Blockchain Enabled Software-Defined Networks for IoT Applications: A Survey

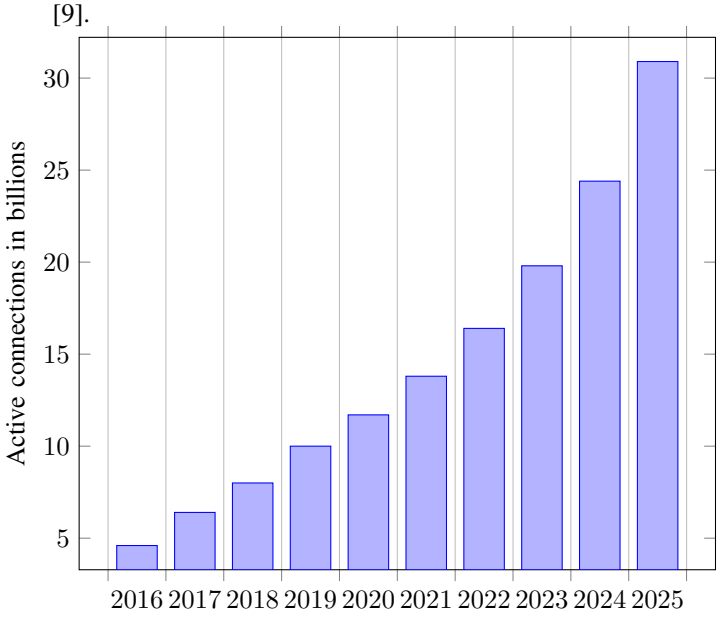
1st Austin J Derbique
School of Computing, Informatics, and Decision Systems Engineering
Arizona State University
Tempe, USA
aderbiqu@asu.edu

***Abstract*—Within the last decade, there has been a meteoric rise in Internet-of-Things (IoT) devices, connecting our world in ways that wouldn't have been possible just years ago. These data producing, networked devices are typically connected to some cloud resource off-site in order to provide compute, storage, and networking. While implementations of cloud based IoT solutions we have today work to a degree of adequate satisfaction, it is unlikely to scale into the future without performance, reliability, or security problems. As such, there becomes a need for a new way of interconnecting IoT devices together. This paper identifies and discusses a number of proposed solutions to this scalability problem by using Software-Defined Networks in conjunction with Blockchain technology. With both SDN and Blockchain technologies being relatively new, there are a lot of unanswered questions; something that this paper attempts to explore. This paper analyzes various solutions and provides propositions for future research in SDN-Blockchain powered IoT applications.**

***Index Terms*—SDN, Blockchain, IoT, Security, Decentralization, Bitcoin, Ethereum, Peer-to-peer, edge computing, fog computing**

I. Introduction

There are currently 13.8 billion interconnected IoT devices in active use around the world today. It is predicted that by the year 2025, this number will rise to 30.9 billion devices [9].



Currently, IoT devices can be gadgets in your smart home like light bulbs, smart-locks, or smart-thermostats, etc. Other IoT devices that exist outside the home include smartwatches, autonomous robots, and vehicles. In the future, we are likely to see the variety of applications grow to everyday objects like parking meters, street lights, stop signs, inventory tags in super markets, etc. The possibilities are nearly endless. With all these emerging IoT devices, comes emerging new problems, such as network management, compute, and data storage.

