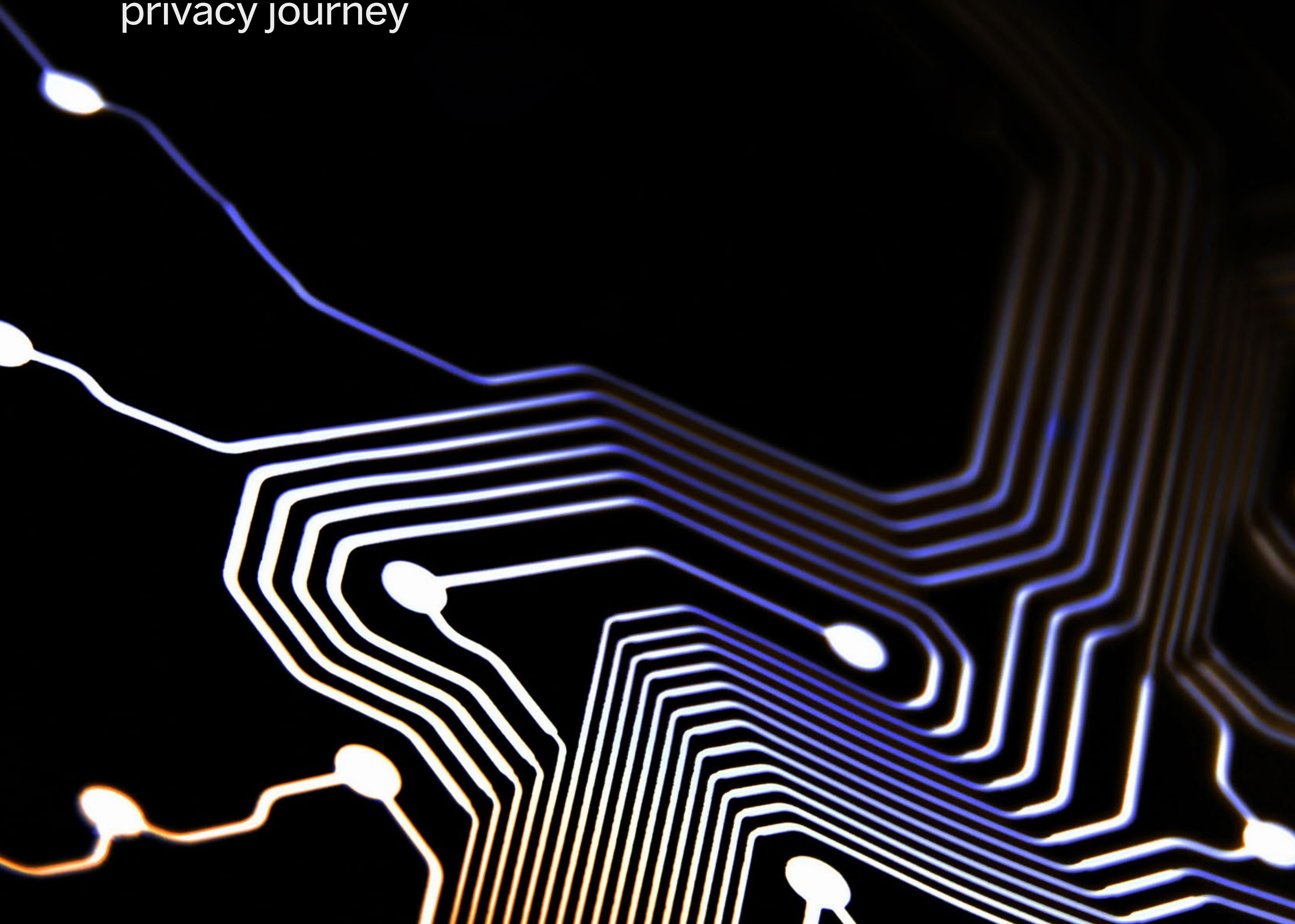
OliverWyman | MatterLabs

ALL ROADS LEAD TO ROME

Blockchains' scalability, interoperability and privacy journey



CONTENTS

EXECUTIVE SUMMARY

In ancient times, Rome was more than just the capital of an empire; it was the nexus of connectivity and commerce, linked by a sophisticated network of roads. Mirroring this in the blockchain universe, both public and private domains reflect these ancient pathways and side gardens, especially in financial services. Though each brings unique challenges akin to different terrains, they all converge towards a shared vision: an interoperable and scalable ecosystem. While public and private blockchains offer distinct solutions to safeguarding privacy and enabling interoperability, today, they both cater to specialized use cases. This paper offers an overview of the evolving blockchain landscape, equipping financial institutions, regulators and policymakers with insights into the sector's challenges and the innovative solutions developed over time.

The potential of blockchain

At its core, blockchain technology emerges as a transformative force with the potential to reshape legacy operations and business models within the Financial Services sector to streamline operations, enhance data integrity, and simplify transactional processes. Leading institutions and Central Banks, across the world, have embarked on numerous experiments and initiatives, which stand as a testament to the profound benefits embedded in the technology. This commitment is echoed by both the industry and regulators, evidenced by the growing number of proofs of concept, pilots, and blockchain-based solutions launched across the sector.

Public and private blockchains

Blockchains can fall into two primary types: public blockchains, which are generally open networks accessible to anyone, and private blockchains, which are deployed within corporate or consortium domains. Both spaces are in constant evolution, each introducing advancements that address their unique challenges and capitalize on inherent strengths. Public blockchains, akin to renting cloud space, provide shared utility but often face hurdles such as privacy concerns, costs, and potential security risks. Conversely, private blockchains, while offering tailored control and enhanced privacy, often grapple with issues related to scalability beyond their original design and interoperability across networks.

Challenges and evolution

Blockchain technology's journey is epitomized by both significant advancements as well as a myriad of hurdles across areas including security, regulation, and adoption, which the nascent industry has been attempting — and continues — to navigate. One of the prominent challenges for public blockchains was the Blockchain Trilemma, which highlights the trade-offs between decentralization, security, and scalability. The emergence of "Layer 2s (L2s)" sought to address some of these limitations by creating a secondary layer atop the foundational blockchains, now referred to as "Layer 1 (L1s)" systems. These L2s focused primarily on enhancing scalability.

L2s observed their own set of hurdles, notably interoperability and privacy, which sparked the evolution of "application chains (appchains)". Designed as natively interoperable ecosystems, appchains offer the flexibility to create tailored network applications while exhibiting selective characteristics of private networks, such as controlled access. This design echoes the scalability of Web2 apps and allows protocols and platforms to establish ecosystems and migrate existing infrastructure due to the adaptable network structure. Parallel to these advancements, private blockchains continue to develop in their own realm. While private blockchains are inherently designed for scalability in a controlled setting, they cater to entities seeking to craft solutions within such confined environments. Yet, conversations around unifying ledgers for financial services for certain use cases are gaining traction, underscoring the need for policy-driven leadership and the potential role of regulated entities in network node management.

Essentials for advancement

Blockchain's future as an interoperable and scalable tool in financial services hinges on a series of essential advancements, such as enhanced privacy, digital identity management, prudent security, balanced governance structures, compatible protocols, and appropriate regulations. In addition to industry participants, regulators and public policy makers must deepen their understanding of blockchain to effectively address their statutory objectives, foster growth within safe-rails, and simultaneously support continued innovation.

FIVE KEY TAKEAWAYS

1 Foundational values of blockchain and its evolution

Blockchain technology offers transformative potential for modernizing legacy systems and business models that could reshape the future of finance. Historically, public blockchains often emphasized transparency, collaboration, democratized access, and credible neutrality, while private blockchains often prioritized enablement of tailored operational needs and use cases

2 Challenges of public chains and L2 solutions

The blockchain trilemma introduces trade-offs amongst balancing security, scalability, and decentralization. Many projects gravitated towards optimizing two dimensions, which shaped the evolution of alternative blockchain designs. L2 solutions emerged as a response to this challenge, especially scalability by employing mechanisms like plasma chains, optimistic rollups, and "zero knowledge (zk)" rollups

3 Appchains as solution for public chain privacy and interoperability challenges

Beyond the trilemma, challenges around privacy and interoperability persist. Appchains, layered over L1s and L2s, offer tailored solutions for these issues. By their ability to scale horizontally like Web2 apps and foster agile, adaptable environments, appchains are increasingly used to migrate previously limited blockchain application into viable ecosystems, representing a new phase in creating scalable blockchain applications and ecosystems

4 All roads lead to Rome: Combining public and private blockchain solutions

Inspired by the adage ”All roads lead to Rome“, public blockchains explicitly aspire towards an interoperable and scalable future, with solutions such as L2s and appchains offering a solution for financial harmonization. For their part, private blockchains, operating within their own confined environments, continue to grow and are optimized for specific use cases, and industry-wide efforts for standardization and collaboration are increasing to create a more decentralized and harmonized environment

5 Building a sustainable future

Blockchain's integrated future relies on a series of essential advancements, including enhanced privacy, digital identity management, prudent security, balanced governance structures, compatible protocols, and appropriate regulations to the satisfaction of both retail and institutional end-users to forge a cohesive ecosystem

Chapter 01

VALUE OF BLOCKCHAIN FOR FINANCIAL SERVICES

Blockchain, a distributed ledger-based technology, is emerging as a transformative force with the potential to reshape legacy operations and business models within the financial services sector. As a ledger-based technology, blockchain directly impacts systems reliant on ledgers — which Financial Services has been dependent on since its inception. By unifying the multiple ledgers that each entity in a transaction owns, the shared ledger that blockchain provides acts as a single source of truth. This simplifies operations and eliminates cumbersome reconciliations while, establishing a uniform data format across connected ledgers.

