Issues in Information Systems
Volume 17, Issue IV, pp. 222-226, 2016

A LAYERED ARCHITECTURAL APPROACH TO UNDERSTANDING DISTRIBUTED CRYPTOGRAPHIC LEDGERS

Robert E. Samuel, Widener University, Robert.Samuel@ieee.org

ABSTRACT

Government officials and industry experts increasingly highlight today's data privacy and security vulnerabilities require new approaches to mitigate risk. Additional methods and techniques to address current vulnerabilities are needed especially between responsible parties within a large ecosystem like finance, healthcare, and education. New approaches leveraging cryptographic ledgers and blockchains are emerging as a potential solution. This paper proposes a layered architectural approach for cryptographic ledgers to aid in security and privacy controls of digital solutions.

Keywords: Cryptographic Ledgers, Blockchain, Architecture

INTRODUCTION

Government officials and industry experts are increasing awareness regarding data privacy and security vulnerabilities (Curran, 2016). The call to regulators, information/computer science industry experts and academia is being made to find techniques to counteract the data and privacy challenges of today. It is possible that an emerging approach based on the concept of distributed cryptographic ledgers – the authoritative open record of secure transactions – will be the future standard. However, to increase the understanding and adoption of this often-misunderstood technology, a simplified model is needed. If the desire is to educate the next generation of cyber security professionals, then a model that supports the simplification of a complex technology is warranted. This paper proposes a layered architectural approach to aid in the positioning of cryptographic ledgers in digital solutions.

Over the past several years, the term Bitcoin, the virtual currency, has become more widely known due to attention from the press reporting on technology, the rise illegal use by criminals, and the increased monetary value of the virtual currency (Kiviat, 2015). Extance (2015) highlights that the birth of Bitcoin in January 2009, raised out of the cryptography community, was based on the original 2008 white paper *Bitcoin: A peer-to-peer Electronic Cash System* by Satashi Nakamoto (pseudonym) (Nakamoto, 2008). The core technology behind Bitcoin is known as the *blockchain*, as it serves as the official cryptographic ledger of every Bitcoin transaction (Hurlburt, 2016). Extance (2015) further explains "many people see this blockchain architecture as the template for a host of other applications including self-enforcing contracts and secure systems for online voting and crowdfunding." Several emerging potential approaches are using marketing descriptions such as "fabric", "platforms", and "blockchain as a service" to represent the blockchain layered architecture that serves as a distributed cryptographic ledger (Valdes R., et. al, 2016).

Extance (2015) reports that "the blockchain is a remarkably powerful idea that could be applied to much more than just transaction records … One use might be to develop computerized, self-enforcing contracts that make a payment automatically when a task is complete." Forrester Research predicts that the adoption of a distributed cryptographic ledger layer using blockchain will take around five years (around 2021) to reach maturity (Bennet, 2016). One indication that academia is starting to investigate the distributed cryptographic ledger technology is highlighted by the launch of the first academic journal, Ledger, in September 2015. Extance (2015) predicts that "it's a remarkable body of knowledge, and we're going to be teaching this in computer science classes in 20 years."

Cryptographic Ledger using Blockchain Overview

Kivat (2015) provides the following metaphor to explain cryptographic ledgers using blockchain technology - "In the physical world, security requires locks, vaults, and signatures; in the digital world, it requires cryptography, or techniques for securing digital information and transactions." Blockchain at its basic definition is a cryptographic technology that allows transactions to occur without a trusted third-party using an online decentralized ledger method. Kivat (2015) supports this definition stating "the blockchain establishes trust between two parties to a transaction through both a decentralized public ledger and a cryptographic mechanism that ensures transactions cannot be changed after the fact." The term blockchain is shorthand for an overarching technology concept that follows the principles of an append-only, cryptographically secured, distributed, replicated store of records (Bennet, 2016). Kraft (2016) expands on the functionality by stating, "all transactions that change the distributed ledger are grouped into blocks. Each block represents thus an atomic update of the ledger's state. In order for a block to be valid, it has to fulfill a proof-of-work condition: a particular cryptographic hash involving the block's content is formed, and must be below a threshold value. In addition to current transactions, each block also contains a reference to a preceding block. In other words, from a given block, a chain of other blocks linking it to the initial network consensus can be constructed." Therefore, one can construct a ledger by following the chain of block constructed and the encoded transactions.

