FUTUREMATTERS™
CENTRE OF EXCELLENCE

PERMISSIONLESS BLOCKCHAIN IN FINANCIAL SERVICES

August 2024

CONTRIBUTORS

Stefan Grasmann
Chief of Blockchain
Zühlke

Ammar Ahmad
Senior Consulting Manager
Zühlke

POINT ZERO FORUM™
Policymakers | Leaders | Investors

Content

Executive Summary

Blockchain technology has the potential to democratise finance through increased liquidity, disintermediation and transparency. However, incumbents have primarily focussed on private ledgers, which lack public verification. Despite the challenges, there is growing interest in public blockchains. A roundtable discussion held at the Point Zero Forum in July 2024 addressed the topic of "Permissionless Blockchain in Financial Services". The discussion focussed on the reasons behind the limited adoption of these blockchains and the changes necessary to facilitate their wider adoption.

The State of Play

1. **Settlement finality:** Financial institutions require deterministic settlement finality, unlike the probabilistic nature of blockchain finality. Current blockchain research is exploring solutions to improve this.
2. **KYC/AML:** The implementation of KYC/AML regulations presents a challenge primarily due to the lack of a standard identity scheme. However, technological advancements and multi-layer frameworks are improving KYC processes and traceability on permissionless blockchains, implying that this is a temporary hurdle.
3. **Cost:** Moving to a public blockchain entails substantial costs, including exchange fees and compliance with regulatory frameworks. These costs are expected to decrease with wider adoption and emerging solutions for cost reduction.
4. **Risk management:** It is difficult to meet the high standards for risk management and operational resilience for public blockchains due to a lack of clear standards and requirements. Regulatory specificity is needed to support investment, adoption and scale.
5. **Confidentiality:** Public blockchains' transparency conflicts with privacy requirements. Research into Zero-Knowledge Proofs (ZKP) and Fully Homomorphic Encryption (FHE) aim to address these issues, but practical solutions have yet to be developed.
6. **Interoperability:** Technical complexity in interoperability have slowed down blockchain adoption as users determine which chains they wish to invest in. A standardised protocol for universal integration across different blockchains would derisk investment and focus competition on value creation rather than costs to change. This is a desired future state for the maturing of this technology.

Recommendations

1. **Collaborate internationally:** Greater international cooperation among regulators is needed. An international sandbox and shared identity scheme could provide the litmus tests to address regulatory concerns more quickly.
2. **Define requirements:** Regulators should clearly define public blockchain requirements, providing legally binding definitions and differentiating based on industry needs.
3. **Embrace innovation:** Stakeholders should be open to new technologies and business models that meet client and regulatory needs. For instance, innovative solutions which embed KYC.
4. **Seize the momentum:** The finance industry recognises blockchain's potential. Swift action and collaboration can accelerate adoption and deliver benefits such as financial inclusion, greater transparency and workflow efficiencies, similar to the evolution of cloud technology.

