Blockchain empowerment: Investigating integration with software-defined networks and its impact on IoT privacy

Sanjay Kumar Sinha\textsuperscript{a, b, c} | Sweta Kumari\textsuperscript{b, c} | Ansh Kataria\textsuperscript{d, e} | Narmadha Thangarasu\textsuperscript{d} | Girija Shankar Sahoo\textsuperscript{d}

\textsuperscript{a}Vivekananda Global University, Jaipur, India, Department of Computer Science & Engineering.
\textsuperscript{b}ATLAS SkillTech University, Mumbai, Maharashtra, India, Department of ISME.
\textsuperscript{c}Chitkara University, Rajpura, Punjab, India, Centre of Research Impact and Outcome.
\textsuperscript{d}JAIN (Deemed-to-be University), Ramanagara District, Karnataka, India, Department of Computer Science Engineering.
\textsuperscript{e}Maharishi University of Information Technology, Lucknow, India, Maharishi School of Engineering and Technology.

\textbf{Abstract} The swift expansion of Internet of Things (IoT) devices has brought forth exceptional prospects for automation and data-driven decisions. Software-Defined Networking (SDN) is an instance of network architecture that divides network devices into a control plane and a data plane. SDN provides a dynamic and adaptable method of managing the growing complexity of IoT devices with its programmable design and centralized control. A network's capacity to handle an increasing number of IoT devices is facilitated by SDN's improved scalability. Custom network policies and services that are suited to the distinctive requirements of various IoT applications can be established because of SDN's programmability. SDN and blockchain integration can improve network transaction and configuration security. Here, blockchain technology is decentralized. There is not just one point of failure, which lowers the possibility of malicious attacks and illegal access. The study demonstrates that IoT environments can be enhanced more efficiently, transparently and safely by integrating blockchain technology with SDN. A summary of SDN is presented and then block-chain technologies are examined with a focus on consensus protocols. After that, it explores the difficulties of implementing blockchain-based SDN into practice, concentrating on security issues. Furthermore, this study explores the mutual effects of IoT and blockchain, emphasizing the complementary relationship between the two developing technologies. This review highlights that block-chain as well as SDNs could work together to strengthen IoT privacy and establish a more robust digital future.

**Keywords:** blockchain, Software Defined Networking (SDN), Internet of Things (IoT), consensus protocols, decentralized, privacy

1. Introduction

The IoT is an adaptable, self-configuring network that makes it possible for physical items to interact and communicate with one another, turning them instead of being blind to intelligence. The IoT has become more significant due to its enormous influence on every part of our lives. The IoT is expected to have an extensive range of applications across numerous sectors, radically changing our way of life (Asaithambi et al. 2022). These include remote monitoring, smart homes, smart cities, smart cars and healthcare. The IoT has enormous potential for several industries, including software developers, hardware makers and service providers. Smart connections between billions of disparate objects are anticipated through the IoT, which is the third generation of the network (Latif et al. 2022). High restrictions on network coverage, high system dependability, privacy and security, integration with other current networks for communication, volume of traffic, and latency requirements for specific applications are placed on the entire system structure coupled with architecture because of the enormous number of connected devices. To overcome these obstacles and attain increased system efficiency, emerging innovations along with communication paradigms that facilitate IoT networks can be used. These can link an enormous number of devices. These concepts include blockchain, SDN, distributed edge computing (such as fog computing) and network virtualization (Muthanna et al 2019).

A dynamic network topology is produced by SDN, which divides the control and forwarding planes. Switches or distributed forwarding devices are found in SDN networks, together with a centralized or distributed controller (Jiasi et al 2019). An open standard interface protocol, such as the open flow (OF) protocol, connects and exchanges data with network devices.
on behalf of the controller. Increased system flexibility and capacity are well-known benefits of SDN. To control dispersed peripheral cloud units and defend against diverse cyber security threats, block-chain technology has been implemented for IoT networks. Decentralization can be made possible in a trustworthy way by using the blockchain paradigm on IoT networks (Alzoubi et al 2022). The integration of blockchain technology into IoT networks yields several significant advantages, such as managing decentralized computing resources, enhancing system flexibility, increasing system security by blocking multiple types of privacy, increasing security threats and attacks and lowering system operating costs. Blockchain technology is a peer-to-peer distributed ledger that records all allowed events and transactions. In addition to crypto-currency systems, the blockchain concept has been applied for assisting software and communication networks (Rahouti et al 2020). The goal of this research is to create a transparent and safe infrastructure by revealing the potential advantages of combining blockchain with SDNs. By exploring the interface between these technologies, this research aims to understand how SDNs could be strengthened by the improved security characteristics of blockchain, thereby augmenting the security and confidentiality of IoT networks.