The long-term viability of Bitcoin is seriously questionable due to lack of efficiency, utility and regulatory challenges as expressed by the leading Bitcoin developer Mike Hearn. However, the blockchain distributed ledger technology for business transactions seems to be more viable and growing acceptance (Hurlburt, 2016). For example, new cryptographic ledger approaches use blockchains to execute simple tasks of verifying contracts. Hurlburt (2016) explains, "the blockchain, a means to accurately tracking any form of transaction, has significant value beyond the realm of monetary transfer." The potential range of the blockchain utility spans intellectual property (e.g. app development, digital content, music, photos, text, patents), digital identity (e.g. medical records, ride sharing credits, consumer privacy, elections, endorsements, digital storage), market security (e.g. sales, securities/derivatives, contracts, escrow/custodian, equity transference, anti-counterfeit), and internet of anything (e.g. home automation, transport automation, network activity, sensor activation).

RESEARCH METHODOLOGY

Our research centered upon the following research question:

R_1: Which required attributes are represented with the blockchain architecture layer within a cybersecurity conceptual model?

To address this research question, the author used the qualitative opinion-based research methodology approach using informal individual interviews of subject matter experts. A review of peer-reviewed scholarly publications was used to determine the boundaries of the problem space and create interview questions. The interview questions derived from articles that are within the computer science, software and systems engineering, information science, and security domains. The interviews involved a convenience sample size of twelve industry experts and system architects. The interview questions were assembled based on key domain topics and issues observed during the review of existing peer-review scholarly publications. The interviews were conducted during the April and May 2016 timeline via phone and in-person.

RESULTS

There is significant lack of academic publications that address the use of blockchains for cybersecurity considerations. Majority of the existing publications highlight the crypto-currency aspects of benefits and challenges of Bitcoin rather than the information systems implementation approaches of distributed ledgers. There is a fundamental difference between cryptocurrency (Bitcoin) and distributed ledgers; as distributed ledgers require

legal identities with permissioned nodes to validate transactions. However, many publications highlight that blockchain/distributed ledger implementations have just as much an economic and law considerations as its primary field of computer science and security. This is emphasized by the use case examples of developing incentives based programs and regulatory and legal reviews as a precursor for distribute ledger application participation.

As highlighted earlier in this report, the literature review and subject matter experts highlighted multiple business domains and use cases for implementation considerations including:

- Multiple party coordination (e.g. financial remittance) by means to "replace a complex, slow, and potentially error-prone process – reduce cost and complexity by moving from the existing system of individually maintained databases and a complex web of connections and intermediaries toward an environment where all parties involved have a copy of the same shared, replicated ledge of secure, irrefutable transaction records, and less or not need for intermediaries" (Bennet, 2016)
- Micro-payment solutions by "providing consumers more flexible payment options – exploring the potential of blockchain technology to provide consumers with more flexible payment mechanisms" (Bennet, 2016)
- Securing intellectual property by proving provenance, ownership, usage rights, or status of a record
- Proof of identity
- Ensuring data privacy
- Automatic execution of contractual agreements (e.g. smart contracts)
- Validation of equipment status and certifications (e.g. Internet of Things devices)

Bennett (2016) of Forrester Research states that "blockchain technology is best described as a concept that involves a number of key components including (but not limited to): validation, a consensus mechanism, replication, and storage." These themes were consistent focus points codified from the subject matter expert interviews. Expanding on these key themes, important cryptographic ledger components include:

- Consensus Mechanism
- Smart Contract Execution
- Validation
- Peer-to-Peer Replication
- Storage
- Auditability
- Identity and Authentication
- Exception Handling
- Read and Write Permission
- Confidentiality and Privacy

With these components are the basis of the analysis from the subject matter expert interviews and supported by the content analysis, the primary observation consists of the logical separation of functionality necessary for distributed ledger implementation. It was highlighted that a common misunderstanding is that the data elements are included in the blockchain itself. Rather, there is a separation between the application messaging, the data storage or system of record, and the distributed ledger layer as shown as a conceptual model in Figure 1.