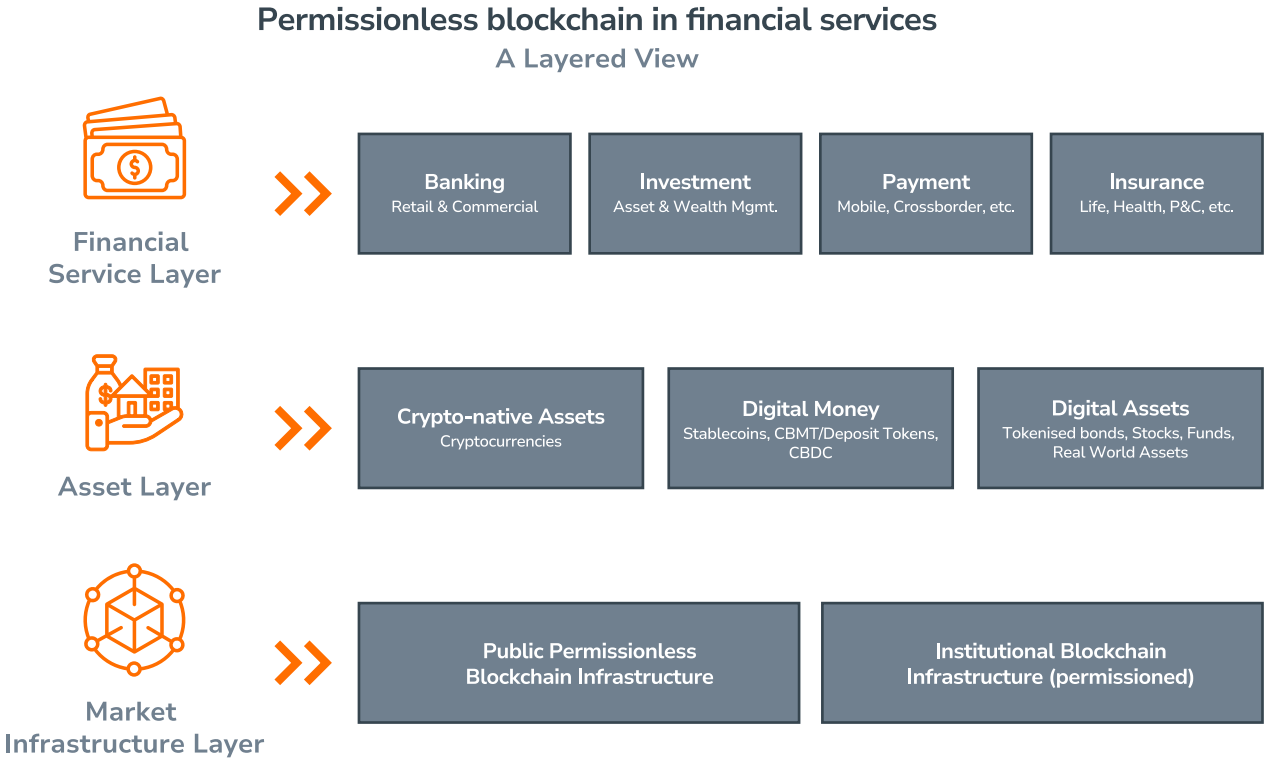
Introduction

Blockchain technology has long held the purported promise of democratising finance by providing increased liquidity, disintermediation and transparency. Early efforts at harnessing technology in Traditional Finance (TradFi), however, focussed more on private ledgers. Private blockchains are typically controlled by a single entity or a consortium of corporations without the element of public verification. Many of these so-called consortium blockchains have failed – such as B3i or ASX (R3, 2022; Melis, 2019), and it remains difficult for financial institutions to adopt public blockchains.

This was the context against which participants gathered at the Point Zero Forum in July 2024 to attend a roundtable, with distinguished guests representing policymakers, financial institutions and technology leaders.
The topic under discussion was "Permissionless Blockchain in Financial Services", with an in-depth debate about why permissionless blockchains have not made major inroads with industry incumbents so far, and what is needed for this to change.

To set the scene and help with structuring the discussion, a multi-layer framework on blockchains' use cases for financial assets was introduced by Zühlke. This framework differentiated three layers that require different levels of control, access and confidentiality.

Figure 1: A layered view on blockchain solutions in Financial Services



Source: Adapted from Zühlke, 2024

What are the main obstacles for the adoption of permissionless blockchains?

3.1 Settlement finality

The issue of settlement finality is crucial for regulated financial institutions. Regulatory requirements are such that the finality of settlements must be deterministic, not probabilistic.

WHAT IS SETTLEMENT FINALITY?

Settlement finality is the assurance that a settlement is executed, properly recorded in the accounting books, legally binding and final, i.e. immutable. Any modification requires a new transaction to reconcile the already finalised settlement. Times for reaching finality vary greatly and depend on the technology and jurisdiction. For interbank transfers within a currency zone, it is usually T+2, meaning that the transaction is finalised within two business days. For cross-border payments requiring several correspondent banks, this might take much longer. Currently, there is a movement in the industry towards T+1 or even T+0, but since traditional IT systems and processes have been built with T+2 in mind, this change is costly and complex.

Blockchains have a different notion of finality. Here, finality is a probabilistic statement: A transaction is considered final if the effort to change the outcome of that transaction is prohibitively expensive. How long this takes differs for each type of blockchain. For Bitcoin, it is usually after an hour (six generations of 10-minute blocks); for Public Ethereum, it is after 15 minutes. For layer-2 blockchains (i.e. asset layer), being an off-chain network, system, or technology built on top of a blockchain to extend the underlying blockchain's capabilities, this can be mere seconds.

Blockchains work in a probabilistic way: there might be validated transactions that get rolled back after a short period of time because a majority of validators decide to take another branch as "valid". How long it takes before a transaction can be deemed "final" – with a sufficiently low probability of being rolled back, is blockchain dependent. The uncertainty around when blockchain transactions may be deemed final are expected to be resolved with the conclusion of blockchain research into the topic of "single slot finality" (Ethereum Foundation, 2024a) and preconfirmations (Ethereum Research, 2023).

Financial institutions and their customers are typically willing to accept two business days in the traditional interbank settlement process for deterministic finality of settlements. At the roundtable, the discussants recognised that customer expectations were moving towards faster settlements (T+1 to T+0). Thus, finality is not a question of technological possibility, but rather a necessary outcome for financial institutions seeking to remain relevant as business models evolve.

For the benefits of the technology to be maximised, interoperability and fungibility for multi-asset transactions across instruments, organisations and IT systems offering atomic settlement remains the aspirational state. Achieving this will not only speed up transactions, but also dramatically reduce the effort involved in handling failed transactions.

