A View of Blockchain Technology From the Information Security Radar

Blockchain is a distributed database that maintains a continuously growing list of records called blocks that are secured from any kind of tampering and revision efforts. Each block contains a time stamp and a link to the previous block. A blockchain consists of blocks that hold batches of valid and approved transactions. Each block includes the hash of the prior block in the blockchain linking the two. The linked blocks form a chain, which is called a blockchain.

What Is Blockchain Technology?

Blockchain is a new-age disruptive technology that revolutionizes the way in which:

- Financial transactions can be performed in a trusted manner
- Accountability and transparency can be maintained while streamlining business processes
- Transactions can be made and secured between users

Blockchain is the foundational technology on which the popular bitcoin platforms are built and is a technology that efficiently organizes and secures data so that it can reduce the cost and complexity of transactions to a greater extent. Blockchain is still considered an emerging technology, but many global organizations have already started making significant investments in blockchain-based application development efforts. Many global organizations such as Microsoft and Google are experimenting with blockchain technology in efforts to ensure security and integrity of transactions carried out by the applications developed using their technologies. The global banking industry, in particular, has embraced the implementation of blockchain technology in a wider manner. Many global banks have already announced their blockchain initiatives. By storing data in blockchain, banks can improve the security and portability of the data stored inside a blockchain. The United Arab Emirate (UAE) government has launched a Blockchain Council to support and oversee blockchain-driven developments happening across the nation.[1] The UAE government provides funding support for blockchain Proof of Concept (POC) pilot projects undertaken by any of the organizations in the UAE. The government of Dubai has made significant progress on this by devising an exclusive blockchain strategy for implementing a citywide blockchain platform enabling quick payments.[2, 3] The Singapore government also has started building blockchain systems to protect the banks in Singapore.[4]

How Blockchain Technology Works

The following are the steps followed for transactions using a blockchain:

- Person A creates a transaction that is digitally signed.
- This transaction is sent to a miner. A miner is a verifier who verifies the validity of the transaction and endorses the transaction's validity.
- The miner broadcasts the transaction as a block to all the connected nodes in that blockchain if the transaction is verified as valid.
- The nodes accept this block only if all transactions in it are verified as valid.

Vimal Mani, CISA, CISM, Six Sigma Black Belt
Is the head of the Cyber Security Program at the Bank of Sharjah. He is responsible for the bank's end-to-end cyber security program. Mani coordinates cyber security efforts within the banking operations spread across the Middle East. Mani is also responsible for coordinating bankwide cyber security strategy and standards, leading periodic security risk assessment efforts, leading incident investigation and resolution, and coordinating the bank's security awareness and training programs. He is an active member of the ISACA® Chennai (India) Chapter. He can be reached at vimal.consultant@gmail.com.

> **Due to its decentralized nature, the data elements are transparent to all individuals who share their data elements with others in a single blockchain.**

- Ownership of blocks that include the transaction are transferred to the target account (the digital address) of person B.
- Person B receives the money (digital currency such as bitcoins).

Figure 1 depicts how blockchain technology works.

The CIA Triad and Blockchain Implementation

In a typical blockchain, transactions are grouped into blocks that are restored in a chain of blocks, linking each new block chronologically with the hash of the preceding block. In a blockchain, data elements are not stored in one central location. Rather, data elements are stored across the blockchain network, which ensures the security of the data elements stored in the blockchain.

Conventional information security practice enforces the implementation of the principles of confidentiality, integrity and availability (CIA triad). Blockchain implementation does not enforce confidentiality aspects as strongly as it enforces the integrity and availability of the information stored inside it.

