Xu, Jennifer J.

Article

Are blockchains immune to all malicious attacks?

Financial Innovation

Provided in Cooperation with:
Springer Nature

Suggested Citation: Xu, Jennifer J. (2016) : Are blockchains immune to all malicious attacks?, Financial Innovation, ISSN 2199-4730, Springer, Heidelberg, Vol. 2, Iss. 25, pp. 1-9, https://doi.org/10.1186/s40854-016-0046-5

This Version is available at:
https://hdl.handle.net/10419/176438

Xu *Financial Innovation* (2016) 2:25
DOI 10.1186/s40854-016-0046-5

Financial Innovation

RESEARCH Open Access

Are blockchains immune to all malicious attacks?

Jennifer J. Xu

Correspondence: jxu@bentley.edu
Bentley University, Waltham, MA 02452, USA

Abstract

Background: In recent years, blockchain technology has attracted considerable attention. It records cryptographic transactions in a public ledger that is difficult to alter and compromise because of the distributed consensus. As a result, blockchain is believed to resist fraud and hacking.

Results: This work explores the types of fraud and malicious activities that can be prevented by blockchain technology and identifies attacks to which blockchain remains vulnerable.

Conclusions: This study recommends appropriate defensive measures and calls for further research into the techniques for fighting malicious activities related to blockchains.

Keywords: Blockchain, Online malicious attacks, Fraud detection, Hacking prevention

Introduction

Blockchain, an innovation by FinTech, has attracted considerable attention since its origin as a technology to enable bitcoin-based online transactions (Pilkington 2016; Sundararajan 2016). Although bitcoin is a controversial form of digital currency facing skepticism and distrust (Hur et al. 2015) and its legal, social, and economic impacts have been inadequately studied (Mainelli and Smith 2015), blockchain technology is acknowledged for its advantages in recording transactions and events. Many believe that blockchain, similar to the Internet, will revolutionize how people and organizations will manage transactions and assets (Swan 2015).

Blockchain technology enforces a distributed consensus and cryptographic transactions, rendering it difficult to compromise the integrity of its records without being noticed by an entire network. Many advocates believe that it can completely prevent such malicious activities as double-spending and hacking (Baxter 2016; Camp 2016). However, others still remain skeptical.

This paper answers the question of *what can blockchain technology do and not do to fight malicious online activity*. Section 2 defines the characteristics and innovative applications of blockchain technology. Section 3 reviews state-of-the-art technologies for detecting online fraud and intrusion. Sections 4 and 5 explore the types of frauds and attacks that blockchain technology might prevent and behaviors to which it remains vulnerable. Section 6 recommends anti-attack measures and the last section calls for new research on how blockchains can fight online malicious attacks.

Background

A blockchain is essentially a public ledger of transactions or events recorded and stored in chronologically- and linearly-connected blocks. Later blocks then maintain the hash of previous blocks (Crosby et al. 2016). Blockchain technology is best described as one that enables records to be "shared by all network nodes, updated by miners, monitored by everyone, and owned and controlled by no one" (Swan 2015, p. 1). Nodes are users' computers or mobile devices. Miners are nodes with extensive computational resources that can be used for transaction validation purposes. Figure 1 illustrates the process of fund transfer using blockchain technology. Blockchain has been regarded as one of the most important disruptive computing paradigms after the Internet (Crosby et al. 2016; Pilkington 2016; Swan 2015). Several unique characteristics make it a breakthrough technology for registering, verifying, and managing transactions.

Distributed consensus

With the traditional data-management infrastructure, transactions between a party (e.g., an individual or organization) and others often are recorded and stored in data repositories maintained and controlled by the particular party or by central authorities (e.g., government agencies, banks). The integrity of the data, to a large extent, depend on the data management capability and functionality of the repository.

