

Article

Not peer-reviewed version

IOTASDN: IOTA 2.0 Smart Contracts for Securing SDN Ecosystem

[Mohamed Fartitchou](#) , [Ismail Lamaakal](#) , [Yassine Maleh](#) ^{*} , Khalid El Makkaoui , [Zakaria El Allali](#) , [Paweł Pławiak](#) , [Fahad Alblehai](#) , [Ahmed A. Abd El-Latif](#) ^{*}

Posted Date: 15 July 2024

doi: 10.20944/preprints2024071200.v1

Keywords: Blockchain (BC); Distributed Ledger Technology (DLT); IOTA 2.0; Security; Smart Contracts (SCs); Software-Defined Networking (SDN).




Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article

IOTASDN: IOTA 2.0 Smart Contracts for Securing SDN Ecosystem

Mohamed Fartitchou ¹, Ismail Lamaakal ¹, Yassine Maleh ^{2,*}, Khalid El Makkaoui ¹, Zakaria El Allali ¹, Paweł Pławiak ^{3,4}, Fahad Alblehai ⁵ and Ahmed A. Abd El-Latif ^{6,7,*}

¹ Multidisciplinary Faculty of Nador, Mohammed Premier University, Oujda, Morocco; fartitchoumed@gmail.com (M.F.); ismail.lamaakal@ieee.org (I.L.); kh.elmakkaoui@gmail.com (K.E.M.); z.elallali@ump.ma (Z.E.A.)

² Laboratory LaSTI, ENSAK, Sultan Moulay Slimane University, Khouribga, Morocco

³ Department of Computer Science, Faculty of Computer Science and Telecommunications, Cracow University of Technology, Warszawska 24, 31-155 Krakow, Poland; pawel.plawiak@pk.edu.pl

⁴ Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland

⁵ Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia; falblehi@ksu.edu.sa

⁶ Information Countermeasure Technique Institute, School of Cyberspace Science, Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China

⁷ Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt

* Correspondence: yassine.maleh@ieee.org (Y.M.); ahmedabdellatif@ieee.org (A.A.E.-L.)

Abstract: Software-Defined Networking (SDN) has revolutionized network management by providing unprecedented flexibility, control, and efficiency. However, its centralized architecture introduces critical security vulnerabilities. This paper presents an innovative approach to securing SDN environments using IOTA 2.0 smart contracts. The proposed system leverages the IOTA Tangle, a directed acyclic graph (DAG) structure, to enhance scalability and efficiency while eliminating transaction fees and reducing energy consumption. We introduce three smart contracts—Authority, Access Control, and DoS Detector—to ensure secure network operations, prevent unauthorized access, and mitigate denial-of-service attacks. Through comprehensive simulations using Mininet and the ShimmerEVM IOTA Test Network, we demonstrate the efficacy of our approach in enhancing SDN security. Our findings highlight the potential of IOTA 2.0 smart contracts to provide a robust, decentralized solution for securing SDN environments, paving the way for further integration of blockchain technologies in network management.

Keywords: blockchain (BC); distributed ledger technology (DLT); IOTA 2.0; security; smart contracts (SCs); software-defined networking (SDN)

1. Introduction

SDN is precipitating a transformative effect on network management and operations. It introduces levels of flexibility, control, and efficiency previously unattainable by elements that are quintessential in the rapidly evolving landscape of digital technology. This paradigm shift in networking not only redefines traditional network architecture but also aligns seamlessly with the dynamic requirements of contemporary digital ecosystems [1–7].

While SDN offers several advantages in terms of network management and efficiency, it also introduces a new set of security challenges that are critical to address. The centralized nature of SDN controllers presents a potential single point of failure, making the network susceptible to targeted attacks that could compromise the entire network infrastructure. This is because SDN is dynamic and programmable, which is good for network flexibility but also makes it easier for hackers to attack. They can use flaws in the software layers to launch attacks like denial of service (DoS), man-in-the-middle, and data theft. These challenges necessitate robust security mechanisms and policies to ensure the integrity, confidentiality, and availability of network resources in an SDN environment [8–12].

In tackling the security challenges inherent in SDN, machine learning (ML) and blockchain (BC) emerge as pivotal solutions [13–20]. ML algorithms aim to enhance the SDN network's capability to intelligently detect, predict, and respond to cyber threats. By analyzing network data, identifying

patterns, and learning from past incidents, ML algorithms provide a dynamic and proactive approach to network security, significantly improving the ability of SDN environments to safeguard against a wide range of cyber threats. The integration of BC technology into SDN architectures aims to achieve several key objectives: enhancing operational transparency, fortifying network security, and ensuring data integrity.

BC technology is a decentralized and distributed digital ledger system characterized by its immutability, transparency, security, smart contracts, tokenization, interoperability, efficiency, anonymity, privacy, and programability [21,22]. These features make BC a promising technology for various applications in addition to cryptocurrencies (e.g., Bitcoin and Ethereum), including agricultural product traceability [23], healthcare [24,25], renewable energy management [26], education [27,28], Internet of Things (IoT) cybersecurity [29–31], and more. Nevertheless, BC technology faces several challenges, including scalability, energy consumption, throughput time, and transaction fees [32–35].

The emergence of the IOTA Tangle represents a revolutionary shift in distributed ledger technology. In contrast to traditional BCs, which rely on a linear chain of blocks, the IOTA Tangle employs a directed acyclic graph structure to address the scalability and efficiency issues associated with conventional BCs. The IOTA enables parallel processing of multiple transactions, eliminating the need for miners and significantly reducing transaction fees and energy consumption [36–38]. The distinct features of the IOTA Tangle include high scalability, feeless transactions, fast transaction speeds, and low energy consumption, making it a promising technology for a diverse range of applications, e.g., IoT [39,40], healthcare [41], industrial sectors [42,43], and federated learning [44].

In this paper, for the first time, we employ IOTA 2.0 smart contracts to secure the SDN ecosystem. The original contributions presented in this research are as follows:

- **Introduction of IOTA 2.0 Smart Contracts for SDN Security:** We leverage the IOTA Tangle's unique directed acyclic graph (DAG) structure to implement scalable, efficient, and feeless smart contracts specifically designed to address the security challenges of SDN environments.
- **Development of a Comprehensive Security Framework:** We propose and implement three distinct smart contracts—Authority, Access Control, and DoS Detector—that work in unison to provide robust security mechanisms, ensuring secure network operations, preventing unauthorized access, and mitigating denial-of-service attacks.
- **Integration and Simulation in Realistic Environments:** Through extensive simulations using Mininet and the ShimmerEVM IOTA Test Network, we validate the efficacy of our approach in real-world scenarios, demonstrating significant improvements in SDN security and resilience.
- **Evaluation and Comparison with Existing Solutions:** We conduct a thorough comparative analysis of our proposed system against existing blockchain-based security solutions for SDN, highlighting the advantages of IOTA 2.0 in terms of scalability, energy efficiency, and transaction costs.

The remainder of this paper is structured as follows: Section 2 gives an overview of recent studies on the use of BC technology to enhance SDN security. Section 3 gives the necessary background, providing an overview of SDN security challenges and of IOTA 2.0 smart contracts. Section 4 presents the IOTA 2.0 smart contracts-based system for fortifying the security of SDN. Section 5 focuses on the practical implementation of IOTA 2.0 SCs within SDN environments and presents a comprehensive analysis of the results obtained. Section 6 concludes the paper by summarizing the key findings and contributions of the research.

2. Related Work

This section provides a comprehensive review of recent research focusing on the application of distributed ledger technologies (DLTs), e.g., blockchain, to enhance the security of SDN.

Weng et al. [45] proposed a BC-based monolithic secure mechanism to enhance SDN security by decentralizing the control plane, ensuring authenticity and accountability of application flows,

implementing access control mechanisms, and integrating secure protocols with smart contracts on the BC. By recording network events on the blockchain, the mechanism enables traceability and auditing of network behaviors, addressing single-point failures and improving scalability in SDN environments. The paper concludes that this innovative approach offers a comprehensive solution to SDN security challenges, leveraging BC technology to provide a secure, decentralized, and accountable framework for network management and control.

Pourvahab and Ekbatanifard [46] presented a novel forensic SDN-IoT architecture that utilizes BC technology to enhance security and efficiency in digital forensics processes within IoT environments. The proposed architecture demonstrates superior performance in terms of delay, throughput, accuracy, response time, processing time, and security compared to previous works. The study emphasizes the importance of blockchain in ensuring data integrity, preventing tampering, and establishing a secure chain of custody for digital evidence. Future validation plans include testing the architecture in a large-scale network environment and implementing additional authentication and load-balancing mechanisms. Overall, the paper highlights the effectiveness of integrating BC technology with SDN-IoT to address digital forensics challenges and improve security provisioning in IoT environments.

Yazdinejad et al. [47] presented a novel approach to enhancing security in SDN through the BC-enabled packet parser (BPP) architecture. By leveraging BC technology and FPGA hardware, the BPP architecture demonstrates efficient attack detection capabilities with a low false positive rate and a high detection rate. The study emphasizes the importance of integrating security measures into both the control and data planes of SDN networks, as well as BPP's potential to improve network security by detecting and communicating attacks to the SDN controller. The findings underscore the importance of security in SDN environments and suggest future research directions to further optimize the BPP architecture for enhanced network security.

Aujla et al. [48] explored the integration of BC technology with SDN to address challenges faced by smart cities, such as channel congestion and limited scalability. By proposing BlockSDN as a solution, the study aims to enhance data transmission efficiency and security in smart city environments. It emphasizes the role of SDN in providing improved bandwidth capabilities and flexibility for dynamic data transmission requirements. Additionally, the paper highlights the security concerns associated with SDN architectures, particularly the vulnerability of the centralized controller to attacks. Through the innovative approach of combining BC and SDN, the research contributes to advancing the development of secure and reliable network infrastructures for smart city applications.

Shashidhara et al. [49] introduced SDN-chain, a BC-based privacy-preserving protocol for software-defined networks, aiming to address vulnerabilities in existing security protocols such as ARP poisoning and DDoS attacks. By integrating BC technology, SDN-chain enhances network reliability, safety, and decentralization, mitigating the risks associated with centralized SDN controllers. The proposed security model includes initialization, registration, and authentication phases, supported by a delegated proof of stake algorithm implemented on the Ethereum BC. Through informal security analysis and simulations, SDN-chain demonstrates improved network efficiency with reduced delay and bandwidth, offering a promising solution to strengthen security in SDN environments and prevent various network attacks.