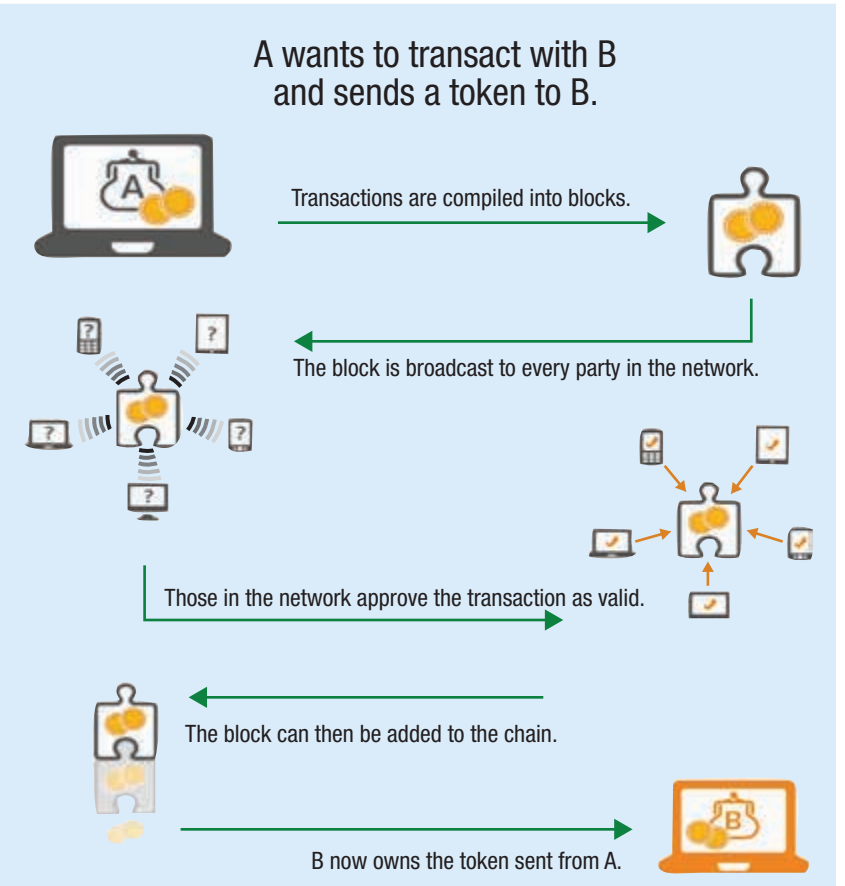
Due to its decentralized nature, the data elements are transparent to all individuals who share their data elements with others in a single blockchain. Because of this, the confidentiality element of this technology is not readily enforceable. Data fed into a blockchain can be seen by all participants with no restrictions. The decentralized nature of blockchain has led to negative consequences such as allowing anyone to read and write transactions into a blockchain. Consequently, bitcoin transactions across the globe have fueled a significant amount of black market trading activity.

At this time, the data kept inside the blockchain are not editable, so the integrity of data elements is easily enforced. However, it is worth mentioning that an adequate amount of research on strengthening the network architecture and ensuring an adequate amount of confidentiality, integrity and privacy of transactions are registered into blockchain is being carried out.

Cryptography-Supported Security Infrastructure

Blockchain technology uses cryptography technology to sign messages and encrypt data with the help of a private-public key mechanism.

Figure 1—The Process Flow of a Blockchain-Based Transaction



Cryptography technology supports organizations in ensuring the confidentiality, integrity, authentication and nonrepudiation of transactions performed. With the use of cryptography-supported infrastructure, blockchain technology has enabled fully secure transactions with the use of cryptocurrencies (such as bitcoin and Ethereum). Research efforts around implementing a public key infrastructure (PKI) type of cryptography mechanism to improve the security of blockchain-based data management are currently in progress.[5] PKI is a method of using cryptography-driven security based on public keys. PKI encryption technology integrated with encryption features helps mitigate the identity management-related issues presented by blockchain implementation.

> **"The immutable database architecture of the blockchain helps in identifying any fraud or error and correcting it immediately."**

Blockchain Helps Establish the Right Security Intelligence

A majority of the nodes in the blockchain network should sign on every transaction happening in a blockchain to mark it as a valid transaction, otherwise, the transaction is deemed invalid and void. Each node in the blockchain should approve the changes made in any of the linked blocks in that blockchain. This enables organizations to ensure the traceability of transactions occurring in a blockchain and build quality security intelligence around those transactions.

Blockchain Provides Protection Against Cyberattacks

Blockchain technology has an immutable database architecture which mandates that every transaction is hashed into a block, and the current block has the hashes of all the previous blocks distributed across nodes. In a blockchain, each new block is coupled with the previous transaction and validated. Therefore, if something gets changed, the blockchain becomes invalid at that point and the error is broadcast to all the nodes in the blockchain. Consequently, if a past data entry is changed by a successful hacking attempt, the block will be invalid, which will cancel the specific transaction. The immutable database architecture of the blockchain helps in identifying any fraud or error and correcting it immediately. The ability to restrict access and reduce the likelihood of cyberattacks makes blockchain a preferred platform by most organizations, especially banks.

