International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Blockchain Risk Assessment and Enterprise Management Framework

Vikash Kumar

Abstract: ***There is plenty of hype around blockchain technology, which is a concept having the potential to change business processes, enable new businesses, and even revolutionize the world economy. According to a recent study nearly two - thirds of large businesses are looking to deploy new blockchain projects. With Blockchain technology, the participants can interact directly and can make transactions across the internet without the interference of a third party. Such interactions through Blockchain will not share any personal information regarding the participants and it creates a transaction record by encrypting the identifying information. The most exciting feature of Blockchain is that it greatly reduces the possibilities of a data breach. In contrast with the traditional processes, in Blockchain there are multiple shared copies of the same data base which makes it challenging to wage a data breach attack or cyber - attack. With all the fraud resistant features, the block chain technology holds the potential to revolutionize various business sectors and make processes smarter, secure, transparent, and more efficient compared to the traditional business processes. At the core, changing the business process to use blockchain is not a simple task. It requires time, effort, and most importantly, a good investment to get started. Failure is not an option. If risk management is not done correctly, then you can lose resources, and also have a chance of project failure.***

Keywords: Blockchain Data Management, Blockchain And Risk, Risk Assessment, Bitcoin, Bitcoin Management, Data technology

1. Introduction

Enterprise Blockchain is all about risk management. That's why, in this article, we will be focusing deeply into the blockchain risk assessment.

Blockchain is a new technology, and not all enterprises or business knows how to successfully implement it. If your business is thinking of transiting to the blockchain, it has to do proper blockchain risk management before diving deep into it.

At the core, changing the business process to use blockchain is not a simple task. It requires time, effort, and most importantly, a good investment to get started. Failure is not an option. If risk management is not done correctly, then it is you can lose resources, and also have a chance of project failure.

Do not worry, as, in this article, we will explore proper blockchain risk assessment that will cover different parts of a blockchain project.

Blockchain Enterprise Risk Assessment and Management Framework

Before we dive deep into the idea of blockchain risk assessment, let's understand blockchain in short.

Blockchain is a decentralized peer - to - peer ledger. It brings multiple benefits, including efficiency, decentralization, distributed ledger, immutability, and irreversibility. With blockchain, companies can invest more time innovating, and less time managing. Blockchain also lets companies automate with smart contracts.

Smart contracts are equivalent to a legal contract. They provide the necessary tools to automate the network.

One more thing that is crucial to the success of the blockchain or distributed ledger technology (DLT) is the consensus method. Bitcoin utilizes Proof of Work (PoW), but it is not ideal for enterprise blockchain. For enterprises, there are many good alternatives, including Hyper ledger Fabric, Quorum, IBM blockchain, and others. In short, you can utilize the blockchain to gain substantial improvement in your business processes.

Is your enterprise ready for risks associated with blockchain?

Blockchain is undoubtedly one of the most innovative technology. It has also made risk practitioners change how they perceive risks using the technology. It is promising, and that's why risks are glaring than ever.

The focus right now is to minimize risks as much as possible. In some cases, it is possible to eradicate the risks associated with blockchain implementation completely. However, the risks are new, and there are many ways malicious actors can cause harm to the system. Not only that, but risks are also within the network itself.

For example, the enterprise needs a permissioned network to work flawlessly. Without a proper permission management system, it would become hard for enterprises to set up their blockchain solution. Permissions should be layered so that no critical information gets leaked. After all, the data is what distinguishes them, and any leak can make their market grasp lose.
But, the good news is that risk practitioners acknowledge that blockchain can act as a tool for migrating risks. It brings the features that no other technology ever bought before. The key integral part is decentralization. It makes blockchain as the facilitator of trust.

However, as an organization, your job is to ask key questions.

- Will blockchain bring risks to your organization?

- If it does? What types of risks will it bring?
- Are the risks associated with blockchain migratable?

Blockchain ensures better risk management but brings new risks that were not part of the system. On top of all these, the organization also needs to take care of the regulatory authorities that govern the enterprise or the decentralized networks. It is mandatory for the firms to follow the rules set by the regulatory authority on their blockchain - based business model.