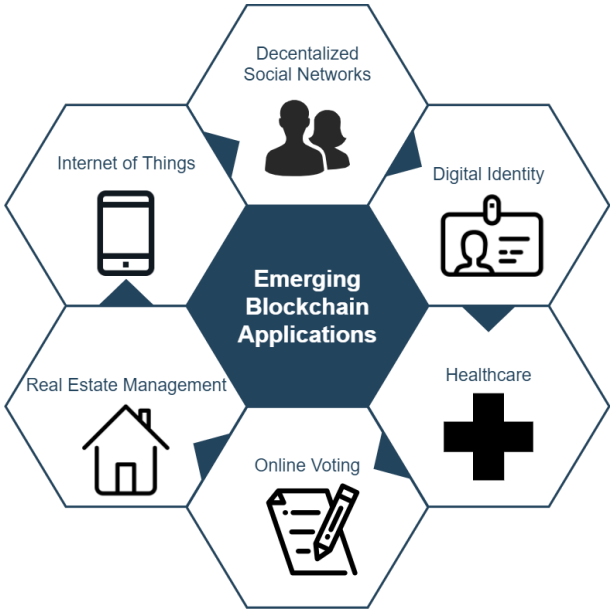


Fig. 1. Emerging Blockchain Applications

The use of blockchain technology has been on a steady rise since the recent popularity spike in blockchain's most popular implementation, Bitcoin [31]. Bitcoin is most famously known by the general public as a cryptocurrency, or digital currency. A cryptocurrency is a digital asset designed to work as a medium for peer-to-peer payments between multiple parties, storing transactions in a ledger on a decentralized database [16]. Bitcoin can be used to purchase goods or services, just like a fiat currency. In fact Elon Musk, CEO of Tesla Inc. recently announced the company would be accepting Bitcoin as a form of payment for their Tesla vehicles [27].

This mainstream adoption is a likely indicator that blockchain technologies will become a cornerstone of our future society.

It is a common misconception that blockchains can only be used as a means to spend or receive digital currency. On the Ethereum blockchain, smart contracts, which are computer programs running in an Ethereum virtual machine, execute a series logic programmed by the developer. In fact, Ethereum smart contracts are considered Turing complete, meaning the contract can carry out any set of actions that a Turing machine is capable of [3][28]. This expansive capability is powering more and more use cases every day, such as banking, healthcare, transportation, supply chain, voting, and many more not yet imagined [7]. Figure 1 shows some of these emerging use cases. This proposes the idea of what else can blockchain be used for? In this paper, we take a more in depth look at how it may be used for IoT applications.

Unlike blockchain which is decentralized in nature, software-defined networking (SDN) relies heavily upon a centralized controller node for network configuration and management. But what is SDN and why is it relevant to IoT? A software-defined network is a paradigm conceived in the mid 2000s as way of separating control between a network manager's control plane and data plane [10]. The motivation behind decoupling these two planes is to allow for agile, dynamic network implementation with a high degree of flexibility. The use case for SDN saw a significant rise in popularity with the explosion of virtualization and cloud computing. Increasingly congested and complex networks became more difficult to manage, leading for the need to design a new set of networking standards [13].

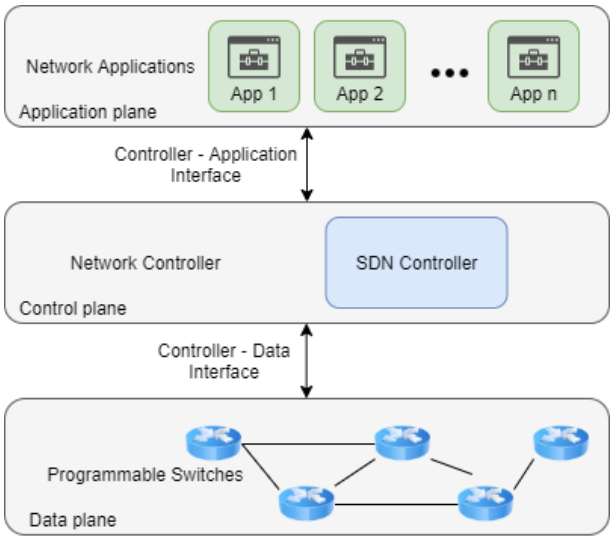


Fig. 2. Software-Defined Networking Abstraction [13]

In Figure 2, three different network planes are shown: the application plane, control plane, and data plane. The separation in these planes relinquishes decision making from the network switches, essentially turning them into basic forwarding devices. All control logic is then handled by a centralized SDN controller. We explore more in detail the consequences of this standardized approach and the security concerns that arise from having a single point of failure. But with a way to improve on SDN's shortcomings, we gain many benefits. While SDN is capable of all traditional network functionalities such as routing, load balancing, and bridging, it is also capable of functionalities not supported by legacy paradigms. These include dynamic traffic shaping, QoS administration, reduced power consumption, and data center management [13].

With SDN, Blockchain, and IoT all being new technologies brought about by the information age, it is the purpose of this paper to survey what the interoperability between these technologies and evaluate if Software-Defined Networks for IoT applications on the blockchain has a promising future ahead.

II. Background

The topics covered in this survey are relatively new in the field of computer science (within the last decade), and as such, require a basic understanding in order for the papers surveyed to appropriately be understood. Therefore, essential technical concepts are presented relating to Blockchain technologies, software-defined networks, and Internet-of-Things. Only then can we form a comprehensive evaluation of integrating these technologies together.