Algarni et al. [50] introduced BCNBI, a blockchain-based security framework for the Northbound Interface in SDN, aiming to enhance security by addressing confidentiality, integrity, and availability concerns. BCNBI utilizes a lightweight BC architecture to authenticate applications and the SDN controller, enforce access control policies, and monitor application behavior. By comparing with existing solutions and demonstrating superior performance in handling transactions, BCNBI showcases its efficiency in securing the SDN environment. This research not only sets a new standard for network security but also highlights the potential of BC technology to revolutionize security measures in SDN.

Kovacs et al. [51] investigated a range of critical topics concerning network optimization and security within the realm of BC-enabled SDN controllers and IoT deployments. The research delved into secure storage and access for task-scheduling schemes on consortium BC and the Interplanetary

File System, as well as the development of proof-of-authentication mechanisms for scalable BC in resource-constrained distributed systems. Furthermore, the paper explored cooperative traffic control schemes among ISPs using bargaining game approaches, analyzed the impact of zero-rating content on internet quality of service, introduced machine-learning-based action recommenders for network operation centers, and discussed enhancements in SDN security for IoT deployments through blockchain integration. These findings underscore the importance of robust network infrastructure, collaborative strategies for efficient traffic management, and innovative security measures to ensure optimal performance and reliability in modern networking environments.

The aim of this paper is to enhance the security of Software-Defined Networking (SDN) environments by leveraging IOTA 2.0 smart contracts. Our proposed system introduces three distinct smart contracts—Authority, Access Control, and DoS Detector—to provide robust security mechanisms that ensure secure network operations, prevent unauthorized access, and mitigate denial-of-service attacks. By utilizing the IOTA Tangle’s directed acyclic graph (DAG) structure, our approach aims to enhance scalability, efficiency, and energy consumption, while eliminating transaction fees. Through comprehensive simulations using Mininet and the ShimmerEVM IOTA Test Network, this paper seeks to demonstrate the efficacy of IOTA 2.0 smart contracts in providing a decentralized and efficient solution for securing SDN environments.

Table 1 provides a comparative analysis of our proposed IOTA 2.0 smart contract-based system against existing systems using distributed ledger technologies (DLTs) for enhancing SDN security.

Table 1. Comparison of the proposed system with other existing systems based on DLTs.

Ref.	Focus Area	Key Contributions	DLT	SC	Limitations
[45]	BC-based monolithic secure mechanism for SDN.	Decentralizing control planes, ensuring authenticity and accountability of application flows, access control mechanisms, and integrating secure protocols with SCs.	BC	✓	Potential scalability challenges, performance overhead, SC complexity, and interoperability issues. The type of SCs used is not specified.
[46]	Forensic SDN-IoT architecture with BC.	Enhancing security and efficiency in digital forensics, ensuring data integrity, preventing tampering, and securing the chain of custody for digital evidence.	BC	✗	Potential scalability challenges and overhead of BC integration in large-scale SDN environments.
[47]	BC-enabled packet parser architecture.	Enhancing security in SDN through FPGA hardware, efficient attack detection, a low false positive rate, and a high detection rate.	BC	✗	Scalability challenges inherent in BC implementation at the data plane level of SDN networks.
[48]	Integration of BC with SDN for smart cities.	Addressing challenges in smart cities, enhancing data transmission efficiency and security, and improving bandwidth capabilities and flexibility.	BC	✗	Complexity and potential overhead introduced by integrating BC technology into SDN infrastructures.
[49]	BC-based privacy-preserving protocol for SDN.	Addressing ARP poisoning and DDoS attacks, enhancing network reliability, safety, and decentralization, and reducing delay and bandwidth.	BC	✓	Potential scalability and performance challenges for real-world network operations.
[50]	BC-based security framework for Northbound Interface in SDN.	Enhancing security by addressing confidentiality, integrity, and availability, authenticating applications and SDN controllers, and enforcing access control policies.	BC	✗	Potential challenges related to scalability, performance overhead, and the computational resources required for BC operations.
[51]	Network optimization and security in BC-enabled SDN and IoT.	Secure storage and access for task scheduling, the development of proof-of-authentication mechanisms, cooperative traffic control, and ML-based action recommenders.	BC	✗	Challenge of scalability and performance issues for large-scale Infrastructure Networks.
Our System	IOTA 2.0 SCs for Securing SDN.	Introducing a novel approach to secure SDN environments using IOTA Tangle, leveraging smart contracts for authority, access control, and DoS detection	IOTA Tangle	✓	Potential reduction in quality of service, increased latency, and impact on data traffic due to the integration of the DoS Detector smart contract

3. Background

In this section, we establish a fundamental understanding of the key areas our research addresses. Initially, we examine the security challenges inherent in SDN, highlighting the need for enhanced

protective measures. After that, we present IOTA 2.0 SCs, clarifying their potential as an innovative solution to these challenges.

3.1. Comprehensive Analysis of SDN Security Challenges

SDN represents a paradigm shift in network management by decoupling the control plane from the data plane, enhancing programmability, flexibility, and control. However, this innovation also introduces several security challenges inherent to its novel structural design [9,52–56]. In SDN, various security threats and vulnerabilities are present across the different layers and interfaces of the network architecture, as shown in Figure 1.

- (1) **The SDN switch** is typically a distinct device comprising both hardware and software components, vulnerable to threats like flow table modification, topology spoofing, and DDoS attacks. Attackers can insert malicious nodes or modify flow rules, disrupting network integrity.
- (2) **The link between switches:** The SDN architecture's lack of encryption on links between SDN switches allows hackers to intercept information, thereby compromising network security.

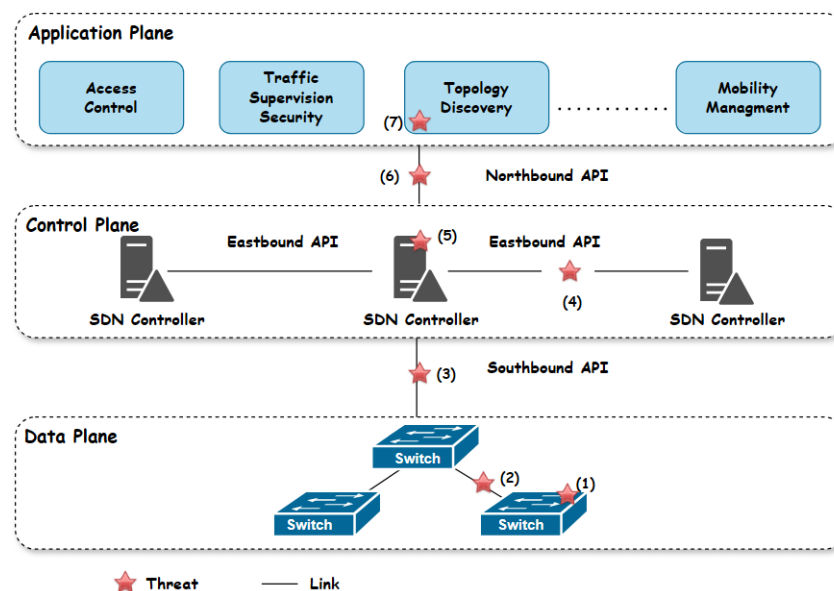


Figure 1. Security Threats and Vulnerabilities Analysis in SDN by Layer.

- (3) **The eastbound interfaces** are vulnerable to security threats due to the lack of encryption on the links connecting controllers. This vulnerability compromises the integrity of inter-controller communications, allowing hackers to manipulate network behavior and share false information.
- (4) **SDN controllers**, due to their centralized architecture, confront significant security challenges. They are particularly vulnerable to DDoS attacks, unauthorized access stemming from inadequate access control mechanisms, and interception risks, all of which compromise network scalability and availability. The lack of standardized security protocols further exacerbates these vulnerabilities, rendering SDN controllers susceptible to network disruptions and compromises. Attackers can also use the Link Layer Discovery Protocol to change information about the network's topology and separate switches that have been hacked. Malformed packets can cause OpenFlow to flood with packets, which wastes resources and makes the network slow.
- (5) **The northbound interface**, a communication interface between applications and controllers, is vulnerable due to weak authentication and inappropriate authorization. This can lead to identity theft attacks and unauthorized access. Hackers can use multiple requests to create flow modifications, bottlenecks, and processor overload, compromising security and reliability between controllers and multiple applications.

- (6) **The applications plane** faces distinct security challenges, primarily due to its integral role in managing network behaviors and policies. This plane, often lacking robust authentication and access control mechanisms, is vulnerable to the introduction of malicious applications, which can lead to policy conflicts, unauthorized access, and resource exhaustion. The plane's direct interaction with the SDN controller, where compromised applications can alter network configurations or launch attacks like DDoS, exacerbates these vulnerabilities. Furthermore, the absence of standardized security protocols on the application plane heightens the risk of tampering and eavesdropping.

3.2. Overview of IOTA 2.0 Smart Contracts

While BC technology offers benefits such as decentralization, security, transparency, and immutability, its integration into resource and power-constrained IoT devices poses significant challenges, including issues related to scalability, high energy consumption, transaction fees, throughput time, and network latency [57–61]. To address these challenges, the IOTA Tangle [62] was proposed as an alternative DLT specifically designed for the IoT ecosystem. In contrast to conventional BCs, which employ a linear chain of blocks, the IOTA Tangle implements a directed acyclic graph (DAG) structure, facilitating parallel transaction processing and enhancing scalability.

The IOTA 2.0 Tangle [63] has undergone several significant enhancements and upgrades since its initial conception, transforming its architecture, consensus mechanisms, and overall functionality to address the scalability, security, and decentralization challenges inherent in previous releases [64,65]. IOTA 1.0, the first version, introduced Tangle, a novel DAG data structure designed for IoT, enabling immutable data, fee-less microtransactions, low resource consumption, and security based on PoW consensus, honest majority transaction issuers, and coordinator node checkpoints. IOTA 1.5 (Chrysalis) [66] was proposed to enhance IOTA 1.0 in terms of security and usability. It addressed issues with the original transaction data structure by introducing improvements like better tip selection, autopeering, atomic transactions, adoption of the UTXO model [67], increased throughput, and faster confirmations. IOTA 2.0 (Coordicide) [68] represents the first fully decentralized version of the network, incorporating SCs. In contrast to IOTA 1.0 and 1.5, which relied on a centralized coordinator for transaction validation, IOTA 2.0 employs a decentralized consensus mechanism. This innovation enables network nodes to independently validate transactions and achieve consensus without the need for a central authority [69].