Unlike this centralized approach, a blockchain registers and stores transactions in a peer-to-peer network. Each network node maintains an identical copy of the blockchain. No global repository stores this public ledger, that is, a blockchain is completely distributed. When a new transaction occurs between two parties in the network, it is broadcasted network-wide; and the network's community of miners examines and verifies it. Only after this collective verification can a new block containing the transaction be added to the end of the blockchain. Individual copies of the blockchain stored in all network nodes are refreshed and updated simultaneously and consensus is achieved by synchronizing all copies. Thus, a blockchain is "shared by all network nodes, updated by miners," and "owned and controlled by no one" (Swan 2015, p. 1).

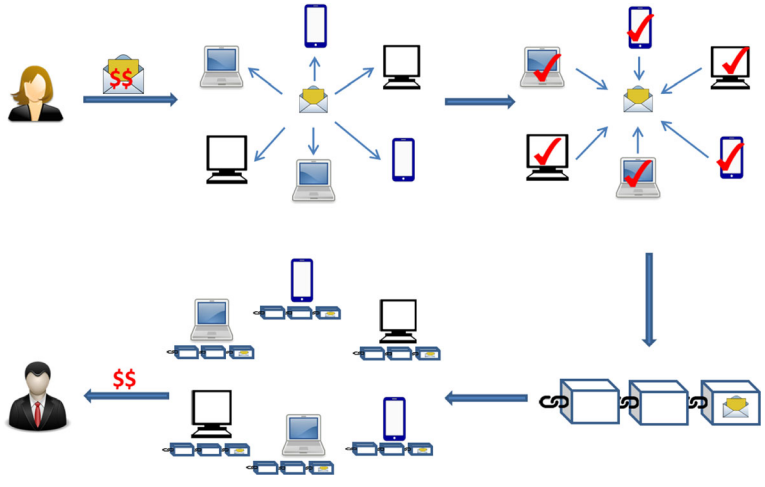

Fig. 1 The process of fund transfer (Adapted from (Wild et al. 2015))

Trustless

Traditionally, online transactions often are carried out with the help of an intermediary or central authority that validates, safeguards, and preserves them (Crosby et al. 2016). For example, when one individual transfers funds to another, a third party, such as a bank, assures that the individual willing to transfer funds has sufficient funds to do so (Wright and De Filipp 2015). With blockchain technology, each transaction is collectively verified and validated by miners, eliminating intermediaries. No party needs to trust the other, because transactions unfold before the entire network, making deception almost impossible. In this sense, blockchain technology facilitates trust-free transactions.

Cryptographic

Distributed, trustless consensus is impossible without the cryptographic mechanism embedded within the blockchain. Blockchain was originally used to track bitcoin transactions. Bitcoin and other digital currencies are called cryptocurrency in that transactions involving them are secured by cryptography. With a blockchain, all transactions are encrypted using public-private key pairs.

For example, people use bitcoin eWallets to transfer funds. An individual who wishes to transfer bitcoins creates a message containing information about the amount and the recipient's eWallet address, akin to sending an email. The message is encrypted using the sender's private key and then broadcasted to the entire network. Miners use the public key published by the sender to recover the content of the message, compare the amount with the sender's most recent balance recorded in the blockchain, and examine the validity of the transfer. If the message is valid, the transaction is executed, and the block containing it is appended to the end of the blockchain. Altered, hacked, or intercepted messages are deemed invalid and the transaction rejected.

Transactions stored in a blockchain are anonymous and irreversible. Although parties in the network release no private information, their transactions are traceable and visible network-wide. Transactions registered and added to the blockchain cannot be modified or "rolled back."

Blockchains can be used to register, record, and transfer tangible (e.g., houses and cars) and intangible (e.g., music, copyrights, and patents) assets (Crosby et al. 2016; Swan 2015). One promising application of the blockchain technology is smart contracts (Crosby et al. 2016; Kosba et al. 2016). Smart contracts are autonomous, self-sufficient, decentralized agreements controlled by programming codes that execute automatically under certain conditions (Swan 2015). For example, a smart contract might pay a service provider automatically once work is complete. Blockchain may also be applied in a wide range of other domains such as IoT (Internet of Things), real estate, supply chain management, insurance, healthcare, and sports management (CB Insights 2016).