2. An introduction to software-defined networking

SDN is a networking technique that offers the convenience of an administrative structure and seeks to separate the process of data transport from the devices intended for processing (Rahman et al. 2022). The presence of several layers is the basis of this perspective, with every one of the layers in charge of carrying out distinct tasks: (i) the data layer handles the forwarding of packets, (ii) the control layer determines navigation by applying rules to a flow table to treat packets that arrive in the right way, and (iii) the application layer manages the services provided to users (Farooq et al. 2023). The topology of a typical SDN architecture is shown in Figure 1, and the planes are explained in the following sections (Hassan et al. 2019).

![Figure 1 Structure of SDN.](https://link.springer.com/article/10.1007/s10922-022-09682-4/figures/5)

2.1. Data Plane

This layer includes a variety of network devices that can help with network data forwarding, including routers and switching equipment. This includes the transmission and handling of the data flow.

2.2. Control Plane

Through the use of a centralized SDN controller, this layer controls the whole network infrastructure, including the gathering topology and network data. The southbound APIs can be used to establish network connections in the information plane layer.

2.3. Application Plane
This layer provides different SDN apps and devices with an open platform for the use of network resources such as statistics and topology. Through the northbound APIs, several applications can interact with the SDN controller and one another. Additionally, these programs can provide comprehensive solutions for real-world businesses.

3. Blockchain Technology

Blockchain (BC) is a form of distributed ledger technology (DLT) where every node or member of a network of peer-to-peer (P2P) shares and changes an encrypted ledger database that is appended exclusively. A record of the ledger is kept in each participating node or member. Every digital link can be resourceable, effective, visible, safe, auditable and recordable. It has the potential to impact sectors and facilitate the emergence of new commercial structures (Iqbal et al 2020). BC’s decentralized and secure characteristics have elevated it to a formidable position in the progression of several research domains, including artificial intelligence (AI) and the IoT. As companies optimize the advantages of each technology while avoiding the dangers and limits associated with it, combining BC, AI and IoT can develop the technology. Bitcoin, Ethereum and other cryptocurrencies have successfully used BC (Tran et al 2021).

3.1. Types of blockchain

The qualities of user activities and data accessibility could be used to classify BC. Permitted BC, private BC and public BC are the three categories of BC. Everyone can utilize the BC network in public BC without obtaining permission from outside parties. Anyone can operate as a miner/validator or as a basic node. However, network access is limited in private BC (Ahmed and Salah 2023). Consortia and businesses define access control and primary node selection to manage access inside the BC.

3.2. Key technologies of blockchain

The following are the primary technologies used in BC (Ferrag and Shu 2021):

3.2.1. Public key cryptography

Algorithms that employ the public key (PK) and the private key as a pair for encryption and decryption are known as public key cryptography, also known as asymmetric cryptography. In Ethereum and Bitcoin, transactions are authorized and authenticated using the elliptic curve digital signature technique (ECDSA). Both utilize the secp256k1 elliptic curve. Because the addresses are obtained from the participants’ PKs, the ECDSA gives participants their identities (Alharbi et al 2022).

3.2.2. Merkle trees

Binary hash trees or Merkle trees are useful tools for confirming and summarizing data integrity. Merkle trees are utilized by Bitcoin and Ethereum to provide a block summary of transactions. The block header of every block has a Merkle root. The Merkle root is used to validate the contents of each transaction as well as the consistency of several databases. Because of hash quality, even a small inaccuracy could result in different Merkle roots (Bhushan et al 2021). Figure 2 depicts an illustration of a Merkle tree with four hash structures.

![Four hash Merkle trees](https://doi.org/10.1587/transinf.2019ini0002)
3.2.3. Hash functions for cryptography

Hashing algorithms for cryptography are one-directional functions that allow users to take any amount of data and create a fixed-size hash. The secure hash algorithm 256 (SHA-256) is the hashing algorithm used by Bitcoin. Keccak-256 was also used by Ethereum (Chang et al. 2021).

3.2.4. P2P network

P2P networks are open, decentralized, distributed and networked systems in which the network's constituent machines function as competitors to one another. There is no hierarchy or server and no centralized services in the network. The nodes themselves can function as clients and service providers simultaneously. These nodes are responsible for maintaining the shared ledger in the case of cryptocurrencies such as Bitcoin (El-Masri et al. 2021).

