THE POWER OF PUBLIC BLOCKCHAINS

Public blockchains represent the next era of public financial infrastructure, write Marcelo Prates (left), policy director, and Alex Wu (right), policy and government relations manager, Stellar Development Foundation.

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 decentralised manner, which should be seen not as a drawback but as a desired feature.

Decentralisation, rather than denoting a total absence of control, really means that no single party has control over the network. The development, maintenance and use of a public blockchain are spread across multiple parties and follow internal rules embedded in its protocol that are automatically applied and enforced. No stakeholder can unilaterally change the rules or arbitrarily decide who can build upon or use a public blockchain.

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 digital contracts.

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.

In almost 15 years of continued operation, the bitcoin network has gone down twice – in 2010 and 2013 for a total of 15 hours. To date, the network has an uptime percentage of 99.99%. Similarly, the Stellar blockchain 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. 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 centralised organisations demonstrates that centralisation and traditional legal entities don't guarantee a flawless performance.

Private versus public blockchains

There's a false equivalence that private, permissioned networks are safer and more efficient than public, decentralised 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.

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.

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.

'Decentralisation, rather than denoting a total absence of control, really means that no single party has control over the network.'

'THERE'S A FALSE EQUIVALENCE THAT PRIVATE, PERMISSIONED NETWORKS ARE SAFER AND MORE EFFICIENT THAN PUBLIC, DECENTRALISED ONES. WHILE PRIVATE NETWORKS MAY OFFER COMPETITIVE BANDWIDTH AND THROUGHPUT, THEY DON'T COME WITH THE SAFETY OF THEIR PUBLIC COUNTERPARTS.'

This process gives public blockchains strong operational resilience 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.

Ensuring control over assets

It's also important to distinguish between the decentralised nature of public blockchains, the roads upon which digital assets run, and the assets themselves. The assets are generally issued by a centralised entity and can be configured to comply with applicable regulatory requirements. While blockchains may be 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 tokenised 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 customise 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.

Public blockchains represent the next era of public financial infrastructure, providing an open and neutral platform for everyone to securely interact, innovate and exchange ideas and value online. They are ready to pave the way for the payments and financial vehicles of the 21st century.