Because blockchain technology enables decentralized, trustless, encrypted transactions and events to be recorded and stored publicly, optimists believe it can prevent online fraud and attacks (Camp 2016; Freedzai 2016). Others express reservations (Zafar 2016). To assess these capabilities of blockchain technology, we first check existing techniques for battling malicious attacks in cyberspace.

Malicious online activities

Any asset, property, or resource can be attacked. Maliciousness on the Internet spans identity theft, fraud, and network or system intrusions (e.g., hacking, viruses, and malware). Online fraud, identity theft, and hacking are particularly relevant to blockchain-supported exchanges.

Fraud is a type of malicious activity intended to obtain advantage or benefit by deceiving others. Fraud may cause serious consequences and losses to its victims and has long concerned the financial industry. Phua et al. (2010) categorized four types of financial fraud: internal, insurance, credit, and telecommunication. Internal fraud refers to behaviors such as fraudulent reporting of a company's business activities and financial status; insurance fraud occurs when one files fraudulent health or property claims; credit transaction frauds are often seen in credit card related transactions and mortgage loan applications; and telecommunication fraud may involve activities that are intended to illegally acquire money from telecommunication service providers or their customers. Among these, the most frequently studied is credit card fraud.

The benefits of cyberspace-low entry barriers, user anonymity, and spatial and temporal separation between users-make it a fertile field for deception and fraud (Xiao and Benbasat 2011). As economic exchange becomes increasingly Internet-based, online fraud increases. For example, on eBay, the largest online auction platform in the United States, sellers and buyers might commit fraud (Gavish and Tucci 2008). Seller fraud includes shilling, misrepresenting products, counterfeiting, and triangulation. Buyer fraud includes payment defaults and bid shielding.

Numerous techniques have been proposed and used to identify fraudulent transactions and activities that deviate from regular patterns of behavior. Common outlier analysis methods include supervised classifications such as decision trees, support vector machines, genetic algorithms, Bayesian belief networks, and neural networks. For example, neural networks and genetic algorithms were used to detect credit card fraud in a dataset covering 13 months and 50 million credit card transactions (Paasch 2008). Unsupervised methods, such as clustering analysis, have been used to identify financial fraud (Sabau 2012) or to filter fake online product reviews and ratings on e-commerce websites (Akoglu et al. 2013).

Hacking and intrusions "attempt to compromise the confidentiality, integrity or availability of a resource" (SANS 2016). These activities may attack computer networks and individual systems. Intrusion detection techniques include signature-based and anomaly-based. Signature-based techniques compare behaviors against pre-defined behavioral profiles (signatures). Anomaly-based methods resemble outlier analysis. They compare observed activities with previously gathered baselines of normal activity to detect unusual or suspicious activities.

Fraud and attack prevention using blockchain

Blockchain technology impedes two specific types of online malicious activities: *double-spending* and *record hacking*.

Double-spending occurs when someone makes more than one payment using one body of funds (e.g., a quantity of bitcoins). This is possible in a peer-to-peer network because there may be propagation delays when pending payments are broadcast to the network or the network's many nodes receive unconfirmed transactions at different

times. Blockchain tackles this problem by requiring miner nodes to solve a complex mathematical problem ("mining") in order to verify the transaction. The complexity of the computation is adjusted so that, on average, it takes 10 min to solve a problem using the miners' processing powers (Crosby et al. 2016). Because only blocks with correct answers to the mathematical problem (the proof-of-work) can be added to the blockchain, only one among multiple payments is accepted and registered on the blockchain, making it almost impossible for parties to double-spend funds.

Centralized data-storage and management systems are susceptible to hacking, intrusion, and breaches, but blockchain's distributed consensus mechanism prevents hacking (Freedzai 2016). Each transaction must be verified by the community of miners, leaving fraudulent transactions unable to pass collective verification and validation. Because the blockchain is constantly monitored by the entire network of nodes, each of which maintains a copy of the blockchain, malicious users have no means of inserting fraudulent blocks into the public ledger without immediately being noticed by others. Thus, it is impossible to compromise the integrity of records in the blockchain. Even if one or several of the ledgers are hacked, the large number of other network copies provide reliable backup and overwrite the hacked version.