Figure 2: Settlement finality times for selected layer-1 blockchains and traditional payment systems (as of July 2024)

System	Block generation time	Average finality time	Description
		Layer-1 Blockchains	
Bitcoin (BTC)	Approx. 10 minutes per block	1 hour	Uses a Proof-of-Work (PoW) consensus mechanism, which can lead to a longer average settlement time during high network congestion
Ethereum (ETH)	Approx. 13–15 seconds per block	15 minutes	Uses a Proof-of-Stake (PoS) mechanism; the settlement time also depends on network congestion
Solana (SOL)	Approx. 400 milliseconds per block	Less 1 second	Uses a Proof-of-History (PoH) consensus mechanism combined with PoS, allowing for faster settlement times
		Traditional Payment Systems	
SWIFT		1–4 days	Message network used by banks and financial institutions to transmit information and instructions via a standardised system of codes
Fedwire		Real-time (within seconds to minutes)	Real-time gross settlement (RTGS) system, operated by Federal Reserve Bank, that allows immediate settlement of transactions
CHIPS		Same day – usually within hours	A large-value payment system in the USA that settles domestic and international payments

Note. Block generation times are taken from Statista (2024). Descriptions come from Antonovici (2024). Details about Fedwire are based on Ahmed (2024), whilst information on CHIPS is from The Clearing House (n.d.). Data on Ethereum's average finality time and block generation are provided by the Ethereum Foundation (2024a).

3.2 Compliance with KYC/AML regulations

Purpose of KYC

"Know-Your-Customer" (KYC) is a regulation that requires financial institutions to verify:

1. the identity and/or beneficial owner of the counterparty, be it individual or entity ("Who is it?"),
2. the value of the exchange ("How much is it?") and
3. the purpose of the transaction ("What is it for?").

The primary purpose of KYC is to prevent illegal activities such as money laundering, fraud and terrorism financing. Typically, KYC checks involve collecting and verifying documents such as a government-issued ID, proof of address and sometimes additional information. Compliance with KYC regulations helps to ensure that financial institutions understand who their customers are and that they are operating within the law, maintain the integrity of the financial system and support the sanctions framework.

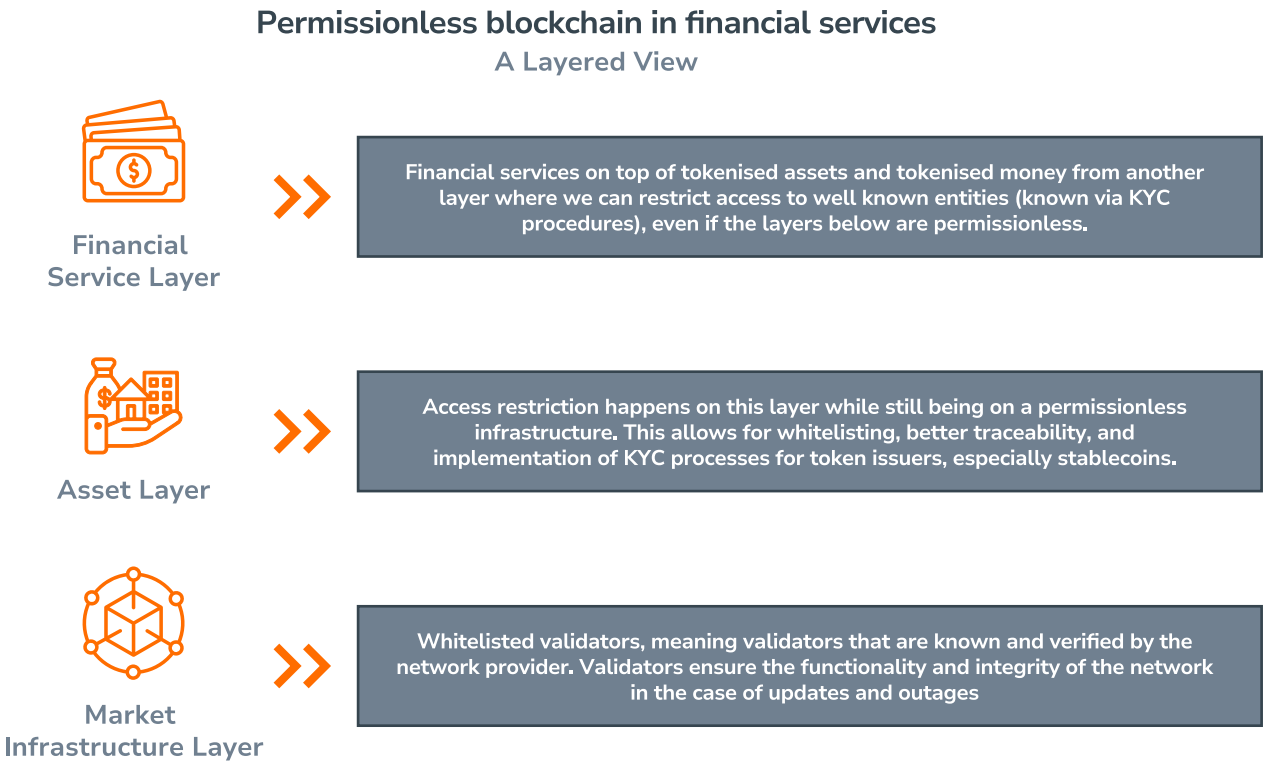
Regulated financial institutions face the reality that dealing with a non-KYC counterparty on a public blockchain is not possible. Therefore, any transactions on a public blockchain must be traceable, identifiable and verifiable.