A. Blockchains

Although commonly referred to as "Blockchain" or "The Blockchain", a *blockchain* is really just a concept of chaining data together in a cryptographically verifiable way. This section is entitled "Blockchains" because there are many different types, each with their own unique properties. For the purposes of this paper, we will only cover two different blockchains: Bitcoin and Ethereum.

First, we talk about what a blockchain is in a technical sense, something that all blockchains have in common. A blockchain is a decentralized, cryptographically verifiable ledger which operates under a consensus mechanism.

1) Decentralization: A blockchain network consists of multiple nodes all interconnected together. This is known as peer-to-peer communication and is important to guarantee the network operates in a reliable and secure fashion. These peer-to-peer nodes share resources such as compute and storage. This increases the durability and availability of data in the event there is a partial outage or degredation. As a result, the risk of a bad actor or natural disaster bringing down the entire network is greatly reduced [18].

2) Cryptographically Verifiable Ledger: All blocks of data added to the blockchain exist forever. This is because blockchains are really a data management solution which provide a way to guarantee that data added to the chain is immutable once the block is confirmed. In Figure 3, three blocks are shown. A hash of the first block is used as one of the inputs for the second block. The contents of the second block are hashed and used as one of the inputs for the third block. By changing even a single bit in the contents of the first block, the hash will be different and provide a different

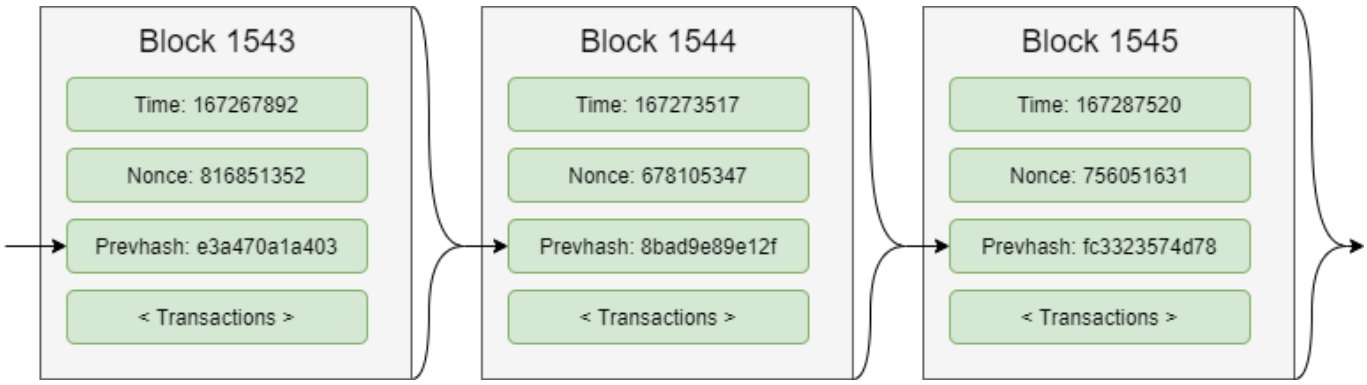


Fig. 3. Blockchain Mining [3]

input to the second block, therefore changing the hash for the third block. Therefore, we can verify the authenticity of blocks by checking the hash against confirmed blocks across nodes on the network. There is a situation where two blocks consisting of different bits of data yield the same hash, but this is considered infeasible with today's current computational power. This is known as a pre-image attack [17]. In conclusion, blocks confirmed on the chain can be verified to ensure authenticity.

3) Consensus Mechanism: Consensus is what determines whether or not a proposed block is added to the blockchain. Bitcoin uses the proof of work consensus algorithm and Ethereum uses the proof of stake consensus algorithm.

- **Proof-of-Work:** Miners must solve a mathematical puzzle in order to win the miner's fee. This mathematical puzzle consists of taking the hash value of the proposed block, incrementally trying a different nonce value each time until the target hash is achieved. Once a miner solves the puzzle, the miner shares the nonce value with the rest of the miners on the network for them to verify the solution to the puzzle. In Bitcoin, at least 51% of the nodes connected to the network need to agree before consensus is achieved. Upon consensus, the block is considered confirmed and a new block will be created for future transactions.
- **Proof-of-Stake:** Also known os PoS, mining power is proportional to the amount of coins staked by the miner. Similar to PoW, a miner must complete a mathematical puzzle. However, a miner is chosen to complete the computational puzzle, unlike PoW where the first miner to solve the puzzle gets the reward. PoS is seen as a much more environmentally friendly option as the algorithm uses a fraction of the amount of energy required to mine a block compared to it's PoW equivalent.