Coordicide has numerous features, including:

- **Tangle technology:** Coordicide uses a directed acyclic graph called the Tangle, unlike traditional blockchains, which use a linear chain of blocks. This structure enables parallel transaction processing, ensuring high scalability and high throughput transaction per second (TPS).
- **Decentralization and scalability:** IOTA 2.0 eliminates the Coordinator, a special node for transaction validation. Moving towards a fully decentralized system enhances the network's scalability and security.
- **Energy efficiency:** The Tangle's design, which eliminates the need for miners, significantly reduces computational power for transaction validation, simplifying the process and making IOTA more energy-efficient compared to traditional proof-of-work blockchain systems.
- **No transaction fees:** IOTA 2.0 maintains its no-fee transaction feature. This feature makes microtransactions viable and opens up a range of applications, particularly in the Internet of Things domain.
- **Interoperability:** IOTA Tangle 2.0 facilitates the transfer of value between different BC networks due to its interoperability with other BC platforms.
- **Smart contract capabilities:** With IOTA 2.0, the network introduces support for SCs, allowing developers to create more complex decentralized applications. This feature aims to make IOTA a more competitive platform in the broader landscape of distributed ledger technologies.

IOTA 2.0 SCs introduce a decentralized network with enhanced security, scalability, and suitability for IoT applications. SCs operate on a distributed network, where multiple validators execute and verify code. They go through four phases: creation, deployment, execution, and completion. By utilizing programming languages like Solidity and running on subchains linked to the main Tangle, the IOTA SCs protocol (ISCP) reduces reliance on the main network. This setup supports parallel execution, inter-chain communication, and the Ethereum virtual machine, which enables feeless transactions and faster execution of Solidity-based contracts on the IOTA network. Figure 2 illustrates ISCP chains, which manage state and contract execution, with validator nodes validating state changes and publishing them to Layer 1. This setup lowers transaction costs, minimizes network strain, and supports Solidity-based contracts. IOTA SCs enhance scalability and support complex contracts. ISC chains operate on Layer 2 within the IOTA Multi-Asset Ledger, and they interact seamlessly with both Layer 1 and other ISC chains.

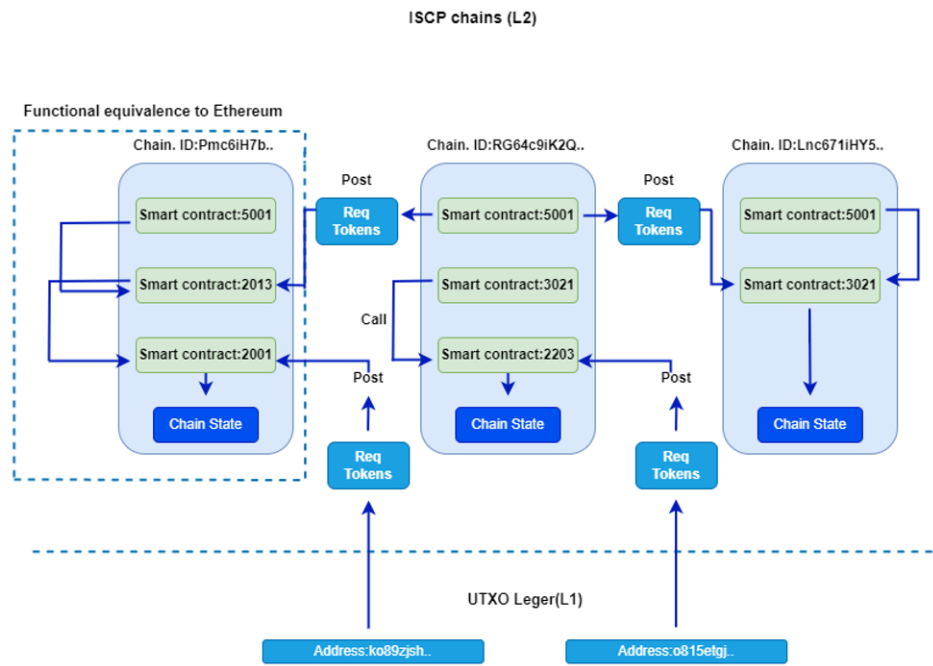


Figure 2. IOTA Smart Contracts Protocol Chains.

IOTA Tangle has opened new opportunities for various application domains due to its unique smart contracts, feeless transactions, and fully decentralized nature. These domains include healthcare [41,70], Industry 4.0 [43,71], the Internet of Things (IoT) [72], and autonomous IoT systems [73].

Table 2 concludes the subsection with a comprehensive comparative study between IOTA 2.0 and well-known BC-based cryptocurrencies, specifically Bitcoin [74], Ethereum [75,76], and Hyperledger [76]. The Table 2 provides a comparative study of IOTA 2.0 and other blockchain-based cryptocurrencies, highlighting their features, transaction speeds, scalability, energy consumption, consensus mechanisms, security protocols, and limitations.

Table 2. Comparative study between IOTA 2.0 and BC-based cryptocurrencies.

Feature/ Criteria	IOTA 2.0	Bitcoin	Ethereum	Hyperledger
Transaction	Up to 1,000 TPS	3-7 TPS	15-30 TPS	1,000-10,000 TPS
Speed				(varies by implementation)
Scalability	High	Low	Low	Low
Energy	Very low	High	Medium-High	Low to Medium
Consumption				
Consensus Mechanism	FPC binary voting protocol	PoW	PoW, transitioning to PoS	PBFT variants, Raft, etc.
Security Protocols	EdDSA	ECDSA	ECDSA	ECDSA
Decentralization	Fully decentralized	Fully decentralized	Fully decentralized	Permissioned (Partially decentralized)
SC Support	✓	✗	✓	✓
SC Speed	Fast execution (parallel Transactions)	-	Slower execution	Slower execution
Micro-transactions	✓	✗	✗	✗
Transactions fees	Very low	-	High	High
Limitations	Early stage of development	Scalability issues,	Scalability issues,	Limited Decentralization,
	Limited adoption	high energy consumption	gas fees	complexity
	Potential network stability issues			

4. Proposed IOTA-SDN System

This section presents our innovative proposal for an IOTA-based system designed to effectively manage and secure SDN. Illustrated in Figure 3 is the architecture of our IOTA-based SDN, where SDN controllers play a central role, guaranteeing both secure horizontal and vertical communication with switches.

IOTA 2.0 has incorporated resilient mechanisms to mitigate the consequences of denial-of-service (DoS) attacks. Nevertheless, ongoing development and testing indicate that the network is not completely immune to such threats. The IOTA Foundation and its community are continually striving to enhance the network’s security and scalability , a finite resource that diminishes over time, thus impeding its prolonged accumulation. Furthermore, we proposed integrating a smart contract-based DoS detector, which is critical to proactively counter potential threats, thereby strengthening the system’s security posture.

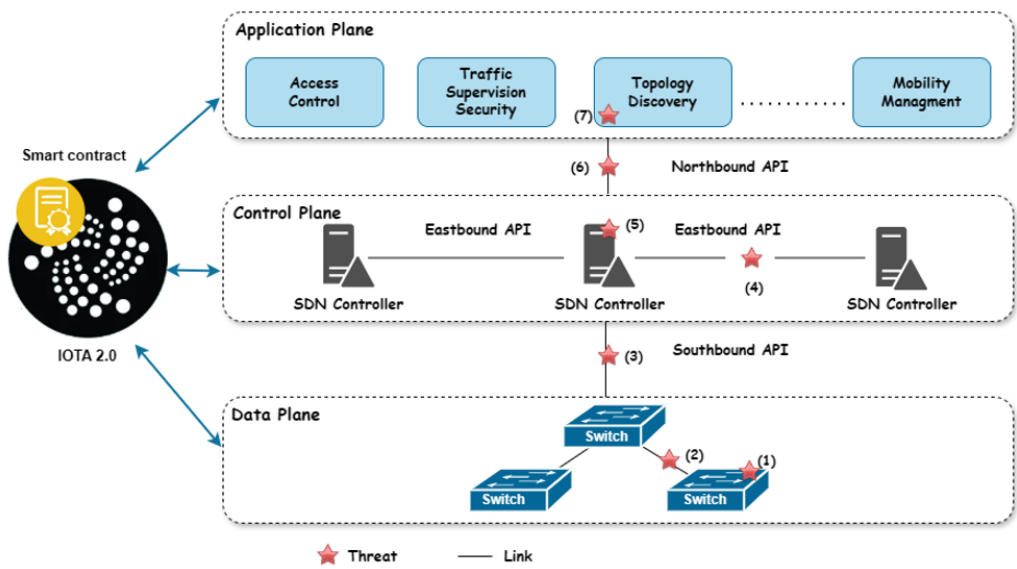


Figure 3. IOTA-based SDN.

Our system involves ISPs, each overseeing its own dedicated controller linked to a set of switches, functioning as primary administrators and standby controllers for other domains. Collaborative efforts among ISPs are essential to extend network coverage across various ISPs domains. It’s imperative to monitor this collaboration to prevent any ISPs from violating regulations or operating independently within the network. The contracts we’ve designed establish an access control framework for controllers, ensuring secure, regulated, and well-organized collaboration in the network’s operations. This ecosystem involves three key actors, as illustrated in the accompanying Figure 4.

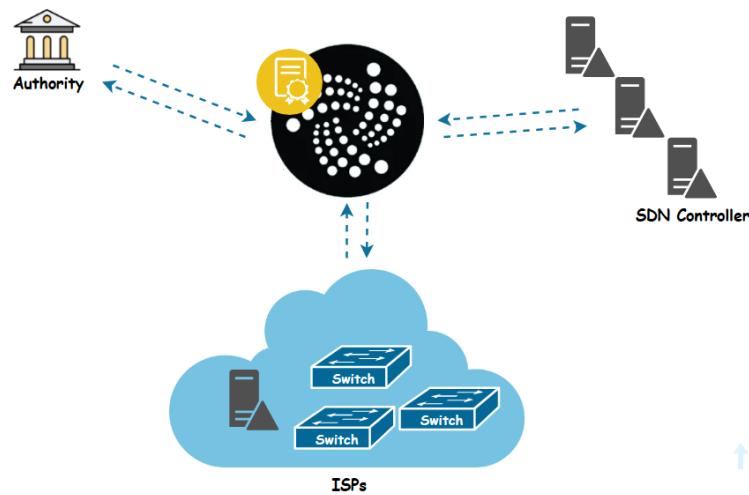


Figure 4. IOTA-based system for SDN.

