IT Risk Management Using Blockchain

1. Introduction

Blockchain Technology has its origins in the paper “How to Time-Stamp a Digital Document” published in 1991 by Stuart Haber and W. Scott Stornetta. But it came into limelight after the release of the whitepaper “Bitcoin: A Peer-to-Peer Electronic Cash System” by the pseudonymous author (Nakamoto, 2008) followed by the release of its implementation in 2009. Bitcoin gained popularity in no time as increasing number of people were willing to invest in bitcoin. It was the first cryptocurrency that allowed reliable financial transactions without the need of a trusted central authority, such as banks and financial institutions (Tschorsch & Scheuermann, 2016). Blockchain is the technology underlying the Bitcoin. Simply put, a blockchain is a cryptographically linked chain of blocks, each of which contains time-stamped records. It is a decentralized system where each user has the access to all records. The records stored on a blockchain are immutable and are verified by multiple parties through various consensus protocols. A blockchain has been described as a value-exchange protocol (Wikipedia). It has the potential to address the pressing issues in the exchange of digital assets such as Lack of Trust, Double-spending, Repudiation and Theft (including fraud). Blockchain Technology has the potential to change several other industries apart from the Finance industry. One of the fields that naturally pairs with blockchain is Information Technology. Almost every industry today - Healthcare, Pharmaceuticals, Agriculture, Automotive, Media, Finance, Manufacturing, Transportation, Government, Trade, Education has embraced Digitization and is dependent on the Information Technology industry. Digitization has revolutionized the way we transact, communicate and commute making it faster and more efficient. Digitization makes an industry more productive, but it also introduces risks and vulnerabilities. The IT risks introduced by Digitization include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods (Business Queensland). Such events have a negative impact on the company and affect its clients. Many solutions have been proposed to address various IT risks till date. But the risks still persist, a major reason being that many solutions rely on centralization. Blockchain has a decentralized structure. It is a type of distributed ledger. Each block is linked to the previous block by a cryptographic hash. Any tampering with one block causes all the further blocks in the chain to become invalid. This rigid infrastructure of blockchain has the potential to offer cybersecurity solutions to the threats faced by various components of Information Technology such as IoT devices, networks and data storage and transmission.

1. Information Technology risks

In the IT field, the most valuable asset is considered to be an individual’s data. This is a data-driven world. Companies request for the data of a customer which can help to enhance the services provided by the company. The users have no choice but to provide their data and hope that it is not being misused or shared with other parties.

Some of the main risks in the IT field are:

1. *Data Security:* Data Security risk is one of the most crucial risks in the IT field. Over the years, the number of data breaches and their magnitudes have increased exponentially. They are associated with the theft of medical information, account credentials, confidential emails, and other forms of sensitive information. A consumer has to face several consequences due to a data breach such as identity theft, fraudulent credit card activities and temporary account cancellations. One in three data breach victims later go on to experience an identity crime (Steve Turner). The average data breach now costs a company up to $3.92 million (IBM study). The aftermath of a data breach at a major organization is chaotic, with a fall in share prices of the company, underperformance for nearly a year and damage to the trust of its customers. 2019 witnessed some of the largest data breaches of the decade, including the data breaches at Equifax, Facebook, Instagram and many Healthcare organizations. In addition, there are several data breaches that go unnoticed by companies and uninformed to the public. Thus, there is a large room for improvement in the techniques currently being implemented to safeguard data.
2. *User Data Privacy:* Technology is evolving rapidly. Increasing amounts of data is being collected for enhancing user experience, but this has given rise to potentially serious privacy concerns. It is predicted that more than half of global enterprises currently using some form of cloud solutions will have adopted a full cloud strategy by 2021 (Brian Lee). This will lead to increased dependence on third-party providers for data storage and data privacy. Many businesses are embracing Artificial Intelligence to drive value through automation due to which there is collection of more data and hence increased privacy failures that arise with the creation of new types of metadata. Another area of concern is the weak security configurations of Internet-of-Things (IoT) devices. It is predicted that by 2025 the total installed base of IoT connected devices will be close to 75 billion. IoT technology increases the number of access points multiplying the risks of compromise of personal information.
3. *Cloud computing:* It is predicted that by 2025 the amount of data worldwide will reach an overwhelming 175 zettabytes, almost 49% of which will be stored in public cloud environments.But cloud computing is faced with several serious issues of security, compliance, governance, migration, licensing and multiple cloud management. Examples of cloud data breaches include the 2018 Aadhar India National ID database breach which exposed the data of 1.1 billion citizens and the Cambridge Analytica accessing Facebook data to profile voters. There is heavy centralization in the cloud environment due to the dominance of the giants like Google Cloud, Amazon Web Services (AWS), Alibaba, IBM and others. This can have a huge impact as demonstrated by the [2018 cloud outage incidents](https://www.crn.com/slide-shows/security/300107391/the-10-biggest-cloud-outages-of-2018-so-far.htm) of Amazon Web Services (AWS), Google Cloud and Microsoft Azure. When an organization uses external cloud services, the data visibility and control gets reduced. Cloud Service Provider (CSP) APIs are accessible via Internet making them more vulnerable to attacks that lead to compromise of cloud assets. Other threats to cloud computing include failure of separation among multiple tenants, incomplete data deletion, infeasible migration from one CSP to another, unauthorized data access to insiders and accidental data deletion by the CSP. It is important to address these cloud computing risks to protect the enormous amount of data that we store on the cloud daily.

1. *IoT:* IoT devices collect user data to personalize user experience and provide utility to the users. The dark side of this increasing data collection is the possible creation of a virtual biography of user activities, exposing life style patterns and private information. Several intrinsic features of IoT amplify its security and privacy challenges including: lack of central control, heterogeneity in device resources, multiple attack surfaces, context-aware and situational nature of risks, and scale (Dorri, Kanhere, Jurdak). It is estimated that the total number of IoT connected devices in the world will be around 38.5 billion by the end of 2020 (Juniper Research). With the increase in number of IoT devices, there is an increase in the number of cyber-attacks and botnets. IoT devices have a weak security configuration due to which they fall victims to malware which allows the attacker to control the devices forming an IoT botnet. Attackers make use of such botnets to launch Distributed-Denial-of-Service (DDoS) attacks. Linux.Aidra, Bashlite, Mirai and IRCTelnet are some of the largest IoT botnets till date. The Mirai Botnet was responsible for DDoS attack on Dyn Server in 2016, it was the largest of its kind causing disruption of the internet service across US and Europe. Several solutions have been proposed but still security of IoT devices continues to be a pressing issue that needs to be addressed urgently.
2. *Trust:* The internet was not built with trust-building in mind (Rainne, Anderson). The two major players that influence online trust are Corporations and Attackers. Corporations are concerned about their users’ data security but their primary interests are not the same as those of their users. The attackers constantly invent new ways to break into a system and access unauthorized data. As the users become aware of the growing number of data breaches taking place, they become distrustful towards online services. However, most users continue to do online interactions as they make life easier. There is a belief among users that no one wants their data, they trust that the corporations will ensure data security and hence give in to risks. Lack of trust is a major issue in centralized systems. For example, in the Public Key Infrastructure (PKI), both the transacting parties must trust the Certificate Authority (CA) to sanction valid certificates for the exchange of digital assets in a secure way. When we make online payments, we need a trusted-third-party like a financial institution or central bank to complete the transaction. The trust between users and service providers will soon diminish as the number of data breaches, identity thefts and hacking incidents grow.
3. *Single Point of Failure (SPOF):* A single point of failure (SPOF) is a part of a system that, if it [fails](https://en.wikipedia.org/wiki/Failure), will [stop the entire system from working](https://en.wikipedia.org/wiki/Cascading_failure) (Wikipedia). Single Point of Failure is synonymous to Centralization. It threatens the availability and reliability of centralized systems. An example of low efficiency and risks introduced due to centralization is the antivirus agencies of today, which follow a centralized model. A small team is responsible for detecting all threats and malwares for their users. With the increasing number of users, this model puts a large burden on the team thus decreasing the efficiency of detecting threats and makes the user device vulnerable to malware. SPOF maybe be caused due to hardware, Internet Service Provider (ISP), an offsite data storage location like the cloud. People also constitute to SPOFs in many organizations. SPOFs provide the attackers an easy way in to the database of an organization. Another possibility is that an SPOF may get triggered accidentally due to human errors. In either case, there is a breakdown of the system causing the company to incur heavy loss in terms of capital as well as trust of its consumers.
4. Blockchain in IT Risk Management
5. Trust, single point of failure:

<https://stackoverflow.com/questions/45309100/how-to-avoid-the-fabric-ca-beeing-a-single-point-of-failure>

Let me try to answer the two questions also, perhaps a little more directly.

QUESTION1: if I understood correctly, every peer in a fabric blockchain network (somehow interconnected through gossip) will only accept incoming connections from other peers if they use a HTTPS connection with a public key signed by the Fabric CA. Is that correct?

ANSWER1: No, this is not correct. You said "the Fabric CA", but each fabric blockchain network has multiple trusted CAs where each may be a Fabric CA or another CA or a combination. There is no single trusted CA root in this model. Also, the connections from peers are over GRPC rather than HTTPS.

QUESTION2: So in my understanding, the Root-CA becomes the single point of failure because one could modify it and from then on modified Root-CA certificates will propagate to the nodes and eventually no node can connect to each other anymore. Is this correct?

ANSWER2: No, this is not correct. There is no SPoF (Single Point of Failure) because: a) a single Fabric CA can run in a cluster b) there are multiple Fabric CA clusters (or other CAs) in a blockchain network. c) the peers and orderers do not connect directly to a CA. They operate off of crypto material that is locally available from the file system or its copy of the ledger. There is also no SPoT (Single Point of Trust) because: a) their are multiple root CAs without a common root key, and b) configuration updates which affect who trusts whom may require signatures from multiple identities from different roots of trust. For example, changing a trust policy could require signature from an administrator from every organization in the blockchain (or in hyperledger terminology, in the channel).

1. Decentralization

<https://medium.com/hackernoon/what-huawei-teaches-us-about-single-points-of-failure-3fd4f5c32cf7>

“***The best time to start thinking about decentralization was 10 years ago, the next best time is now.***”

**Open Source ≠ Decentralization**

Despite popular beliefs, open source does not necessarily lead to decentralization. Google and their Android’s operating systems are a prime example of this. On one hand, Android enables companies around the globe to gain access to a fully modifiable operating system that they can customize for a wide variety of use cases and not have to develop it from scratch. On the other, it features essential Google services — a lack of which could be a deal breaker for the majority of users (especially outside of China). Additionally, these rely on software updates (including security ones) that are not included in the Android Open Source Project.

1. Analysis of the findings
2. Potential benefits
3. Challenges and open issues
4. Conclusion
5. References
6. <https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/>
7. <https://www.zdnet.com/article/these-are-the-worst-hacks-cyberattacks-and-data-breaches-of-2019/>
8. <https://chapters.theiia.org/san-diego/Documents/Seminars/SD_IIA___ISACA_Event_041112_Deloitte_IA_Top_Ten_Risks.pdf>
9. <https://en.wikipedia.org/wiki/Blockchain#History>
10. <https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html>
11. <https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/>
12. <https://www.pewresearch.org/internet/2017/08/10/theme-6-trust-will-diminish-because-the-internet-is-not-secure-and-powerful-forces-threaten-individuals-rights/>
13. <https://medium.com/polyswarm/why-blockchain-is-perfect-for-securing-our-expanding-online-world-971101ca7991>
14. Key-words (temporary section)
15. Data breach
16. Cloud computing risks
17. IT risks solved by Blockchain
18. Single point of failure risk blockchain