The Unintentional Risk or Liability of Implementing, Deploying, or Adopting a Private Blockchain Network

Dr. Mark Pisano
Department of Business Information Systems
Southern Connecticut State University
Pisanom1@southernct.edu

Dr. Richard Bassett
Department of Business Information Systems
Southern Connecticut State University
Bassettr3@southernct.edu

Abstract. Blockchain technology is growing in adoption within large financial organizations and beginning to be adopted by additional industries. As more organizations begin to adopt private blockchain networks, the security risks and vulnerabilities that plague the public blockchain networks will still be present. A private blockchain network that is closed to the public and accessible by trusted parties does not eliminate the security risks or vulnerabilities.

Immutability, a key security feature of blockchain networks, can also become a large liability for organizations, especially when the data being written to the blockchain is done so from trusted users and is assumed to be acceptable content.

Risks increase with enhancements to blockchain standards such as larger ledger or block sizes. The strict format for laying out the data, even though there is space for arbitrary data or freeform space, also increases as the ledger or block sizes grow. The larger block size has allowed users in the public networks to write files out to the blockchain posing a large risk that illegal content will remain on the network indefinitely and be replicated across all of the nodes. This concept can easily become a problem for the private blockchain networks, opening up the organization to many types of legal problems.

This research paper explores the business, technical, and legal risks which organizations expose themselves to by implementing, deploying, or joining private blockchain networks.

I. Introduction

Blockchain technology has been growing in popularity for the past several years. This technology is viewed as being very safe and secure. Due to this, it has seen significant growth in the financial industry and began to grow in other industries. Its expansion from cryptocurrency with the addition of smart contracts has allowed for many industries such as the technology, healthcare, real estate, legal, and shipping to begin evaluating and introducing blockchain networks. These private blockchain networks have gained traction, and a clear example of this is the pilot program in use at the Federal Food and Drug Administration.

As more industries and organizations adopt blockchain networks and continue to believe that they are safe and secure, the security risks and liabilities will continue to exists or grow. The current risks seen in the public blockchain networks, such as Bitcoin, will be part of the private networks that industries are beginning to implement.

A key feature of blockchain technology is immutability. This feature ensures that data written to the network cannot be deleted but instead lives on forever. Additionally, another great benefit to blockchain networks is that the entirety of the data is replicated across all of the nodes, leaving all members with identical copies of the network data. The replicated storage blocks could leave unsuspecting member organizations at risk.

As blockchain technology advances, there has been an increase made to the size of the blocks that can be written to the network. The size increase has thus opened up the network to large and different types of content and potential exploits being uploaded to the network. This paper looks to discuss these potential exploits and risks that can be found in a public blockchain network and how they can be seen in the private blockchain networks.

II. Blockchain in Industry

Blockchain technology began its commercial use in the finance industry. Mainly as a supporting technology for cryptocurrency, such as Bitcoin. Since its introduction, we have seen the introduction and growth of new cryptocurrencies along with new public blockchain networks. The financial industry has fueled all of this with significant organizations such as American Express, Goldman Sachs, MasterCard, and others investing around a billion dollars by 2015 [1].

III. Blockchain in Other Industries

Due to the significant and continued growth of blockchain, mostly in the financial industry, other industries such as technology, healthcare, real estate, legal, and shipping have begun to create blockchain networks actively. These networks are mostly used for research or developmental purposes. An evaluation of organizations hiring via LinkedIn has shown that outside the financial industry, the hires are geared towards discovery and exploratory role for the uses of blockchain. Companies such as IBM, Amazon, Overstock, and Samsung are currently exploring the uses of blockchain to meet their needs [1].

Secondary industries where blockchain has started to gain traction based on available jobs are the technology industry and supply chain. The technology industry is mostly offering blockchain to organizations as a service or product, while the supply chain industry is taking advantage of the smart contracts and automation components available.

A great example of the use of a private blockchain network outside of the financial industry is the pilot program being run by the United States Department of Food and Drug Administration. The FDA is running a pilot program of a blockchain network to help streamline the auditing of medication. The hopes are that with this network in place the time to audit the distribution of medication will be reduced significantly while increasing accuracy. Enhancing these functions and creating more efficiencies will then allow the FDA to increase the number of medications that require the audit trails, making the nation's drug supply safer. If all is successful, there has been mention of expanding the audit capabilities to help keep track of the nation's food supply [2]. Additionally, the Department of Health and Human Services and the Center for Disease Control and Prevention have also invested in programs that utilize this technology [16].

IV. Coin Use and Smart Contracts

In its original commercial use, a blockchain network was created to support the cryptocurrency of Bitcoin. Cryptocurrency has allowed for the value exchange to take place without the need for a central authority or bank [11]. As with most technology, other products or services began to spring up around Bitcoins success. More development and improvement to blockchain has meant that new features and uses could be created.