Technological challenge

From a technological perspective, permissionless public chains provide better traceability. Technological solutions for permissionless blockchains that have solved some of the key issues regarding KYC are already available. One can build better, more resilient KYC processes with decentralised chains.

A multi-layer approach, for instance, can be applied – as shown in Figure 3.

Figure 3: Overview of multi-layer approach for KYC-compliant permissionless blockchain use cases.



Source: Zühlke

This approach does not necessarily mean that all transactions are transparent to all actors on the chain. Advancements in cryptography enable "veiled transactions", where only the participants who need to see the parties to the transaction can see them, ensuring privacy whilst maintaining traceability and compliance.

An example for whitelisting—the process of pre-approving specific wallet addresses or accounts to engage in activities on a public blockchain—is the "EUR CoinVertible" (EURCV) stablecoin that was successfully launched on Ethereum by SG-FORGE in April 2023. Initially only permissioned for their institutional clients, the whitelisting restrictions were lifted when the Markets in Crypto-Assets Regulation (MiCA) entered into force (Société Générale Forge, 2024), to ensure that the capabilities of an open stablecoin, including free transferability, were met in compliance with the MiCA regulation.

Identity challenge

The lack of a shared, standard identity scheme leads to both technical and practical problems. Without a commonly accepted, standardised identity framework, each new blockchain pilot project must create its own identity scheme, fragmenting the approach and leading to inconsistent quality of assurance.

A common identity standard is most likely to be accepted when coming from an established institution like SWIFT, due to its cumulative value, distribution network and the trust it garners. Attempts to establish standards, like GLEIF (Global Legal Entity Identifier Foundation, 2024), are already underway.

Whilst Tier 1 financial institutions might form a consortium and agree on a shared identity scheme, achieving this on a global level is challenging, especially for small- and medium-sized digital banks or fintech companies. Therefore, the need for a global identity standard is paramount to solving the practical KYC problems.

3.3 Cost

As with any new technology, costs are the main hurdle for market participants to become early adopters. This is no different for blockchain and is arguably one of the main reasons for large financial institutions to first experiment with private chains.

Transition cost

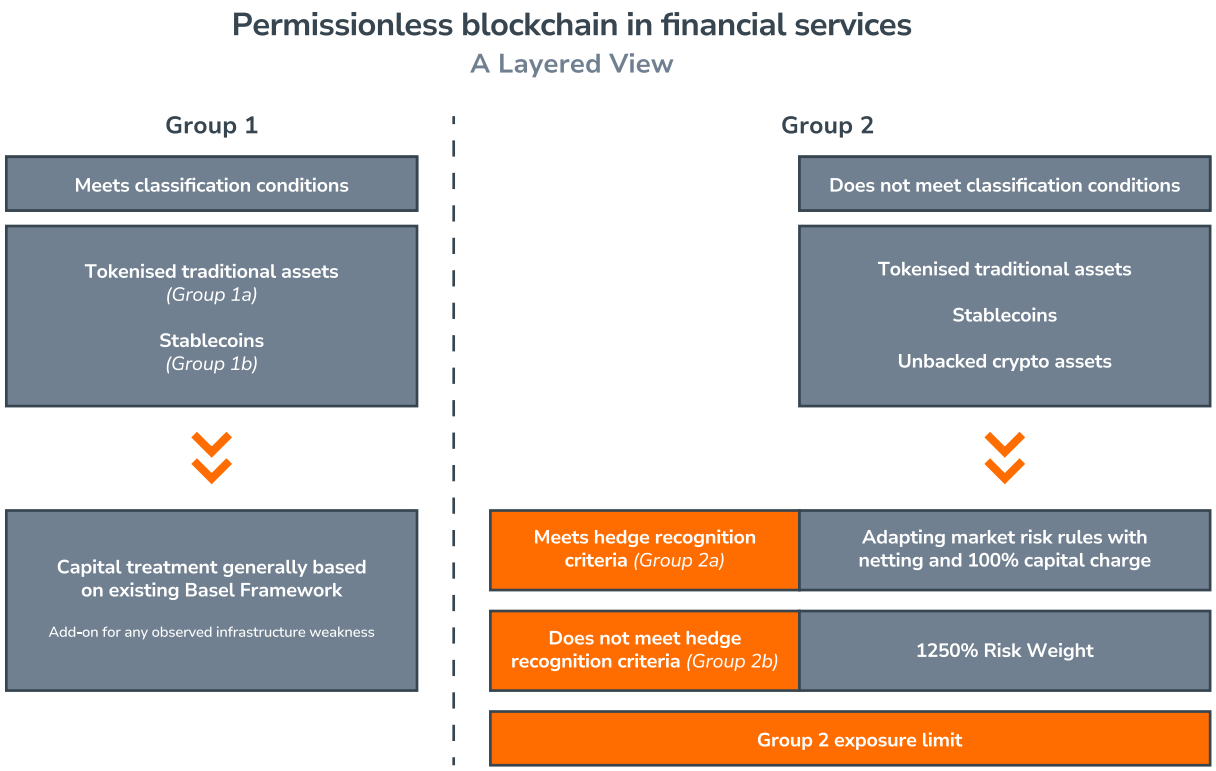
Under transition cost, we summarise the overall costs a financial institution faces when moving towards a public blockchain. This includes both operational and economic costs.

