Integrating IoT and blockchain to ensure cyber safety

IoT and blockchain have become buzzwords in the current technological era, a time when technology can help to solve problems, yet also generate new challenges. Cybersecurity is one such major challenge that is hindering the fearless usage of technology. The solution lies in how effectively these technologies are integrated and implemented. Hence, this article is an overview of the integration of IoT and blockchain to ensure cyber safety. It also discusses the essential security measures, and lists the IoT security challenges.

An IoT overview

The network of physical electronic devices, machines, and other objects, which are implanted with sensors and software for the purpose of communicating and exchanging data with other devices and systems through the internet, and each of which has an IP address, is referred to as the Internet of Things (IoT). Today, IoT plays a major role in transforming our lives, and as technologies are enhancing, hackers and cybercriminals are developing new, high-tech ways to breach secure and private data. However, with significant advancement in the IoT range, the issues related to data and information security need to be addressed.

The IoT has enormous advantages, however, it often lacks security. Ideally, user data must be kept private and safe. For this reason, better security measures must be created, maintained, and made the norm for IoT and linked devices in order to keep data secure. In addition, the IoT makes it possible to share data and information via blockchain.

Some of the major IoT security challenges include:

- Visibility and transference
- Data privacy, confidentiality, and integrity
- Authentication, authorization, and accounting
- Secure communications
- Date encryption
- Middleware security

A blockchain overview

Blockchain is an indispensable technology that has been hitting the headlines due to the popularity of cryptocurrencies such as Bitcoin and Ethereum. Is blockchain only concerned with cryptocurrencies? The answer is an emphatic no. Blockchain technology has moved beyond cryptocurrencies to another level. Blockchain is a distributed, decentralized, immutable ledger that can be used to record transactions and track assets in a business network; with blockchain, the intermediary in digital transactions is eliminated. So simply put, in a blockchain, each block in the chain represents a record, and the chain links all of the blocks together.

Key security features of blockchain:

- **Cryptographic security**: Hash functions are one-way functions where it is simple to go ahead (from input to output) but computationally impossible to move backward (output to input).
- **Identity management**: Blockchain identity management systems address current identity issues such as inaccessibility, data insecurity, and fraudulent identities.
- **Multisignature**: Blockchains use digital signatures to ensure the authenticity and integrity of transactions; multisignature requires multiple private keys to generate a valid digital signature, allowing multiple parties to approve a transaction. Furthermore, in blockchain technology, it is infeasible to break public key cryptography, even by brute force guessing.
- **Data privacy**: As data in blockchain is immutable, and blockchain networks can be configured in private/public or permissioned/open blockchains, it offers the potential for enhanced data privacy and control. In a blockchain, data is stored in a decentralized and distributed manner across multiple nodes. Each transaction of data added to the blockchain networks is cryptographically hashed and linked to the previous block, creating an immutable and transparent ledger.

- **Secure communication**: Blockchain can ensure that an attacker cannot monitor and change the communications occurring between nodes, thus maintaining the integrity and confidentiality of the network.

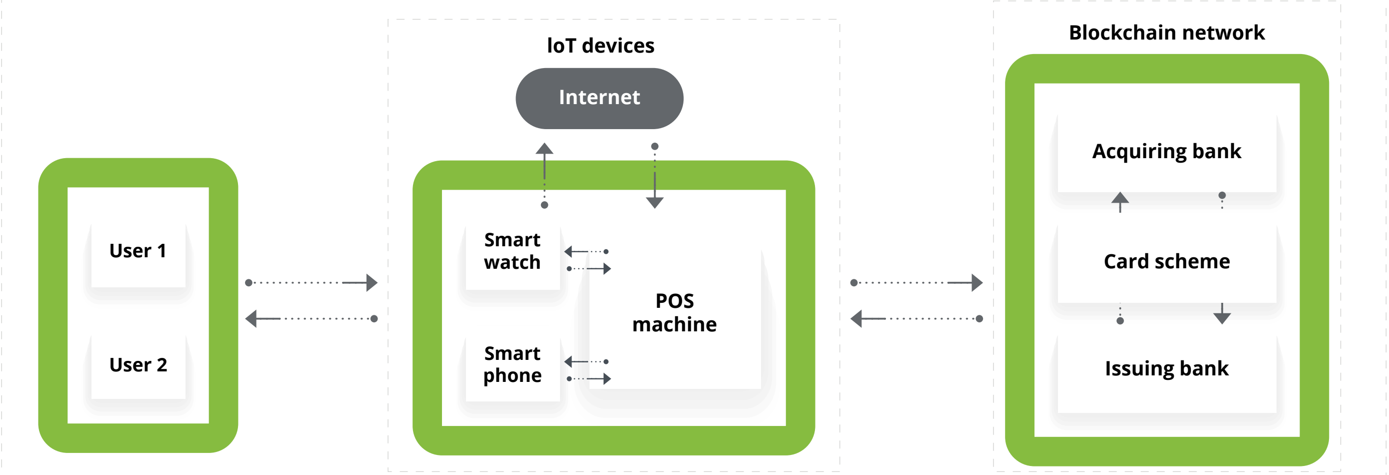
IoT and blockchain are both fantastic innovations on their own, but when they are combined and implemented, they can generate astounding outcomes that are beneficial for cyber safety.