Why is consensus so important? In a recent article published, it was found that the Bitcoin network is consuming more energy than New Zealand and Belgium combined [30]. Proof-of-Work consensus has been found to be extremely expensive and inefficient to operate. We will explore in this paper whether using a PoS consensus model makes sense for SDN enabled IoT networks.

B. Software Defined Networks

As alluded to in the introduction, Software Defined Networks have significantly risen in popularity as virtualized computing and large data center environments continue to grow. But how does that affect distributed computing? In order to understand a distributed network utilizing SDN, we must first describe in detail what each component of SDN is responsible for and how each of the layers interoperate. These components include the application layer, control layer, and infrastructure layer. Additionally, we cover basic advantages and disadvantages of utilizing a SDN compared to legacy networking methods.

1) Infrastructure Layer: Starting at the bottom of the architecture stack is the infrastructure layer. This layer is composed of underlying networking equipment in order to carry out the forwarding of traffic for the network. These can either be physical bits of hardware, commonly network switches and routers, or they can be virtualized. In SDN, the infrastructure layer is only responsible for forwarding of traffic, not for making decisions of any kind. Examples of software-based infrastructure layer services include Open vSwitch while a physical, hardware-based examples is OpenFlow [13].

2) Control Layer: In the middle tier of SDN is the control layer. This is the core piece to the paradigm, responsible for setting up one or more centralized controllers that manage the underling infrastructure layer hardware. In addition to pushing rules and forwarding information out to the switches, the control layer also monitors the environment allowing for real time and dynamic management of the configured rules and forwarding. The SDN controller exposes two APIs. A northbound API for the application layer and a southbound API for the infrastructure layer.

- **Northbound API:** This interface communicates with the application layer and allows for the controller to be programmed by applications in a more abstract way. This communication is typically handled through REST APIs, although there is no set standard.
- **Southbound API:** Unlike the northbound API which deals with abstract data models, the southbound interface

is meant for communication with lower level, infrastructure devices. As such, these protocols are much more rudimentary, and are typically one of the following: Openflow, Ovsdb, or Netconf. While others exist, these are the most popularized protocols.

3) Application Layer: Finally, we have the application layer, an abstract area that is the most friendly to users. Here exists applications like network topology, network states, statistics, flow programming, and monitoring, etc.

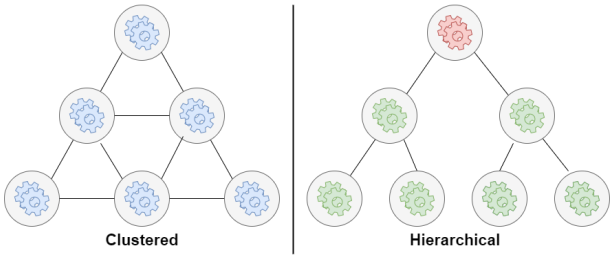


Fig. 4. Distributed controller classes [13]

Having SDN architecture split into different layers allows for isolation between data plane and control plane, while still allowing a basic set of basic communication protocols between each other. But this also leads some troubling challenges. One key disadvantage is the centralization of the controller logic inside the control plane. In an era where computing is more distributed than ever, having a single point of failure for routing decisions poses a risk to the integrity of the network. There exists research that explores the possibility of having multiple nodes, either in a master-slave role, or equal role. In Figure 4, we see a clustered approach on the left where all nodes are equal, but only one is a master at a given time, and a master-slave approach on the right where one master controls all other nodes. The usage of a distributed controller environment splits the roles of the SDN controller into smaller responsibility slices, reducing the consequences if one node becomes compromised to experiences an outage. But is this good enough? We survey various papers that attempt to build upon the distributed controller approach by utilizing blockchain technology.

C. Internet of Things

The Internet of Things, often referred to as IoT, is a paradigm that promises to integrate everyday ”things” in our world like home appliances, medical devices or vehicles and network them together as part of an internet environment. By connecting networkable, every day objects together, new avenues of innovation are possible that will accelerate progress towards a better quality of life and utilization of resources [4]. Imagine a smart city with autonomous vehicles, food delivery robots, package delivery drones, intelligent street lights, etc. Also think about agricultural applications where crops have sensors indicating nutrition level, UV exposure, or yield reports. In order to realize the full potential of IoT, we must first understand basic architecture, data and knowledge management, and security considerations.

1) Architecture: In Figure 5, there are four layers presented.

