Stellar Development Foundation

475 Brannan St, Suite 400
San Francisco, CA 94107

November 1st, 2024

European Commission
Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA)
Director Horizontal policies
1049 Bruxelles/Brussel
Belgium

Submitted via: Fisma-B4@ec.europa.eu

> Subject: Response to call for contributions on the use of distributed ledger technology as infrastructure for financial services.
> FISMA.B/MH/es/fisma.b.4(2024)6244475

Dear Mr. Haag,

The Stellar Development Foundation (SDF) is pleased to submit a response to your call for contributions on the use of distributed ledger technology as infrastructure for financial services. In this response, we demonstrate how public blockchains can offer the digital economy as much–if not more–stability, security, and resilience as any infrastructure used today for settling payments and financial transactions.

SDF and the Stellar network

SDF is a US-based nonstock, nonprofit organization that contributes to the development and growth of the Stellar network and the "Stellar ecosystem"–the individuals, developers, and businesses who build on or interact with Stellar. Stellar is a public blockchain network that connects the world's financial infrastructure. Founded in 2014, SDF helps maintain Stellar's codebase, supports the technical and business communities building on the network, and serves as a speaking partner with policymakers, regulators, and institutions. Our mission is to create equitable access to the global financial system, using the Stellar network to unlock the world's economic potential through blockchain technology.

Public blockchain as financial infrastructure

If digital payments and financial transactions are the vehicles that help move the modern economy forward, the roads they run on are as important as the vehicles themselves.

These roads must offer the stability, security and resilience required for all vehicles to reach their destination smoothly and on time.

National payments systems controlled by public or private actors like T2 in Europe and CHAPS in the UK are traditional examples of such roads. More recently, public blockchains have appeared as a robust alternative for the financial transit of the digital world. And they do so in a decentralized manner, which should be seen not as a drawback but as a desired feature.

The benefits of decentralization

Decentralization, rather than denoting a total absence of control, really means that no single party has control over the network. Public blockchains don't have an identifiable legal entity behind them. But they're supported by communities of developers working collaboratively to identify and solve problems and contribute to code changes and updates, ensuring timely improvements to the blockchain's protocol. Many decisions about changes and updates are made through discussions among these community members rather than simply relying on the routine execution of automated code.

While these arrangements may not follow traditional accountability structures, public blockchains introduce new ways to achieve the safety and vitality that are expected from any financial infrastructure. And public blockchains have built an impressive track record to support that claim.

For example, the Stellar blockchain, designed with payments and everyday financial services in mind, has faced 67 minutes of total downtime in its 10 years of 24/7 operations. In 2021, Stellar continued to operate as designed even when many of its validator nodes went offline.

Ensuring that market infrastructures operate smoothly can be challenging. The European payments system T2 (then TARGET2) suffered a 10-hour outage on 23 October 2020. A 6-hour failure also hit the UK's CHAPS payments system on 14 August 2023. The downtime of payment systems operated by centralized organizations demonstrates that centralization and traditional legal entities don't guarantee a flawless performance.

There's, moreover, a false equivalence that private, permissioned networks are safer and more efficient than public, decentralized ones. While private networks may offer competitive bandwidth and throughput, they don't come with the safety of their public

counterparts. Private blockchains are likely to have fewer developers, nodes and data storage facilities supporting their operations. Private networks therefore have fewer sets of eyes ensuring their safety and resiliency.

Strong operational resiliency

Public blockchains, on the other hand, have hundreds if not thousands of parties running full nodes that maintain these networks. Some of them validate and confirm transactions according to the related consensus mechanism, from bitcoin's proof of work, based on the nodes' investment of computational power and energy, to Stellar's proof of agreement, based on the reputation of the entities running validator nodes, as discussed in more detail below.

Public blockchains also host a wide array of developers and users who benefit from network improvements. Unlike traditional financial infrastructures or private blockchains, network updates aren't decided unilaterally. Developers and users alike can propose software changes that must be approved by a majority of nodes–only then can a change be implemented and executed.

