Blockchain as Security Solution

by

Dwayne Hodges, Ed.D, CISSP, CCISO
October 14, 2018

October is Cyber Security Awareness Month and I would be remiss if I did not use this as an opportunity to reemphasize to all the cybersecurity leaders and warriors, that we, as cybersecurity leaders, should not remove the human input from the process, despite the plethora of cyber security tools available on the market.

It is critical that we continue to examine how various technologies can improve security, as well as how those technologies that can accelerate business processes. One of my favorite technologies is the Blockchain. Satoshi Nakamoto published his paper on Blockchain, in which he provided a solution to digital trust by offering a more secure method completing transactions. The defining characteristics of Blockchain, transparency, decentralization and time-stamped, also make Blockchain an attractive alternative for conducting nonfinancial transactions.

Blockchain solves more than one problem by establishing trust in a peer to peer network within a distributed system[1] and the distributed network itself can confirm all transactions through a process called mining.[2] Furthermore, Blockchain can alert the network to any alterations within that blockchain after the final transaction occurs. In my opinion, one of the greatest features blockchain technology offers as a use case for many organizations is it can create and maintain a permanent public ledger for transactions that can never be changed. Once any party within the distributed network creates a transaction, this transaction cannot be altered in any fashion without notifying the entire blockchain of the change.

This level of transparency creates a large amount of trust in a decentralized distributed network. Contrary to traditional organizations, such as banking institutions, a bank may be dependent on administrative policies in addition to technical controls to detect and mitigate fraud. In a traditional centralized system, such as a bank, all the transactions are generally recorded on a single ledger. This ledger is maintained by one central authority, making fraud and abuse easy to hide. Traditional banks try to use administrative policies such as mandatory vacation, lease privileges and separation of duties as a system of checks and balances, but even these checks and balances are vulnerable.

Because of blockchain technology, deceptive practices such as "cooking the books" and "turning profits into expenses" may no longer be possible if the original transactions and associated data is in the blockchain. This basic summary of how a blockchain works is not the definition of a "bitcoin" or completely related to financial transaction; therefore, blockchain technology just may offer a plethora of imaginative use for a variety of organizations beyond the

[1] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, (https://bitcoin/bitcoin.pdf)

[2] Ibid.

financial community[3]. By addressing the issue of trust and creating an environment of transparency, other uses such as smart contracts allow blockchain technology to confirm transactions and detect and/or mitigate fraudulent activity.

In a blockchain, the ledger is distributed to multiple parties; therefore, the trust is "distributed" and transparent and allows everyone to verify timestamps and transactions. Distributing the ledger to multiple parties also allows everyone to detect any changes in the transactions. This is where blockchain may offer more unique uses beyond the traditional bitcoin currency for organizations that use smart contracts.

A blockchain is composed of transaction data, timestamp data, and mathematical hash values of the data itself along with a mathematical hash value of the previous block of data. This is where the magic of the blockchain works. Every block of data in the chain has fixed data (hash value) from the previous block that is used to compose the new block. When a new transaction or record is created within the entire blockchain, the very last mathematical hash value that was generated on the blockchain is sent out to everyone in the network.

According to the National Institute of Standards of Technology (NIST), a hashing algorithm will generate a message digested and detect changes since the digest was created[4]. A hash function is a cryptographic one-way function generally used for protecting the integrity of data. As data is passing through a hashing algorithm, such as SHA-2 and a fixed representation, the message digest of the data is computed. This digest is appended to the original message to allow parties to compare the digest to the original message to ensure the message was not altered. The slightest deviation from the original data will have an avalanche effect on the message digest. There are many hashing algorithms and sizes out there to consider.[5]Although there are more details to the blockchain than I explain here, Blockchain creates a cryptographic secure "chain" of blocks all linked together. In this fashion, data from the previous block is used to compute the hash of the next block.[6] This process makes every transaction unique. It also makes it extremely difficult for any party to commit fraud.

Some experts maintain that the blockchain cannot be tampered with. Beck even maintains that blockchain is tamper-resistant in today's application[7]. In my opinion, the blockchain is a very secure process where changes can be detected. Technology security is never absolute. Regardless if the attack is theoretical or actual, it is just a matter of work factor and computing power, and therefore a matter of time. In the case of blockchain, a mathematical collision is possible with a high work factor and high computing power along with a weak hashing algorithm. The lower the bit value, the higher the probability of a collision.[8] It would also likely require a proof of work on every block; therefore, the larger the chain the more

---

[3] Let's go beyond the blockchain use cases to real blockchain networks https://www.ibm.com/blockchain/use-cases

[4] NIST Computer resource Center, FIPS 180-4 Secure Hash Standard https://csrc.nist.gov/publications/detail/fips/180/4/final

[5] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, (https://bitcoin/bitcoin.pdf)

[6] Di Pierro, Massimo IEEE Computing Edge, What is the Blockchain, www.computer.org

[7] Beck, Roman, Computing Edge, Beyond Bitcoin, The Rise of Block Chain World, www.computer.org

[8] Hash collision probabilities https://preshing.com/20110504/hash-collision-probabilities/

impractical this attack could be, impractical meaning higher work factor. I do not anticipate any malicious actors in 2018 going after a smart contract that holds the transactions for the sale of a car. However, I can foresee the work factor being considered for something more interesting to a well-funded and highly organized Nation state level APT actor in the foreseeable future.

There are also some growing questions as to whether blockchain technology conflicts with the General Data Protection Regulation (GDPR) requirement[9]. Although there may be some legitimate concerns, the GDPR just went into effect in early 2018. Like many new regulations, the GDPR is evolving and must mature and adapt to new and improved technologies, as well as evolving threats. The GDPR is about giving people more control over their personnel data and protecting data. Although the blockchain does not allow anyone to erase any data stored in the block chain, at some point in the future there may need to be discussions on creating balance between privacy, trust, security and confidentiality. If we reduce the security of the blockchain to satisfy GDPR, we will almost certainly open the door for a host of "known" attacks and vulnerabilities against the blockchain, and the bad guys will surely follow suit.

The path forward may be to evaluate information and information systems, along with organizational processes to evaluate how and where the blockchain is best applied. The GDPR should not be a cookie cutter design or a silver bullet approach. In some cases, the trust may very well trump privacy. The blockchain is an evolving technology. Furthermore, GDPR is an immature law that must be refined. The European blockchain body stated, "there is a lack of clarity between blockchain technology and GDPR law".[10]

As stated earlier, that are a multitude of nonfinancial applications of blockchain technology. Some of these uses include enhancing the security, integrity and privacy in

---

[9] GDPR In conflict with blockchain? https://medium.com/bitclave/gdpr-in-conflict-with-blockchain-6882f5032724

[10] GDPR Could Hinder Blockchain Innovation, Warns EU Body https://www.ccn.com/gdpr-could-hinder-blockchain-innovation-warns-eu-body/

healthcare data, database information, legal entities, luxury goods networks, custom declarations, trade, group benefits, supply chain compliance and many more.

Dwayne Hodges, Ed.D is the CEO and President for DH-Cyber Security Solutions, a Services Disabled Veteran Owned Small Business, and a full Professor in CyberSecurity at UMUC. He is retired Army Officer with over 20 years military service and holds several industry certifications to include the CISSP with ISC^2 and Certified CISO with EC-Council.