- **Sensing Layer:** IoT in its most basic form is just a collection of sensors that collect percepts of the real world and translate this information in a way a computer can understand. These sensors include but are not limited to: cameras, position, audio, light, heart rate, temperature, moisture, and time.
- **Gateway and Connectivity Layer:** Sensors are typically connected to some kind of networkable interface. Common interfaces include celluar, wired LAN, bluetooth, or wifi. This diagram is intentionally generic with routing, as many different implementations exist. We will go more into detail of how IoT devices can be routed using SDN later in the paper.
- **Processing Layer:** Now that there is a data producing sensor connected to the network, the information needs to be processed and stored. In an example, this third layer takes sensor data from a temperature module and makes the data available via API to an IoT device such as a smart thermostat in order to make a decision with the data provided, such as turning on the heater.
- **Application Layer:** Finally, we have the application layer, which is where intelligent decisions are made. These applications consume information from the data processing layer, like in the previous example of the smart thermostat retrieving the temperature from the processing layer.

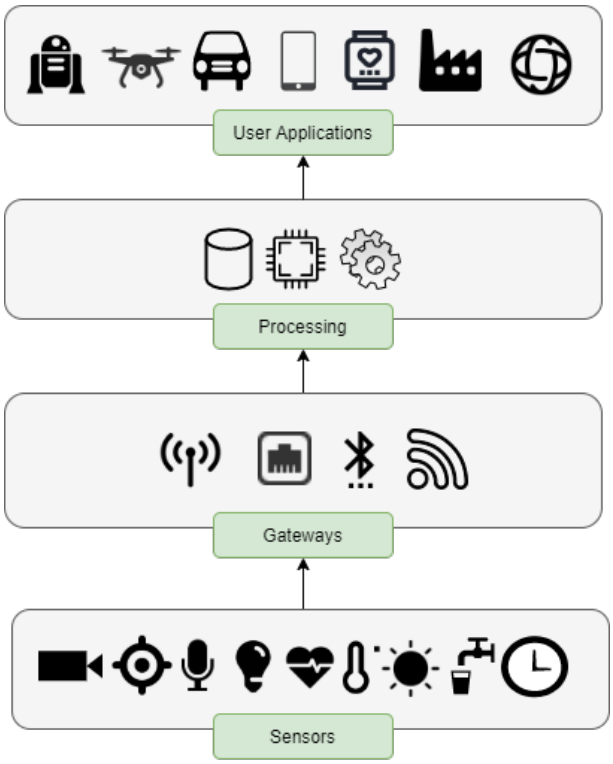


Fig. 5. IoT Architecture Layers [26]

2) Data and Knowledge Management: Internet of Things centers around data. These sensors are constantly producing information recorded of their surrounding environment. All this data needs a place to go where it can be processed as quickly as it comes in. This has led to the emergence of stream processing. Unlike batch processing which relies heavily on processing blocks of data that have already been stored for some time, stream processing allows for real time analysis of the data, allowing for key decisions to be made in the fraction of time a batch processing job would take. [29]. Stream processing has become synonymous with IoT for this reason. Popular open source stream processing platforms include Apache Kafka, Apache Storm, Apache Flink, and Apache Spark [15]. In the world of cloud, Amazon Kinesis is another popular commercial solution.

Powering the storage component of all of this data are databases. In recent years, NoSQL databases have risen to be a leader in modern distributed system data management solutions. NoSQL allows for a great extent of flexibility in data representation with support for fine grained access control, all while supporting scalability and availability needs of the application [5].

3) Security Considerations: Given the distributed nature of IoT, it is easy to see that when there are a lot of moving pieces, there is opportunities for problems to arise. Not only are IoT devices just publishing data to the internet, they are also consuming data from other devices. In a sense, these devices interconnect with one another, both on the public internet and on private networks. All this open communication allows for hackers or malformed configurations to compromise the privacy and security [4]. There are three broad categories of threats we will explore: Capture, Disript, and Manipulate.

- **Capture Threats:** Relating to capturing or obtaining system information or data traversing through the system.
- **Disrupt Threats:** Relating to destroying, denying, or disrupting the acting system.
- **Manipulate Threats:** Relating to modifying data as it is passed through. These could be false packets in order to spoof a particular device.

The most common threats include masquerading the identity of a different entity, man-in-the-middle attacks [6], or replay attacks.