Smart contracts introduce a realm of technological advancements by encoding and streamlining contract and process logic for complex financial transactions and business processes. This enables business process automation, not just within a single entity, but across multiple entities, leveraging a single source of data that all participants can trust. They offer benefits such as: the mitigation of manual errors, lower execution risk, reduced overhead costs, enhanced transparency, and the ability to handle sensitive data in a compliant manner, all secured through blockchain technology.

Another profound feature of blockchain is data immutability as entities can be certain that data cannot be erased or tampered with. This essentially means that data is automatically audited, a closed audit for the past blocks and real-time auditability for new blocks, and operational errors due to data changes are minimized. This uniformity brings about efficiencies, including reduced transaction costs, real-time processing, fewer intermediaries, and mitigation of single point of failure risks.

Additionally, a significant benefit lies in addressing trade breaks in equities and bond settlements. Presently, incorrect information can halt the settlement of financial instruments, a significant industry pain point. This issue necessitates tens of thousands of person-hours daily to pinpoint and rectify the root cause, leading to high overhead costs and increased operational risk. As the industry transitions to T+1 or T+0 settlement, this problem will intensify. However, with consistent data, trade breaks can be significantly reduced or even eliminated.

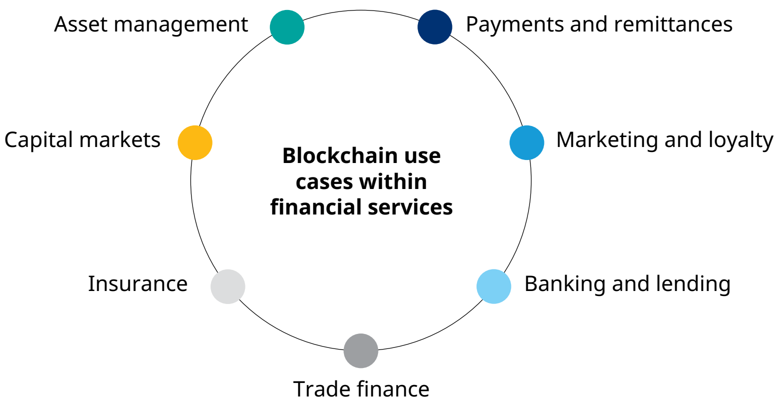
However, transitioning from traditional database or ledger systems to blockchain, particularly in complex financial institutions, is a significant undertaking which involves risk and complexity. The value of blockchain applications, as well as their capacity to scale in real-world scenarios, is an area of great debate, with opinions divided between advocates and sceptics. While the benefits associated with expedited settlements and reduced operational risks are high, display a compelling promise, their practical execution on an expansive scale is yet to be demonstrated. Furthermore, meeting compliance requirements, adhering to risk frameworks, and ensuring operational reliability all demand rigorous development and consistent attention.

As the debate over blockchain's potential and limitations continues, there's observable interest in the technology across the spectrum of financial institutions. Banks, asset managers, insurance companies, and payment platforms are increasingly recognizing its inherent value and array of tangible benefits. Blockchain's potential ramifications extend across various financial domains, including capital markets, asset management, global payments, trade finance, and insurance. But its efficacy, scalability, and broader implications remains an active subject of ongoing research and experimentation. For an in-depth look at potential implications within financial services, refer to Exhibit 1.

There are many central banks globally actively engaging in blockchain projects, reflecting the technology's potential in the financial services sector. Collaborations between these central banks and industry players on selected experiments emphasize the collective drive to explore blockchain's potential. A notable example is the Monetary Authority of Singapore's Project Guardian, which underscores the opportunities of extending decentralized finance into the realm of real-world assets with several financial institutions (please see Oliver Wyman's insights on Project Guardian). This project aims to test the feasibility of unified liquidity pools in an environment that manages risks effectively. The overarching objective of such initiatives is not only to optimize operations but also to ensure that the technology integrates seamlessly with the current infrastructure while upholding the highest standards of financial stability and integrity.

Simultaneously, many financial institutions are actively engaging in research programs, pilot projects, proof of concepts, and even full-scale initiatives. The goal for many is not just to understand the technology's potential merits but to configure the necessary guardrails to scale. These organizations are experimenting to determine how blockchain may fit within their operational frameworks and where adjustments may be required. This proactive exploration underlines the sector's intent to understand, and if deemed viable, harness the potential advantages of blockchain while maintaining their business and risk models.

Exhibit 1: Use case universe



Identified use cases	**Key impact areas** (non-exhaustive)
● **Payments and remittances**	
• Domestic retail payments • Domestic wholesale and securities settlements • Cross border payments • Tokenized forms of digital money	**Real-time transactions:** Ensures and enables real-time domestic and cross-border payments for retail and wholesale payments **Verification:** Digital KYC/AML systems mitigate fraud by offering immediate authentication and transaction transparency **Risk reduction:** Implements atomic settlement to reduce settlement risk; leverage smart contracts to automate specific regulatory and compliance procedures
● **Marketing and loyalty**	
• Loyalty programs management • Marketing efforts optimization • Personalized marketing campaigns • Customer data analysis	**Customer loyalty:** Tokenized rewards systems enhance loyalty point value by offering tradable digital tokens **Data-driven marketing:** Utilizes user data for personalized campaigns, leading to more meaningful engagements
● **Banking and lending**	
• Credit prediction and credit scoring • Loan syndication, underwriting and disbursement • Asset collateralization	**Dynamic credit analysis:** Harnesses networked user data for expedited and autonomous decision-making in credit assessments **Loan process innovation:** Streamlines the lending journey, from syndicate formation to fund disbursement via automation **Enablement of capital markets solutions:** Enhances and reduces costs for originate-to-distribute businesses
● **Trade finance**	
• Letters of credit and bill of lading • Financing structures • Provenance databases	**Financing models:** Digital and secure networks enable the creation of distinctive financing structures across the entire value chain **Asset digitalization:** Accelerate and enable settlements with tokenized assets to enhance liquidity

Identified use cases	**Key impact areas** (non-exhaustive)
● **Insurance**	
• Reinsurance markets • Fraud prevention • Claims processing and disbursement • Policy issuance and administration	**Claims automation:** Smart contracts expedite claims and reduce errors and biases for payment processes **Policy management:** Establish tokenized policies to optimize data management and processes across the value chain **Reinsurance digitization:** Enable efficient open marketplaces with enhanced liquidity, transparency, and risk management
● **Capital markets**	
• Issuance • Sales and trading • Post-trade services • Asset servicing • Custody clearing and settlement	**Global liquidity:** Enables a global 24/7 environment to enhance liquidity, and broadens capital markets for traditionally illiquid and physical assets by integrating with IoT solutions **Risk reduction:** Implements atomic settlement, ensuring secure and finalized asset transfers to minimize settlement risk, ensure a consistent calculation of settlement amounts, reduce or eliminate settlement breaks **Enhanced access:** Reduced cost of intermediation and broadening across capital markets from both the issuer and investor side
● **Asset management**	
• Transfer agency • Cap table management • Fund launch and management • Fund administration	**Diversification and global access:** Facilitates wider reach to diverse assets and international liquidity through asset tokenization **Advanced portfolio management:** Enables portfolio optimization by utilizing real-time data and smart contracts **Streamlined operations:** Utilizes tokens and smart contracts to simplify and automate fund launches and management processes

Source: Oliver Wyman and Matter Labs analysis

Chapter 02

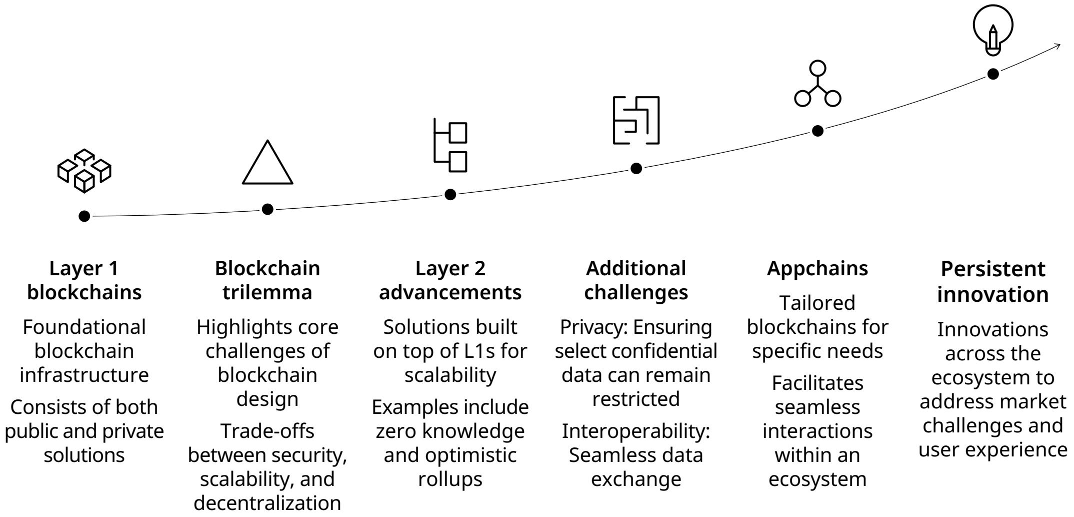
THE EVOLUTION OF BLOCKCHAIN SOLUTIONS

The evolution of blockchain solutions is a testament to the dynamic nature of technology and its adaptive response to prevailing challenges. Initially, L1 blockchains heralded the potential of decentralized networks but soon encountered the blockchain trilemma, the trade-off between decentralization, security, and scalability.