- **The Authority:** functioning as a Certificate Authority (CA), holds pivotal responsibility in overseeing the involvement of trusted entities, specifically ISPs, within our proposed system. Its primary role lies in ensuring the exclusive authorization of an ISP to integrate its controller, switches, and standby controller components. Moreover, the CA serves as a cornerstone in upholding the security and integrity of the system by meticulously managing the authorization procedures for these entities. Furthermore, it defines the expiration parameters of digital certificates and offers essential revocation services to invalidate non-expired certificates when necessary.

- **ISPs:** within our system, only trusted entities (ISPs), approved by the Authority acting as (CA), are granted access. Each ISP assumes a critical role, maintaining its controller and switches. These controllers serve as primary administrators, intricately connected to a network of switches, facilitating efficient data transmission and network management. Notably, ISPs wield the authority to manage access permissions, authorizing or withdrawing access and integrating or excluding backup controllers across different network domains. This architecture ensures both robust network functionality and stringent security standards, empowering ISPs to oversee their network infrastructure effectively.
- **The SDN controller:** within the system architecture, the controller assumes a dual role of paramount importance. Firstly, it functions as the primary administrator within its designated domain, overseeing and orchestrating network operations, managing data flow, and ensuring the smooth functioning of connected switches. As the primary administrator, the controller holds authoritative control over the domain's network infrastructure, making critical decisions to optimize performance and maintain security. Additionally, the controller assumes the crucial responsibility of serving as the standby controller for other domains within the system. In this capacity, it stands ready to assume control in the event of a primary controller failure or disruption, ensuring seamless continuity of network operations. This dual functionality not only enhances the efficiency and reliability of network management within individual domains but also contributes to the overall resilience and fault tolerance of the system as a whole.

4.1. Overview of the Architecture and Components of the Proposed System

The workflow of our proposed model involves actors and SCs in IOTA based SDN, Which is implemented by three SCs illustrated in Figure 5.

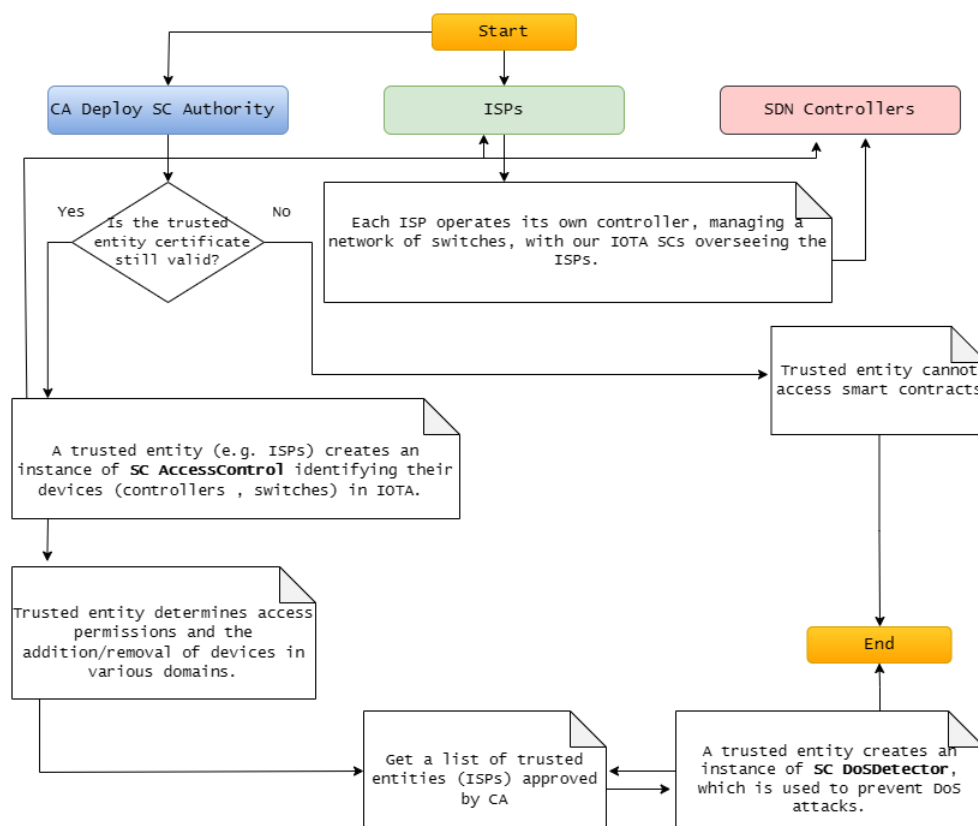


Figure 5. The workflow of our proposed model.

We clarify our solution's workflow by involving the actors and the previously presented SCs. Initially, the CA deploys an SC Authority instance in IOTA and maps trusted entities (ISPs) by linking their IOTA addresses to their public key certificates. Each ISP then creates an SC Access Control instance to manage its devices (SDN controllers and switches), determine access permissions, and manage devices. Once the CA approves a list of trusted entities, the ISP creates an SC DoS Detector instance to protect against DoS attacks.

Finally, each CA-approved ISP operates its own SDN controller, managing a network of switches. These SDN controllers serve as primary administrators and standby controllers for other system domains. Furthermore, our system facilitates collaboration among ISPs to extend network coverage across various ISP domains, with our SCs overseeing the ISPs to secure SDN environments.

4.2. Smart contract Authority of CA

It is responsible for managing the approval and authorization of trusted entities (ISPs) to participate in our proposed network. Figure 6 illustrates the functions within the SC and the actors involved.

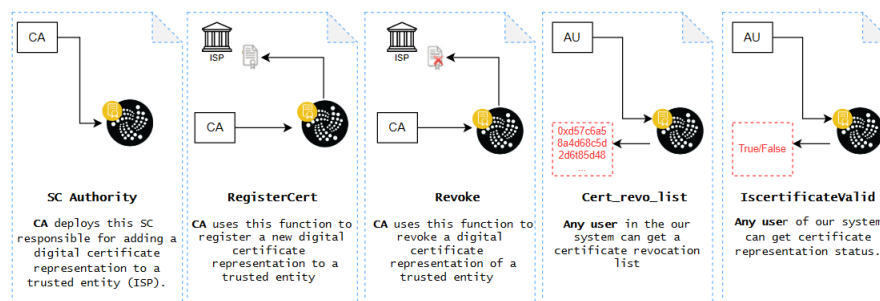


Figure 6. The workflow of the smart contract Authority along with the actors involved in IOTA.

Rectangles labeled "CA" in steps 1, 2, and 3 denote Certificate Authority, while those labeled "AU" in steps 4 and 5 represent any user within the IOTA-based SDN. Step 2 provides registration certification representation for the ISP, while Step 3 presents revoke registration certification representation for the ISP. Step 4 offers a list of revocation certifications, and Step 5 presents certification representation status.

Further details about the SC Authority are presented in the simulation results section.

4.3. Smart contract Access Control of CA

This SC governs access control between devices within their respective domains in an SDN environment. Figure 7 shows the functions in the SC along with the actors involved.

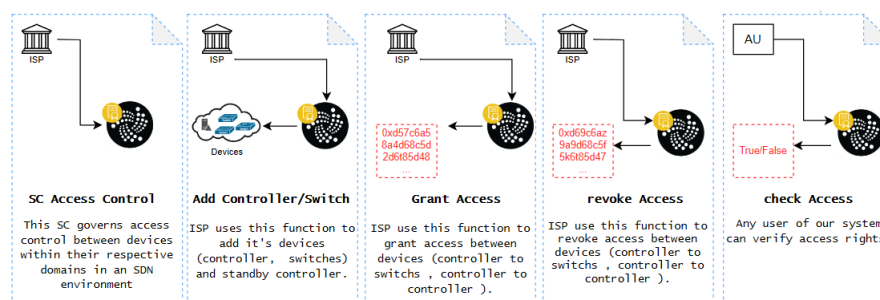


Figure 7. The workflow of the smart contract Access Control along with the actors involved in IOTA.

The ISP, approved by CA in steps 1, 2, 3, and 4, is recognized as a trusted entity. Step 2 involves presenting devices such as SDN controllers and switches. Step 3 entails furnishing a list of granted

access between devices (controller to switch, controller to controller). Step 4 involves providing a list of revoked access between devices (controller to switch, controller to controller). Step 5, denoted as "AU," represents any user in the IOTA-based SDN. The simulation results section provides more information about SC Access Control.

4.3.1. Smart contract DoS Detector of CA

This contract mitigates DoS attacks by monitoring individual devices, recording their request counts and timestamps. It enforces a limit on the maximum number of requests allowed within a specified timeframe. Figure 9 shows the functions in the SC along with the actors involved.

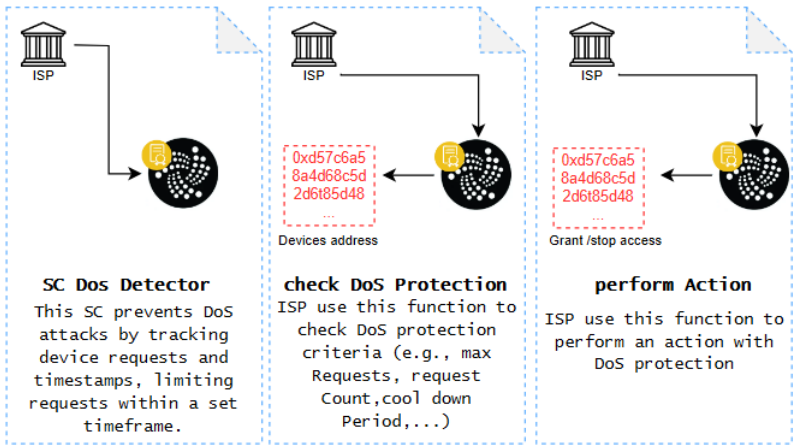


Figure 8. the workflow of the smart contract DoS Detector along with the actors involved in IOTA.

