ExpertInsights@IBV

Central banks and digital ledger technology governance

IBM Institute for Business Value

An expanding market

Central banks and financial system regulators around the world are asking themselves how blockchain is going to change their technology underpinnings and those of the commercial banks and financial institutions they regulate. These executives are especially concerned about the non-functional requirements for blockchain.

Their concerns are warranted. The global blockchain market is expected to grow to USD 5.43 billion by 2023 – a compound annual growth rate (CAGR) of 57.6 percent.[1] And a recent survey revealed that 91 percent of banks plan to invest in blockchain solutions for deposit taking by 2018.[2]

Emerging questions

In our discussions about applying distributed ledger technology and smart contracts to aspects of the financial system, we received many questions pertaining to blockchain's non-functional attributes, including:

- How might blockchain affect financial stability?
- How should central banks continue to manage the governance of blockchain technology?
- What do regulators need to know about consensus mechanisms?
- What are the considerations for operational risk and resilience?
- How do "regulator nodes" figure into risk management of blockchain networks?

Financial stability

Financial stability can result when central banks manage the operational risks of a financial system's components in a way that fosters resiliency and smooth operation. Going forward, stability will also depend on how the blockchain-based solution is governed and by whom – hence the governance discussion and the potential use of regulatory nodes.

Central banks should strive to ensure that systemically important applications and processes that rely on blockchain technology are designed and reviewed against agreed-upon standards, created by central banks, as part of the governance approach. Central banks should also consider the usability of new blockchain-based solutions and approaches, especially in the context of stakeholder engagement, accessibility, fair trading and dispute resolution, to support smooth operation in the real economy.[3]

Governance

Governance of blockchain implementations requires both technical and policy oversight. Blockchain implementations typically involve a network of participants and multiple services providers' systems and technologies, making governance more complex than it is with in-house systems or hierarchical networks.[4]

For technical governance, central banks should consider the source, currency and integrity of the underlying blockchain fabric used as key issues when designing and operating applications that apply blockchain technology. When a smart contract is used in conjunction with a blockchain-based application, governance can be more complex. Considerations for "chaincode" governance include the specification of the chaincode (especially the quality of coding), the fit to the business language (which articulates the desired outcome) and the quality of the documentation that links the business outcome requirements to the chaincode implementation.

For policy governance, central banks should consider the tradeoffs of blockchain and chaincode implementations, starting with the consensus algorithm used. Next, they should evaluate questions of availability versus consistency, security versus throughput, and access. When blockchain and smart contracts are being used to support a new way of doing business, then the governance considerations may include the availability and use of manual processes to mitigate the potential risks of the contracts and the inability of achieving consensus, similar to exception processing in traditional systems.

Consensus

Consensus is the mechanism by which participants in a blockchain-based network agree on the data within transactions. In open, permissionless blockchains, such as Bitcoin or Ethereum, the most common consensus mechanism is "proof of work." Proof of work requires participants to solve a complex problem with specialized computers, thereby allowing a new block to be written to the chain while providing a reward (such as Bitcoins or Ether) for creating consensus.[5]

In private, permissioned blockchains such as Hyperledger Fabric, achieving consensus is generally simpler than it is for public blockchains because all participants are known.

From a central bank's perspective, the important consideration is whether the consensus algorithm in a particular use case actually achieves the consensus desired securely, at a reasonable cost and within a reasonable amount of time.[6]

Operational risk and resilience

Blockchain technology, as implemented in distributed ledgers and smart contracts, focuses on the intersection of internal and external processes and the people and the systems who interact with them. As a result, blockchain may either be a source of – or a solution to – operational risks, including the resiliency of the processes.[7]

Central banks need to apply the same principles for operational risk as are applied to important systems, focusing on the resiliency of chaincode and recognizing that multiple technologies and participants will be involved. The following is a checklist for reviewing plans for addressing the resiliency of blockchain-based systems:

- Operational performance: Provide the necessary capacity to meet peak and peak-peak processing requirements and growth demands.

- Operational performance (transaction latency): Design in the ability to handle network failures, so if one occurs and a node is unavailable in the blockchain-based business network, records can still be written and consensus achieved.
- Operational performance (exception handling): Design for potential errors or failures in chaincode execution, with a combination of exception handling and alternate routing to both write to the blockchain and interact with off-blockchain processes.
- Systems availability (planned): Call out any times reserved for hardware and software maintenance and upgrades, testing, intrusive security audits and system restarts.
- Systems availability (unplanned): Articulate the amount of time permitted when transactions cannot be processed during normal operating hours.
- Data integrity: Agree upon and document the number of lost transactions and associated data loss that will be allowed in the design.
- Business continuity: Agree upon and document the human and technology support required to continue: reading and writing to the blockchain, achieving consensus, executing smart contracts and interfacing with traditional systems if the infrastructure hosting the blockchain nodes is unavailable.
- Manageability: Ensure that provisions are included in the design specification for software version control and configuration management, hot hardware upgrade mechanisms and replacement, end-to-end monitoring, operational alerts and control tools.
- Ability to test/validate/certify: Design requirements for sufficient hardware capacity and isolations to support regression testing, performance testing, pre-production testing and validate results.
- Security: Implement the security framework so that when writing to the blockchain and appending it after consensus is reached, the underlying infrastructure and interfaces are secure from threats such as penetration, spoofing and Distributed Denial of Service (DDoS) attacks.