A smart contract is a feature of the current implementation of blockchain which allows for contracts to be made in a digital format. When criteria of the contract are met, an automated process is kicked off. This could be to issue a new contract or something simple such as transferring a payment [1]. The automation is a valuable feature, and the ability to offer smart contracts has led to the adaptation of blockchain networks in other industries.

V. Immutability and Block Sizes

One of the great features built into a blockchain network is the immutability of the data written. The immutability feature ensures that all of the blocks written to the chain cannot be deleted. In other terms, once something is put onto the blockchain network, it is there forever. Immutability is a critical function when it comes to record-keeping and creating an audit trail.

As the use of blockchain networks has continued to mature, advancements have been made. Sizes of the blocks have been increased to help offer the ability to write out larger ledgers and pieces of data. These blocks have a format and set structure as to what and how they can be presented and written to the network [10]. Within this structure, there is some space to include arbitrary data.

It is possible to abuse this space and inject data that was not intended to be written to the chain [13]. This type of abuse has been seen on the public Bitcoin network [12]. Users have written messages, upload documents, images, and gif files. The aforementioned type of opening can produce several types of security risks or liabilities, as outlined in the following sections.

In order to help illustrate this concept, an evaluation of the popular public network of Bitcoin was done. The currently supported production Bitcoin network supports block sizes of 1MB. With the introduction of the new core version (0.18), the Bitcoin network began the process of introducing a segregated witness network which has allowed for expanding the size of the block from the current 1MB to a size of 4MB. That change does not happen instantly but will take a long time to be phased in; it is currently in a testing phase [3]. The earlier versions of Bitcoin core allowed for the writing of 80 bytes of arbitrary data and was then changed in 2014 to be limited to 40 bytes [4]. The 40 bytes of space is ample enough to write a document, image, or miscellaneous file.

An additional look at a competing public blockchain network shows that it also supports the use of arbitrary space. However, in theory, this blockchain network will allow for arbitrary data of any size to be written to the network. This service does it in two ways, writing out a script in a smart contract or writing out as a log event. Using a smart contract to write out the arbitrary data has a size limit of 32 bytes while writing out a log event has no limit [4]. Again, this is more than enough space to place documents, images, or miscellaneous files.

A previous study has found 1557 readable files on the Bitcoin network. Of these files, the authors believe they have found the following types of violations: copyright, malware, privacy, politically sensitive, illegal, and condemned content. The most damaging find where two instances of 274 links to child pornography [5]. Clearly, material that was not intended to be stored on the Bitcoin network and something that cannot easily be erased or modified without compromising the core functions of blockchains immutability.

Additionally, there are several tools available online that will help users view and write content out to the Bitcoin network. One of the most popular tools available is `cryptograffiti.info`. Cryptograffiti will break the content down into 20-byte chunks, link them together, and write the content to Bitcoins network. This service also allows a user to view random human-readable content that it searches for and streams across its feed [6].

VI. Security Risks Around a Private Network

A private blockchain network operates and functions in the same way that a public network does. However, when the stigma of a public network is removed, end-users tend to believe that a privately run network is inherently safe and secure. This thought can lead to riskier behavior when it comes to the use of the private network.

As nonpublic networks grow among industries, there is an additional risk when it comes to industries or partner organizations becoming members of these private networks. Member organizations will not be able to control the security practices of other members. If an organization's security practices are weak, it can put the entire network at risk, and this type of network is only as secure as the weakest member. Along with the security practices of member organizations, end-users would be more inclined to trust the data that is being shared through the blockchain network. The idea is that since the data has come from a trusted partner, then it must be safe.

It is difficult to control what and how all users of a private blockchain network use the network. Unintended methods or uses can arise. For example, users may decide to use space in the block to send messages or exchange files that contain copyrighted material. It can become a serious liability for any organization to have copyrighted material being used and stored when permission has not been given.

A more serious issue could arise when users believe that they are immune to detection due to the reputation of the blockchain for being anonymous [14]. Many technical shortcomings and counter measures have been identified but complete security and privacy have not been accomplished [15]. This false sense of anonymity could result in the exchange of illegal images or files that reference where these images, videos, and content can be located. Unintended content has been an issue for public blockchain networks such as Bitcoin; it was discovered that people where uploading images and documents with links to some very questionable content.

Unsanctioned content, as mentioned above, may not sound like a serious risk or issue, but the very nature of blockchain technology compounds it. Building or being a member of a private blockchain network would mean that most likely each organization would have its management servers. This would mean that the organization has in its possession servers that would have a current replicated copy of all the data on the network, even when the transactions are between other organizations. In essence, all the organizations with management servers would be in possession of illegal or questionable content and could violate federal laws as they are written.