The CA establishes the ISP as a trusted entity in steps 1, 2, and 3. Step 2 evaluates the Dos protection criteria, including maximum requests, timestamp, request count, and cooldown period, for each device address. Step 3 entails taking action (granting or stopping access) based on the Dos protection criteria. The simulation results section provides more information about the SC Dos Detector.

4.4. Key Benefits of the Proposed System

Our innovative system integrates an IOTA 2.0 layer, enhancing the security of SDN infrastructure. Utilizing SCs ensures robust security for both horizontal and vertical communication channels. This system also establishes a trusted entity (ISP) to oversee its domain, including controllers, switches, and standby controllers. This trusted entity meticulously manages access permissions in collaboration with other accredited entities, bolstering the system’s overall security framework. Furthermore, our proposed model includes a Certification Authority (CA) serving as the trusted service provider for safeguarding the SDN infrastructure. It achieves this by authenticating trusted entities through the mapping of their IOTA addresses to their corresponding public key certificates. Specifically, our proposal entails the inclusion of trusted entities possessing valid certificates authorized by the Certification Authority (CA), permitting them to actively engage within our system.

Our proposed IOTA-SDN system integrates stringent security measures like authority, DoSDetector, and access control through SCs within IOTA 2.0. This robust approach ensures data integrity and prevents unauthorized access, positioning it as a strong defense against diverse attacks in distributed SDN environments. IOTA’s innate security features add an extra layer of protection, fortifying the SDN against potential threats like DoS attacks.

5. Simulation Results and Discussion

In this section, we detail the integration of smart contracts into our proposed system, developed using the Remix IDE and written in Solidity. We deploy this system on the ShimmerEVM IOTA Test

Network, a sophisticated testing environment that evaluates protocol changes before applying them to the IOTA mainnet. After connecting to the ShimmerEVM network and adding SMR funds to the MetaMask wallet, Figure 9 shows the account balance. Our approach uses Mininet and Python to create the SDN environment and seamlessly integrate IOTA 2.0. The initial implementation of IOTA Smart Contracts (ISC) will take place on ShimmerEVM, adhering to Ethereum standards. Figures provide visual insights into the test transactions and other relevant data.

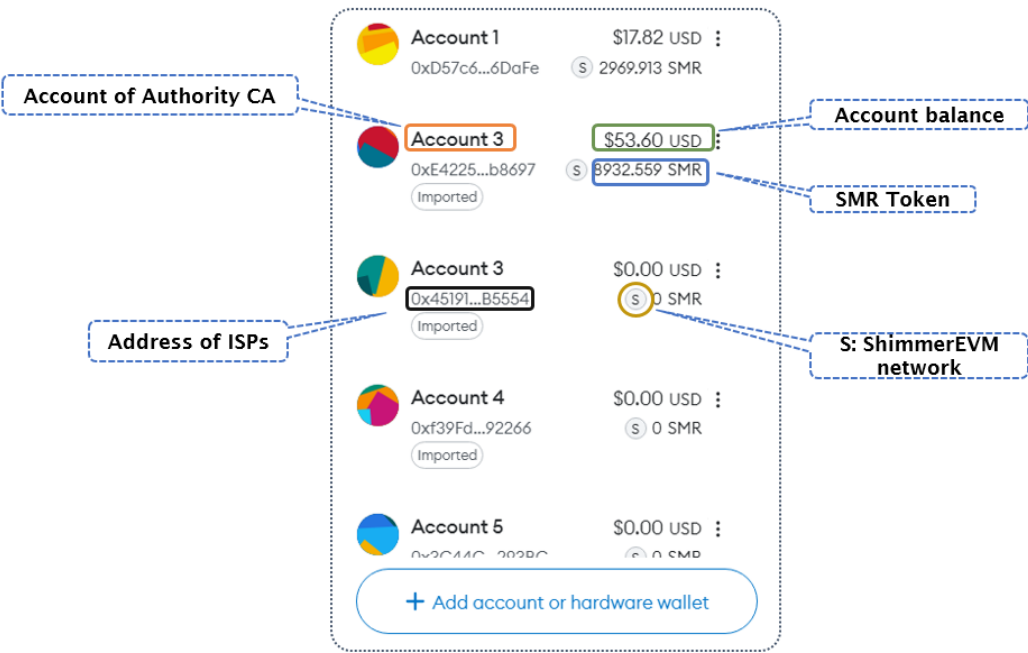


Figure 9. Account balance after adding the ShimmerEVM network and obtaining SMR funds in the MetaMask wallet.

5.1. Emulation SDN using Mininet

Mininet is a leading emulator in the field of SDN, providing academics and developers with a flexible platform for creating virtual networks, exploring SDN concepts, and examining network applications. Mininet effortlessly combines with prominent SDN controllers like OpenDaylight, ONOS, and Ryu, enabling customers to evaluate the effectiveness of their SDN applications across various controller platforms. Mininet enables users to create complex network setups using Python scripts or command-line tools, thanks to its user-friendly interface and powerful network simulation capabilities. The fact that it is open-source encourages collaboration within the community, and its extensive use in academic circles highlights its important function as a teaching resource for networking and SDN curriculum.

In summary, Mininet replicates real-world network environments, empowering us to seamlessly construct and operate virtual networks optimized for research and development purposes. Indeed, our network comprises two topologies, each comprising 1 controller, 2 switches, and 4 hosts, as illustrated in Figure 10. By default, Mininet runs Open vSwitch in OpenFlow mode, which necessitates the inclusion of an OpenFlow controller. Once we established our network via a Python script in Mininet, we ensured secure communication among networking devices (controllers, switches, and hosts) through the IOTA 2.0 network, facilitated by the three SCs detailed in the next sections.

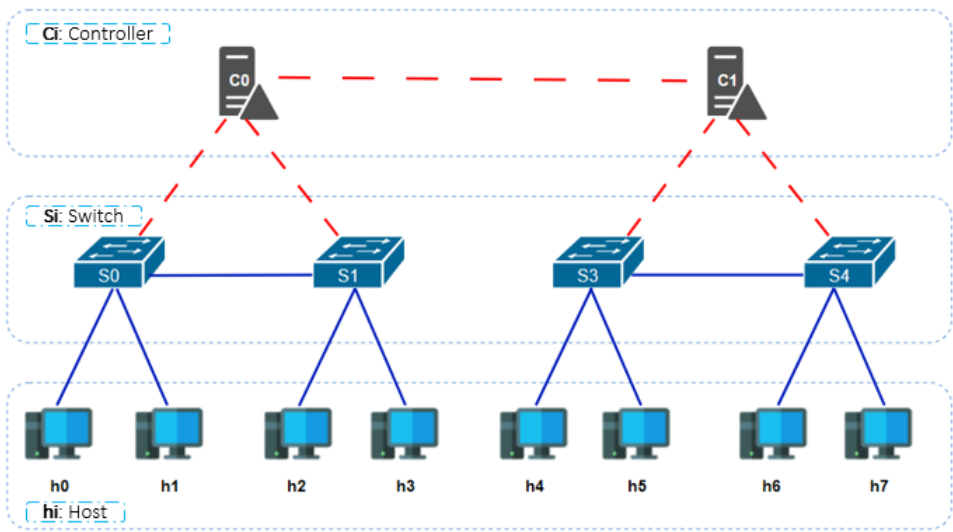


Figure 10. Topology of our system for Securing SDN Based IOTA 2.0.

5.2. Smart Contract Authority

We use this SC to regulate which trusted entities (ISPs) can participate in our proposed system. Figure 11 details the transaction specifics for deploying an instance of ‘SC-Authority’. It indicates the transaction status, as well as the contract and sender addresses. Additionally, it specifies the transaction destination, which is the smart contract constructor.

DEPLOY & RUN
TRANSACTIONS

ENVIRONMENT

Injected Provider - MetaMask

Custom (1073) network

ACCOUNT

0xE42...b8697 (8933.072289)

GAS LIMIT

Estimated Gas

Custom

3000000

VALUE

0

Wei

CONTRACT

Authority - contracts/Authorit

Deploy

Deploy the Authority SC on the ShimmerEVM using the Remix IDE.

Transaction log: Example of adding a digital certificate representation

✓ [block:1596676 txIndex:-] from: 0xe42...b8697 to: Authority.RegisterCert(address,bytes32,uint256) 0x605...96413 value: 0 wei data: 0x115...cdf5 logs: 1 hash: 0x6ed...39829

Status: 0x1 Transaction mined and excution succed

Transaction hash: 0xf9b577068fe8e58501d3e34ccc9b0beb8ab9bf4a1088540529a2f10a17d825e2

Block hash: 0x6edd3d1caf1eba397011bd077ea81c892d74fcfd28f1430906d1f74e4f839829

Block number: 1596676

Contract address: 0x605601b1121e1d91fe5626c0ad5c934caf96413

From: 0xe422568f3c95990e5f58be87b27f0804017b8697

To: Authority.RegisterCert(address,bytes32,uint256)

Gas: 630036 gas

Transaction cost: 630036 gas

// include ISPs address, public key and digital certificate expiration
Input : address,bytes32,uint256
{
 "address ISPs": "0xD57c6a55439A61e8874160502f591bD1bf96DaFe",
 "bytes32 publicKey": "0x51897b64e85c3f714bba707e86791429...",
 "uint256 expiry": "1979505397"
}
Log & event: "Certified"

Figure 11. Remix IDE screen of our deployed Authority smart contract.

Once deployed on the ShimmerEVM Network, the authority can invoke the SC’s functions using the SC authority address shown in Figure 11. Specifically, to add a digital certificate representation within the ShimmerEVM network, the authority utilizes the *RegisterCert* function. Figure 12 illustrates the ShimmerEVM network’s deployment and interaction with SC-Authority.