The struggle to optimize these three key attributes gave rise to L2 solutions, focusing primarily on addressing scalability concerns without undermining the foundational pillars of security and decentralization. However, as the technological landscape matured, challenges beyond the trilemma, particularly those related to interoperability and privacy, emerged as pivotal barricades.

To navigate these multifaceted issues, the concept of appchains emerged. These innovative structures built atop traditional L1s and L2s, present tailored blockchain solutions with an emphasis on seamless interaction and customizability. This section delves deep into this evolutionary journey, charting the progression from L1 blockchains to the sophisticated realm of appchains.

Exhibit 2: We can summarize the evolution of blockchain in six stages



Layer 1 blockchains

Foundational blockchain infrastructure

Consists of both public and private solutions

Blockchain trilemma

Highlights core challenges of blockchain design

Trade-offs between security, scalability, and decentralization

Layer 2 advancements

Solutions built on top of L1s for scalability

Examples include zero knowledge and optimistic rollups

Additional challenges

Privacy: Ensuring select confidential data can remain restricted

Interoperability: Seamless data exchange

Appchains

Tailored blockchains for specific needs

Facilitates seamless interactions within an ecosystem

Persistent innovation

Innovations across the ecosystem to address market challenges and user experience

Source: Oliver Wyman and Matter Labs analysis

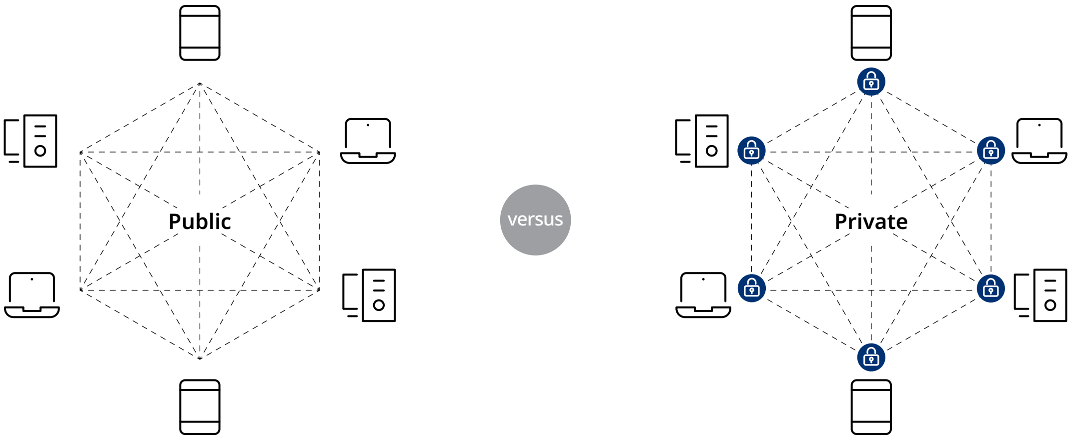
LAYER 1 BLOCKCHAIN SOLUTIONS

Since Bitcoin's inception in 2009, the blockchain landscape has evolved rapidly in terms of variety and sophistication of solutions across both public and private domains. Bitcoin marked the dawn of L1 solutions, acting as the foundational layer of the blockchain ecosystem while serving as the backbone for all subsequent blockchain innovations. L1s, also known as base layer protocols, represent the underlying blockchains that execute core consensus mechanisms and maintain the universally shared ledger.

As the foundational pillars, security, decentralization, and scalability, became fundamental for L1 design parameters, different blockchains were designed with varying objectives. While trailblazers like Bitcoin and Ethereum have driven blockchain adoption with their decentralized nature and commitment to security, private chains such as R3 and Hyperledger emerged with their attributes tailored for financial institutions and regulators, offering discrete and controlled transaction environments.

Both public and private blockchain systems, while rooted in the same core concept of a decentralized ledger, have distinct characteristics that cater to different purposes, audiences, and environments.

PUBLIC VERSUS PRIVATE BLOCKCHAINS



Public blockchains

Public blockchains are typically decentralized platforms that are open to everyone, allowing for both observation and transactions. With transactions being often publicly verifiable and validators distributed globally, they offer a robust and ready-to-use infrastructure. This shifts the economic dynamics from high upfront capital investments to a more consumption-based model. Public blockchains exhibit commercial viability, with monetary incentives embedded within the network fostering a self-sustaining ecosystem, paralleling how the internet operates, where entities like Cisco and various ISPs contribute to a foundational infrastructure that benefits all users. This transition mirrors the broader industry shift towards plug-and-play SaaS tools and public cloud infrastructure, making blockchain more accessible to a global audience. This consumption-based model generally opens access to anyone, enabling participants globally to join and validate transactions.

While the "ready-made" nature of the technology does lower certain barriers to entry, integrating public blockchains into an adopter's pre-existing environment poses its own set of challenges. The expertise in blockchain technology remains both niche and in high demand. Consequently, the investment required for this integration and subsequent support must be carefully balanced against the benefits the technology offers.

One of the defining features of public blockchains is their security. Their decentralized nature, bolstered by a robust incentive structure, makes them costly and challenging (though not impossible) to breach. For instance, Ethereum, with its eight-year track record, has remained resilient against outages from external attacks, though it's worth noting that some smart contracts on the platform have been compromised due to coding flaws.

The open structure of public blockchains paves the way for coherent upgrades and data sharing models, drawing upon global collaborative efforts.

Private blockchains

In contrast to public blockchains, private blockchains are tailored primarily for business and organizational applications to operate within a controlled environment. They often promise controlled access and enhanced privacy by revealing transaction details to involved parties. However, this can come at the cost of interoperability due to varied interests amongst entities in infrastructure and design preferences. This approach can result in multiple private blockchains, inhibiting seamless communication between them. Additionally, the burden of setting up, managing, and running this infrastructure can be onerous and complex. In many instances, broadening private blockchain networks can become a cumbersome task.

Central to these developments, the principle of credible neutrality emerged as a core theme for public blockchains. This concept emphasizes that for a platform to gain trust and wide adoption, it shouldn't favour any participant over another, ensuring an impartial environment where all parties, irrespective of their size or influence, are treated equally. The concept of credible neutrality can be explored across four facets: accessibility, transparency, decentralization, and rule setting.

In essence, while public blockchains champion transparency, global collaboration, and democratized participation, private blockchains cater to tailored requirements of confidentiality, accessibility, and operationality. Fundamental to the ethos of public blockchains is the concept of credible neutrality, a commitment to a design that doesn't appoint unfair advantage to any participant. While public blockchains lean on structural and transparent mechanisms to ensure credible neutrality, private blockchains depend more on governance structures and the integrity of their participants. As the ecosystem evolved, the shortfalls of L1s emerged as cornerstones of the industry that introduced trade-off models and limitations surrounding interoperability and privacy as we will delve into in the subsequent sections.

CREDIBLE NEUTRALITY

Factor	Public blockchains	Private blockchains
Accessibility	Anyone can join a public blockchain, participate in its consensus mechanism, and validate transactions	Restricted to a specific set of participants and entry is controlled, and new participants need to adhere to set admission criteria; not everyone can validate transactions
Transparency	All transactions on public blockchains are typically transparent and can be audited by users of the network	While transactions might be transparent to participants of the private blockchain, they are usually not open to the public
Decentralization	Distribute power and control across a wide network of participants, thereby making it challenging for a single entity to seize control	Since they are restricted to a select group, private blockchains typically run a higher risk of centralization
Rule setting	Immutable rule operations based on pre-defined rules and consensus mechanisms. Changes require broad consensus from network	More flexibility to change rules or adapt the system as they see fit

Source: Oliver Wyman and Matter Labs analysis

TradeLens, a trade finance based blockchain developed by Maersk in partnership with IBM is an example of the perils of not getting the neutrality right. The value proposition of centralizing data and automating processing using blockchain for trade finance is clear and well accepted by both the shipping and financial services industry. However, the network was impaired by challenges of neutrality; fast follower adopters questioned whether a network designed and operated primarily by Maersk could truly provide a level of access and neutrality. After five years of operation, IBM and Maersk had decided to wind down the blockchain.[1]

THE BLOCKCHAIN TRILEMMA

From its inception in January 2009, the blockchain ecosystem has grown and diversified immensely. A significant part of this diversification has been the advent of solutions aiming to address certain foundational limitations inherent to blockchain technology. Ethereum's co-founder, Vitalik Buterin, encapsulated these challenges in the blockchain trilemma, suggesting a trade-off between security, decentralization, and scalability.

