uses the CBDC solely as a payment token rather than as an intermediary between two distinct payment tokens. In this scenario, access to the CBDC token as a payment token is restricted to specific authorized parties, such as the state's tax authority.

As the ecosystem is anticipated to incorporate various blockchains, it is imperative to facilitate composability across these blockchains and the assets issued on them. This versatility is particularly necessary for enabling interaction between more permissioned, centralized blockchains and the more decentralized and public segments of the ecosystem, even if some of these blockchains are fully private.

Looking Forward

Ultimately, the future of finance will be shaped by the symbiotic relationship between permissionless and permissioned blockchains. Permissionless blockchains will advance transparency and accessibility, while permissioned blockchains will provide the governance and control necessary for secure operations. Interoperability is the key to unlocking the full potential of this hybrid ecosystem, enabling seamless interactions across blockchain networks.

For financial institutions, the strategic imperative is clear: adopt a balanced, hybrid approach that harnesses the strengths of both blockchain models while investing in robust interoperability solutions. This strategy will not only ensure survival but also leadership in the rapidly evolving financial landscape.

If your institution is developing new digital asset strategies, exploring innovative use cases, or building wallet solutions, Fireblocks is here to support your journey with a secure, versatile, and interoperable blockchain infrastructure. We invite you to collaborate with us to shape the future of finance.