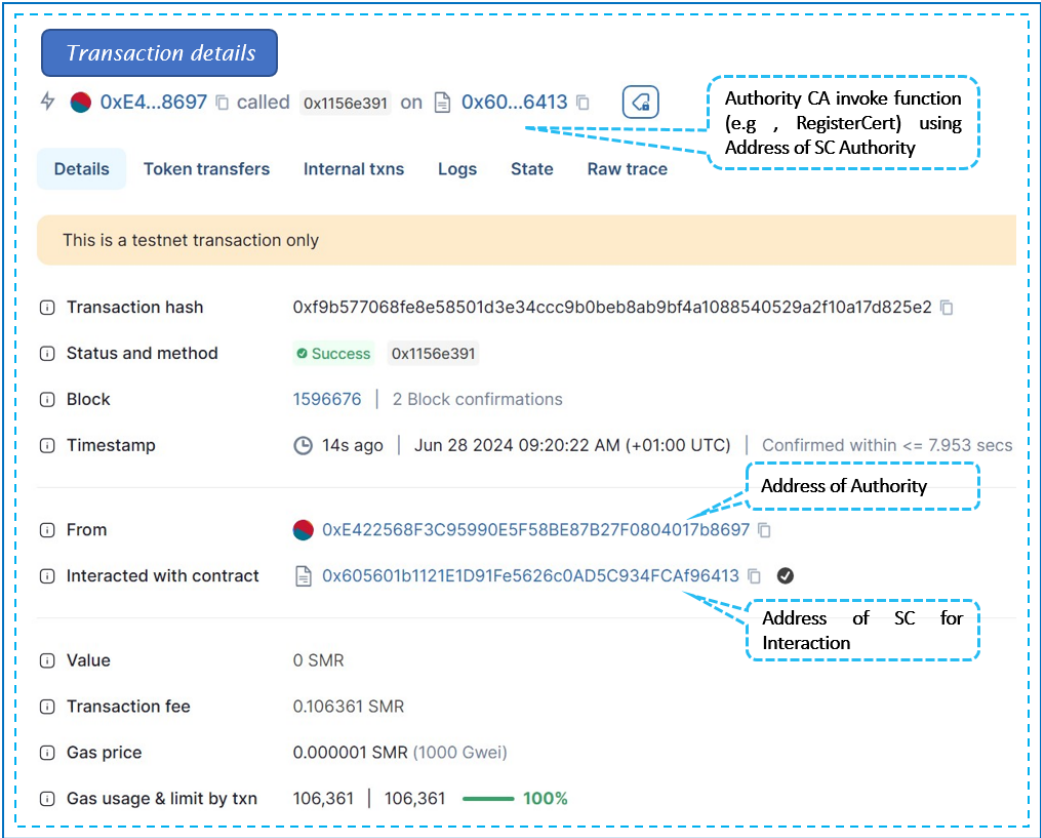


Figure 12. EVM testnet shimmer network screen of interaction with our smart contract Authority.

Furthermore, events are implemented for each addition in the IOTA (refer to Listing 2), accessible for use by listening applications. Listing 2 showcases the log of the "certified" event after the SC owner triggers the *RegisterCert* function.

Listing 1. The Example of event Register certificate.

```
event Certified(address from, address to, uint date);
logs[
{
  "from": "0x8d9df211b95dc762ce18d8a732bd78dd92b044a0",
  "event": "Certified",
  "args":{
    "from": "0xE422568F3C95990E5F58BE87B27F0804017b8697",
    "to": "0xD57c6a55439A61e8874160502f591bD1bf96DaFe",
    "date": "1717521759"
  }
}]
```

The validation of the ISP’s certificate’s authenticity is obtained through the *isCertificateValid* function. Additionally, the authority has the ability to revoke a digital certificate using the *revoke* function. Furthermore, a digital certificate is rendered invalid upon expiration. The function *cert_revo_list* provides an array of addresses belonging to trusted entities whose certificates have been revoked.

5.3. Smart Contract Access Control

This contract manages access control between controllers and switches within their respective domains in an SDN setup. The AccessControl constructor designates ISPs as the owners of the SC,

achieved by incorporating the address of the previously deployed authority contract and the address of the trusted entity with a valid certificate. Figure 13 outlines the transaction details for instantiating 'SC-AccessControl'. It includes the transaction status, followed by the contract and sender addresses, and specifies the transaction's destination, which is the SC constructor.

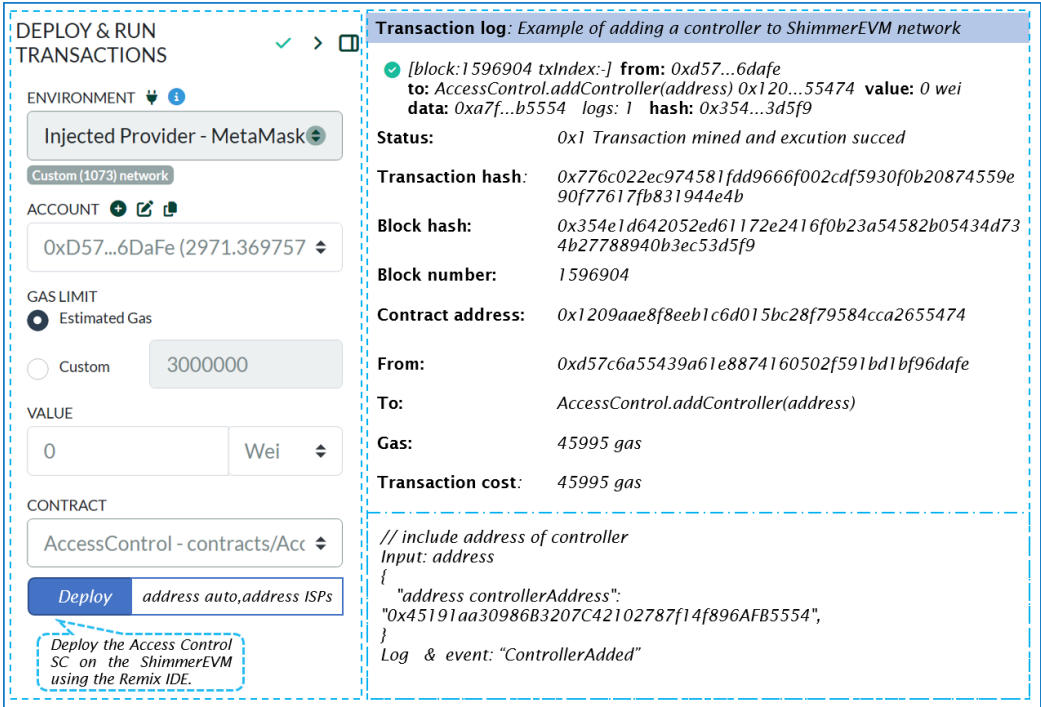


Figure 13. Remix IDE screen of our deployed Access Control smart contract.

Once deployed on ShimmerEVM, ISPs can invoke the SC's functions using the address of the AccessControl SC shown in Figure 13. Specifically, to add controllers to the ShimmerEVM network, ISPs utilize the `addController` function.

Listing 2 displays the log of the "ControllerAdded" event that occurs after the SC owner triggers the `addController` function.

Listing 2. The Example of event add controller.

```
event ControllerAdded(address from, address to, uint date);
logs[
{
  "from": "0xdd913e4bde911a89f96a16cbe3d410fe0e10348c",
  "event": "ControllerAdded",
  "args":{
    "to": "0x73C964F73738931B54686bF02E6Cc774f2Db44e8",
    "date": "1702817133"
  }
}]
```

ISP administrators can grant or revoke access controls, add or remove standby controllers across domains, and manage controllers and switches with this contract. The contract features functions like `checkAccess` to verify access rights and `grantControllerAccess/revokeControllerAccess` to regulate communication among controllers. These functionalities enhance security and facilitate efficient management within the SDN environment.

5.4. Smart Contract DoS Detector

This contract monitors individual devices by tracking their request counts and timestamps, enforcing a limit on the maximum number of requests permitted within a specified cooldown period. Figure 14 outlines the transaction specifics for deploying an instance of SC Dos Detector. It includes the transaction status, followed by the contract and sender addresses, and details the transaction destination, which points to the SC constructor.

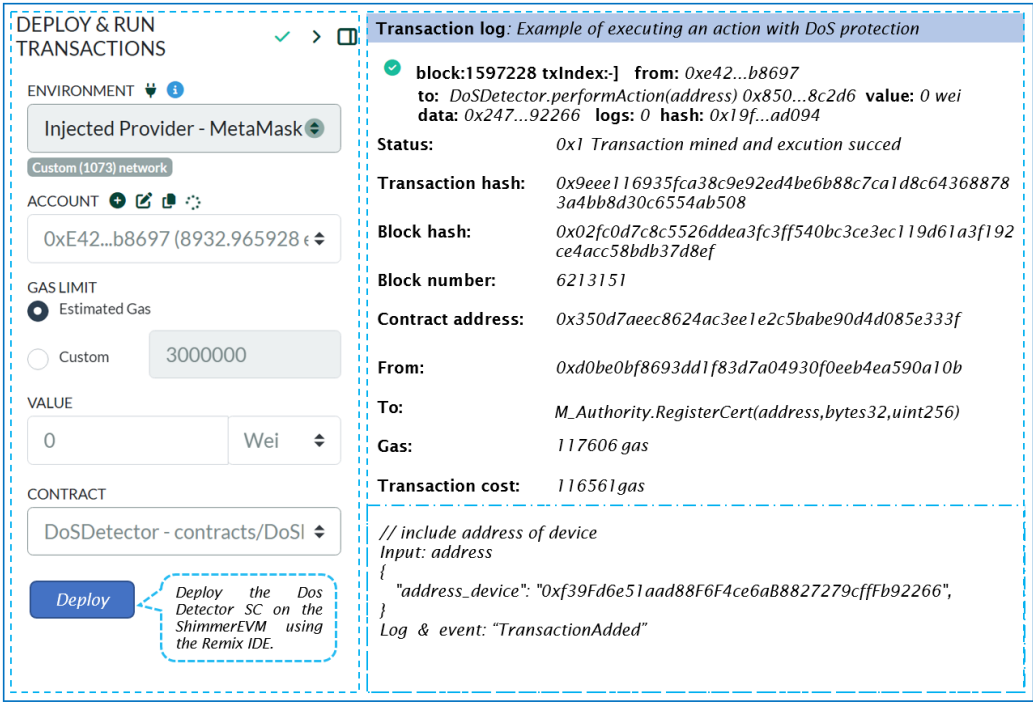


Figure 14. Remix IDE screen of our deployed DoS Detector smart contract.