III. Existing Research and Findings

While there exists a lot of research on either SDN or Blockchain, there are significantly fewer papers published on enabling SDN with the power of blockchain technology. In this section, we discuss existing reasearch including the proposed problems and solutions, and provide a critical analysis of the work completed. In order to determine whether or not the future of blockchain powered SDN is promising, we must ask ourselves several research questions. These research questions can be found in Table I, along with several follow up discussion topics to provide a more comprehensive analysis.

TABLE I
Research Questions

Research Question	Further Discussion
How can blockchain improve the existing SDN paradigm?	Determine if improvements can be made to security, availablity, and performance.
Is blockchain powered SDN a realistic solution to the IoT scalability problem?	Is there a reason to use one consensus mechanism over another? Does a permissioned blockchain make sense here?

A. Question 1: How can blockchain improve the existing SDN paradigm?

To answer this question, we much look at several important attributes in computing. These include security, availability, and performance.

In the paper SmartBlock-SDN [22], the authors propose a Blockchain-enabled SDN-IoT architecture that is capable of identifying and isolating rogue switches on the network. This is achieved by keeping track of all flow-rules by storing them on the blockchain and enforcing those rules to guarantee consistency is maintained within the cluster controller. The authors use OpenFlow as a means of connecting the blockchain ledger to the SDN controller via REST API.

Another form of security improvement comes from the proposal to use proof of stake (PoS) consenus on a permissioned blockchain for adding flow-rule blocks onto the chain [1]. Unlike the SmartBlock-SDN paper, this work proposes a central controller that stakes its network topology repository. In doing so, flow tables and packets are secured on the permissioned blockchain. This prevents bad actors from adding bad blocks and having them confirmed. Another scenario this paper proposes is in the mitigation of DDoS attacks at the control plane. Because the network is considered *permissioned*, a node will need to request to join the network. In short, each member of the blockchain will need to verify the requestor, before transactions from that entity are confirmed. Using a blacklist log, the identity verifier checks for any malicious flows from the requestor's identity. In the event the requestor is malicious or a trusted node is hijacked, the bad flows will be identified on the next block confirmation and the malicious entity will be blacklisted.

B. Question 2: Is blockchain powered SDN a realistic solution to the IoT scalability problem?

In order to answer this, we need to know whether or not blockchain is flexible enough to support the rapid growth of IoT devices and the data being produced by them. In a piece of work that focuses on SDN computing with fog nodes at the IoT edge, the authors try to answer exactly that: whether or not blockchain is an adequate solution for this scalability problem [24]. In a future with intelligent things like sensors, laptops, smart cars, home devices, etc, a huge volume of data is being produced every second. The paper raises the concern of scalability and performance of channelling all this data through strained networks to the data center for processing, and then all the way back to the device. As a result, the concept of blockchains for distributed cloud storage is explored. Not

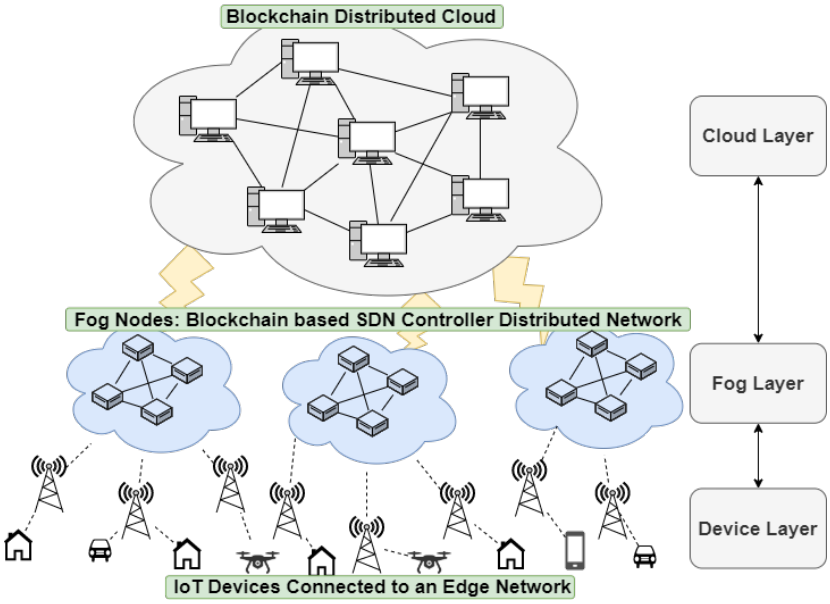


Fig. 6. IoT Blockchain CDN [24]

only does the paper show that this localizes the data to the consumers, it also provides natural redundancy as the dataset is stored in multiple copies across the blockchain. It was also found that storing a terabyte of data on Amazon S3 costs roughly $25 per month, whereas it would cost around $2 per terabyte per month on the blockchain [12].