Blockchains can prevent fraud involving assets (e.g., gemstones and art) other than currency and credit (Donnelly 2016). For example, by registering and tracking all transactions (e.g., trading, financing, insurance) involving a piece of art and recording its attributes, it becomes more difficult to replace the original with counterfeits. Moreover, smart contracts can be used as escrow (Buntinx 2016) to ensure transacting parties comply with contracts, reducing defaults by buyers or poor service by providers.

In addition, because of the absence of the third-party intermediary or central authority, which itself may suffer from corruptive, fraudulent, malicious, or illegal activities originated from inside, the trustless feature of blockchain reduces the risks and possible losses attendant to third-parties.

Potential risks for blockchain

Although blockchain technology prevents several types of malicious attacks and reduces many associated risks, it does not eliminate all attacks. Its preventative mechanisms (e.g., distributed consensus, cryptography, anonymity) may impair its resistance to other types of frauds and maliciousness. These include the 51% attack, account takeover, digital identity theft, money laundering, and hacking.

The 51% attack

A 51% attack may occur when a single miner node, which happens to have exceptionally more computational resources than the rest of the network nodes, dominates the verification and approval of transactions and controls the content of a blockchain. As it possess more than half (51%) of the network's processing power, the dominant node can outpace all other nodes, manipulate the blockchain, insert fraudulent transactions, double-spend funds, or even steal asset from others. Although no 51% attacks have occurred in the bitcoin network since January 2009, when the first genesis block was created and added to the blockchain (Crosby et al. 2016; Sundararajan 2016), the risk does exist, especially in blockchains with small networks (Swan 2015).

Identity theft

Although blockchains preserve anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If one's private key is acquired or stolen, no third party can recover it. Consequently, all the assets this person owns in the blockchain will vanish, and it will be nearly impossible to identify the thief. The consequences may be more devastating than identity theft in the offline world, where third-party institutions (e.g., credit card companies) or central authorities safeguard transactions, control risks, detect suspicious activities, or help find culprits. Also, current cryptography standards are not completely uncrackable (Swan 2015). With the advent of quantum computing, it is not impossible for cryptographic keys to be cracked quickly, demolishing the foundation of blockchain technology (Crosby et al. 2016).

Illegal activities

Blockchain technology can become a venue for illegality. The Silk Road website is an online marketplace where anonymous sellers and buyers of illegal drugs do business using bitcoins (Hong 2015). Cryptocurrency that uses blockchain technology may also facilitate money laundering. Although bitcoin is not yet treated as a fiat currency, it makes it possible to create an "underground" channel for illegal movement of funds within its network.

System hacking

It is difficult to hack and alter records stored in a blockchain, but not the programming codes and systems that implement its technology. MtGox, once the largest Tokyo-based bitcoin exchange, was hacked in March 2014, and bitcoins worth $700 million were stolen. Poorly-maintained and outdated codes allowed malefactors to double-spend (Bitcointalk 2014). A more recent incident afflicted a DAO (Decentralized Autonomous Organization) that holds large quantities of Ethereum, a cryptocurrency similar to bitcoins (Price 2016). The hacker exploited a software vulnerability and stole $50 million worth of Ethereum.

Recommendations and future work

Distributed consensus, trustlessness, anonymity, cryptography, and numerous features highlight the innovativeness of blockchain technology in its bookkeeping and attack prevention capabilities. However, blockchain is not completely immune to all sorts of fraud, hacking, attacks, and other malicious activities. The technology is still evolving and maturing as more people and organizations learn, experiment with, and accept it. The following recommendations identify ways to enhance its robustness, anti-fraud, and anti-hacking capabilities.

Detection technologies

Although blockchain technology prevents fraudulent behaviors, it cannot detect fraud by itself (Ngo 2016). Malefactors may find unforeseen ways to steal funds and commit fraud. Although blockchain developers are strengthening its technology, innovative techniques and methods are needed to detect attacks. Existing techniques using

machine learning and data-mining algorithms may find new applications in detecting fraud and intrusions in blockchain-based transactions. By profiling, monitoring, and detecting behavioral patterns based on people's transaction histories, supervised machine learning approaches, such as deep-learning neural networks, support vector machines, and Bayesian belief networks may help detect outlier behaviors.