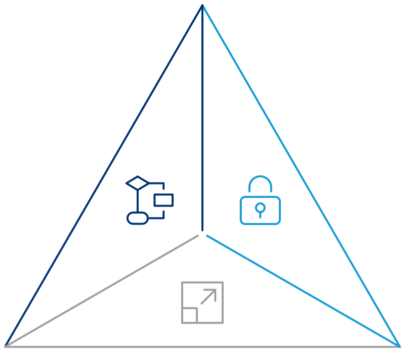
Blockchain projects approached the design of new network protocols through prioritizing two of these aspects, at the expense of the third. Central to these design decisions are the consensus mechanisms and protections against sybil attacks. Blockchain networks utilize protocols that allow participants to reach consensus on valid transactions without the need for mutual trust. These protocols also incorporate safeguards to deter malicious actors from undermining or hijacking the network.

[1] https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens.

Two pivotal protocols in this arena are proof-of-work (PoW) and proof-of-stake (PoS). PoW, epitomized by Bitcoin, offers robust security by validating transactions through energy-intensive computations. However, this method often demands a significant amount of electricity, making it costly and potentially constraining scalability. On the other hand, PoS provides an eco-friendlier alternative where validators must "stake" or lock up funds in the network. They are rewarded for correctly validating transactions but face financial penalties for any malicious actions.

PoS has emerged as the blockchain industry's approach with most networks now being either PoS based or using a protocol that is derived from PoS.

Exhibit 3: The trilemma



Decentralization ensures that decision-making power is not concentrated to a single actor and equitably distributed across a vast network of nodes and validators. Decentralization stands as a testament to blockchain's design promise of democratizing access and control, eliminating the potential for undue influence from a singular, dominant entity

Security is the bedrock upon which the trust in blockchain is built. It embodies the system's resilience against both external threats and internal malfunctions, ensuring that transactions are consistently validated, data remains immutable, and the trustworthiness of the entire ecosystem is upheld

Scalability refers to the capability of a blockchain to process vast volumes of transactions swiftly and efficiently. As applications proliferate and user bases grow, a scalable blockchain can manage high traffic while maintaining low costs and prompt transaction times

Source: Oliver Wyman and Matter Labs analysis

Private blockchains, with their distinct design ethos, often navigate the trilemma from a different vantage point. Their restricted, permissioned nature often compromises decentralization as the number of nodes or participants in these networks is limited, often to known and vetted entities. They can hence offer more robust security measures within a controlled setting and achieve enhanced scalability, often leveraging specialized consensus mechanisms tailored to their specific needs.

Exhibit 4: Stage 1 of evolution

The three key designs across public L1s allude to how blockchains are typically designed wherein there is typically a trade-off between components of the trilemma. Private L1s typically have key design that incorporates security and scalability as they are centralized

	Public L1s			**Private L1s**
	Three key designs			One key design
Blockchain trilemma				
Decentralization	●		●	
Security	●	●		●
Scalability		●	●	●
Beyond trilemma				
Privacy				●
Native interoperability				

Note: This exhibit provides a bird's eye view of how blockchains are typically designed and their respective characteristics. While it may not capture all the blockchains in the ecosystem, it offers a holistic oversight of key and prevailing designs and structures

Source: Oliver Wyman and Matter Labs analysis

LAYER 2 BLOCKCHAIN SOLUTIONS

As blockchain technology progressed and the challenges of the trilemma proliferated, the advent of L2 blockchain solutions marked a paradigm shift in the industry's approach to overcome foundational obstacles. Emerging in response to the trilemma's congestion and scalability challenges, L2s address the challenges hindering widespread blockchain adoption. Their underlying concept revolves around optimizing the existing infrastructure and overlaying secondary frameworks that offer rapid and efficient transaction processing. This leads to enhanced user experience due to the reduction in latency and increased throughput. These solutions function by offloading a substantial portion of transaction processing from the mainnet.

The predominance of Ethereum as the platform of choice for L2 development stems from its dynamic ecosystem and widespread adoption. While aiming to address the blockchain trilemma, L2s, especially on Ethereum, aim to enhance scalability without compromising the principles of security and decentralization of the mainnet.

L2 solutions have evolved in stages, each aiming to address the inherent challenges of blockchain scalability. Initially, the field was dominated by plasma chains and optimistic rollups. These were early attempts at boosting scalability, acting as the pioneers in the L2 landscape. However, as the industry progressed, zk rollups emerged, building on the strengths of their predecessors while introducing enhanced features, such as low latency in transaction finality. Notably, zk technology places its trust in cryptography and mathematics, rather than any entity, for transaction validity. This ensures that even if a zk chain operator turns malicious, the most they can do is stop transactions, rather than manipulating or fabricating them. While these advancements are pivotal, it's essential to recognize their unified goal: to provide a decentralized, secure, and scalable environment that meets the evolving demands of contemporary applications and users.

Exhibit 5: Key L2 Designs (non-exhaustive)

Overview	Why were they created?	Key flaws of the design
2017 — Plasma chains		
Solution for Ethereum to scale its transaction throughput by creating "child" blockchains that can handle their own transactions and only communicate with the main chain when necessary, such as for settlements or in case of disputes	• Ethereum throughput and gas fees became a bottleneck for adoption • The concept of "child" blockchains emerged to process transactions separately, enhancing scalability • Child chains lead to reduced fees due to the absence of mainnet block space competition	• Doesn't fully inherit Ethereum security given not all data is posted • Users face hurdles in fund access if a Plasma chain operator acts maliciously • Withdrawal times are delayed by several days, and if too many users try to exit at the same time, mainnet could get congested • Requires users to constantly monitor chains and challenge any suspicious activity
2019 — Optimistic rollups		
Scaling solutions designed to sit atop existing blockchain networks, such as Ethereum. Their primary function is to enhance transaction throughput by executing transactions off-chain, while still leveraging the underlying security of the main chain. They assume that all transactions are correct unless proven otherwise	• Exit process on plasma chains were too complex • Improves the execution of smart contracts compared to plasma • Transaction data is posted on the main chain, ensuring data availability and less of a burden to infrastructure	• Users must wait several days to withdraw funds due to the design of optimistic chains • Challenges to a false state post are restricted to a specific time frame, potentially causing subsequent issues • Validators must provide a bond (lock up capital) before producing blocks. This also requires economic incentives for validators to always act honestly. Relies on game theory to keep the network safe
2019 — zk Rollups		
Like optimistic rollups, they also bundle many off-chain transactions into a single batch, but the validity of these transactions is ensured using zero knowledge proofs; which guarantees the correctness of all transactions in the rollup without needing them to be individually processed	• The withdrawal process on Optimistic rollups was too long. With zk there is no need to rely on honest network participants and validators. Only relies on cryptography. As a result there is no waiting period for transaction finality • Optimistic rollups must post a lot of data back to Ethereum. With the zk approach, it is possible to still make sure data is available, yet in compressed format to achieve scalability	• Generating zk-proofs requires trusted setup on SNARKS (however this is not the case for STARK based provers, which are gaining adoption now) • Proof systems are extremely complex and require very large computational power. This makes them fairly hard to operate and manage and drives up costs • Newer technology with complex mathematical underpinnings which limits the pool of developers with a profound understanding

Source: Oliver Wyman and Matter Labs analysis

The blockchain industry has seen continuous development of various design consensus mechanisms, with the current focus shifting toward building well-versed models that address scalability, security, and interoperability. Within this context, the zk technology stack has emerged as a leading option. Similarly, Optimism has pursued two proposals to add zk-proofs to its network, responding to a request for a proposal aimed at enabling secure and efficient cross-chain communication.[2] These transitions underscore the zk technology's burgeoning influence, a sentiment echoed by Buterin who has identified zk technology as a solution that, while challenging to build, is likely to supersede optimistic rollups.[3]

While acknowledging the complexities involved in zk technology, Buterin has also emphasized that its robust fundamentals would likely make zk Ethereum's preferred scaling solution.[3] Further innovations, such as zkSync's Boojum, which operates on commodity 16GB GPU hardware, and the general transition to STARK from SNARK proofs, which eliminate the need for trusted setups, showcase the resilience and cost-efficiency of zk technology. As zk's potential continues to solidify, its role as a pivotal force in shaping the industry's future is becoming increasingly evident.

BEYOND THE TRILEMMA

L2s have undoubtedly transformed the public blockchain landscape, enhancing scalability, security, and decentralization. However, for highly regulated industries such as Financial Services, the challenges go beyond the foundational trilemma that L2s were designed to overcome. Notably, financial institutions seek robust solutions for privacy and native interoperability.