Storage aside, it is also important to address the scalability of compute for IoT. Currently, the industry standard is to send all sensor data to the cloud for processing, and have that information sent back. Not only does this burden the already congested network, it also means that processing a piece of data takes longer than if information was localized. Using a Fog computing approach or edge computing like in DistBlockBuilding [21] allows for compute to take place geogrpahically close to the IoT devices. In many cases, within the same local network.

One such way of localizing compute near the IoT devices is to use the blockchain network itself as a cloud distributed network. In the paper BSS: Blockchain Security over Software Defined Network [1], the authors use Ethereum Smart Contracts to execute their logic programs. Using an approach like this allows for a multitude of different types of programs to be executed locally on the blockchain, bringing compute from a datacenter to your blockchain network. An added benefit to this approach is that the blockchain can span across multiple locations, allowing distributed access to compute and data from existing data centers or your local LAN.

In Figure 6, an example of distributed cloud computing over blockchain is depicted that is proposed in the Fog computing paper [24]. Here we see a plethora of IoT devices all connected to small, multi-interface base stations. These act as the gateways allowing IoT devices to communicate with the software defined network in the fog layer. Fog computing, or sometimes referred to as fog networking, is an architecture that utilizes edge devices to carry out computation, storage, and communication locally without the need to traverse all the way to the cloud [11]. This compute, storage, and communication localization reduces the the amount that needs to occur on the cloud, therefore lowering the requirements of bandwidth constraints. For the data that does need to be interconnected with the cloud, information traverses to the blockchain distributed cloud, on the top layer of the diagram. This is a blockchain network with cloud compute aggregated on top, offering compute resources for application layer programs.

C. Challenges

Upon analyzing various works of research on the topic of Blockchain enabled SDN for IoT, it is evident that there are still several challenges faced.

1) Concern with compute availability on the blockchain: Apart from proof of concept simulations executed within these research papers, is it possible to scale up to large scale workloads? Given bandwidth limitations and time required for consensus, is it feasible to transfer a large quantity of data or execute compute intensive workloads?

2) Difficulty translating virtualized test cases to the real world: Currently, blockchain networks still seen as largely experimental, with only a handful of production systems operating on them. Most existing implementaitons exist only within a virtualized environment or partitioned off test network not available to the outside world. Thhe benefit of a blockchain being immutable can also be a drawback if an error is discovered in the chaincode. That is, developers need to write in their own exit strategy into the smart contracts in the event a program needs to be terminated. This is risky, especially when dealing with sensitive information.