Security Concerns Around the Use of Blockchain Technology

While blockchain is very efficient with respect to transactions, there are concerns about the security of blockchain-based transactions. These vulnerabilities exist in the blockchain ecosystem now:

- Blockchain can be hacked like any other platform/protocol. If someone chooses to save their bitcoin and private keys on an Internet-connected device, they can be stolen. Once private keys are stolen, it does not matter how secure the blockchain architecture and encryption features are to hackers. Incidents like this have occurred in the past, for example the Bitfinex attack in August 2016 in which US $65 million was lost and the Ethereum attack in June 2016 in which US $150 million was lost.[6]
- Blockchain can be infected by malware. This has been proven through a POC software that was demonstrated by Interpol at Black Hat Asia in March 2015. This POC software was morphed into malware that could circumvent the blockchain used by bitcoin and introduced data unrelated

to transactions into the blockchain. Researchers have also demonstrated that botnets have the ability to send messages utilizing the bitcoin network. Fujacks Trojan, a botnet backdoor, has successfully proven that it can remotely control infected computers that are nodes in a blockchain, collect information, and install other malware or tools into the blockchain.

- Banks have concerns about transactions' confidentiality, securing private keys and the strength of cryptographic algorithms used in blockchain-based transactions.
- Any blockchain transaction is dependent on trust between two or more counterparties. Most people use bitcoins at exchanges and trust the exchange will look after them. Many money exchange firms are not fully regulated entities. They cannot offer assurance on the transfer of digital currencies.

Using Blockchain Technology

Figure 2 depicts some of the use cases that are applicable across industries.

In early 2017, global banks including HSBC and State Street successfully tested blockchain technology in bond transactions. More recently, UBS and Santander have been trying the technology for cross-border payments, while Bank of America has announced a partnership with Microsoft to experiment with blockchain technology-driven systems.[7, 8, 9, 10]

> **"Since data stored in a blockchain are irreversible, it provides a single source of facts that helps minimize the risk of anomalies, redundant data or defective data elements."**

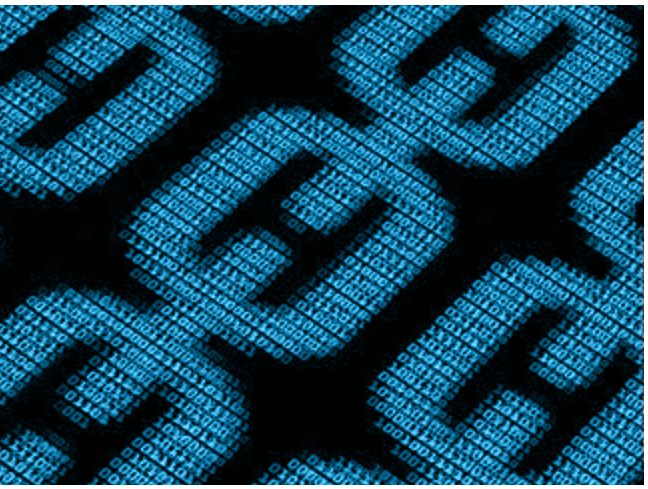
Several blockchain use cases that have been successfully implemented in the banking sector include:

- **Know your customer (KYC)**—KYC statements collected by banks can be stored in a blockchain. This has been successfully tested by a number of global banks. Once a bank receives a KYC

Figure 2—List of Future Use Cases of Blockchain Technology Implementation

Cross Industry	Financial	Governance	Health Care	Insurance	Manufacturing Retail and Consumer Products
Shared reference data	Letter-of-credit	Land Registry	Medical records	Claims processing	Supply chain
Internal financial ledger	Cross-currency payments	Vehicle registry	Medicine supply chain	IoT integration for policy monitoring	Product parts
Audit and compliance enablement	Mortgages (and contracts)	Citizen ID			Provenance tracking
Regulatory view	Collateral management	Education certification			Digital property management
Improved efficiencies	Post-trade settlement	Voting			Real estate, cars
IoT cars, robots, drones					Trade agreements, contract

Source: V. Mani. Reprinted with permission.



from a new customer, it can then put the same information in a blockchain that can then be used by other banks and other accredited organizations (i.e., insurers, loan providers). As the customer identification documents would have been independently checked and verified, these organizations need not carry out their KYC checks again. They can simply rely on the verification performed by the blockchain itself. This helps reduce administrative burdens and costs. Data stored in a blockchain provide a single source of facts that help minimize the risk of anomalies, redundant data or defective data elements.

There could be doubts and questions that arise around the security and privacy of KYC information stored in blockchain. The data in the blockchain is a reference point that is digitally signed. This gives banks access only to relevant client information in a repository separate from the blockchain. This helps ensure the safety and security of KYC information collected and stored by the banks.