Regulatory nodes and risk management

Some implementations of blockchain technology include a read-only regulator node that can see all records added to the blockchain in real time and a full audit trail of those that have been appended. For applications critical to the financial system, we recommend the use of regulatory nodes to actively manage the potential risks of that application of blockchain technology. In this context, active participation calls for the regulatory body to perform (or block) transactions primarily to manage systemic risk.

Central banks should review their role in proposed blockchain-based applications or solutions and take a position on whether insight about the blockchain is made available by means of regulatory nodes. That insight could be a benefit for central banks.

Understanding the risks and rewards of blockchain technology

Blockchain technology continues to evolve and will for some time to come. The drivers of these changes will come from a broad range of entities – from start-ups to established IT vendors, and from financial institutions to industrial companies.

Central banks will need to consider how to stay abreast of developments and setbacks associated with the technology. One approach is to actively support start-up incubators.[8] Another is to establish an advisory council composed of key stakeholders. Still another is to form an ongoing working group that engages with everyone working with blockchain technology, thereby fostering the in-house skills necessary to evaluate proposed use cases critically.

Whatever approach or mixture of approaches a central bank may choose, it is important that all central banks have a means and mechanism to understand the development and application of blockchain technology. Banks should welcome central banks' interest in blockchain. In a recent survey, 56 percent of banking executives identified regulatory constraints as a barrier to using blockchain; it was the most cited response.[9]

Looking ahead

Blockchain is evolving from a novel technology into an important asset for the transformation of business-to-business networks. Many of the blockchain use cases under discussion include banks and financial markets participants both directly (clearing and settlement, reference) and indirectly (trade finance, supply chain finance and asset ownership authentication).

The level of transformation under consideration for many basic intercompany banking processes can be a source of risk to the financial system and even the economy. Choosing wisely from among the various forms of distributed ledger technologies is an increasingly critical decision for central bank executives.

About ExpertInsights@IBV reports

ExpertInsights@IBV represents the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

Experts on this topic

Michael Aaron

Blockchain Business Development Leader
IBM Australia and New Zealand
https://www.linkedin.com/in/michael-aaron-7717b6/?ppe=1
sbaaaro@au1.ibm.com

Mark Ebeling

Chief Technical Officer (CTO) Finance Industry
IBM Global Markets, Enterprise
https://www.linkedin.com/in/markebeling
mebeling@au1.ibm.com

Route 100
Somers, NY 10589
Produced in the United States of America
June 2017

Notes and sources

1 “Blockchain Distributed Ledger Market by Type (Private Blockchain & Public Blockchain) and End User (Government, BFSI, Automotive, Retail & e-commerce, Media & Entertainment, and Others) - Global Opportunity Analysis and Industry Forecast, 2017-2023.” Press release. Allied Market Research. March 2017. https://www.alliedmarketresearch.com/blockchain-distributed-ledger-market

2 Bear, Keith, Nick Drury, Peter Korsten, et al. “Leading the Pack in Blockchain Banking: Trailblazers Set the Pace.” IBM Institute for Business Value and the Economist Intelligence Unit. September 2016. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbp03467usen/GBP03467USEN.PDF

3 Yermack, David. “Corporate Governance and Blockchains.” NYU Stern School of Business and National Bureau of Economic Research. November 29, 2015. https://mbs.edu/getattachment/fircg/FIRCG-2016/Highlights/Blockchains-20151129.pdf

4 Ibid.

5 Natoli, Christopher, and Vincent Gramoli. “The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example.” arxiv.org. https://arxiv.org/pdf/1612.09426v1.pdf

6 “Discussion Paper on distributed ledger technology.” Financial Conduct Authority. April 2017. https://www.fca.org.uk/publication/discussion/dp17-03.pdf

7 “After the IBM Growth Markets white paper: National Payment System Design Considerations.” IBM Corporation 2012; For a more detailed discussion on understanding and managing the implications of blockchain in systemically important clearing and settlement systems, refer to “Distributed Ledger Technology in Payment, Clearing and Settlement: An analytical framework.” February 2017. Committee on Payments and Market infrastructures. BIS.

8 Carney, Mark. Governor of the Bank of England. “Building the Infrastructure to Realise FinTech’s Promise.” International FinTech Conference 2017. Old Billingsgate. April 2017. www.bankofengland.co.uk/speeches

9 Bear, Keith, Nick Drury, Peter Korsten, et al. “Leading the Pack in Blockchain Banking: Trailblazers Set the Pace.” IBM Institute for Business Value and the Economist Intelligence Unit. September 2016. https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbp03467usen/GBP03467USEN.PDF

GBE03842USEN-01