The address of the DosDetector SC shown in Figure 14 enables access to the contract’s functions once deployed on the ShimmerEVM Network. Specifically, the *performAction* function is used to execute actions related to DoS protection.

Listing 3 shows the changes made to requests within our system. Specifically, it defines the maximum permitted requests within a given time period and sets the cooldown duration in seconds.

Listing 3. The adjustment of requests within our system.

```
// Maximum allowed requests per time period
uint256 constant public maxRequests = 10;

//Cooldown period in seconds
uint256 constant public cooldownPeriod = 1 minutes;
```

Our SC adopts a comprehensive approach to prevent Denial of Service (DoS) attacks, which includes checks on frequency, time, boolean values, and request volumes. Upon calling *performAction*, the contract verifies if the user’s request count breaches the predefined maximum limit within the cooldown period. If the limit remains unexceeded, the action is executed, and both the request count and timestamp are duly updated.

5.5. Limitations of the Proposed System

Our system leverages the IOTA 2.0 Tangle and the SMR token of the IOTA ShimmerEVM test network to securely record critical SDN parameters. Additionally, ISCs are implemented to ensure robust oversight of the SDN. By integrating stringent security measures, such as authority, DoS Detector, and access control through SCs within IOTA 2.0, our proposed IOTA-SDN system safeguards data integrity and prevents unauthorized access, providing robust defense against various attacks in distributed SDN environments.

However, integrating the SC DoS Detector has introduced limitations, particularly a reduction in the quality of service within our network. This has negatively impacted data traffic and increased latency. These challenges highlight the need for further improvements to balance security and performance effectively.

6. Conclusion and Future Work

This research introduces an innovative approach to securing Software-Defined Networking (SDN) environments using IOTA 2.0 smart contracts. By leveraging the IOTA Tangle, our proposed system enhances scalability and efficiency while eliminating transaction fees and reducing energy consumption. We introduced three smart contracts—Authority, Access Control, and DoS Detector—to ensure secure network operations, prevent unauthorized access, and mitigate denial-of-service attacks. Comprehensive simulations using Mininet and the ShimmerEVM IOTA Test Network demonstrated the efficacy of our approach in enhancing SDN security. Our findings highlight the potential of IOTA 2.0 smart contracts to provide a robust, decentralized solution for securing SDN environments. The results indicate that integrating IOTA 2.0 smart contracts into SDN can significantly enhance network security, reduce the risks associated with centralized control, and improve overall network resilience. Additionally, our approach offers a scalable and efficient solution, addressing the limitations of traditional blockchain-based systems. Future work will focus on enhancing the system's capabilities by integrating machine learning (ML) and deep learning (DL) algorithms to intelligently identify, predict, and mitigate cyber threats, such as DDoS attacks. By incorporating advanced ML and DL techniques, we aim to develop a more adaptive and resilient network that maintains high-quality service while ensuring robust security measures. Additionally, further research will explore optimizing the smart contracts' execution to minimize latency and improve overall system performance. Finally, we plan to extend our simulations to more complex and large-scale network environments to validate the scalability and robustness of the proposed system in real-world scenarios.

Author Contributions: Conceptualization, M.F., I.L., and Y.M.; data curation, M.F.; formal analysis, M.F., I.L., K.E.M., Z.E.A.; funding acquisition, A.A.A., P.P., and F.A.; methodology, M.F., I.L., K.E.M., Z.E.A., and Y.M.; project administration, I.L., K.E.M., Y.M., and M.F.; software, M.F., I.L.; supervision, Y.M., K.E.M., Z.E.A., F.A. and P.P.; validation, M.F., I.L., K.E.M., P.P., F.A. and Y.M.; visualization, M.F.; writing—original draft, M.F., I.L.; writing—review and editing, Y.M., K.E.M., P.P., F.A. and A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Researchers Supporting Project No. RSPD2024R564, King Saud University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their deepest gratitude to the Multidisciplinary Faculty of Nador, Mohammed Premier University, Oujda, Morocco, for their invaluable support. Additionally, they are profoundly thankful to the Researchers Supporting Project No. RSPD2024R564 at King Saud University, Riyadh, Saudi Arabia, for their essential contributions and support.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

We presented the complete implementation of our proposed system, IOTA 2.0-based SDN Smart Contracts, at: https://github.com/MedFartitchou/SDN_IOTA.

We tested IOTA 2.0-based SDN Smart Contracts at: <https://rb.gy/g0esua>.

References

1. Sezer, S.; Scott-Hayward, S.; Chouhan, P.; Fraser, B.; Lake, D.; Finnegan, J.; Viljoen, N.; Miller, M.; Rao, N. Are We Ready for SDN? Implementation Challenges for Software-Defined Networks. *IEEE Commun. Mag.* **2013**, *51*, 36–43.
2. Hu, F.; Hao, Q.; Bao, K. A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation. *IEEE Commun. Surv. Tutorials* **2014**, *16*, 2181–2206.
3. Kreutz, D.; Ramos, F.M.V.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *Proc. IEEE* **2015**, *103*, 14–76.
4. Singh, S.; Jha, R.K. A Survey on Software Defined Networking: Architecture for Next Generation Network. *J. Network Syst. Manage.* **2016**, *25*, 321–374.
5. Abdulghaffar, A.; Mahmoud, A.; Abu-Amara, M.; Sheltami, T. Modeling and Evaluation of Software Defined Networking Based 5G Core Network Architecture. *IEEE Access* **2021**, *9*, 10179–10198.
6. Bonanni, M.; Chiti, F.; Fantacci, R.; Pierucci, L. Dynamic Control Architecture Based on Software Defined Networking for the Internet of Things. *Future Internet* **2021**, *13*, 113.
7. Boukraa, L.; Mahrach, S.; Makkaoui, K.E.; Esbai, R. SDN Southbound Protocols: A Comparative Study. In *Lecture notes on data engineering and communications technologies*; 2022; pp. 407–418.
8. Ahmad, I.; Namal, S.; Ylianttila, M.; Gurtov, A. Security in Software Defined Networks: A Survey. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2317–2346.
9. Maleh, Y.; Qasmaoui, Y.; Gholami, K.E.; Sadqi, Y.; Mounir, S. A Comprehensive Survey on SDN Security: Threats, Mitigations, and Future Directions. *J. Reliab. Intell. Environ.* **2022**, *9*, 201–239.
10. Farooq, M.S.; Riaz, S.; Alvi, A. Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. *Electronics* **2023**, *12*, 3077.
11. Bhuiyan, Z.A.; Islam, S.; Islam, Md.M.; Ullah, A.B.M.A.; Naz, F.; Rahman, M.S. On the (in)Security of the Control Plane of SDN Architecture: A Survey. *IEEE Access* **2023**, *11*, 91550–91582.
12. Setitra, M.A.; Fan, M.; Benkhaddra, I.; Bensalem, Z.E.A. DoS/DDoS Attacks in Software Defined Networks: Current Situation, Challenges and Future Directions. *Comput. Commun.* **2024**.
13. Polat, H.; Polat, O.; Cetin, A. Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. *Sustainability* **2020**, *12*, 1035.
14. Bahashwan, A.A.; Anbar, M.; Manickam, S.; Al-Amiedy, T.A.; Aladaileh, M.A.; Hasbullah, I.H. A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking. *Sensors* **2023**, *23*, 4441.
15. Liu, Z.; Wang, Y.; Feng, F.; Liu, Y.; Li, Z.; Shan, Y. A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. *Sensors* **2023**, *23*, 6176.
16. Alshahrani, M.M. A Secure and Intelligent Software-Defined Networking Framework for Future Smart Cities to Prevent DDoS Attack. *Appl. Sci.* **2023**, *13*, 9822.
17. Faezi, S.; Shirmarz, A. A Comprehensive Survey on Machine Learning Using in Software Defined Networks (SDN). *Hum.-Centric Intell. Syst.* **2023**, *3*, 312–343.
18. Boukraa, L.; Essahraoui, S.; Maleh, Y.; El Makkaoui, K.; Ouahbi, I.; Esbai, R. MACHINE LEARNING-BASED INTRUSION DETECTION SYSTEMS FOR SDN: AN EMPIRICAL STUDY USING KNIME. *EDPACS* **2024**, *69*, 46–59.
19. Alharbi, T. Deployment of Blockchain Technology in Software Defined Networks: A Survey. *IEEE Access* **2020**, *8*, 9146–9156.
20. Kovacs, R.; Buzura, S.; Iancu, B.; Dadarlat, V.; Peculea, A.; Cebuc, E. Practical Implementation of a Blockchain-Enabled SDN for Large-Scale Infrastructure Networks. *Appl. Sci.* **2024**, *14*, 1914.
21. Guo, H.; Yu, X. A Survey on Blockchain Technology and Its Security. *Blockchain: Res. Appl.* **2022**, *3*, 100067.