3.3. Protocols with consensus

Consensus procedures guarantee that the BC itself cannot be altered or subject to fraudulent transactions. In a distributed and decentralized network, consensus or agreement over the BC's current state is necessary. The distributed, trustless consensus problem of BC is comparable to the Byzantine dilemma. As a result, the Byzantine fault tolerance (BFT) property should be shown by the consensus protocol. Table 1 presents the categorization of a few of these consensus protocols (Imran et al. 2021).

3.3.1. Proof of work (PoW)

PoW uses miners to perform verifiable tasks that could require considerable computing power for block production to reach consensus. Following that, the solution is made public. During the process for nodes to validate and attach the new block to their local BC copy, it is transmitted around the network and added to the chain. However, the drawbacks of the PoW method include high energy consumption, high transaction rates and significant delays.

3.3.2. Proof of stake (PoS)

The amount of bitcoin that an attacker has invested in determines whether he or she can verify a mass. When Bitcoin is staked, it prevents fraudulent validation attempts made by dishonest parties after transactions are fraudulently validated (Gadekallu et al. 2021).

3.3.3. Proof of authority (PoA)

The reputation of the validator is at attack in the PoA. As with PoS and DPoS, the BC is secured, and block generation is limited to an assortment of validators exclusively. The reputation of the validators is at stake since their identities are visible and verifiable. Ethereum testnets such as Kovan and Rinkeby are investigating PoA.

3.3.4. Delegated PoS (DPoS)

Token holders can select delegates to serve on a panel of witnesses by casting votes in DPoS that are proportionate to their holdings. These witnesses do not require a large stake to protect the BC network. Consequently, it provides greater flexibility than PoS and PoW (Gai et al. 2019).

3.3.5. Proof of elapsed time (PoET)

Every validator has to operate for a predetermined amount of time, which is picked at random. The peer network as a whole is informed of the essential information when the first person to finish the allotted waiting period exists.

3.3.6. Proof of capacity (PoC)

Miners attempt to save many answers to different problems as they mine PoC. A block is added to the BC by selecting the worker who completes the challenge fastest as the leader. PoC has a greater energy economy. There is a chance that some users will pool their storage capacity, which could force the network to become more centralized (Javed et al. 2022).

<table>
<thead>
<tr>
<th>Consensus Protocol</th>
<th>PoW</th>
<th>PoS</th>
<th>DPoS</th>
<th>PoA</th>
<th>PoET</th>
<th>PoC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptocurrency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Public</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Permissioned</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Source:</td>
<td><a href="https://doi.org/10.1002/ett.3741">https://doi.org/10.1002/ett.3741</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Structure of Blockchain-Powered SDN

SDN can separate network management from the data plane, allowing for greater versatility in network architecture and global visibility. SDNs have many drawbacks. For example, distributed controllers can be attacked by insiders, while centralized controllers can end up appearing as a single source of error (Monrat et al 2019). The academic community has started examining the performance of merging SDN with blockchain. Blockchain technology can enable unknown entities to connect without the assistance of a reliable third party. A general framework for blockchain-based SDN, which applies blockchain technology to SDN architecture (Atlam et al 2020). The standards allow for the simplification of the control plane and application layer into two major components, where specific security measures could be put in place to offer protection. The security of different data plane forwarding devices and distributed controllers could be improved with the use of blockchain technology. Designing the structure between applications, controllers, security measures and pertinent interactions is essential for implementing the framework in practice. SDN and blockchain technologies are combined in the proposed distributed IoT architecture, called DistBlockNet (Li et al 2020). To prevent attacks, they included several security features, including the OrchApp and Shelter modules.

4.1. OrchApp

This module's goal is to guarantee adaptability to new and dynamic network situations by providing programming-characterized fortifications at the proper application layer. Here, a variety of security guidelines and threat intelligence can be used in connection to data security, access control and several detection techniques. For example, it uses a security convention paradigm to govern access across different IoT network devices. Threat intelligence continuously monitors and looks at sources that are internal and external.

4.2. Shelter

The SDN environment is shielded from numerous threats, including insider attacks, by the use of this module. A packet migration component and a flow control analyzer make up its two main parts. The former holds the charge of overseeing the primary operations of the network infrastructure, including any harmful events that could occur, and can be used as a controller layer of control application. The latter lessens the effect of unfavorable incidents (Rejeb et al 2023).

4.3. Security issues in blockchain-based SDN

Blockchain-based SDN has numerous advantages, but several security problems and difficulties can persist. This could be attributed to the constraints of SDN or blockchain technologies. This section addresses several possible security issues. Attackers could try to undermine the network’s availability, secrecy and integrity by taking advantage of SDN vulnerabilities (Ahmed et al. 2022).