For a financial service provider, moving towards a permissionless blockchain requires significant on- and off-ramping efforts to exchange fiat currency with cryptocurrency, even if it is a stablecoin. Typically, this involves an exchange fee to the crypto exchange and a transaction fee to the network. These costs can be significant.

Furthermore, holding cryptocurrency on their balance sheet is costly due to the capital costs and tax expenses imposed. Most countries impose taxes on the appreciation of cryptocurrency assets over specified periods.

The Basel Committee on Banking Supervision (BCBS) Crypto Asset Framework proposes conservative capital requirements for cryptoassets that do not meet their low-risk classification conditions, to be adopted into national legislation by 1 January 2025. This includes tokenised assets and stablecoins with ineffective stabilisation mechanisms and unbacked cryptoassets (e.g. Bitcoin). Consequently, most cryptoassets fall under this group (Group 2 in Figure 4).

Figure 4: Classification of cryptoassets according to BCBS' "Prudential treatment of cryptoasset exposures."



Other applicable elements: operational risk, adapted liquidity requirements, leverage ratio, large exposures

Source: Zühlke, data adapted from the Bank of International Settlements, 2022

Thus, large-scale financial use of permissionless blockchains comes with practical economic challenges.

Cost per transaction

In this paper, the total economic cost per transaction for Proof of Work (PoW) blockchains refers to the fee plus the block reward divided by the number of transactions in the block. For Proof of Stake (PoS) blockchains, it refers to the transaction fee, which in the case of Ethereum consists of a base fee and an optional priority fee, plus the net of newly minted tokens (i.e., the yield on staked tokens). The ratio between these two components can fluctuate and is highly dependent on the maturity level of a given PoS chain.

Transaction costs on public blockchains are variable and more difficult to predict compared to traditional payment systems. High network congestion can drive the costs to unsustainable levels. This phenomenon can be observed on both layer-1 and layer-2 chains.

At the time of writing, the average cost per transaction on Ethereum is around $0.95, and $0.03 on Solana. As one participant pointed out, this compares to "$0.01 for the US Automated Clearing House and less than $0.01 for the Mexican Interbanking Electronic Payment System (SPEI) according to internal analyses". Due to its PoW mechanism, the average cost per transaction for Bitcoin is much higher, making an apt comparison difficult. It is worth noting that while there were differing opinions on costs at the roundtable, it was also recognised that there are many different ways to measure costs for different chains.

Figure 5: Total economic cost per transaction for selected blockchains and traditional payment systems (as of July 2024)

System	Transaction fee	Additional costs	Total economic cost per transaction
		Layer-1 Blockchains	
Ethereum (ETH)	$0.952 (5-year-avg.)	Voluntary priority fees	$0.952 + priority fees
Solana (SOL)	$0.003–$0.030		$0.003–$0.030
Bitcoin (BTC)	$1.504 (5-year-avg.)	$54.38 (5-year-avg.)	$55.75
		Layer-2 Blockchains	
Base	$0.0012		$0.06
		Traditional Payment Systems	
US ACH	$0.20–$1.50	Negotiated rates and discounts for high-volume transactions	
Fedwire	Per transfer, volume-based price: $0.190–$0.940 Pre-incentive and incentive transfer fees: $0.038–$0.940	Extra fees (e.g. access fees, surcharges and additional fees) might be charged	

Note. The sources for data on transaction fees and additional costs are as follows: Ethereum's (ETH) transaction fee is based on data from YCharts (2024c). Solana's (SOL) transaction fees are detailed in CoinCodex (2024). Bitcoin's (BTC) transaction fees are sourced from YCharts (2024a), the block reward is provided by Coindesk (2024) and information on the average number of Bitcoin transactions per block is from YCharts (2024b). The base layer-2 transaction fee is reported by The Block (2024). US ACH transaction fees are discussed in Tipalti (2024), and Fedwire transaction fees are outlined by the Federal Reserve Bank Services (2024).

It is important to note that blockchain is early in its cost evolution cycle. Significant cost reductions have already occurred, and this trend is likely to continue with wider adoption. A new development is the concept of subsidising gas fees via paymaster services to lower or eliminate transaction costs for end users completely. In principle, networks would pay the gas fees in their own token for users during times of high gas fees (e.g. gas-free stablecoin transfers on TRON [Richardson, 2024] or gas token on Celo [Celo Foundation, 2022]).