Identity and reputation blockchains

Cryptographic keys and anonymous transactions make blockchain vulnerable to account takeover and digital identity theft because an identity is protected only by its private key. Loss of a key means loss of identity on the network. One solution is to build an identity and reputation system using a blockchain that records "fingerprint" events (Baxter 2016; Nordseth 2016). Instead of recording the personal identifiers customarily used offline (e.g., social security number, birth certificate, passport), the blockchain may track life events (e.g., births, schooling, acquiring student loans, opening bank accounts, buying cars, or purchasing homes). These events recorded in the irreversible identity blockchain become a digital identity that is difficult to steal because it is unforgeable, time-stamped, and publically monitored.

Regulation and law

With an absent central authority and the autonomy enabled by its distributed consensus feature, blockchain may eliminate the administrative functions of government agencies (Swan 2015). However, anarchy may propagate maliciousness and illegality. Bitcoin, for example, falls under multi-jurisdictional laws and regulations, and criminals can exploit jurisdictional gaps between countries (Wright and De Filipp 2015). Agencies, lawmakers, and legislatures should understand, investigate, and examine the mechanisms and impacts of blockchain technology and cooperatively develop and implement laws, policies, and regulations to govern the use of blockchain technology. Doing so may ensure the security and functioning of the emerging peer-to-peer economy that has spawned innovative business models (Sundararajan 2016).

Wide adoption

Even if blockchain technology becomes sufficiently robust to prevent attacks and malicious activities, widespread adoption is essential for its full effectiveness (Hur et al. 2015). In other words, any mechanisms and protections inherent in the technology cannot work unless it is widely accepted and adopted by the majority of the society. The technology itself is not able to create a "maliciousness-free" business world. While only a small percentage of transactions are taking place and recorded in blockchains, fraudsters, malefactors, and criminals can still acquire what they want through other channels. Therefore, widespread adoption is essential for successful prevention of fraud and other types of attacks (Swan 2015).

Table 1 provides a summary of the varieties of malicious attacks to blockchain and the potential tactics and strategies that can be employed to battle them.

Table 1 Malicious attacks to blockchain and defensive measures

Malicious Attack	Definition	Defensive & Preventive Measures
Double Spending	An individual makes more than one payment using one body of funds.	The complexity of the mining process
Record Hacking	Records in the ledger are modified or fraudulent transactions are inserted into the ledger.	Distributed consensus
51% Attack	A single miner node with more computational resources (51%) than the rest of the network nodes dominates the verification and approval of transactions.	Detection techniques; wide adoption of the blockchain technology
Identity Theft	The private key of an individual is stolen.	Identify and reputation blockchains
Illegal Activities	Parties transact illegal goods or commit money laundering.	Detection techniques; laws and regulations
System Hacking	The programming codes and systems that implement a blockchain are compromised.	Robust systems and advanced intrusion detection methods

Conclusion

This paper has introduces the blockchain technology and its defining characteristics, reviews the state-of-the-art technologies for detecting online fraud and intrusions, identifies certain fraud and malicious activities that the blockchain technology can effectively prevent, and makes recommendations for strategically fighting various attacks to which blockchain may be vulnerable. Further research is needed to improve the technology and related anti-attack measures.

Acknowledgements
I would like to thank Dr. Leon J. Zhao for his ideas and thoughts on the topic.

Competing interests
The author declares that she has no competing interests.