4.3.1. Scanning

Cybercriminals use this as their initial step to learn about the state of the network, including its architecture, host IP, server placement and other details. To obtain the necessary data, attackers can passively watch every layer and each their communication connections.

4.3.2. Spoofing attack

Attackers can attempt to enter the SDN network without authorization by disguising themselves as either an authentic external party or an inside party. By changing pertinent data, they can assume the identity of a device, switch, or even the controller based on the information gathered from scanning. Spoofing attacks can be broadly classified into two categories: IP spoofing and Address Resolution Protocol (ARP) spoofing.

4.3.3. DoS attack

The primary objective of DoS is to prevent authorized users from accessing any devices, SDN apps, or network resources. The data plane resource consumption is an early DoS attack that is unique to SDN networks. Attackers must determine whether a network uses OF switches before they can start creating forged flow requests that are sent. This approach can offer many pointless rules, overloading the data plane (Nguyen et al 2020).

There are additional difficulties in an SDN context in addition to the assaults mentioned above. For instance, dispersed SDN Controllers are susceptible to insider assaults since there is no trust management mechanism in place. However, blockchain is a young technology with many practical issues that need to be resolved. Additionally, it can draw hackers as a target. Table 2 lists Blockchain and SDN-based attacks for the security problems addressed in this section.

4.3.4. Security issues
Many classic attacks, such as DoS, remain possible since the blockchain is insecure. Furthermore, it is necessary to keep the shared ledger in a single location, which makes it susceptible to single points of failure. Increased participant numbers moreover, the complexity of trust management could pose a risk of illegal access.

4.3.5. Privacy Issues

All transactions ever made on a public blockchain could become publicly accessible, which presents several issues. Sensitive data in several industries, including the financial and medical sectors, can be included. Furthermore, blockchain-based applications that require a transaction to be associated with an individual could jeopardize identity privacy (Rahman et al. 2020).

<table>
<thead>
<tr>
<th>Attack/Issue</th>
<th>Purpose</th>
<th>Used technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning (Li et al 2020)</td>
<td>Identify key information about the network, such as its architecture, host IP address and server location, etc.</td>
<td>Architecture, host IP address, server location</td>
</tr>
<tr>
<td>Spoofing Attack (Li et al 2020)</td>
<td>Unauthorized access to SDN networks through the use of a false identity, either internal or external.</td>
<td>SDN</td>
</tr>
<tr>
<td>DoS Attack (Li et al 2020)</td>
<td>Limited access to SDN devices, applications and network resources to approved users only.</td>
<td>OF switches</td>
</tr>
<tr>
<td>Security Issues (Li et al 2020)</td>
<td>Examine obstacles including insider threats against distributed SDN controllers and real-world blockchain problems.</td>
<td>SDN, Blockchain</td>
</tr>
<tr>
<td>Privacy Issues (Li et al 2020)</td>
<td>Address issues with sensitive data exposure and identity privacy that is jeopardized by transactions on a blockchain being accessible to the public.</td>
<td>Blockchain</td>
</tr>
</tbody>
</table>

5. Impact of the IoT based on Blockchain

The IoT offers an enormous range of devices that can be used for remote monitoring in several applications across multiple domains. The IoT is a revolution that is reshaping our society, and it is widely employed in smart sectors, connected vehicles, healthcare, military items, etc. The primary problems are privacy and security because of its amazing proportions and scattered nature (Zhang et al. 2019). A variety of frameworks have been proposed to protect IoT settings, among which BC has been employed to protect IoT networks. Within closed settings, private BC in BC-based IoT systems works effectively and economically, whereas public BC can link several IoT environments simultaneously. Trust must be managed in this situation, and it must be done so centrally and independently of outside parties (Wadhwa et al. 2022). This section addresses several problems and obstacles that could improve the effectiveness of blockchain-based IoT devices.

5.1. Blockchain Vulnerabilities

IoT devices are susceptible to security breaches even if blockchain offers reliable methods to protect them. By abusing the consensus system, an attacker can host and generate a blockchain by compromising the hashing of miners. Due to their scarcity, private keys are vulnerable to attack. To prevent assaults such as race attacks, which cause a person to double-spend during a transaction, efficient security measures need to be implemented.

5.2. Identity-Based Attacks

The attackers plan to assume the identity of authorized users to acquire access and carry out a modification attack. The key threat, replay attack, impersonation assault and Sybil attack are examples of identity-based attack types (Sankar et al. 2021).