Types of Blockchain and the risks that they bring

To better understand blockchain risk assessment or the risks of blockchain, we need to look at the types of blockchain.
Blockchain can be broadly divided into two types:

- **Permissioned blockchain:** This type of permissioned blockchain ensure that only selected participants can take part in the blockchain network.
- **Permissionless blockchain:** In this blockchain type, anyone can join and be part of the network.

When it comes to **permissionless blockchain,** it is easy to see the risks associated with it. There are no know your customer (KYC) associated with the users. Also, there is a need for miners to power the network and validate the transactions. Miners also bring their own set of risks — including **51% attack**. There is also a chance of money laundering, privacy issues, and scalability when it comes to permissionless blockchain. All of these risks makes it not fit for enterprise or financial institutes.

Permissioned blockchains, on the other hand, is safe from the drawbacks that permissionless blockchain brings. The first thing that you will notice is that there is no need for miners to run it. The lack of miners also means that there is no need for cryptocurrency. At the heart of a permissioned network, some nodes are capable of validating transactions — making it ideal for closed blockchain networks. But, to make the network functional, a different type of consensus algorithm is required.

Permissioned based blockchains also have no issues when it comes to privacy and scalability. No one can know who is part of the network other than the administrators. This is crucial for the long - term success of an enterprise blockchain. Also, if there is suspicious activity, it can be quickly handled by the security team — considering that they have the maximum information about the network.

Smart Contracts and their role
Smart contracts are what makes businesses take advantage of blockchain. After all, it is where business logic is encoded. Without it, there would not be any proper way of automating business processes. They are capable of processing information and execute themselves once a condition is met. This also makes them the number one target for malicious actors.

To ensure that smart contracts are planned and executed correctly, the enterprise needs to ensure proper testing of smart contracts. The idea is to mitigate risk with thorough testing.

For institutes, it is necessary to understand all the associated risks and act accordingly. If not done correctly, it can lead to loss of data and other risks.

Risk considerations that you should consider
To give you a clear picture, we will be considering risks under broad risk categories. They will define what needs to be done. The four main risk considerations include the following

- Standard risk considerations
- Smart contract risk considerations
- Value transfer risk considerations

Standard Risks
Standard risk considerations are risks that are considered common to all the blockchain projects. They are about general risks. Let's go through the blockchain risks below:

Business continuity risk
One of the common blockchain business risks is business continuity risk. As a business, you need to cope with ever - changing governance and regulations. It is also required to equip the business process with all the necessary protection against cyber attacks. To resolve the issue, the firm needs to have proper continuity plans and have a short response time when the need arises.

Strategic Risk
Another standard risk of blockchain is strategic risks. Blockchain is not a universal solution. It is not everyone. However, some firms believe that they need to change to blockchain to have a competitive edge. But, in reality, there is no need to do so. Blockchain is still a new technology, and hence require time to mature. Apart from the fact that it is new technology, businesses also need to take note of how the entities will impact once changed to the blockchain. It is also necessary to learn the limitations it will bring to the product/service ecosystem.

Information security risk
Just like any other technology, blockchain is also not free from information security risk. It provides better internal security when it comes to cryptography or distributed database. But, things can go wary when we take the account or wallet security into account. The ownership of the account can be taken over by malicious actors. Blockchain is also not 100% secure and is vulnerable to attacks.

Reputational risk
Reputational risk comes in when companies fail to integrate blockchain to their legacy system. If not done correctly, it can result in poor customer experience — and can easily hamper the reputation of the company.

Regulatory risk
Regulations have always been the number one issue among companies as they look to adopt new technology. With each government or authority having their own regulations, it becomes hard for global companies to manage those regulations and act within them. The main risks include cross - border transactions. In this use - case, companies need to manage data and privacy protection. FINRA – a regulatory body, wants all the deals to follow the rules,

regulations, state law when trading securities. Not only it affects companies, but it also affects the core idea behind distributed ledger technologies.

Operational and IT risks
Changing from standard operating procedures and policies can be a daunting and risky task. The change also needs to encompass the business new processes. The IT team also needs to take care of the scalability, interface, and speed.