Below are the use cases on integrating IoT and blockchain to ensure cyber safety:

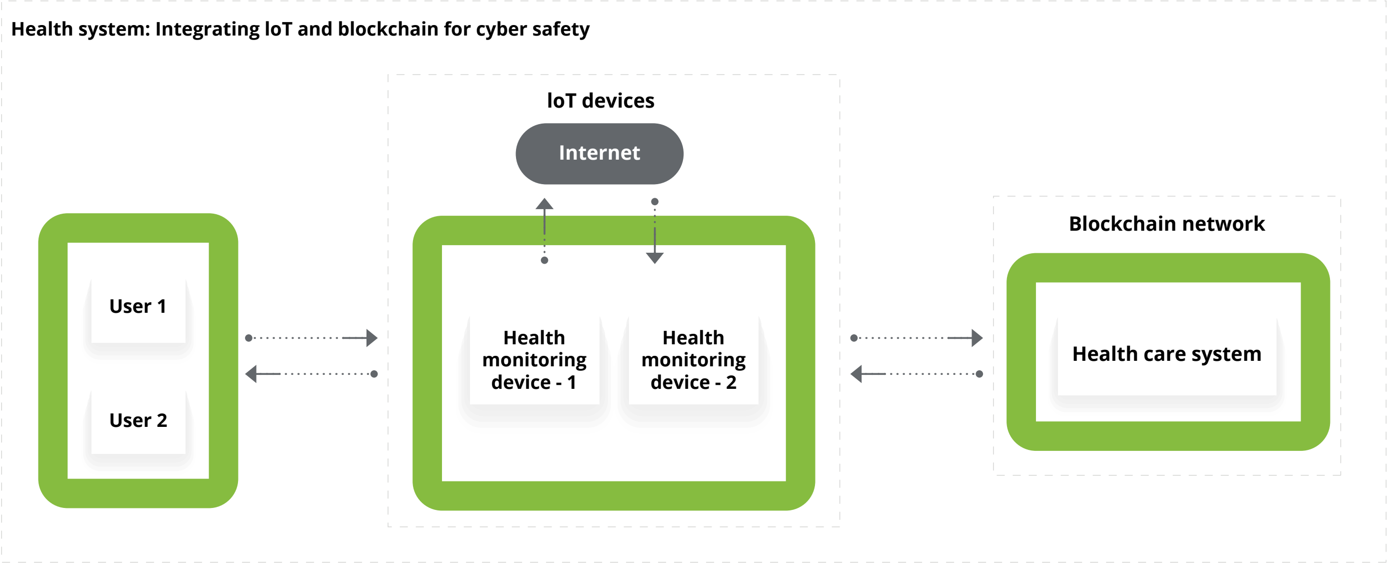
Blockchain is a distributed, decentralized, immutable ledger that can be used to record transactions and track assets in a business network; with blockchain, the intermediary in digital transactions is eliminated

Use case A:

Payment system: Integrating IoT and blockchain for cyber safety



Use case B:


Health system: Integrating IoT and blockchain for cyber safety
IoT devices
Internet
User 1
User 2
Health monitoring device - 1
Health monitoring device - 2
Blockchain network
Health care system

Currently, IoT technology is used with conventional databases. In the high-level block diagrams (Use case A and Use case B) the payment and health care systems can be replaced by blockchain technology. However, the process and flow remain the same.

By adopting blockchain technology, it is possible to address the following IoT cyber security concerns:

- Blockchain is based on the peer-to-peer network in which all nodes have the same copy of records, which solves data integrity issues.
- Blockchain can be implemented in private/public permissioned/open blockchains. It ensures access control, and prevents unauthorized access for data privacy. Furthermore, blockchain can keep track of data gathered by sensors, and prevent fraudsters from duplicating it with other harmful types of data.
- ECDSA (Elliptic Curve Digital Signature Algorithm) solves the limitation of IPV6 address.
- Blockchain network can track every transaction and record, which addresses the problems with trusted accountability.
- Blockchain network will be connected to multiple nodes; it will be resilient and fault tolerant, which solves the problem of single points of failure.
- Blockchain hashing function generates a unique ID that can be assigned to each IoT device. Furthermore, each transaction/record will be tracked in the blockchain network, which will solve the problem of identifying the trusted origin of data.
- Blockchain operates on read and write operations only; data in blockchain is immutable, which will address the data compromise and data manipulation issues.

IoT and blockchain are both fantastic innovations on their own, but when they are combined and implemented, they can generate astounding outcomes that are beneficial for cyber safety

- Blockchain technology is third party risk free, as it can perform operations without the intermediary or third party.
- Smart contract programs help to develop access rights and customize the policies based on the requirements.

The future of the financial sectors and other industries is becoming increasingly digital, which makes the process more convenient for end consumers. Internet of Things (IoT) and blockchain technology are part of this rapid transition towards the bank of the future; both end users and financial sectors, as well as other industries, need to adapt to these trends for cyber safety. Thus, with the development of high-speed networks and sophisticated network devices, IoT is unquestionably an emerging technology. IoT currently faces security limitations and concerns, some of which can be addressed by incorporating blockchain technology. The challenges of technology and cybersecurity are two sides of the same coin. The importance of cyber safety increases as technology evolves.

By **Govinda Mengji**, Specialist Master, Risk Advisory, Cyber & Strategic Risk, Blockchain, Cloud, IT-DR, Deloitte Middle East

> The future of the financial sectors and other industries is becoming increasingly digital, which makes the process more convenient for end consumers. Internet of Things (IoT) and blockchain technology are part of this rapid transition towards the bank of the future; both end users and financial sectors, as well as other industries, need to adapt to these trends for cyber safety.