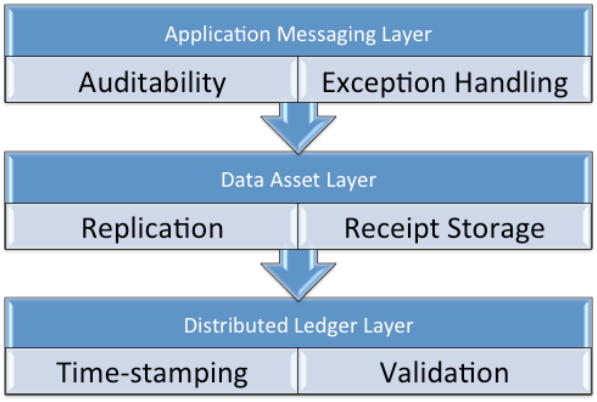

Figure 1. Distributed Ledger as a Layered Architecture

The Application Messaging Layer is responsible for the primary library to interface with business logic within the application. This layer performs the functions of auditability and exception handling when ledger requirements are necessary. The Data Asset Layer is responsible for the data storage/replication and associating the hash receipt to the appropriate data records. This layer performs the permissions read/write of the data records and associated receipt flag from the distributed ledger. The Distributed Ledger Layer is responsible for the journaling and consensus mechanisms. This layer performs the time-stamping algorithm and validation services for auditing.

SUMMARY

In conclusion, based on the limited published content and minimally available subject matter experts available for interviews, this paper highlights the potential of representing blockchain technology as a layered architecture to simplify the cybersecurity model. Time-stamping and digital identity attributes are the primary characteristics of a blockchain layer to differentiate from traditional database solutions using distributed architectures and consensus algorithms.

Further work necessary includes the detailed interaction model and standards for integration between the layers. Within the marketplace, the following is a representation of consortiums, open source projects and vendors working the standards:

- R3 (http://r3cev.com/) - leads the Distributed Ledger Group – in April 2016, R3 announced a partnership with Microsoft and also went public with its own proposed software development called Corda
- Linux Foundation Hyperledger Project (https://www.hyperledger.org/) - originally named Open Ledger Project - is supported by IBM and Digital Asset Holding for the purpose to develop a common open source blockchain framework for all industry players
- Factom (http://factom.org/)
- Ethereum (https://www.ethereum.org/) - used on Microsoft Azure
- Tierion (https://tierion.com/)
- Ripple (https://ripple.com/)
- Stellar (https://www.stellar.org/)
- Intel (http://intelledger.github.io/)
- IBM (http://www.ibm.com/blockchain/)

There are significant issues and challenges pertaining to the distributed ledger technology space including:

- by definition, a replicated ledger shared in different countries would involve the copying of data to all countries involved. Unless regulation is changed, participation in such a blockchain would be a compliance breach.
- Blockchain is not immune from malicious attack.
- Before blockchains become a replacement for transactional databases, additional standards must be established.
- Current blockchain scalability is limited to seven transactions per second.

REFERENCES

Bennet, M. (2016). Q&A: Forrester's Top Five Questions About Blockchain. Forrester Research. April 20, 2016.

Extance, A. (2015). Bitcoin and Beyond. Nature. Macmillan Publishers Limited. October 1, 2015. Vol. 526, pp. 21 – 23.

Kiviat, T. I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal. 65*(569). pp. 569 – 608.

Kraft, D. (2015). Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking Applications. Springer. 2016:9. Pg. 397-413.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. https://bitcoin.org/bitcoin.pdf

Nurlburt, G. (2016). Might the Blockchain Outlive Bitcoin? IT Pro. March/April 2016. pp. 12 – 16.

Ohlhorst, F. (2016). Blockchains: the next generation of secure web. April 15, 2016. Gigaom. https://gigaom.com/2016/04/15/blockchains-the-next-generation-of-the-secure-web/

Rashid, F. (2016). IBM Brings Blockchain Framework to IBM Cloud. InfoWorld. April 29, 2016. http://www.infoworld.com/article/3063538/cloud-security/ibm-brings-blockchain-framework-to-ibm-cloud.html

The Economist. (2015). The next big thing: Blockchain. May 9, 2015. http://www.economist.com/news/special-report/21650295-or-it-next-big-thing

Valdes R., Furlonger, D. and Chesini, F. (2016). The Bitcoin Blockchain: The Magic and the Myth. Gartner Research. April 8, 2016.