- **Management of fraud**—The blockchain ledger can provide historical records of all data elements in the entire blockchain and compliance activities undertaken for each banking customer. This serves as evidence that a bank has fulfilled its regulatory obligations should regulators ask for such clarification. Based on the needs of the regulators, the data within a blockchain can be examined by the banks to identify and trap any fraudulent activity. This is an advantage for the current banking and payment systems, which are more vulnerable to internal fraud and external cyberattacks.
- **Management of payments**—Blockchain is used by banks to make payments in real time using Ripple. Ripple is a Real Time Gross Settlement (RTGS) system, currency exchange and remittance network. Released in 2012, Ripple purports to enable "secure, instant and nearly free global financial transactions of any size with no chargebacks."[11] Ripple's distributed financial technology allows banks around the world to directly transact with each other without the need for having any correspondence.[12] Ripple supports tokens representing cryptocurrency used by blockchain. It helps banks by eliminating the need for common intermediaries in payment transactions. This saves on costs incurred for those intermediary organizations. The disadvantage of Ripple is that it is a proprietary blockchain platform that cannot yet connect with other systems. To connect Ripple to other blockchain protocols, an interledger protocol must be developed, tested and implemented.
- **Clearing and settlement**—Clearing and settlement has been verified as the most active use case in banking, as it provides a short-term win with noticeable cost savings. Clearing and settlement costs billions of US dollars, and according to one report, moving this into a blockchain is estimated to save the industry US $20 billion or more a year in overhead costs. Distributed ledger technology used by blockchain technology could save banks money by eliminating central authorities and bypassing slow, expensive payment networks.[13]
- **Peer-to-peer lending**—People around the world can connect to borrow and lend using bitcoins and other digital currencies that are executed using a blockchain. Countries that lack a local credit scoring system are allowed to receive loans using a blockchain platform based on in-house credit-scoring algorithms.

Key Challenges Observed in Blockchain Implementation and Maintenance

Though implementing blockchain technology helps in improving security and authenticity of the transactions, its implementation encompasses quite a few challenges. Blockchain transactions create risk for financial services.[14] Practical challenges faced by organizations in the implementation of blockchain technology include:

- Settlements made using a blockchain are a relatively slow process. All the nodes in a blockchain need to come to an agreement that the transaction executed is valid. This has proven to be a slower process than having a conventional verification performed by a bank.
- Lack of structured blockchain governance is an important challenge in maintaining data in a blockchain.
- Blockchain technology has a number of security and privacy concerns that need to be addressed before organizations feel comfortable putting their critical data into a blockchain. As the data in a blockchain can be viewed by other members in that blockchain, data privacy is an area of concern with blockchain technology.
- There are also regulatory concerns with blockchain as there is no common regulatory standard for managing blockchain protocols.
- Due to the unpredictable growth of transactions registered into a blockchain, an ambiguity exists about the scalability of a blockchain platform with respect to the increasing amount of business transactions centered on the blockchain platform.
- A risk of false transactions getting approved by other nodes in a blockchain exists and could lead to fraudulent activity.
- Technologies used for implementing blockchain are also vulnerable to a variety of cyberattacks.

“Lack of structured blockchain governance is an important challenge in maintaining data in a blockchain.”

Blockchain Technology’s Most Useful Attributes

Some of the most useful attributes of blockchain technology are noted here:

- Blockchain implementation ensures a high availability of data related to transactions that are entered inside the blockchain. Based on thousands of nodes in a peer-to-peer blockchain network, the transaction data is replicated and updated on every node. Even if any of the nodes leave the network accidentally, purposefully or become otherwise inaccessible, the network as a whole will continue to work. This ensures that the blockchain system is highly available.
- In blockchain use, data integrity can be well maintained. Once data have been registered into the blockchain, they are extremely difficult for anyone to tamper with and change. The fact that changing data is extremely difficult and almost impossible in blockchain is a significant benefit.
- In blockchain use, data quality can be maintained very well using the high-volume database replication and computational trust driving the entire blockchain concept.
- Blockchains are much better platforms that emphasize ease of handling by users compared with the traditional record keeping practice, which still requires physical access to view.

> **“By integrating with the Internet of Things and other disruptive technologies, blockchain technology can simplify daily life for most individuals.”**

- In blockchain usage, applications can be added to the network without needing to wait for someone’s approval. There is no need for a trusted third party or intermediary to validate the transactions registered into the blockchain. Rather, a consensus approach is used to agree on the validity and integrity of transactions registered into the blockchain.
- Blockchain technology ensures a very high level of security of transactions registered into a blockchain through the cryptography technology used in building a blockchain.
- Overall, the decentralized trust, transparency and efficiency demonstrated by blockchain implementation are the intangible benefits an organization can reap from blockchain use, in addition to the tangible cost savings promised by blockchain technology implementation.