This governance arrangement allows for a comprehensive risk management of public blockchains, with developers, nodes and validators depending on each other. All the parties benefit from knowing that the network will work according to its programmatic protocol rules and that changes will be implemented only after proper vetting and if incentives are aligned.

This process gives public blockchains strong operational resiliency as it eliminates single points of failure or attack. As no single party controls the network, no one can disrupt its functioning or shut down operations, either willingly or accidentally. No individual breakdown or outage at the developer, node or validator levels is enough to affect the operation of a public blockchain.

Finally, as no stakeholder can unilaterally change the rules or arbitrarily decide who can build upon or use public blockchains, they guard against entrenched forces driving out competition and favor interoperability. Much like the Internet, and in contrast to private networks, public blockchains are based on standardized protocols that facilitate the interaction between different systems through the open development of cross-chain communication solutions.

475 Brannan St, Suite 400
San Francisco, CA 94107

Ensuring control over assets

It's also important to distinguish between the decentralized nature of public blockchains, the roads upon which digital assets run, and the assets themselves. The assets are generally issued by a centralized entity and can be configured to comply with applicable regulatory requirements. While blockchains may be open and public, the issuers of assets deployed on many of those blockchains can choose the degree of control they want to have over their assets, especially when they need to comply with existing regulations.

For example, many public blockchains offer optional features that issuers can easily add to new assets, like the possibility of clawing back or freezing tokens. Issuers can choose the degree of control they want or need over each issued asset, from no control at all (for unregulated assets like non-fungible tokens) to more stringent controls (for regulated assets like tokenized securities).

On Stellar, these control features are native to the platform and can be implemented directly without additional programming or smart contracts. In fact, the Stellar network has intuitive 'asset flags' that can be used to turn on control features at the time of asset issuance.

Issuers can fully customize and control their assets according to compliance needs and regulatory requirements. And this is all transparent to users, who can view the profile of each asset and decide which ones they are willing to hold or use.

Superior settlement finality

When it comes to settlement finality, public blockchains are also ready to provide a robust infrastructure for the financial needs of the digital world.

Public blockchains are similar to the real-time gross settlement (RTGS) systems many jurisdictions currently use. RTGS systems process transactions in real-time, with each transaction settling individually and not netted against other transactions, to avoid settlement risk. Transactions completed on a public blockchain can yield similar results with the added benefits of transparency, increased availability, and faster settlement time.

As an initial matter, it is important to distinguish settlement finality from instant processing and protection in bankruptcy. First, settlement finality does not require instant settlement

but irreversibility, in the sense that after a transaction is finalized or settled, from a technical and legal perspective, no one can reverse, delete, or otherwise change it.

Irreversibility is only achieved when funds or assets flow from one account to the other, regardless of when the transaction was initiated by being broadcasted to the network. In terms of settlement finality, whether these two moments happen in instant succession or after some time is all but irrelevant.

The second clarification regarding settlement finality is that this status does not prevent a bankruptcy court–or any court for that matter–from deciding that a settled transaction is void and must be reversed because of creditor preference, error, or fraud. Technically, though, the court's directive is not to "undo" the original transaction but to initiate a new transaction that reverses the effects of the original one, resulting in two separate and final transactions.

The effects of settlement finality are never absolute, not even in traditional financial infrastructures. Courts always have the power to correct transactions made in error, with fraud, or against applicable rules.

With these two points made clear, we can get back to blockchain finality. The fundamental point is that settlement finality is an essential part of public blockchains. At their core is the process of validating transactions and putting them in a new block that is then added to the chain so that the transactions it carries become immutable, gaining irreversibility.

The different types of blockchain governance

But this process isn't the same for all public blockchains. The way each blockchain works affects how and when the finality of transactions is achieved. So, to discuss blockchain finality, we need to look at different types of blockchain governance, especially at how transactions are validated and how frequently each block of validated transactions is added to the chain.

For blockchains that rely on proof of work to validate transactions and create new blocks, like Bitcoin, finality is achieved in stages. As many miners compete to group transactions into a block, add the block to the chain, and receive the reward, some blocks might be added to the chain at the same time, creating a type of fork. But as only one block can be

added to the chain every 10 minutes, only one of the simultaneous blocks will survive and remain connected.