In addition, comparing the total economic cost per transaction on blockchains to the transaction cost in traditional payment systems is flawed. It was pointed out that the relevant factor from a transaction perspective is the direct cost of that transaction.

One must take into consideration the distribution effect of public blockchains.

One aspect of the distribution effect is cost amortisation. A comparison to cloud providers was made arguing that a new provider might offer the same service at a lower cost than AWS, but the challenger is spreading costs across fewer users. AWS benefits from cost amortisation due to its larger scale.

Another aspect is access to liquidity, which correlates to the number of active participants on a chain. It was argued that historically, the trade-off for higher complexity and cost is broader distribution. Ethereum is chosen not for its low cost or efficiency, but because launching a DeFi protocol on Ethereum provides access to the largest number of private keys. The decision often comes down to whether to launch on a platform with significant purchasing power or a more efficient technology with lower fees but fewer users and resources.

The importance of the distribution advantage is evident in recent examples of the world's largest asset managers launching tokenised funds on public blockchains, such as BlackRock's USD Institutional Digital Liquidity Fund (BUIDL) (Securitize, 2024). Asset managers have realised that public blockchains currently provide access to the largest markets. We posit that if financial institutions launch private blockchains and move client accounts onto those networks, the distribution advantage will shift from public to private blockchains.

Therefore, the question of what level of transaction cost is acceptable should be preceded by the question of which blockchain offers the best trade-off between market access and technological fit.

3.4 Risk management

Standards and expectations for risk management and operational resilience in public blockchains are exceptionally high. Financial institutions have made it clear that they place significant trust in blockchain, viewing public chains as more resilient than many other systems. For instance, Ethereum runs on client software that adheres to a common standard whilst being implemented by different development teams in different programming languages, thus avoiding a super majority (Ethereum Foundation, 2024b). This level of resilience and diversification is hardly ever seen in other commercial software products. However, to achieve the required quality of resilience, clear standards and policies must be established and enforced.

The discussants recognise that regulators are improving their understanding of the technology. This progress is partly due to banks explaining in detail their expectation for control and clarifying that the primary risk involved is operational, rather than a liquidity or credit risk. Nonetheless, the dialogue between regulators and industry players needs to become more concrete. It is essential to identify specific risks and to explore potential mitigation strategies. The central question in this area is that of accountability. In the end, who is accountable for the functionality of decentralised chains? Who is liable in the case of financial loss due to bugs or deceit?

This point of uncertainty is exemplified with Service Level Agreements (SLAs). Banks are facing the challenge of a perceived lack of enforceability of the SLAs in place. However, it was pointed out by the technology side that they are operating with SLAs similar to those that cloud providers typically use. This issue is repeatedly raised by compliance departments: “No bank’s TRM (Technology Risk Management) and outsourcing guidelines is going to pass a platform with anonymous service providers.”

The path forward involves not only clearer and more specific discussions between regulators, financial institutions and technology providers, but also enforceable standards and accountability measures.

3.5 Confidentiality

How much confidentiality and privacy is needed? How can the right level of confidentiality be ensured at each layer? These are key questions around the topic of confidentiality.

Public blockchains, by their very nature, are transparent. This transparency is both their greatest strength and their most significant weakness. The General Data Protection Regulation (GDPR), which enshrines the right to be forgotten (GDPR-info.eu, n.d.), fundamentally clashes with the core principles of blockchains, which are designed to be immutable and transparent.

One of the most critical roadblocks for B2B use cases on public blockchains is the lack of confidentiality. As long as the users’ balance sheets and the payload of all transactions can be viewed and tracked by everyone, including third parties not involved in the transactions, businesses will remain wary. This issue is a major field of research and continues to hinder broader adoption.

Most private blockchains utilise the same technology as public chains, such as Ethereum, which is used in platforms like Hyperledger Besu and Quorum. The confidentiality problems inherent in Ethereum extend to these private and consortium chains. Without specific countermeasures, all participants in these networks can see all transactions. Consequently, many solutions incorporate off-chain features to address typical privacy issues, albeit with certain downsides.

There is ongoing research aimed at enhancing confidentiality in public blockchains through technologies such as Zero-Knowledge Proofs (ZKP) and Fully Homomorphic Encryption (FHE), exemplified by innovations like Zama fhEVM (Zama, n.d.). FHE enables smart contracts on public blockchains to include confidentiality about token balances or transaction payloads.

To mitigate these issues, improvements must occur incrementally. For instance, token balances could be stored in additional encrypted fields, allowing smart contract logic to use FHE to work with encrypted data. ZKP could also be employed to verify that a counterparty has sufficient liquidity for a trade without disclosing the exact amount. Since most of these components are still in development, they are not yet readily available in common public or private blockchains.

3.6 Interoperability

Interoperability remains a consistent technical challenge that encompasses all previous obstacles. It not only refers to bridging tokens between blockchains, but also interactions among public or private chains and between the fiat and blockchain world. This pervasive issue slows down the broader adoption of blockchain technology, as it introduces major attack vectors for hackers.