Privacy ensures that data, especially sensitive financial data, remains confidential and only accessible to relevant parties. In the era of digitized finance, the privacy of transactions and user data are paramount. While blockchain's transparent nature can offer complete accountability and traceability, not every piece of data should be open for scrutiny. L1s, with their foundational structures, often prioritize universal visibility due to their inherent designs, which can inadvertently expose sensitive data. L2s, while designed to scale transactions, remain tied to their foundational layers for security and finality, thereby sharing the same privacy constraints as the mainnet. Balancing the need for transparency with the rightful demand for privacy becomes a new dimension of challenges.

Native interoperability concerns the ability for different blockchain systems to communicate directly, share data, and carry out transactions cohesively. As blockchains multiply and address diverse needs, it becomes increasingly important for these disparate systems to

[2] https://github.com/ethereum-optimism/ecosystem-contributions/issues/61.

[3] https://www.theblock.co/post/162098/zk-rollups-likely-to-be-main-layer-2-solution-for-ethereum-says-vitalik-buterin.

directly exchange data and information without impediments. Most L1s, both public and private, with their unique consensus mechanisms and protocols, struggle with seamless native interoperability, often resorting to third-party bridges or relying on smart contract wallet bridges and wrappers. While these solutions offer a form of interoperability, they can be either less secure or economically inefficient, making them an inadequate solution for facilitating adoption.

Consequently, public L2s, linked to their foundational parent network, inherit the same challenges as their underlying L1. In the domain of Financial Services, overcoming challenges associated with interoperability is crucial to streamline operations in sectors involving multiple entities and systems. This ensures minimized inefficiencies and fosters collaborative settings.

As the ecosystem delves into these advanced challenges, the need for solutions that can encompass all of these requirements — from addressing the trilemma to ensuring privacy and promoting native interoperability — becomes an imperative facet. It’s critical to understand that the objective isn’t to find a “flawless” solution. Rather, the objective is to pinpoint a solution that adeptly combines these elements, striking a balance among these components that best align with their unique requirements and risk tolerance levels.

Exhibit 6: Stage 2 of evolution

One key design across public L2s that aim to address the blockchain trilemma to capture all three facets

	Public L1s			**Private L1s**	**Public L2s**
	Three key designs			One key design	One key design
Blockchain trilemma					
Decentralization	●		●		●
Security	●	●		●	●
Scalability		●	●	●	●
Beyond trilemma					
Privacy				●	
Native interoperability					

Note: This exhibit provides a bird’s eye view of how blockchains are typically designed and their respective characteristics. While it may not capture all the blockchains in the ecosystem, it offers a holistic oversight of key and prevailing designs and structures

Source: Oliver Wyman and Matter Labs analysis

APPCHAIN BLOCKCHAIN SOLUTIONS

Appchains have emerged as an innovative layer in the blockchain landscape, strategically positioned on top of traditional L1s and L2s. Designed with the dual capability to bolster privacy standards and foster interoperability, whilst also dismantling the trilemma, their introduction provides a twofold opportunity to the financial sector: firstly, the capacity to harness blockchains tailored specifically to certain needs; and secondly, the ability to functionwithin an ecosystem where these tailored blockchains can interact seamlessly.

Unlike traditional L1s and L2s that bolster the capability of an individual mainnet node (also known as vertical scaling), appchains can expand by adding parallel chains, also known as horizontal scaling, which distributes the workload and augments transaction throughput. Horizontal scaling ensures that as the demand increases, new chains can be integrated into the network to handle the extra load, ensuring that the system remains agile and responsive. The reduction in waiting times, combined with the potential for lower transaction fees due to increased efficiency, translate to an enhanced user-friendly experience. This approach not only allows for easy migration but also enables entities to create their own specialized application ecosystems. The benefits of appchains address many of the limitations posed by the blockchain trilemma and the intricate challenges of privacy and interoperability.

Appchains, in their design and consensus mechanisms, exhibit a wide variety of approaches tailored to address specific challenges. Many appchains also adopt distinct designs and consensus mechanisms emphasizing different facets to align with their desired use cases. A notable approach is demonstrated by zkSync's zk technology stack which allows anyone to build their own fully customized Layer 2 or Layer 3 app chains, also known as hyperchains, utilizing zkSync's zk-proof technology. Each hyperchain runs execution and transaction validation in parallel and users can choose a number of options for privacy, compliance, and data interoperability. Through this horizontal scaling, anyone using the zk technology stack could achieve their desired level of throughput for their application while maintaining security through the use of zk-proof technology for transaction validation. Meanwhile, platforms such as Avalanche subnets achieve scalability by allowing many blockchains to run in parallel within a subnet environment. On the other hand, Polygon's supernets utilize parallel chain infrastructures to ensure transaction validity off-chain.

However, it's critical to understand that appchain models may differ in terms of their technology stack, which may inherently impact the degree of privacy and interoperability. Platforms such as Avalanche use the appchain model for executing subnets, that enable blockchains to run in parallel. In contrast, zk fractal appchains employ zk-rollup technology to ensure data integrity and scalability while also inheriting the security properties of Ethereum. This makes zk fractal appchains fundamentally different, providing distinct security and interoperability features. On the other hand, Polygon's supernets utilize parallel chain infrastructures to ensure transaction validity off-chain, providing yet another design mechanism of the nuanced technical distinction.

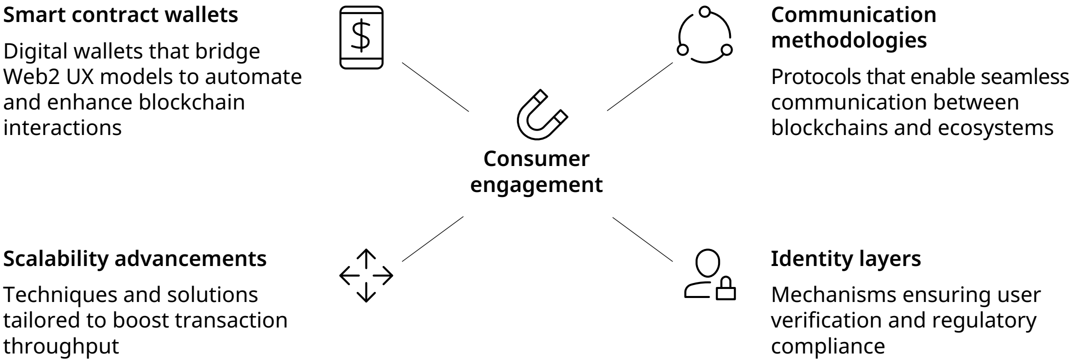
Altogether, appchains offer precise solutions to the issues posed by blockchain privacy, providing entities with granular privacy controls that allow them to dictate transactional privacy levels, ranging from full disclosure to selective element protection. For example, by utilizing zk-proof technology, certain appchains can validate transactions without revealing the specifics of the transaction itself, thus ensuring data confidentiality while maintaining the integrity of the blockchain. Crucially, validity-based general messaging systems, such as hyperbridges, are pivotal to native interoperability. Unlike the more common trusted bridges, which are susceptible to hacks, these hyperbridges provide a more secure and robust connection. In terms of interoperability, appchains can seamlessly communicate within their ecosystem and enable native bridges that enable instantaneous data transfers.

Outside of the two intricacies of privacy and interoperability, appchains promote flexibility in both decentralization and data storage, ensuring they meet regulatory standards and resonate with internal policies. This flexibility extends to control over sequencer functionality, enabling entities to control transaction processes and designate validators. They can also decide where data is stored, whether on public ledgers, private networks, or even standard servers. On the economic front, their potential for very low gas operations significantly reduces costs in comparison to traditional L1s and L2s.

PERSISTENT INNOVATION

Appchains represent a pivotal evolution in the blockchain space, allowing enhanced integration with web 2.0 platforms and other ecosystems. Specifically tailored for distinct verticals and use cases, they simplify the implementation of services and foster better user engagement.

Exhibit 7: Key advancements



Smart contract wallets

Digital wallets that bridge Web2 UX models to automate and enhance blockchain interactions

Communication methodologies

Protocols that enable seamless communication between blockchains and ecosystems

Consumer engagement

Scalability advancements

Techniques and solutions tailored to boost transaction throughput

Identity layers

Mechanisms ensuring user verification and regulatory compliance

Source: Oliver Wyman and Matter Labs analysis

SMART CONTRACT WALLETS

At the forefront of enhancing user interaction with blockchains are smart contract wallets. These digital wallets, entirely programmable by nature, represent the next step in simplifying and securing blockchain experiences. Unlike traditional wallets, which require users to manage cumbersome seed phrases, smart contract wallets automate many aspects of blockchain interactions. Users can define spending limits, employ authentication methods, predefine financial strategies, interact with a multitude of decentralized applications, and perform complex blockchain transactions with greater ease. Furthermore, the interoperability of these wallets allows users to effortlessly navigate diverse blockchain ecosystems and participate in a myriad of activities and ecosystems. Notably, these wallets offer financial institutions the flexibility to transact exclusively in fiat through intermediaries that facilitate on-and-off-ramping to align with regulatory constraints.

