Chapter 5
Blockchain Risk and Uncertainty in Automated Applications

Devesh Kumar Srivastava
SCIT, Manipal University, Jaipur, India

Saksham Birendra Bhatt
SCIT, Manipal University, Jaipur, India

Divyangana
SCIT, Manipal University, Jaipur, India

ABSTRACT

Blockchain could be called a string of blocks that acts like a ledger that is also distributed. Members in a defined P2P network are given access to the blockchain and can create new blocks. When the data is stored in a blockchain, changing it becomes virtually impossible. The data stored within blocks is time-stamped to avoid tampering. Blockchain has applications in numerous fields like IoT, digital currency, financial services, reputation systems, smart contracts, security services, etc. If any virtual or real asset transaction is happening online, blockchain technology can be easily applied to optimize and secure the transaction better. Blockchain-based applications bring controversies, and yet many exceptional and diverse use-cases have been found for blockchain in both financial and non-financial sectors. Although it holds immense promise, it doesn't come without risks and uncertainties. This chapter elucidates the growing risks and uncertainties which accompany the use of blockchain in automated systems.

INTRODUCTION

The IT industry has been growing at a fast pace since its inception. Many breakthroughs have disrupted our lives in ways not possible before. Especially the internet has been a godsend, for its capability to shelter disruptive technologies which encompass all walks of life. Since the creation of the internet, people were itching to come up with mechanisms to shift traditional methods of payment onto the internet. In 1999, Confinity was the first organization to attempt the same. Although they faced countless challenges, their

DOI: 10.4018/978-1-7998-3295-9.ch005

efforts resulted in PayPal and the world could transfer money on the internet without any hassle. This system, however, still had a long way to go. It still relied on some crutches which decreased the speed of transaction and were significant drags on the efficiency of commerce. Whenever two entities made transactions, they all had to pass through some intermediary parties which functioned as trust holders to ensure the safety and integrity of the bargain. In some rare cases of failures, these intermediaries could be held accountable, but the business would end up losing capital anyway.

Which gives rise to questions like

1. Can trust be placed in these parties
2. What happens if a successful hack or attack occurs?
3. What would happen if the data is not secure?
4. Why not communicate peer-to-peer, when intermediaries slow down the entire process?

The solution to the questions asked above is a new technology called "Blockchain".

Blockchains permit different members to attain agreement on exchange of information, i.e., a single adaptation of the truth, without a trusted central specialist or notary function. The innovation in this technology is that multiple anonymous entities can come together and form a consensus which renders the network and the data within the 'blockchain' (shared digital ledger), virtually tamper-proof. The integrity and secrecy of the information within the advanced records are cryptographically ensured. The hype around Blockchain started and rose to noticeable heights in 2008 (Satoshi, 2008) with the distribution of the interesting white paper 'Bitcoin: A Peer-to-Peer Electronic Cash Framework'. Blockchain-based smart contracts are expected to encourage coordinated, straightforward and irreversible exchange of assets from benefactors to those who need them, removing intermediary costs. The healthcare segment also fits the charge flawlessly for blockchain usage. Through its decentralized design, blockchain seems to supplant obsolete, divided and heterogeneous healthcare systems, bringing down healthcare conveyance costs. Potential blockchain applications are quite wide ranging, however, the blockchain may not be a solution for every given problem. Whenever commerce is carried out online, the electronic transactions are regulated and facilitated by financial institutions that act as the intermediary trusted parties. These third parties play a major role in regulating and safeguarding online transactions, and upon their completion take up commission. Instead of systems used for traditional online transactions, blockchain applications use cryptographic proof. Keys of two kinds, one private and the other public, are utilized in the process. Every user owns this duo of keys. When a transaction takes place, it is signed using the user's confidential private key. After signing the transaction with the sender's private key, the receiver gets the transaction at their public key. The private digital signature, i.e., private key signature, is then verified by the receiver using the public key. Every node gets the transaction for verification through a broadcast. After every node is verified, it is added to the distributed ledger. However, it cannot be ascertained that the order in which the sender sent the transactions would be the same as that of the order received by the receiver. To solve the problem above, transactions are grouped and treated as 'blocks', each of which links itself to others by containing the 'hash value' of the corresponding previous block. This whole system is called Blockchain. This leads us to the next problem, which is to determine which node should be selected and broadcasted, as the creation of numerous blocks can occur at the same time. The solution to this problem is the introduction of a puzzle of sorts called "proof of work". Blockchain uses a mathematical puzzle called "proof of work". It is a consensus algorithm implemented in Bitcoin by a node to generate a new block. Miners get into a competition to solve the puzzle and thus help in