Received: 2 November 2016 Accepted: 30 November 2016
Published online: 10 December 2016

References

Akoglu L, Chandy R, Faloutsos C (2013) Opinion fraud detection in online reviews by network effects. In: Proceedings of the 7th International AAAI Conference on Weblogs and Social Media. The AAAI Press, Palo Alto, pp 2–11
Baxter A (2016) Blockchain-Unchaining the world from fraud?., http://www.thepaypers.com/expert-opinion/blockchain-unchaining-the-world-from-fraud-/763845. Accessed Oct 2016
Bitcointalk (2014) List of bitcoin heists., https://bitcointalk.org/index.php?topic=576337#post_silk_road_2_incident. Accessed Oct 2016
Buntinx JP (2016) Ebay can stop fraud overnight using the blockchain., https://news.bitcoin.com/ebay-can-stop-fraud-overnight-using-blockchain/. Accessed Oct 2016
Camp C (2016) Bitcoin may help criminals, but blockchain can help thwart fraud., http://www.americanbanker.com/bankthink/bitcoin-may-help-criminals-but-blockchain-can-help-thwart-fraud-1080937-1.html. Accessed Oct 2016
Crosby M, Nachiappan Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: Beyond bitcoin. Appl Innov Rev 2:6–19
Donnelly J (2016) Everledger plans clockchain database to combat art fraud., http://www.coindesk.com/everledger-announces-partnership-vastari-combat-art-fraud/. Accessed Oct 2016
Freedzai (2016) Nasdaq uses blockchain-based technology to reduce risk and prevent fraud., http://feedzai.com/blog/nasdaq-uses-blockchain-based-technology-to-reduce-risk-and-prevent-fraud/. Accessed Oct 2016
Gavish B, Tucci CL (2008) Reducing internet auction fraud. Commun ACM 51(5):89–97
Hong N (2015) Silk road creator found guilty of cybercrimes. Wall St J 4:2015
Hur Y, Jeon S, Yoo B (2015) Is bitcoin a viable e-business? Empirical analysis of the digital currency's speculative nature, Proceedings of The 36th International Conference on Information Systems. Association for Information Systems, Fort Worth
Insights CB (2016) Banking is only the start: 20 big industries where blockchain could be used., https://www.cbinsights.com/blog/industries-disrupted-blockchain/. Accessed Oct 2016
Kosba A, Miller A, Shi E, Wen Z, Papmanthou C (2016) Hawk: The blockchain model of cryptography and privacy-perserving smart contracts, Proceedings of IEEE 2016 Symposium on Security and Privacy., pp 839–858
Mainelli M, Smith M (2015) Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers. J Financ Perspect 3(3):1–44

Ngo D (2016) How blockchain technology can enhance fraud detection., http://coinjournal.net/how-blockchain-technology-can-enhance-fraud-detection-interview-with-feedzais-cto/. Accessed Oct 2016
Nordseth G (2016) Blockchain: Identity revolution or evolution?., https://www.signicat.com/eid/blockchain/. Accessed Oct 2016
Paasch C (2008) Credit card fraud detection using artificial neural networks tuned by genetic algorithms. Hong Kong University of Science and Technology, Dissertation
Phua C, Lee V, Smith K, Gayler R (2010) A comprehensive survey of data mining-based fraud detection research., Available at https://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf. Accessed Oct 2016
Pilkington M (2016) Blockchain technology: Principles and applications. In: Olleros FX, Zhegu M, Elgar E (eds) Handbook of Research on Digital Transformations. Edward Elgar, Cheltenham
Price R (2016) Digital currency Ethereum is cratering because of a $50 million hack., http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6?r=UK&IR=T. Accessed Oct 2016
Sabau AS (2012) Survey of clustering based financial fraud detection research. Inf Econ 16(1):110–122
SANS (2016) IDFAQ: What is intrusion detection?., https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1. Accessed Oct 2016
Sundararajan A (2016) The Sharing Economy. The MIT Press, Cambridge
Swan M (2015) Blockchain: Blueprint for a New Economy. O'Reilly, Beijing
Wild J, Arnold M, Stafford P (2015) Technology: Banks seek the key to blockchain. Financ Times 1:2015
Wright A, De Filipp P (2015) Decentralized blockchain technology and the rise of lex cryptographia, SSRN., https://ssrn.com/abstract=2580664.
Xiao B, Benbasat I (2011) Product-related deception in e-commerce: A theoretical perspective. MIS Q 35(1):169–196
Zafar S (2016) Can blockchain prevent cybercrime?., https://www.finextra.com/blogposting/13032/can-blockchain-prevent-cybercrime. Accessed Oct 2016