An Overview of the Security Aspects of the Blockchain

COMP116-Introduction to Computer Security

Mentor: Ming Chow

Author: Feiyu Lu

Feiyu.lu@tufts.edu

Dec.14, 2016

Abstract

This paper will discuss how some network security issues can be solved or improved with Blockchain. It will briefly describe what is blockchain and its advantage comparing to TCP/IP and why it has benefits of transparency and immutability. Then I will discuss the security aspects of some applications based on blockchain in areas like money transaction, personal information, electronic voting. Finally, I will write about the problems and challenges of Blockchain security, and potential solutions.

Introduction

Blockchain is a distributed file system where participants keep copies of file and agree on changes by consensus. This file is composed of blocks, where each block includes a cryptographic signature of the previous block, creating an immutable record. Systems built on blockchain are considered safer than the current ones built on the internet infrastructure based on TCP/IP.

However, blockchain does have technology challenges related to scalability, latency, performance and security. Also, blockchain has many operational problems. For example, logging and monitoring which are essential for enterprise environments, have not been addressed yet.

Besides that, application built on blockchain still can have security issues, even if blockchain is airtight. If one wants public accessibility, developers can put that in your application. Without a good design of features, applications can still be vulnerable and exploitable. For database, hackers can replicate the file to get their hands on confidential contract information.

In all, this paper will provide an overview of security of blockchain and its applications. The focus is not on crypto-currency like bitcoin but on other applications built on blockchain.

To The Community

Blockchain can be thought of as an abstraction of the fundamental mechanism of digital-currency like Bitcoin. This distributed abstraction can have many applications and be a solution for internet security, privacy and transparency in many specific scenarios. So, it is very important for the internet community to know about the applications of Blockchain and its impact on security. Unlike bitcoin as a type of currency, Blockchain is for the decentralization of markets more generally, and contemplates the transfer of many other kinds of assets beyond currency, from the creation of a unit of value through every time it is transferred or divided.

The key idea is that the decentralized transaction ledger functionality of the blockchain could be used to register, confirm, and transfer all manner of contracts and property. All financial transactions could be reinvented on the blockchain, including stock, private equity, crowdfunding instruments, bonds, mutual funds, annuities, pensions, and all manner of derivatives.

Public records, too, can be migrated to the blockchain: land and property titles, vehicle registrations, business licenses, marriage certificates, and death certificates. Digital identity can be confirmed with the blockchain through securely encoded driver's licenses, identity cards, passports, and voter registrations. Private records such as IOUs, loans, contracts, bets, signatures, wills, trusts, and escrows can be stored.

Applications in Identity Authentication

The need for blockchain based identity authentication is particularly salient in the internet age. While there exist somewhat imperfect systems for establishing personal identity in the physical world, in the form of Social Security numbers, drivers' licenses and even passports or national identity cards, there is no equivalent system for securing either online authentication of our personal identities or the identity of digital entities. Facebook accounts, now often used as login for different digital applications, and media access control (MAC) addresses, may come close, yet

both can hardly function as trustworthy forms of identification when they can be changed at will.

a. Online Identity

Several blockchain startups are looking to use blockchain for online identity. A ShoCard, for example, is a digital identity that protects consumer privacy. ShoCard strives to be as easy to understand and use as showing a driver's license; and simultaneously be so secure that a bank can rely on it. The key is that the ShoCard Identity Platform is built on a public blockchain data layer, so as a company it is not storing data or keys that could be compromised. According to ShoCard all identity data is encrypted, hashed and stored in the blockchain, where it cannot be tampered with or altered. A start-up in a similar vein that bridges the gap of both human and digital entities, is Uniquid. Uniquid allows for the authentication of devices, cloud services, and people. Uniquid's aim is to provide identity and access management of connected things, as well as humans, utilizing biometric information for the latter.

b. Ownership rights

Another important aspect of identity is the ownership rights. The strong consensus security offered by blockchain without the need for a central certifying authority renders it particularly suitable for the authentication of ownership rights. This includes digital property, intellectual property and physical property, including physical products and land. For example, Ascribe is a startup in this space. It describes itself as a "fundamentally new way to lock in attribution, securely share and trace where digital work spreads". Ascribe creates a permanent and unbreakable link between the creator and his or her creative work. By allowing ownership to be forever verified and tracked, Ascribe leverages blockchain technology to make it possible to transfer, cosign or loan digital creations similar to physical pieces of work. By preventing unauthorized access to creative work, Ascribe also helps creators monetize

their work.

c. Smart Property

The general concept of smart property is the notion of transacting all property in blockchain-based models. Property could be physical-world hard assets like a home, car, bicycle, or computer, or intangible assets such as stock shares, reservations, or copyrights (e.g., books, music, illustrations, and digital fine art).