Exhibit 8: Smart contract wallets

Social recovery
Graduate from managing seed phrases

Spending rules
Define limits to manage spending

Flexible validation
Use familiar authentication methods

Multicall plus sessions
Combine complex blockchain transactions

Custom gas
Pay gas in any token or go gasless

Source: Oliver Wyman and Matter Labs analysis

Presently, the technical complexities of interacting with applications on public blockchains are best navigated by tech-savvy individuals. Nevertheless, innovative solutions are emerging to simplify this experience. Smart contract wallets, such as Clave, are emerging and now incorporate features such as biometric integration to broaden blockchain accessibility to the average user. While wallets have predominantly focused on basic tasks like authorizing individual transactions, there's growing potential for these platforms to evolve and manage more sophisticated financial operations.

SCALABILITY ADVANCEMENTS

L2 scalability on blockchains is undergoing rapid evolution, led by advanced solutions such as horizontal scaling. This approach aligns with the way Web2 apps scale, emphasizing the deployment of multiple Layer 2s and Layer 3 zk rollups that operate without sharing an execution environment. As a result, the system can handle high transaction volumes, potentially scaling up to millions of TPS. Horizontal scaling represents resilience during mass on-chain events which enable an environment to be unaffected by the congestion on other ecosystems.

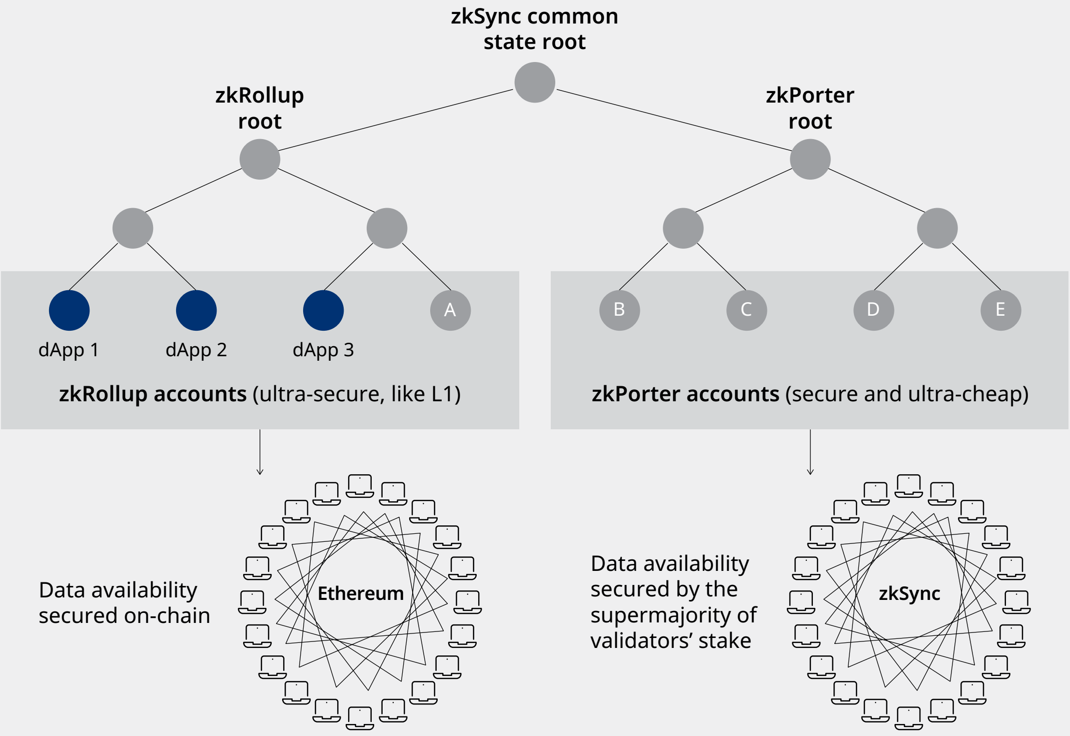
To enhance vertical scalability, design choices like zk and optimism move transactions off-chain. When coupled with upcoming advancements such as sharding, these design choices allow rollups to process not just a few hundred, but thousands of transactions per second.

A prime illustration of this ambitious vision is zkSync's zkPorter, which bifurcates L2 states between on-chain and off-chain data availability. Keeping data off-chain offers significant scaling advantages, as it minimizes on-chain congestion. Touted as a breakthrough, this approach amplifies transactional speed and drastically reduces costs, marking a key avenue for enabling widespread blockchain adoption.

Case study

ZK PORTER IMPACT

zkSync 2.0 has emerged as a compelling solution for scalability, strategically dividing its Layer 2 state into two domains: zkRollup, which alludes to on-chain data availability, and zkPorter, which emphasizes off-chain data. This innovative partition not only ensures seamless interoperability between the two systems but also drastically reduces user fees. This cost-efficiency is attributed to zkSync 2.0's ability to batch transactions. To bolster data security and availability, the system introduces "guardians" that are committed to a proof of stake framework. These guardians underpin the platform's robustness, confirming data availability and security. The innovative approach adopted by zkPorter, coupled with its guardian mechanism, establishes a prudent precedent for the future of scalable blockchain systems that can maintain security while augmenting tangible benefits such as reduced fees, superior throughput, and enhanced privacy.


zkSync common state root
zkRollup root
zkPorter root
dApp 1
dApp 2
dApp 3
A
B
C
D
E
zkRollup accounts (ultra-secure, like L1)
zkPorter accounts (secure and ultra-cheap)
Data availability secured on-chain
Ethereum
Data availability secured by the supermajority of validators' stake
zkSync

Source: Matter Labs analysis

COMMUNICATION METHODOLOGIES

Appchains are ushering in a new era of native interoperability, with each possessing its own built-in messaging and interoperability protocol. This native capability ensures fluid inter-ecosystem communication, enhancing the user experience within the appchain realm. For example, zkSync's zk technology stack includes a shared bridge and an interoperability layer, enabling any set of hyperchains to communicate directly without the need for trusted intermediaries.

However, for communication outside their native ecosystems, cross-chain communication layers are emerging such as Chainlink's "Cross-chain Interoperability Protocol (CCIP)". It's essential to note that Chainlink's CCIP utilizes trusted bridges, which operate on a different technological premise compared to the trustless and completely secure nature of validity-based general messaging systems. While CCIP is emerging as a strong contender in bridging interoperability across blockchains, especially given their partnership with SWIFT and global banks for tokenization to seamlessly connect financial institutions, its approach to ensuring interoperability is distinct from a technology point of view. Though natively interoperable bridges exist to facilitate seamless transfers within a network, tools such as CCIP are critical for enabling interoperability between different infrastructures, such as a hyperchains on zksync and another blockchain. These foundational solutions augment the capabilities of appchains to provide a comprehensive framework for both intra-and-inter-ecosystem communication.

IDENTITY LAYERS

In the evolving confluence of global finance and technology, the importance of security and regulatory demands rigorous attention. Addressing this, identity layers, designed from the ground up, are integrated within blockchain architectures to provide a safe environment for users to attest their credentials without having to hand over their data. Beyond just identity verification, these layers ensure all participants are compliant, and offer intrinsic mechanisms for insurance, AML, and fraud monitoring at the blockchain level. Such a holistic approach means transactions are executed only by verified participants, enabling continuous AML oversight. By blending regulatory mandates with the decentralized ethos of blockchain, KYC layers form a pivotal bridge, paving the way for trusted environments to potentially boast institutional and retail adoption.

SUMMARY OF BLOCKCHAIN SOLUTIONS

Reflecting on the blockchain industry all together, the evolution of blockchain solutions showcases the industry's commitment to addressing inherent challenges. From the foundational L1s, which grappled with the trilemma, to the L2s that emerged with a focus to bridge scalability, every development represents a monumental stride towards a more optimized and dynamic ecosystem. Appchains further the progression by directly addressing challenges vital to financial services, such as privacy and interoperability.

The progression from basic blockchains to advanced appchains is marked by key innovations: from smart contract wallets that revolutionize user interfaces, to scalability breakthroughs ensuring rapid transaction speeds, advanced communication techniques promoting effortless chain interactions, and the incorporation of KYC layers for compliance and security. Together, these pillars highlight blockchain's continuous improvement, versatility and readiness to meet both contemporary and emerging financial challenges. As these public blockchain solutions mature, they not only address known challenges but also pave the way for transformative shifts.

Exhibit 9: Stage 3 of evolution

Many design options as appchains enable users to control blockchain characteristics across all dimensions

	Public L1s			**Private L1s**	**Public L2s**	**Public app-chains**
	Three key designs			One key design	One key design	Many design options
Blockchain trilemma						
Decentralization	●		●		●	●
Security	●	●		●	●	●
Scalability		●	●	●	●	●
Beyond trilemma						
Privacy				●		●
Native interoperability						●

Note: This exhibit provides a bird's eye view of how blockchains are typically designed and their respective characteristics. While it may not capture all the blockchains in the ecosystem, it offers a holistic oversight of key and prevailing designs and structures

Source: Oliver Wyman and Matter Labs analysis

Chapter 03

ALL ROADS LEAD TO ROME

In ancient times, Rome was not just the capital of an empire, but a symbol of connectivity, commerce, and convergence. Drawing a parallel to the blockchain universe, we envision a similar convergence. The diverse blockchain initiatives, both public and private, reflect these ancient pathways and side gardens. Though each brings unique challenges akin to different terrains, they all converge towards a shared vision: an interoperable and scalable ecosystem suitable for an array of financial services use cases.