22. Krichen, M.; Ammi, M.; Mihoub, A.; Almutiq, M. Blockchain for Modern Applications: A Survey. *Sensors* **2022**, *22*, 5274.
23. Yang, S.; Li, S.; Chen, W.; Zhao, Y. A Redactable Blockchain-Based Data Management Scheme for Agricultural Product Traceability. *Sensors* **2024**, *24*, 1667.
24. Lee, S.; Kim, Y.; Cho, S. Searchable Blockchain-Based Healthcare Information Exchange System to Enhance Privacy Preserving and Data Usability. *Sensors* **2024**, *24*, 1582.
25. Kongsen, J.; Chantaradswan, D.; Koad, P.; Thu, M.; Jandaeng, C. A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation. *J. Sens. Actuator Netw.* **2024**, *13*, 13.
26. Taherdoost, H. Blockchain Integration and Its Impact on Renewable Energy. *Computers* **2024**, *13*, 107.
27. Rustemi, A.; Dalipi, F.; Atanasovski, V.; Risteski, A. A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification. *IEEE Access* **2023**, *11*, 64679–64696.
28. Litoussi, M.; Fartitchou, M.; El Makkaoui, K.; Ezzati, A.; El Allali, Z. Digital Certifications in Moroccan Universities: Concepts, Challenges, and Solutions. *Procedia Comput. Sci.* **2022**, *201*, 95–100.
29. Biswas, K.; Chowdhury, M.J.M.; Usman, M. Blockchain of Things: Benefits, Challenges and Future Directions. *Sensors* **2024**, *24*, 934.
30. Ahakonye, L.A.C.; Nwakanma, C.I.; Kim, D.-S. Tides of Blockchain in IoT Cybersecurity. *Sensors* **2024**, *24*, 3111.
31. Arachchige, K.G.; Branch, P.; But, J. An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attacks. *Sensors* **2024**, *24*, 3083.
32. Lamriji, Y.; Kasri, M.; El Makkaoui, K.; Beni-Hssane, A. A comparative study of consensus algorithms for blockchain. In Proceedings of the 2023 IEEE 3rd International Conference on Innovative Research in Applied Science, Engineering and Technology, Mohammedia, Morocco, 18-19 May 2023; pp. 1–8.
33. Alghamdi, T.A.; Khalid, R.; Javaid, N. A Survey of Blockchain Based Systems: Scalability Issues and Solutions, Applications and Future Challenges. *IEEE Access*, **2024**.
34. Rebello, G.A.F.; Camilo, G.F.; De Souza, L.A.C.; Potop-Butucaru, M.; De Amorim, M.D.; Campista, M.E.M.; Costa, L.H.M.K. A Survey on Blockchain Scalability: From Hardware to Layer-Two Protocols. *IEEE Commun. Surv. Tutorials* **2024**, *1*.
35. Rao, I.S.; Kiah, M.L.M.; Hameed, M.M.; Memon, Z.A. Scalability of Blockchain: A Comprehensive Review and Future Research Direction. *Cluster Comput.*, **2024**.
36. Popov, S.; Lu, Q. IOTA: feeless and free. *IEEE Blockchain Technical Briefs* **2019**, *6*.
37. Silvano, W.F.; Marcelino, R. Iota Tangle: A Cryptocurrency to Communicate Internet-of-Things Data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319.
38. Fartitchou, M.; Boussouf, J.; El Makkaoui, K.; Maleh, Y.; El Allali, Z. IOTA TANGLE 2.0: AN OVERVIEW. *EDPACS* **2023**, *68*, 15–26.
39. Gilani, S.M.; Anjum, A.; Khan, A.; Syed, M.H.; Moqurrab, S.A.; Srivastava, G. A Robust Internet of Drones Security Surveillance Communication Network Based on IOTA. *Internet of Things* **2024**, *25*, 101066.
40. Denis, N.; Chabridon, S.; Laurent, M. Bringing Privacy, Security and Performance to the Internet of Things Using IOTA and Usage Control. *Ann. Telecommun.* **2024**.
41. Zhao, L.; Ferraro, P.; Shorten, R. A Smart Mask to Enforce Social Contracts Based on IOTA Tangle. *PloS One* **2024**, *19*, e0292850.
42. Lin, I.-C.; Tseng, P.-C.; Chen, P.-H.; Chiou, S.-J. Enhancing Data Preservation and Security in Industrial Control Systems through Integrated IOTA Implementation. *Processes* **2024**, *12*, 921.
43. Gligoric, N.; Escuin, D.; Polo, L.; Amditis, A.; Georgakopoulos, T.; Fraile, A. IOTA-Based Distributed Ledger in the Mining Industry: Efficiency, Sustainability and Transparency. *Sensors* **2024**, *24*, 923.
44. Mazzocca, C.; Romandini, N.; Montanari, R.; Bellavista, P. Enabling Federated Learning at the Edge through the IOTA Tangle. *Future Gener. Comput. Syst.* **2024**, *152*, 17–29.
45. Weng, J.-S.; Weng, J.; Liu, J.-N.; Zhang, Y. Secure Software-Defined Networking Based on Blockchain. *arXiv (Cornell University)* **2019**.
46. Pourvahab, M.; Ekbatanifard, G. An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology. *IEEE Access* **2019**, *7*, 99573–99588.
47. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. P4-to-Blockchain: A Secure Blockchain-Enabled Packet Parser for Software Defined Networking. *Comput. Secur.* **2020**, *88*, 101629.

48. Aujla, G.S.; Singh, M.; Bose, A.; Kumar, N.; Han, G.; Buyya, R. BlockSDN: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications. *IEEE Network* **2020**, *34*, 83–91.
49. Shashidhara, R.; Ahuja, N.; Lajuvanthi, M.; Akhila, S.; Das, A.K.; Rodrigues, J.J.P.C. SDN-chain: Privacy-preserving Protocol for Software Defined Networks Using Blockchain. *Secur. Privacy* **2021**, *4*, e178.
50. Algarni, S.; Eassa, F.; Almarhabi, K.; Algarni, A.; Albeshri, A. BCNBI: A Blockchain-Based Security Framework for Northbound Interface in Software-Defined Networking. *Electronics* **2022**, *11*, 996.
51. Kovacs, R.; Buzura, S.; Iancu, B.; Dadarlat, V.; Peculea, A.; Cebuc, E. Practical Implementation of a Blockchain-Enabled SDN for Large-Scale Infrastructure Networks. *Appl. Sci.* **2024**, *14*, 1914.
52. Han, T.; Jan, S.R.U.; Tan, Z.; Usman, M.; Jan, M.A.; Khan, R.; Xu, Y. A Comprehensive Survey of Security Threats and Their Mitigation Techniques for Next-generation SDN Controllers. *Concurrency Comput. Pract. Exper.* **2020**, *32*, e5300.
53. Chica, J.C.C.; Imbachi, J.C.; Vega, J.F.B. Security in SDN: A Comprehensive Survey. *J. Network Comput. Appl.* **2020**, *159*, 102595.
54. Ahmad, S.; Mir, A.H. Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers. *J. Network Syst. Manage.* **2021**, *29*, 1–59.
55. Kaur, S.; Kumar, K.; Aggarwal, N.; Singh, G. A Comprehensive Survey of DDoS Defense Solutions in SDN: Taxonomy, Research Challenges, and Future Directions. *Comput. Secur.* **2021**, *110*, 102423.
56. Deb, R.; Roy, S. A Comprehensive Survey of Vulnerability and Information Security in SDN. *Comput. Networks* **2022**, *206*, 108802.
57. Alrubei, S.M.; Ball, E.A.; Rigelsford, J.M.; Willis, Callum.A. Latency and Performance Analyses of Real-World Wireless IoT-Blockchain Application. *IEEE Sens. J.* **2020**, *20*, 7372–7383.
58. Zafar, S.; Bhatti, K.M.; Shabbir, M.; Hashmat, F.; Akbar, A.H. Integration of Blockchain and Internet of Things: Challenges and Solutions. *Ann. Telecommun.* **2021**, *77*, 13–32.
59. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630.
60. Adhikari, N.; Ramkumar, M. IoT and Blockchain Integration: Applications, Opportunities, and Challenges. *Network* **2023**, *3*, 115–141.
61. Helmer, L.; Penzkofer, A. Report on the Energy Consumption of the IOTA 2.0 Prototype Network (GoShimmer 0.8.3) under Different Testing Scenarios. *arXiv (Cornell University)* **2022**.
62. Popov, S. IOTA Tangle Whitepaper, **2018**. Available online: [PDF](#) (accessed on 03 June 2024).
63. Drasutis, E. IOTA smart contracts, **2022**. Available online: [PDF](#) (accessed on 03 June 2024).
64. Müller, S.; Penzkofer, A.; Polyanskii, N.; Theis, J.; Sanders, W.; Moog, H. Tangle 2.0 Leaderless Nakamoto Consensus on the Heaviest DAG. *IEEE Access* **2022**, *10*, 105807–105842.
65. IOTA Wiki. Available online: [Link](#) (accessed on 03 June 2024).
66. Conti, M.; Kumar, G.; Nerurkar, P.; Saha, R.; Vigneri, L. A Survey on Security Challenges and Solutions in the IOTA. *J. Network Comput. Appl.* **2022**, *203*, 103383.
67. Müller, S.; Penzkofer, A.; Polyanskii, N.; Theis, J.; Sanders, W.; Moog, H. Reality-Based UTXO Ledger. *Distrib. Ledger Technol.: Res. Pract.* **2023**, *2*, 1–33.
68. Popov, S.; et al. The coordicide. **2020**, 1–30. Available online: [PDF](#) (accessed on 03 June 2024).
69. Ferraro, P.; Penzkofer, A.; King, C.; Shorten, R. Feedback Control for Distributed Ledgers: An Attack Mitigation Policy for DAG-Based DLTs. *IEEE Trans. Autom. Control* **2024**, 1–8.
70. Minhas, N.N.; Mubeen, M.W.; Khawaja, H. Distributed Ledger Technologies for Electronic Health Care: IOTA-Based Remote Patient Monitoring and Telemedicine System. *Computer* **2023**, *56*, 31–39.
71. Niebla-Montero, Á.; Froiz-Míguez, I.; Varela-Barbeito, J.; Fraga-Lamas, P.; Fernández-Caramés, T.M. IOTA and Smart Contract Based IoT Oxygen Monitoring System for the Traceability and Audit of Confined Spaces in the Shipbuilding Industry. *Eng. Proc.* **2023**, *58*, 120.
72. Akhtar, M.M.; Rizvi, D.R.; Ahad, M.A.; Kanhere, S.S.; Amjad, M.; Coviello, G. Efficient Data Communication Using Distributed Ledger Technology and IOTA-Enabled Internet of Things for a Future Machine-to-Machine Economy. *Sensors* **2021**, *21*, 4354.
73. Sealey, N.; Aijaz, A.; Holden, B. IOTA Tangle 2.0: Toward a Scalable, Decentralized, Smart, and Autonomous IoT Ecosystem. *International Conference on Smart Applications, Communications and Networking (SmartNets)*, Palapye, Botswana, **2022**, pp. 1–8.

74. Apatu, E.; Goudar, P. Bitcoin Use Cases: A Scoping Review. *Challenges* **2024**, *15*, 15.
75. Kushwaha, S.S.; Joshi, S.; Singh, D.; Kaur, M.; Lee, H.-N. Ethereum Smart Contract Analysis Tools: A Systematic Review. *IEEE Access* **2022**, *10*, 57037—57062.
76. Ucbas, Y.; Eleyan, A.; Hammoudeh, M.; Alohal, M. Performance and Scalability Analysis of Ethereum and Hyperledger Fabric. *IEEE Access* **2023**, *11*, 67156—67167.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.