5.3. Manipulation-Based Attacks

These four types of attacks involve illegal access or data alteration. Attacks can be classified as follows: tampering, overlaying, modification and fake data injection.

5.4. Cryptanalytic Attacks

The goal of quantum attacks is to extract private keys from the public key of the elliptic curve digital logarithm. By faking every one of the necessary transactions, the attacker intends to employ information to sign unlawful transactions. The
deterministic wallet seed of the blockchain can be used to extract multiple subprivate keys via a lattice-based signature mechanism.

5.5. Attacks Based on Reputation

The network mediator can use Whitewashing and Hiding Blocks attacks to change their reputation from bad to good (Singh et al. 2022).

5.6. Service-Based Attacks

These assaults cause the gadget to act differently from its features or render the service unavailable. Attacks that fall under this category include those requiring attention, such as DoS attacks, assaults that include refusing to give authorization, overspending attacks and key crashes.

5.7. Adaptability to Joint Attacks

Blockchain-based protection solutions for the IoT address many security concerns, but the fundamental problem remains how to build resilience against coordinated assaults while taking into account the viability of solutions for devices with limited power resources (Snehi and Bhandari 2021).

5.8. Dynamic and Adaptable Security Framework

Low-power to high-end servers are among the IoT devices that have been deployed. It is necessary to have many layers of security rather than a single layer. The security solution should be able to adjust to the available resources before providing services to customers to choose which safety measures to employ. Intelligent security mechanisms that are dynamic and adaptive are dependent on resource standardization.

5.9. Mining that Uses Less Energy

Strong miners are needed since the blockchain expands with more transactions. This growth makes use of storage resources and IoT devices with limited power, which are inadequate to handle the significant computing and power requirements for blockchain processing. It is necessary to have effective energy consensus processes, which is a major scientific problem (Wang et al. 2021).

5.10. Social Networks and Trust Management

Widespread rumors have the potential to hurt an organization's bottom line. Blockchain technology has the potential to reduce rumors.

This review reveals how blockchain and SDNs work together, highlighting the transformative potential of these technologies in safeguarding IoT networks. The authors navigate through the complex network of programmable networks and decentralized ledgers, providing a thorough examination of the privacy issues in the IoT domain.

6. Final considerations

Blockchain is a decentralized network of computers that operates as a distributed database system, securely and transparently recording transactions. SDN is an innovative method of network management that concentrates control in software applications and abstracts the underlying hardware architecture. The combination of SDNs with blockchain presents a potential paradigm that offers a robust and decentralized framework for protecting sensitive data in a global network of connected devices. As the digital world continues to evolve, the author emphasizes the importance of creative solutions to major IoT privacy issues. This study’s investigation highlights the need for careful fusion and cooperation among developing technologies to create a more reliable and resilient IoT. Due to the resource-intensive nature of blockchain processes, latency and potential network performance bottlenecks could increase. Additionally, the influence on IoT privacy poses complications to data confidentiality and access control, even if the impact is meant to be good. The future objectives of this study will focus on scalability as well as real-world application, encouraging industry-wide adoption for improved IoT security and privacy.

**Ethical Considerations**

Not Applicable.

**Conflict of Interest**

The authors declare no conflict of interest.

**Funding**
The current review did not receive any financial support.

References

El-Masri M, & Hussain E M A (2021) Blockchain as a mean to secure Internet of Things ecosystems—a systematic literature review. Journal of Enterprise Information Management, 34(5), 1371-1405. 10.1108/JEIM-12-2020-0533
Ferrag M A, & Shu L (2021) The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. IEEE Internet of Things Journal, 8(24), 17236-17260. 10.1109/JIOT.2021.3078072
Iqbal W, Abbas H, Daneshmand M, Rauf B, & Bangash Y A (2020) An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal, 7(10), 10250-10276. 10.1109/JIOT.2020.2997651
M Rahman Ghaffar, Alshahrani A, Fayaz M, Alghamdi A M, & Gwak J (2021) A topical review on machine learning, software-defined networking, internet of things applications: Research limitations and challenges. Electronics, 10(8), 880. 10.3390/electronics10080880
Nguyen D C, Pathirana P N, Ding M, & Seneviratne A (2020) Integration of blockchain and cloud of things: Architecture, applications, and challenges. IEEE Access, 8, 252125-2549. 10.1109/ACCESS.2020.3009092
Rahouti M, Xiong K, & Yin X (2020) Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends. IEEE Access, 9, 120833-121123. 10.1109/ACCESS.2020.3047996