The city of Rome was not built in a day, nor was it built in isolation. Its rise was marked by the convergence of diverse paths, each representing varied aspirations and potentials. Similarly, in the realm of blockchain, various use cases are gradually emerging, each promising to address real-world problems and unlock profound potential across different capabilities of the financial services industry. Although a lot of the emerging use cases are currently nascent and in exploration stages, they are beginning to demonstrate tangible impacts. Among these burgeoning use cases, tokenization stands out as transformative due to its widespread applications. The process of converting tangible and intangible assets, such as equities, bonds, loyalty points, real estate into blockchain tokens is paving new avenues in the financial landscape. While tokenization is a key highlight, it represents one of the many roads leading to the modern-day “Rome” of a fully comprehended blockchain ecosystem. Each application, as it evolves, promises to address a set of distinct challenges, whether in terms of accessibility, security, convenience, or cost for the financial services industry.

PUBLIC AND PRIVATE LANES TO ROME

Like the intricate web of roads leading to Rome, the blockchain landscape is characterized by diverse pathways, each representing its own set of challenges and opportunities. At a high level, two principal types of paths in this context are public and private blockchains, which have been growing in use in financial services, sometimes in parallel and sometimes with foresight from select private blockchains to merge with other private blockchains to create a network of networks. That said, most recent blockchain developments in the financial sector are phased by a series of use cases with each operating in its unique lane. These lanes, varying in complexity, are shaped by the type of financial institution, their risk parameters, and the regulatory environments they operate within and sometimes lack the benefit of standardization. For instance, while US banks grapple with restrictions preventing engagement with public infrastructure, their European counterparts observe more flexibility. Meanwhile, asset managers in the US can engage directly with public infrastructure. Across geographical boundaries and industry verticals, certain blockchain solutions and use cases shine brighter due to their contingencies tied to requirements of the sector and targeted products. As the complexity of blockchain use cases can range from equity markets to loyalty points, the variances in data management and regulatory prerequisites underline the nuanced differences across lanes, related to their unique risk and complexity profiles. To navigate these lanes, it's essential to understand that each financial institution operates within its own risk parameters, pace, and values.

Exhibit 10: Blockchain use cases complexity

Low → **Complexity** → High

Internal functions within an organization	**Client-specific with individual engagements**	**Multi-clients with cross-client interactions**	**Many-to-many markets for broad interactions**
Overview			
Focuses on internal process improvements and data optimization. No external client involved. The nature of this lane allows for greater risk control and adaptability	Direct engagement between the institution and a single client with no inter-client data sharing. Concerns related to privacy and data overlap are minimized	Involves multiple clients interacting within a closed network managed by a single provider. Critical to ensure that client data remains segregated, protected, and confidential	Involves interactions between multiple institutional entities and their numerous clients. Ensuring data privacy and security is paramount, especially when dealing with sub-transactions
Key characteristics			
Operational efficiency and agility: Improved data management provides real-time views and faster processes and reduced manual intervention Enhanced compliance: Real-time data tracking can aid in meeting regulatory requirements and timely reporting	High customization: Solutions can be designed to cater specifically to the unique use case and set of requirements Strong privacy: With just one client, there's an inherent reduction in risks associated with data sharing domain models	Data segregation: Ensuring that client data isn't accessible or identifiable by another client within the same network Service agreements: The provider of the network needs to establish prudent governance capabilities covering terms and conditions	Sub-transaction privacy: Institutions need mechanisms that prevent the reengineering of transactions, ensuring that data remains confidential Data domain security: Critical to ensure that data isn't comingled across different client domains

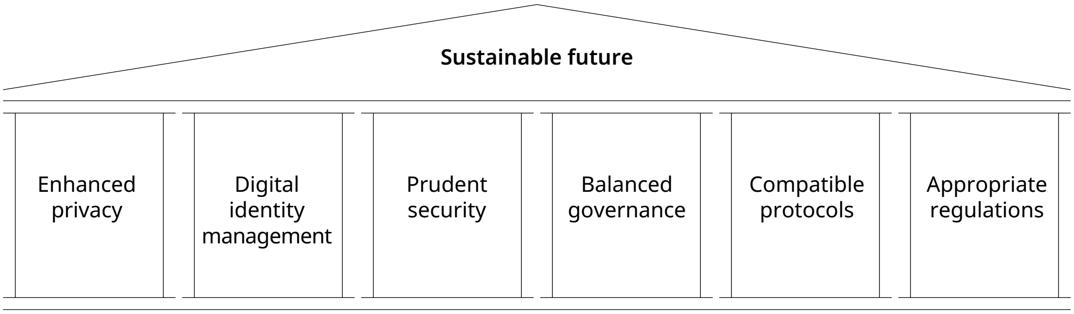
Source: Oliver Wyman and Matter Labs analysis

While innovations are being charted across a number of public and private blockchain domains to explore the viability of both simple and intricate use cases, true harmonization across these blockchain initiatives requires a careful balance between scalability, security, privacy, and interoperability. Just as Rome wasn't built in a day, the vision of an integrated blockchain-based financial sector will demand collaboration, persistence, vigilance, and a commitment to building robust and scalable solutions.

BUILDING A SUSTAINABLE FUTURE

Although the journey to Rome has advanced significantly, with various solutions addressing foundational challenges, there remains a roadmap of crucial components to further streamline the route. Blockchain's interoperable and scalable future in financial services still relies on a series of essential advancements, including enhanced privacy, robust digital identity, prudent security, balanced governance standards, compatible protocols, and appropriate regulations.

Exhibit 11: Building a sustainable future



Source: Oliver Wyman and Matter Labs analysis

ENHANCED PRIVACY

Privacy stands as both a challenge and a cornerstone for user trust. As the industry advances, it becomes imperative to integrate robust privacy measures. In the blockchain ecosystem, transactional anonymity remains a cornerstone. Across a series of use cases, ensuring participants operate with pseudonymity is imperative, shielding them from undue exposure while promoting free interaction. Recent advancements in zk technologies, such as zkSync's zk technology stack, provide operators with the option to publish their data on a private server or a separate blockchain to ensure data privacy. Meanwhile, it still utilizes zk-proofs to validate transactions for all network participants.

However, the same network that ensures this level of anonymity must also be resilient enough to guarantee data recoverability. It is imperative that transactional data remains intact and accessible, making it possible to reconstruct ledgers without putting participant identities at risk or undermining the blockchain's foundational principles. Beyond privacy concerning data, both public and private blockchains, share a key challenge in data privacy, which represents a barrier to adoption for corporate entities that require that their data is not comingled with other participants. Both public and private blockchains have evolved design patterns to address this but remain generally nascent in their maturity and adoption.

DIGITAL IDENTITY MANAGEMENT

Digital identity, at its essence, represents personal information about individuals, organizations, or devices in a digital format. Acting as a universal digital passport, it serves as a key to access services, determines privileges, and anchors trust. This is especially significant in the realm of blockchain, which strives to offer tamper-proof and verifiable records, eliminating the need for selected intermediaries and bolstering overall trust. Such identities can streamline verification, foster rapid customer onboarding, enhance user experiences, and ensure compliance in a rigorous regulatory environment. Beyond mere authentication, they also herald the potential for broader financial inclusion, introducing previously unbanked populations to the global economy. Akin to the interconnected roads of Rome, the incorporation and standardization of digital identity emerge as vital pillars to ensure a secure, inclusive, and democratized digital ecosystem to enhance and simplify user experience.

PRUDENT SECURITY

The very nature of blockchain, where data is immutable and permanently inscribed, presents a nuanced security challenge. While transactions can be anonymized and identities can be protected, the fundamental fact remains that all data is forever present on the blockchain. To mitigate the issue of data being permanently stored on the blockchain, forks and archives serve as a solutions. Forks can be agilely implemented in an appchain ecosystem, where governance protocols are established, making it easier to reach consensus. In contrast, executing forks on L1 and L2 levels can be more cumbersome due to the need for wider network consensus. In a financial world where discretion is paramount, the enduring presence of this data demands security solutions that require avenues to mitigate instances where ledgers can be reconstructed. Ensuring the safety of transactions, especially in a landscape punctuated by regulations, becomes imperative for financial institutions.