Later on, as the next new block must be attached to the previous one, one block will receive the connection from the new one and stay on the main chain, and the other simultaneous blocks will be discarded. With that, the temporary fork will be solved, but all the transactions inside the discarded blocks will have to be resubmitted for a new validation and confirmation process.

So, the probability that a block is discarded and transactions inside them are reversed decreases as new blocks are linked on top of any block that remains on the main chain. The more blocks are added to the blockchain, and the more time passes, the less likely it is that previous transactions will change and the more “final” they become. That’s called probabilistic finality.

Standard-setting organizations like the Bank for International Settlements often question the instability of probabilistic settlement. However, no major fiat-backed stablecoin or tokenized real-world asset runs on proof-of-work blockchains. They run either on blockchains that operate with a combination of probabilistic settlement with deterministic finality, like proof-of-stake Ethereum, or on public blockchains running solely on deterministic voting-based finality, like the Stellar network.

As Stellar relies on proof of agreement to validate transactions and create blocks, finality is achieved in a single step, when each new block is added to the chain. Validator nodes on Stellar don’t compete for a reward. They instead collaborate to create a widespread agreement about the validity of transactions and their addition to the chain through a new block. And all that is based not on the use of computational power and energy but on the reputation of the entities running validator nodes. Once agreement is reached among validator nodes, it’s final and cannot be reversed.

On Stellar, moreover, a block is added to the chain every five seconds, and it carries up to 1,000 transactions–a limit that can be adjusted. This means that the queue of pending and unconfirmed transactions on Stellar, known as "transaction queue” or “mempool,” lasts on average only five seconds. As a result, transactions on Stellar typically reach settlement finality every five seconds, creating little to no exposure to credit or liquidity risks for the transacting parties.

475 Brannan St, Suite 400
San Francisco, CA 94107

Note that even traditional instant payments systems involve some time between sending the transaction to the network and finally settling it. Pix, the Brazilian retail instant payments system launched in 2020, has rules requiring participants to settle instant transactions in under 40 seconds. This time can be extended to 30 minutes or even 60 minutes (for night transactions) if the Pix participant, a financial institution or fintech, suspects the submitted transaction might be fraudulent.

Dispelling flawed comparisons

Note also that the widespread comparison between the number of transactions processed per second (TPS) on public blockchains and that on traditional financial infrastructures, like card networks, can be misleading. The usual argument is that while Visa can execute tens of thousands of TPS, Bitcoin can only handle 7 TPS and Stellar 200 TPS on average. This is not a fair comparison.

TPS for card networks refers to the number of screened and authorized messages requesting funds or assets to flow from account A to account B. The actual flow of funds and, in turn, settlement finality will only happen days later when the cardholder's bank transfers the money that will end up in the merchant's bank account–if a counterorder, like a chargeback, doesn't happen along the way.

TPS for public blockchains, on the other hand, refers to the number of transactions that complete the full cycle of being broadcasted, validated, and finalized, with funds or assets effectively changing from account/address A to account/address B–no matter where in the world these accounts/addresses are. TPS here actually implies settlement finality, as discussed.

No traditional financial infrastructure provides this kind of nonstop finality volume at a global level. And Stellar provides that for a fraction of a penny per transaction and in a sustainable way, as the network's carbon footprint is equivalent to that created by the electricity use of 34 US homes in one year.

As demonstrated here, public blockchains are fully compatible with the relevant international standards and best practices that apply to traditional financial infrastructures. Public blockchains represent the next era of financial infrastructure, providing an open and neutral platform for everyone to securely interact, innovate and exchange ideas and value online.

Stellar Development Foundation

475 Brannan St, Suite 400
San Francisco, CA 94107

* * *

SDF appreciates the opportunity to respond to your call for contributions and would be pleased to continue this valuable conversation.

Sincerely,

Candace Kelly
Chief Legal and Policy Officer
Stellar Development Foundation