Potential Future Uses for Blockchain Technology

Across the globe, there are many new areas in which blockchain technology implementation has started as an experiment. The banking sector, in particular, has embraced blockchain technology. Potential future implementation scenarios/use cases of blockchain technology include:

- Banking industry use of blockchain technology to potentially eliminate the need for intermediary banks in financial transactions.
- Insurance and law enforcement agencies use of blockchain technology to strengthen their fraud prevention activities. Since the customer-identifying documents are independently checked and verified, fraudulent activities can be eliminated with the use of blockchain technology.
- Use of blockchain technology to implement smart contracts by creating protocols that can automatically enforce contracts.
- Use of blockchain technology to improve public administration, e.g., present voting-based election systems. Blockchain technology creates timestamped and signed transactions that cannot be altered or deleted. Recording election records on blockchains would create a secure and permanent record that makes tampering with results much more difficult. When combined with the actual paper ballots used to cast votes, it will become impossible for anyone to manipulate election results.
- Use of blockchain technology to improve business models based on the sharing economy (e.g., Uber)
- Use of blockchain technology to simplify daily life by integrating with the Internet of Things and other disruptive technologies
- Use of blockchain technology to help global governments combat corruption and bureaucratic red tape

Conclusion

The use of blockchain-based systems is an indicator of the transparency and usability of blockchain. Though blockchain does have some problems from a security standpoint and other aspects, these problems are expected to be settled over time, especially with the arrival of more stable and secure blockchain platforms. Finally, it is apparent that blockchain technology is gradually becoming a secure platform. It has a cyberattack-resilient database architecture supported by cryptography, immutability and consensus principles, which are the key ingredients for the

effective implementation of information security in an organization.

Endnotes

1 Government of Dubai, "Dubai Museum of the Future Foundation Announces launch of Global Blockchain Council," 17 February 2016, *http://mediaoffice.ae/en/media-center/news/17/2/2016/dubai-museum-of-the-future-foundation-announces-launch-of-global-blockchain-council.aspx*

2 Smart Dubai, "Dubai Blockchain Strategy," December 2016, *http://mediaoffice.ae/en/media-center/news/17/2/2016/dubai-museum-of-the-future-foundation-announces-launch-of-global-blockchain-council.aspx*

3 Trade Arabia, "Dubai to Implement City-wide Blockchain Payments Platform," 18 April 2017, *https://www.tradearabia.com/index.php?/news/BANK_323628.html*

4 Basu, M.; "Singapore Government Builds Blockchain System to Protect Banks," Gov Insider, 7 June 2016, *https://govinsider.asia/smart-gov/singapore-government-builds-blockchain-system-to-protect-banks/*

5 Corella, F.; "Implementing a PKI on a Blockchain," Pomcor.com, 25 October 2016, *https://pomcor.com/2016/10/25/implementing-a-pki-on-a-blockchain/*

6 Campbell, R.; "Can Blockchain Deliver Security to Banks Against Cyber Attacks?" 12 September 2016, *www.cryptocoinsnews.com/can-blockchain-deliver-security-banks-cyber-attacks/*

7 Perez, Y. B.; "8 Banking Giants Embracing Bitcoin and Blockchain Tech," Coindesk, 27 July 2015, *www.coindesk.com/8-banking-giants-bitcoin-blockchain/*

8 Higgins, S.; "Digital Trade Chain: 7 Banks Could Go Live With Blockchain in 2017," Coindesk, 18 January 2017, *www.coindesk.com/digital-trade-chain-banks-blockchain-2017/*

9 Shen, L.; "Blockchain Will Be Used By 15% of Big Banks By 2017," *Fortune*, 28 September 2016, *http://fortune.com/2016/09/28/blockchain-banks-2017/*

10 Santander, *The Fintech 2.0 Paper: Rebooting Financial Services*, 2015, *http://santanderinnoventures.com/fintech2/*

11 *Op cit.* Perez

12 Bitcoin.com, "Blockchain Exchange Bitsane Introduces Ripple Trading," 7 June 2017, *https://news.bitcoin.com/blockchain-exchange-bitsane-introduces-ripple-trading/*

13 Perez, Y. B.; "Santander: Blockchain Technology Could Save Banks Money by Eliminating Central Authorities," Coindesk, 16 June 2016, *www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/*

14 Samani, R.; C. Beek; "Blockchain Transactions Create Risks for Financial Services," McAfee, 16 December 2015, *https://securingtomorrow.mcafee.com/mcafee-labs/blockchain-transactions-create-risks-financial-services/*