Beyond the security of indefinite data on the blockchain, L2 solutions function through smart contracts with assets typically secured by a singular or a multi-signature key. To mitigate this vulnerability, many L2 solutions are moving along the path to greater decentralization, diversifying the control over assets. The crux of vulnerability lies in the potential breach of these smart contracts, risking sizable fund drainage by adversaries. Given the magnitude of stakes, even rare eventualities are deemed intolerable by the risk management divisions of financial institutions. Consequently, L2 innovations now pivot towards fortifying against such risks. A notable stride in this direction is zkSync’s zk technology stack, which, even under attack, merely halts network operations without compromising the security of the funds. This security arises from its use of zk-proofs where no single entity can produce invalid transactions as those using the zk technology stack inherit Ethereum’s security. This means that to create invalid transactions, an attacker would have to compromise Ethereum.

BALANCED GOVERNANCE STRUCTURES

Governance, within the blockchain paradigm, serves as a central compass to guide the intricate decision-making processes that underpin protocol advancements and adaptations. A pivotal aspect of this governance is ensuring a balanced distribution of nodes, which fortifies the network against centralized control and potential malicious actors, upholding network integrity. In certain instances, originators of private blockchains might migrate towards more distributed node management with new additions to their networks, however, balanced governance goes beyond the mere mechanics of node management. It is about decision-making. As a foundational pillar, it ensures that changes in the financial ecosystem unfold with transparency, ethical considerations, and broad consensus. In an era where finance is rapidly evolving and blockchains are becoming a prominent solution, having a resilient governance model becomes paramount. This model acts as a safeguard to ensure that the ecosystem grows in alignment with the collective aspirations of its users, facilitating innovation without compromising on key parameters such as security or privacy. Just as institutions like ISDA have standardized securities processing language, and entities like DTCC and IHS Markit have been instrumental in creating benchmarks and facilitating coordination in capital markets, effective and balanced blockchain governance guides towards a financial future that's adaptive yet secure.

COMPATIBLE PROTOCOLS

Compatibility of protocols is the linchpin for interoperability within the blockchain universe. For the full potential of blockchain to be realized, a unified set of standardized efforts become essential. As the number of blockchain networks grow, infrastructure operators, both retail and institutional, should collaborate to establish these standards, ensuring efficient communication across various platforms as well as standards for validators. While some systems can effectively operate independently, such as most private blockchains that offer a controlled environment which is essential for regulated entities to meet stringent regulatory requirements, compatible protocols bring benefits such as simplified integrations, reduced system fragmentation, and enhanced network effects. In the process of achieving compatibility, it is vital to maintain a balance as overly stringent standardization can curtail innovation and hinder adaptability. Looking to established models, like the internet's TCP/IP, can offer valuable insights in this endeavour. In the pursuit of a harmonized blockchain landscape, compatibility stands out as a key component for guiding diverse networks towards amassed interoperability.

APPROPRIATE REGULATIONS

As blockchain technology becomes more ingrained in the financial sector, there's a dynamic shift in the associated regulatory environment. For example, across the US, regulators perceive public blockchain technology as introducing emerging risks that don't currently exist in the financial services system. Given this perspective, the bar is set high for adoption and integration. As such, regulators are striving to find the right equilibrium between encouraging innovation and fulfilling their statutory objectives. It's crucial for financial institutions to have clear and consistent regulatory guidelines as they venture deeper into blockchain exploration and implementation. Ambiguities in these guidelines can pose challenges to its widespread adoption, much like any emerging technological advancement. Yet, open dialogues between industry leaders and regulators globally can lead to well-defined frameworks that protect interests while also promoting innovation.

Regulators and policymakers are also positioned to be catalysts for large-scale change. Illustrating this, the BIS advocates for the development of a unified ledger to harness the full potential of tokenization on a programmable platform. Their vision comprises multiple ledgers, each tailored for a specific use case, interconnected via application programming interfaces to ensure interoperability. Moreover, it positions regulated financial services entities at the helm for network node management.

CONCLUSION

Public and private blockchains are similar to the ancient pathways leading to Rome targeting to a nexus of connectivity and commerce in an interoperable and scalable ecosystem. We expect both public and private blockchains to have their distinct roles in the evolving structure and continue to co-exist, with the choice between them being dictated by various criteria, such as specific use case requirements, the nature of the financial institutions involved, their risk appetite, and the regulatory environment.

Private blockchains may continue to appeal to institutions for their tailored controls over validator nodes and data integrity. For large financial institutions or financial market utilities, their inherent economic scale could potentially allow them to operate in siloes. However, these isolated systems ultimately risk curtailed growth and diminished interoperability over time. As the ecosystem evolves, entities may need to transition from confined environments to harmonized ecosystems that can synchronize and interact with one another. This network of networks could herald the next phase of private blockchain evolution. The full potential of this transformation can be harnessed when standardization is prioritized and achieved, or when industry-wide initiatives, driven by policymakers, regulators, or consortiums, move towards harmonious frameworks like a unified ledger.

On the other hand, appchains, which are tailored blockchains, seamlessly integrate with both L1 and L2 public blockchains, melding the strengths of both layers while prioritizing interoperability, privacy, and scalability. Crafted with specific use cases in mind, appchains enhance the benefits of previous layers whilst illustrating selective characteristics of private networks, such as controlled access. These may evolve to bear a striking resemblance to private blockchains in terms of validator selection, rigorous build and release management protocols, prudent risk assessments, and robust security, but may be obstructed by regulatory constraints until the industry, including regulators, develop the necessary safeguards for public blockchains. Yet, their inherent structure is increasingly recognized as enabling establishment and migration of prior blockchain ecosystems with limited functionality or suboptimal characteristics, thereby allowing institutions to tailor the technology to their unique needs. As these appchains become more entrenched, they are gaining acknowledgment as viable solutions for a growing range of specific use cases.

In any case, navigating the intricate roads to Rome demands collaboration, persistent innovation, and increased stakeholder engagement. The sustainable future of blockchain universe still relies on advancements in enhanced privacy, digital identity management, prudent security, balanced governance structures, compatible protocols, and appropriate regulations. There will be three types of market participants: first movers, fast learners, and the decidedly slow. The first movers are intensifying their collaborative endeavours and “coopetition” (cooperative competition) to broaden their footprint. The fast learners must synchronize their investments and involvements with the pace of industry developments, paying special attention to regulatory progressions and feasible benefits. For the decidedly slow, by the time they commence their explorations, develop proofs of concept, build their ecosystems, and cultivate the corresponding capabilities, seizing the upside of blockchain solutions may be too late. While some may consider it wise to adopt a “wait-and-see” approach, this strategy carries significant risk in today’s rapidly evolving landscape. Regulatory bodies and supervisors are increasingly pushing for a more streamlined and efficient Financial Services industry. Staying on the sidelines may result in being too late to enter the city gates, as blockchain solutions demand a proactive approach for experimentation and integration as well as a whole new series of capabilities.

AUTHORS

Ugur Koyluoglu
Partner, Oliver Wyman
ugur.koyluoglu@oliverwyman.com

Ben Jessel
Principal, Oliver Wyman
ben.jessel@oliverwyman.com

Priya Suhag
Engagement Manager, Oliver Wyman
priya.suhag@oliverwyman.com

Karanvir Singh
Senior Consultant, Oliver Wyman
karanvir.singh@oliverwyman.com

Omar Azhar
Head of Business Development, Matter Labs
oa@matterlabs.dev

Pearl Imbach
Business Development Lead for
Financial Services, Matter Labs
pi@matterlabs.dev

CONTRIBUTORS

Michael Wagner
Partner, Oliver Wyman

Eric Czervionke
Partner, Oliver Wyman

Douglas Elliott
Partner, Oliver Wyman

Larissa de Lima
Senior Fellow, Oliver Wyman Forum

Alex Gluchowski
Co-fouder and CEO, Matter Labs

Marco Cora
SVP Business and Operations, Matter Labs

About Oliver Wyman

Global leader in management consulting. With offices in more than 70 cities across 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 6,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities.

Oliver Wyman has a dedicated Digital Assets platform that supports industry powerhouses including i) regulators and public policy makers who are setting transformative requirements and norms, ii) traditional finance companies that are pioneering the digital asset landscape with blockchain-driven products and services, iii) trailblazing crypto natives that have established themselves as leaders in crypto and digital assets, and iv) investors. The team's unparalleled industry experiences have also positioned us as thought leaders, evidenced by a series of publications on digital assets including centerpieces in collaboration with leading institutions in the domain.

For more information, visit www.oliverwyman.com/our-expertise/hubs/digital-assets.html

About Matter Labs

Founded by seasoned software architects and backed by top-tier investors such as a16z, Blockchain Capital and Union Square Ventures, Matter Labs is an engineering team with a passion for blockchain and mathematics. They are the core contributors to zkSync, the first Layer 2 zkEVM, enhancing Ethereum's scalability using advanced zero-knowledge technology. It is designed to scale blockchains like the internet: processing an unlimited number of transactions without compromising on security or decentralization. Its open-source framework is free, and its modularity allows the adopters to build custom, zero-knowledge powered, interoperable Layer 2s and Layer 3s. For more details, visit https://matter-labs.io/

For more information, please contact the marketing department by phone at one of the following locations:

Americas	Europe	Asia Pacific	India, Middle East & Africa
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700	+971 (0) 4 425 7000

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.