Solving the problem of interoperability would make the distinction between public and private chains less important. Once interoperability is achieved, the debate about chain types shifts to finding the most seamless integration across diverse ecosystems. Initiatives like the Global Layer One project are steps in the right direction.

An analogy was drawn to the evolution of the internet, comparing blockchain's potential to a scenario where, today, no one asks about the database being used; instead, everyone transacts over TCP/IP as the standard protocol.

It remains to be seen when a standard protocol for blockchain will emerge, offering complete technical abstraction by simplifying interactions and transactions across disparate blockchain systems.

What needs to change? Four action points.

4.1 Collaborate internationally

We recognise that regulators are being practical in their actions towards permissionless blockchain by creating various Proofs-of-Concept and sandboxes for the industry. However, this effort very rarely spans across regulatory ecosystems.

We see the need for a better joint international debate among regulators. This discussion should not be the sole responsibility of regulators; there must also be clear recognition of regulatory concerns and risks by both new and incumbent industry players.

A practical step forward would be the creation of an international sandbox, endorsed by a consortium of respected regulators. Such a sandbox would enable rapid, safe experimentation with permissionless blockchains. By fostering an environment of controlled innovation, stakeholders can address regulatory concerns whilst accelerating the adoption and integration of blockchain technology.

Furthermore, as described in section 3.2, a shared identity standard on a global level agreed upon by a group of regulators or an established institution would be a tremendous step towards solving the practical challenge of KYC.

4.2 Specify requirements

We urge regulators to clearly define their requirements for public blockchains Uncertainty was expressed about knowing what actually needs to happen for acceptance, and it was noted that this remains unknown today. These requirements must be nuanced and specific to effectively guide the industry.

Specific here means that there must be legally binding definitions serving as clear signposts. For instance, the legal definition of finality, the standards for proper risk mitigation and what constitutes a legally binding transaction should all be explicitly outlined. MiCA defines decentralisation but lacks guidance on the precise scope, which creates regulatory ambiguity.

By nuanced, we mean that it is essential to differentiate requirements based on the varying needs within the industry. Large financial institutions face entirely different challenges compared to small or medium-sized banks or fintechs. For example, SMEs are primarily interested in the network effects of public chains. They do not want fragmented liquidity and are less concerned about interoperability. As they put it, “we want to invest on a chain, not into a chain.”

To effectively move forward, we need a regulatory framework that is both detailed and adaptable to the diverse needs of various financial entities. This will enable a more cohesive and functional integration of public blockchains

4.3 Embrace innovation

All stakeholders in the industry should adopt a forward-thinking, open-minded approach to technology and business models. Whilst legacy business models are bound to change, only a few novel business models will emerge as successful and durable. Openness to new solutions for the main issues discussed above is crucial.

For example, technological solutions exist that can make KYC a more implicit rather than explicit element of the transaction process. AI-based financial surveillance systems can enhance KYC by monitoring transactions and identifying risks in real time.

This open-mindedness can create space for more regulatory-compliant innovation. By embracing new technologies and rethinking traditional models, the industry can better align with evolving regulatory requirements.

4.4 Seize the momentum

We are at a pivotal moment, when the financial services industry widely recognises blockchain as a technology poised to democratise assets. The conversation has shifted from general discussions about the technology to tackling specific issues.

Regulators and industry players must act swiftly to capitalise on this momentum. An apt analogy is the evolution of cloud technology: in its early days, on-premises management was the norm. Over three decades, cloud infrastructure has become standard in financial institutions. It will take time, but the time to act is now.

To accelerate progress, rather than merely lobbying for the adoption of crypto and blockchain, we need a clear articulation and recognition of the issues that regulators face. By identifying these challenges, we can focus on collaborative solutions that bring regulators and industry players together.

Ideally, in the not-too-distant future, we envision a SWIFT-like infrastructure for a global layer-1 blockchain. Such a development would provide a robust, standardised foundation for secure, efficient transactions.

Conclusion

Industry representatives have made it clear that they intend to transition to public blockchains. They have reaffirmed their belief that technological developments and the capabilities of technology providers can facilitate the achievement of this ambition.

We are currently in a crucial phase of transition. This requires the establishment of robust connections across a range of domains, including between fiat and crypto, and between private and public blockchains. There is a general sense of optimism among financial institutions, technology providers and regulators about the future.

It was succinctly noted that things are moving in the right direction, and while there is a desire for them to move faster, the progress is acknowledged and appreciated.

This sentiment captures the collective readiness to embrace and integrate blockchain technology more comprehensively, whilst expressing the desire for an accelerated pace of progress. This optimism underscores the promising trajectory of blockchain in the financial services industry and the need for continued collaboration and swift action from all stakeholders involved.