A concern that all member organization should be evaluating is the risk presented by workstations that have access to the blockchain network. Again, it would be difficult to dictate and control the security practices of all the member organizations making a vulnerable free network very unlikely. All organization workstations are susceptible to botnets and other forms of malware. As these workstations become infected or controllable via a botnet infection, direct or indirect access, and control to the private blockchain network can be possible.

If unauthorized access were to happen and data from the blockchain network were to be taken, it would be a shared data leak. It would take only one-member organization server to be compromised for the data of all members to be put at risk. This is due to the replication of all the management servers, requiring them all have copies of the entire network, even when the transaction or data does not involve the member. This can put everyone's data at risk.

VII. Legal Risks

All of the previously mentioned risks could put any organization in some very serious legal troubles. Although currently there have been no recorded legal cases involving a blockchain network, it could be just a matter of time [7]. Currently, the United States government has begun to investigate cryptocurrency for crimes around the financial industry. The Global Research Center, an arm of the Library of Congress, has put together a survey of foreign entities and their handling of Bitcoin as a currency. The survey has evaluated taxation,

and the use of Bitcoin as a legal currency, and its impact on the current financial instruments in place [8]. Additionally, the Treasury Department has also announced guidelines that the Financial Crimes Network is to follow for the handling of virtual currencies [9]. The survey provides a clear sign of the seriousness of the US governments interest in understanding and potentially investigating financial crimes related to a currency based on blockchain.

As investigators dig deeper into the currency networks, it is feasible that the investigators may stumble upon questionable material. As the government continues to investigate crypto currency and blockchain networks become more widely used, it will only be a matter of time before governments begin to actively investigate these networks for all legal violations.

VIII. Conclusion

As more industries and organizations continue to adopt blockchain networks, it is critical that all the members of the blockchain network make a serious evaluation of all the potential security risks. Using Bitcoins blockchain network as an example, it has been shown that users of the network have uploaded and shared data or content that is either questionable or illegal. Users of blockchain networks can leverage the arbitrary space in the blocks to upload and write this data or content out. Organizations could be opening themselves up to the weak security practices of other network members, assumptions that everything is safe, malware, and unauthorized data access.

The immutability of the blocks in a blockchain network is a desired feature but this prevents data or content that has been stored in arbitrary space from being deleted. This, when coupled with the requirement that all member servers store a copy of all the blocks, means that everyone has a copy of this material on their servers. Governments have begun to investigate crimes related to the currency use of blockchain networks, but as they adopt more networks themselves and as currency crimes become investigated, it will just be a matter of time before the network and its data are investigated.

IX. References

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation,* vol. 2, no. 6-10, p. 71, 2016.

[2] F. D. Administration, "FDA takes new steps to adopt more modern technologies for improving the security of the drug supply chain through innovations that improve tracking and tracing of medicines," ed, 2019.

[3] "Bitcoin Developer Reference." (accessed 2019).

[4] X. Xu *et al.*, "A taxonomy of blockchain-based systems for architecture design," in *2017 IEEE International Conference on Software Architecture (ICSA)*, 2017: IEEE, pp. 243-252.

[5] R. Matzutt *et al.*, "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin," in *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer*, 2018.

[6] cryptograffiti. cryptograffiti.info (accessed 2019).

[7] R. Matzutt, M. Henze, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Thwarting unwanted blockchain content insertion," in *2018 IEEE International Conference on Cloud Engineering (IC2E)*, 2018: IEEE, pp. 364-370.

[8] G. L. R. Center, "Regulation of Bitcoin in Selected Jurisdictions," ed: The Law Library of Congress, January 2014.

[9] D. o. t. T. F. C. E. Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," ed, March 18, 2013.
[10] "Bitcoin Improvement Proposals." https://github.com/bitcoin/bips (accessed 09, 2019).
[11] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," in *12th Student Conference on Managerial Science and Technology*, 2015.
[12] R. Matzutt, O. Hohlfeld, M. Henze, R. Rawiel, J. H. Ziegeldorf, and K. Wehrle, "Poster: I don't want that content! on the risks of exploiting Bitcoin's blockchain as a content store," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016: ACM, pp. 1769-1771.
[13] A. Sward, I. Vecna, and F. Stonedahl, "Data insertion in Bitcoin's Blockchain," *Ledger,* vol. 3, 2018.
[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017: IEEE, pp. 557-564.
[15] Rui Zhang, Rui Xue, Ling Liu. "Security and Privacy on Blockchain. ACM Computing Surveys," Vol. 1, No. 1, January 2019.
[16] James Clavin, Sisi Duan, Haibin Zhang, Vandana P. Janeja, Karuna P. Joshi, Yelena Yesha, Lucy C. Erickson, and Justin D. Li. 2020. "Blockchains for Government: Use Cases and Challenges. Digit." Gov.: Res. Pract. 1, 3, Article 22 (November 2020), 21 pages. https://doi.org/10.1145/3427097