Supplier risks
As it is not practically possible for most businesses to implement end - to - end blockchain solution, the business also exposes itself to third - party vendor associated risks.

Contractual risk
Contractual risk is mainly concerned with how the service - level agreements (SLAs) within the nodes and administrator. Smart contract risks. Smart contracts are at the core of any enterprise blockchain. It helps businesses automate or transform the business logic into reality. They can be used to do financial and legal agreements within the network. Their complexity and importance bring in blockchain business risks with it. After all, it is all about mapping the business logic digitally. Let's take a look at the blockchain risk assessment related to smart contracts.

Business/Regulatory Risks
Smart contracts offer a way to encode legal, economic, or business logic within the parties. Once done, they work seamlessly throughout the network and ensure that everyone can take advantage of it. However, due to regulatory issues, smart contracts should also be equipped with the exception handling. The need for exceptional handling means more risk. And, that's why the smart contracts need to be thoroughly tested across multiple networks, regulations, and other constraints or environment that it needs to be executed.

Legal Risks
Smart contracts also bring in a legal liability issue. As permissioned networks take advantage of a closed - decentralized approach, there is no proper approach on whom to blame when things go wrong. Would that be an admin or the engineers who programmed it? Also, disagreement between nodes can lead to people leaving and crippling the network of the necessary resources.

Information security risks
Smart contracts if not coded properly, can lead to security risks, including breaches by external or internal nodes. The solution is to have a proper amendment to fix smart contracts — and stop any node to utilize the glitch. Furthermore, attention needs to be given to incidents when they happen. To make sure that glitches are found and resolved quickly, a proper incident management process should be implemented. Lastly, care needs to be taken for external entities as they can trigger internal smart contracts by sending wrong or misleading data.

Value transfer risks
With decentralization, peers can now transfer information without the need of any central authority. This new approach has the ability to change how businesses operate, but not without risks. Let's check out the blockchain risk assessments that come along with the peer - to - peer information exchange.

Consensus methods risk
Consensus methods risk is at the core of any blockchain platform. Any transactions happening in the network is completed according to the consensus method choose. Consensus method also utilizes a cryptographic protocol. These consensus methods bring their own associated risk. For example, in a BFT algorithm, it is required for parties to agree on the system membership. Other consensus algorithms have their own problems.

Data confidentiality risk
When it comes to the public blockchain, it is easy to know the transactions in the network. But, when it comes to permissioned networks, the hashed format is used to convey results. But the hashed format reveal information about the nature of the transaction and the participants — which is not ideal in every use - case out there.

Liquidity issue
DLT always brings liquidity issues. Not all crypto or assets within the network have demanded all the time. On top of that, there is always the chance of a dispute — which means more liquidity risks.

Key management issue
Even though DLTs are very secure when it comes to securing stored data — the main issue happens when the users do not protect their private keys. This means that there is always a risk of private keys being stolen. As an enterprise or business, you need to educate users on how to keep their private keys safe.

10 enterprise Blockchain Implementation Risks to Consider
According to OWASP, here are the top 10 web application security risks. We think you should also consider them when it comes to blockchain implementation.

1) Improper Logging & Monitoring
2) Insecure Deserialization
3) Sensitive Data Exposure
4) Cross - Site Scripting (XSS)
5) Injection
6) Security Misconfiguration
7) XML External Entities (XXE)
8) Broken Access Control
9) Using components with vulnerabilities
10) Broken Authentication

BCH Global has also covered a webinar that discusses the blockchain security risks. They have also covered other risks associated with blockchain. For example, in smart contracts & blockchain specific vulnerabilities, there are risks of denial of service, race conditions, timestamp dependence, and so on.

2. Conclusion

This leads us to the end of our blockchain risk assessment. We covered blockchain business risks in detail, including blockchain compliance risks, blockchain cyber risk,

blockchain regulatory risk, and so on. You should also check out the Blockchain risks every CIO should know. It is an interesting take on the risks associated with blockchain.

There is no doubt that more focus needs to be given to the blockchain risk management plan. For that, enterprises need to have proper training on the blockchain. Most of the time it is the lack of knowledge that brings in unwanted risks.