References

- Ahmed, K. (2024, June 16). Fedwire. WallStreetMojo. https://www.wallstreetmojo.com/fedwire/
- Antonovici, A. (2024, March 11). Bitcoin (BTC) vs Ethereum (ETH) vs Solana (SOL): Which is best? TastyCrypto. https://www.tastycrypto.com/blog/bitcoin-vs-ethereum-vs-solana/
- Bank for International Settlements. (2022, December 16). Prudential treatment of cryptoasset exposures. https://www.bis.org/bcbs/publ/d545.htm
- Celo Foundation. (2022). Add gas currency. https://docs.celo.org/learn/add-gas-currency
- CoinCodex. (2024, May 15). Solana gas fees. CoinCodex. https://coincodex.com/article/24933/solana-gas-fees/
- CoinDesk. (2024, April 20). Bitcoin blockchain has fourth halving in 15-year history in show of monetary policy set by code. CoinDesk. https://www.coindesk.com/tech/2024/04/20/bitcoin-blockchain-has-fourth-halving-in-15-year-history-in-show-of-monetary-policy-set-by-code/
- Ethereum Foundation. (2024a, May 3). Single-slot finality. Ethereum.org. https://ethereum.org/en/roadmap/single-slot-finality/
- Ethereum Foundation. (2024b, May 23). Client diversity. Ethereum.org. https://ethereum.org/en/developers/docs/nodes-and-clients/client-diversity/
- Ethereum Research. (2023, November). Based preconfirmations. Ethereum Research. https://ethresear.ch/t/based-preconfirmations/17353
- Federal Reserve Bank Services. (2024). Fedwire. Retrieved July 17, 2024 from https://www.frbservices.org/resources/fees/wires-2024
- GDPR-info.eu. (n.d.). Article 17 GDPR - Right to erasure ('right to be forgotten'). https://gdpr-info.eu/art-17-gdpr/
- Global Legal Entity Identifier Foundation. (2024). GLEIF. Global Legal Entity Identifier Foundation. https://www.gleif.org/en
- Melis. (2019, July 19). Why consortium blockchains are failing. The Dark Side. https://medium.com/thedarkside/why-consortium-blockchains-are-failing-803e2a8d75ac
- R3. (2022, December 15). Unpacking upheaval: Interpreting 2022's blockchain failures. R3 Blog. https://r3.com/blog/unpacking-upheaval-interpreting-2022s-blockchain-failures/
- Richardson, A. (2024, July 8). Justin Sun says TRON team designing new gas-free stablecoin transfer solution. Daily Hodl. https://dailyhodl.com/2024/07/08/justin-sun-says- tron-team-designing-new-gas-free-stablecoin-transfer-solution/
- Securitize. (2024, March 21). BlackRock launches first tokenized fund BUIDL on the Ethereum network. https://securitize.io/learn/press/blackrock-launches-first-tokenized-fund-buidl-on-the-ethereum-network

- Société Générale Forge. (2024, August 7). Société Générale-Forge elevates its stablecoin to accelerate its distribution and free use. Société Générale. https://wholesale.banking.societegenerale.com/en/news-insights/all-news-insights/news-details/news/societe-generale-forge-elevates-its-stablecoin-to-accelerate-its-distribution-and-free-use/

- Statista. (2024). Cryptocurrency transaction speed. Statista. https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/

- The Block. (2024, March). Ethereum layer 2s show a dramatic drop in transaction fees after Dencun.

- The Clearing House. (n.d.). CHIPS. The Clearing House. https://www.theclearinghouse.org/payment-systems/chips

- Tipalti. (2024). ACH fees: How much does ACH payment processing cost? Retrieved July 17 2024, from https://www.tipalti.com/ach-fees/

- YCharts. (2024a). Bitcoin average transaction fee. Retrieved July 17, 2024 from https://ycharts.com/indicators/bitcoin_average_transaction_fee

- YCharts. (2024b). Bitcoin average transactions per block. Retrieved July 17, 2024 from https://ycharts.com/indicators/bitcoin_average_transactions_per_block

- YCharts. (2024c). Ethereum average transaction fee. Retrieved July 17, 2024 from https://ycharts.com/indicators/ethereum_average_transaction_fee

- Zama. (n.d.). FHEVM. https://www.zama.ai/fhevm

- Zühlke. (2024). Zühlke: Technology and business consulting. https://www.zuehlke.com/en

About The Authors

Stefan Grasmann

Chief of Blockchain,
Zühlke

Stefan Grasmann is Partner and Group Head of Thought Leadership & Chief of Blockchain at Zühlke. He is responsible for the thought leadership program of Zühlke and is passionate about Blockchain technology and Decentralised Finance (DeFi). He is a blockchain and technology visionary with more than 30 years of experience in the tech sector. Stefan boasts years of experience in fostering tech innovation, developing businesses in challenging new markets and leading intercultural teams. He has co-founded the cross-industry Blockchain:Circle, a sector-independent discussion circle for Web3 use cases.

Ammar Ahmad

Senior Consulting Manager,
Zühlke

Ammar is a management consultant and writes about innovative solutions to his clients' long-term challenges. This includes innovative business models in the financial services industry, with a focus on topics such as blockchain, generative AI and process optimisation.