BLOCKCHAIN

VOLUME 4, ISSUE 9
OFFICE OF TECHNOLOGY STRATEGIES (TS)

INTRODUCTION

Two major challenges in the digital age are ensuring security and streamlining enterprise-wide technology. Blockchain is an emerging technology that could alleviate these issues. Blockchain has the ability to establish identity and create trust in cyberspace. Using distributed networks to reduce risk, this accounting, or "ledger," system may change workflow and business procedures by opening opportunities for innovation and growth. This Tech Insight provides an introduction and overview to blockchain and its vulnerabilities. Finally, it covers applications for its use in the private and public sectors, specifically within the Department of Veterans Affairs (VA).

WHAT IS BLOCKCHAIN?

A blockchain is a decentralized, digital, transaction record verified by a network of users. Blockchain features an immutable distributed ledger, and dispersed network that is cryptographically secured. Blockchain architecture gives participants the ability to share a ledger, through peer to peer replication, which is updated every time a block of transactions is agreed to be committed. The process of gaining the agreement is called consensus, and there are a number of algorithms that have been developed for this purpose. Users send transaction requests to the blockchain in order to perform the operations. Once a transaction is completed, a record of the transaction is added to the ledger(s) and can never be altered or removed.

There are four key attributes that define a blockchain network. A blockchain is distributed, public, time-stamped, and persistent. This means that the entire network is decentralized and all transactions can be seen by all participants, including the dates and times of transactions. The data will always persist because each distributed computer knows all the transactions necessary to validate the digital record.

NODES ON THE BLOCKCHAIN NETWORK

A blockchain network consists of nodes; each has a local copy of the transaction ledger. Nodes belong to different organizations or computers. The nodes communicate with each other to gain agreement on the contents of the ledger, not requiring a central authority to validate transactions. In simple blockchains, every node and copy of the ledger is identical. In complex

blockchains, differences in the nodes and the ledgers are allowed. Further, some blockchains support "subchains." Subchains may be owned by a different entity and may be accessible to a different set of users. Nodes may be set up so that some nodes participate in one subchain and not in others. The result of this configuration is that the ledger on some nodes will contain transactions for that subchain while the ledgers on other nodes will not. Each node instantaneously encrypts updates to the blockchain through a consensus mechanism, which verifies additions or alterations made to each blockchain.

ADDING BLOCKS TO THE CHAIN

A blockchain grows and becomes more complex with the addition of new blocks of information from each subsequent transaction. Each transaction block documents a change in information, like a stock trade or payment.

Blocks in the chain contain several pieces of information. It carries the time stamp of each transaction and the parties involved: the recipient and the former owner of the asset. Each new transaction of inputs and outputs corresponds to previous transactions. Additional information can be embedded as well. Blockchain relies on the consensus of a distributed group of computers along the chain. If on computer processes a block that does not carry the entire record, the transaction would be rejected. In order to change a block, someone would have to adjust all the previous blocks in the chain, and gain acceptance before any new block is added to the change. To tamper with the blockchain demands notable computing power and control of 51% or more of all nodes in the chain.

Cryptography is also used to secure the blockchain itself and communicates between the elements of the system, by providing integrity on messages from users or between nodes. It ensures participants can see the parts of the ledger that are relevant to them, and that transactions are secure, authenticated, and verifiable.

The authority to make transactions can use either permissioned or permission-less models. For permissioned blockchain, users have to be enrolled before they are allowed to perform trades. The process gives the user credentials that identify the user performing transactions. For permission-less, any person can perform transactions, but only on their own data.

BLOCKCHAIN VULNERABILITIES

Although blockchain is gaining attention, it has weaknesses. One identified security threat is that any group with 51% or more control of the nodes can tamper with it. Bringing blockchain to government scale is not thoroughly tested, so researchers are working to identify vulnerabilities. Testing out single-use applications will help organizations develop skills needed

for advanced applications. Thanks to the emergence of cloud-based blockchain services from start-ups and large platforms like Amazon and Microsoft, experimentation is widely accessible.

APPLYING BLOCKCHAIN

Blockchain can be viewed from several perspectives. First, from a business perspective, blockchain is an exchange network that facilitates transfer of value, assets, or other entities between willing and mutually agreeing participants, ensuring privacy and control of data. From this perspective, blockchains are similar to filing cabinets or databases. From a legal perspective, blockchain ledger transactions are validated and indisputable that do not require intermediaries like lawyers or bankers to verify. Blockchain could disrupt the traditional roles of the financial industry, notary publics, and lawyers in legalizing, generating trust, and authorizing functions. Technically speaking, blockchain is a replicated, distributed ledger of transactions with ledger entries referencing other data stores.

PRIVATE SECTOR APPLICATIONS OF BLOCKCHAIN

The original application of blockchain was bitcoin. Bitcoin, one of the first cryptocurrencies, was launched by Satoshi Nakamoto as a peer-to-peer electronic cash system. Bitcoin is the world's first decentralized currency because it is not tied to the regulations of any country and is not monitored by any one institution, but by a wide community of network users. It is a commodity and a global currency that enables instant payments to anyone, anywhere in the world.

Blockchain technology could be used in supply chain management (SCM) to track the flow of goods, including counterfeit drugs or diamonds, providing "truth registries." SCM blocks can combine information about the transfer of goods at each step, enabling a blockchain to register every product in an enterprise's supply chain, ensuring quality while reducing uncertainty and.

The internet of things (IoT) could create a blockchain that tracks and registers every device that is connected to an enterprise's IoT. Cloud computing could rely on the distributed computing concepts underlying blockchain technology.

FEDERAL USES OF BLOCKCHAIN

The US Federal government and governments around the world are exploring uses for blockchain. In the US, security concerns contribute an amount of opacity between government branches. Building on the open data movement, blockchain could introduce opportunities for departments and agencies to securely share information and services. Governments foresee internally using blockchain as a database to manage physical and digital assets, record internal transactions, verify identities, reconcile internal databases, and increase interoperability.

A registry of all devices connected to the VA's IoT is a potential beneficial use of blockchain. A second could be digitizing the transactions of Veterans' monetary benefits, like pension and compensation. Health researchers are also exploring using blockchain in healthcare records management. Blockchain could be used to securely exchange large volumes of data while ensuring patient privacy and maintaining data integrity. Further, blockchain's record-keeping ability could be used in VA hospitals to track a patient's hospital visit, with developments tracked in a ledger as a transaction.

Blockchain is expected to reduce operational costs, increase digital security, and instantaneously update systems. What uses might you have for such a technology?

Want to read more? You can find all of our Tech Insights here. Read more about blockchain in the Enterprise Technology Strategic Plan's section on emerging technologies.

TS TECH INSIGHT SERIES

The monthly Tech Insight series aims to help readers make better decisions and be more informed customers (of Office of Information & Technology's products and services) by providing them with high-level overviews of technology issues that impact or will impact VA's Information Technology (IT) environment. Tech Insights introduce topics in an easily digestible fashion by presenting background information on the topic, clearly explaining its importance within VA, and providing recommendations for success from TS. View all TS Tech Insights here.

DISCLAIMER: This document includes links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.