The key idea of smart property is controlling ownership and access to an asset by having it registered as a digital asset on the blockchain and having access to the private key. Smartphones could unlock upon reaffirming a user's digital identity encoded in the blockchain. The doors of physical property such as vehicles and homes could be "smart-matter" enabled through embedded technology (e.g., software code, sensors, QR codes, NFC tags, iBeacons, Wi-Fi access, etc.) so that access could be controlled in real time.

Security Issues and Future Directions

One central challenge with the underlying Bitcoin technology is scaling up from the current maximum limit of 7 transactions per second (the VISA credit card processing network routinely handles 2,000 transactions per second and can accommodate peak volumes of 10,000 transactions per second), especially if there were to be mainstream adoption of Bitcoin. Some of the other issues include increasing the block size, addressing blockchain bloat, countering vulnerability to 51 percent mining attacks, and implementing hard forks (changes that are not backward compatible) to the code.

1. 51-percent Attack

There are some potential security issues with the Bitcoin blockchain. The most worrisome is the possibility of a 51-percent attack, in which one mining entity could grab control of the blockchain and double-spend previously transacted coins into his

own account. The issue is the centralization tendency in mining where the competition to record new transaction blocks in the blockchain has meant that only a few large mining pools control the majority of the transaction recording. At present, the incentive is for them to be good players, and some (like Ghash.io) have stated that they would not take over the network in a 51-percent attack, but the network is insecure. Double-spending might also still be possible in other ways—for example, spoofing users to resend transactions, allowing malicious coders to double-spend coins. Another security issue is that the current cryptography standard that Bitcoin uses, Elliptic Curve Cryptography, might be crackable as early as 2015. However, financial cryptography experts have proposed potential upgrades to address this weakness.

2. Compatibility

Another significant technical challenge and requirement is that a full ecosystem of plug-and-play solutions be developed to provide the entire value chain of service delivery. Ideally, the blockchain industry would develop similarly to the cloud-computing model, for which standard infrastructure components—like cloud servers and transport systems—were defined and implemented very quickly at the beginning to allow the industry to focus on the higher level of developing value-added services instead of the core infrastructure. That way, the blockchain industry's development can be hastened, without every new business having to reinvent the wheel.

3. the Need of a Decentralized Storage

There is a need for a decentralized ecosystem surrounding the blockchain itself for full-solution operations. In the case of file serving, the IPFS project has proposed an interesting technique for decentralized secure file serving. IPFS stands for Inter-Planetary File System, which refers to the need for a global and permanently accessible filesystem to resolve the problem of broken website links to files. In the area of archiving, a full ecosystem would also necessarily include longevity provisioning and end-of-product-life planning for blockchains. A blockchain archival system like the Internet Archive and the Wayback Machine to store blockchains is

needed. Not only must blockchain ledger transactions be preserved, but we also need a means of recovering and controlling previously recorded blockchain assets at later dates.

Conclusion

Blockchain holds the promise of enabling the “New Deal on Data”: a greater degree of personal ownership, control, and monetization of personal data, within a framework that allows society to bene t from data aggregation.

References

Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. N.p.: n.p., n.d. Print.

Swan, Melanie. Blockchain: Blueprint for a New Economy. N.p.: n.p., n.d. Web.

Korolov, Maria. "Is the Blockchain Good for Security?" CSO Online. CSO, 01 Apr. 2016. Web. 31 Oct. 2016.

Massachusetts Institute of Technology. Blockchain & Infrastructure (Identity, Data Security) (n.d.): n. pag. Web.

"Common Security Issues and Technologies." Distributed Systems Security(n.d.): 43-54. Web.

Wust, Karl. Security of Blockchian Technology, pp.2.

Clark, Jeremy. Financial Cryptography and Data Security. S.l.: Springer-Verlag Berlin An, 2016. Print.

G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," Security and Privacy Workshops (SPW), 2015 IEEE, San Jose, CA, 2015, pp. 180-184.