Paper Title	Motivation	Analysis	Published	Tags
SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT [22]	There is not an existing framework that meets requirements for a modern IoT ecosystem. This includes energy efficiency and end-to-end delay.	The paper successfully demonstrates the ablility to utlilize a blockchain ledger for the purposes of guaranteeing consistency of flow rules for the SDN controller. The paper develops a cluster-head selection algorithm, and is able to accurately measure how much energy is being used. Ultimately, it is difficult to realize the success of this work without implementing the proposed architecture in the real world.	Feb 2, 2021	Blockchain, SDN, IoT, Cluster Head Selection, flow rule management
BlockSDN: Blockchain as a Service for Software Defined Networking in Smart City Applications [1]	SDN appears to be a great solution to the rise in IoT, but has some large vulnerabilities, namely the centralized controller. There are several security challenges facing SDN that need to be addressed.	A focus on various attack vectors is performed. Several are identified at various layers including application and control planes. The solutions proposed appear to do well in mitigating the attacks, but do not account for all issues. The paper openly acknowledges there are still many open issues that need to be handled effectively in the future to make this framework robust and reliable.	Apr 2, 2020	BaaS, SDN, Smart City, Attack Management
A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT [24]	Rising usage of IoT devices has caused a spike in data uploaded to data centers. This strains traditional networking architectures and leads to a need for improved edge computing.	Fog computing at the IoT edge is proposed as a means of localizing the storage and compute to the IoT devices themselves. This successfully lowers latency and increases reliability of the network. A unique characteristic this paper presents is creating a CDN out of the blockchain network, which in turn opens up a large amount of possibilities for SDNs to be layered on top.	Sep 29, 2017	IoT, Blockchain, Cloud, Fog computing, SDN, Edge Computing
DecOp: Decentralized Network Operations in Software Defined Networking using Blockchain [14]	Citing vulnerabilities of SDN networks, the authors raise concern for centralized control of the network.	Operation of the network is transferred from away from central control in favor of a decentralized, peer to peer network. The proposed methodology incorporates Amazon's Hyperledger Fabric to act as a blockchain ledger, while using Secure Service Contract (SSC) and Secure Network Operator (SNO) chaincodes to handle communication middleware. The authors used Hyperledger fabric as it is easy to deploy, and available commercially, thus drastically reducing the overhead in designing their own blockchain. This raises the question of what parts of the blockchain do we actually need? Can we retain all the benefits by just using a cryptographic ledger?	Jul 9, 2020	SDN, Blockchain, Hyperledger Fabric, Queue Scheduling
BSS: Blockchain Security over Software Defined Network [2]	Software Defined Network security is a concern to the authors and they wish to explore methods of strengthening security against fraudulent activities as well as protect against privacy violations.	This paper simulates a custom SDN topology using Mininet and utilizes Pyethereum for testing. The authors then use the test environment to send and decrypt files across the network. There is not much new knowledge to be gained from this paper, other than a practical hands on walkthrough of what was accomplished.	May 6, 2017	SDN, Blockchain, Mininet, Ethereum, P2P
Permissioned Blockchain-Based Distributed Software-Defined Industrial Internet of Things [19]	In industrial IoT environments, there are many types of data, flows, and smart devices. The need for a distirbuted SDN control plane arises, but this demands consensus for thge SDN controllers, which is no easy feat.	A permissioned blockchain is implementedto syncronize data needs and offer Byzantine fault tolerance to prevent bad actors from degrading the network. Similar to other papers, a cryptographic ledger is used to guarantee consistency between distributed SDN controllers. Q-learning is used to optimize throughput of the network.	Sep 13, 2018	SDN, IoT, Permissioned Blockchain, multiple controllers, Q-learning
DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium [20]	This paper explores the idea of being able to create intra-organization networks where smart buildings are connected and share resources over the network.	In order to achieve the motivation, the authors incorporate SDN, NFG, and blockchain together to create a connected smart home network complete with a condominium automation system. One key part of the paper focuses on the cluster head (CH) algorithm for choosing a new cluster head. While decentralized SDN controllers are still being researched, having an appropriate cluster head algorithm is essential for secure and reliable SDN.	Nov 18, 2020	IoT, SDN, blockchain, NFV, OpenFlow, Smart Buildings
DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management [21]	In recent years, the public and policymakers have raised signifianct concerns regarding the security, privacy, and transparency of IoT sensors. This presents a series of problems to research on how IoT can be more secure.	With the idea of smart buildings in mind, a Blockchain SDN is proposed to securely transfer data between IoT devices. The paper focuses on an SDN-enabled IoT gateway which allows efficient communication between devices. While the paper makes a lot of promises, the work and results are unclear if the authors achieved what they set out to accomplish.	Jul 28, 2020	IoT, Blockchain, SDN, OpenFlow, Smart Buildings

TABLE II
ANALYSIS OF RELATED WORKS

Paper Title	Motivation	Analysis	Published	Tags
DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks [25]	With the rapid increase in number and diversity of IoT devices, concerns arise regarding the flexibility, efficiency, availability, security, and scalability of current day networks. The authors seek to build a distributed network with new communication paradigms that solve these emerging issues.	DistBlockNet seeks to create a high availability SDN controller that is fault tolerant via blockchain empowerment. The authors achieve this with an OrchApp, controller, and shelter module at each local network. The shelter and OrchApp modules handle network security attacks while the controller-application handles flow rules. A concern with this paper is that SDN controller nodes are not easily distributed, and it is unclear how that problem is solved using this solution. Even in the event you have multiple SDN controllers, they need some governing authority.	Sep 8, 2017	SDN, Blockchain, Threat Prevention
Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare [23]	With a focus on smart healthcare and all of the data being generated by sensors, a means for real time processing is necessary. Part of the trouble the authors seek to find a solution for is how to appropriately aggregate geteroneous data from different types of sources.	Using exising technologies like SDN and Blockchain, the paper proposes a way to secure patient records using a decentralized and distributed database that validates, records, timnestamps, and maintains transactions and is available only to authenticated participants. One concern is the paper mentions the use of Tor routing, but does not explain how it is used. The paper presents real world use cases, but presents a limited technical portrayal of how such a system would actually be implemented. More research would be needed.	Jul 7, 2017	IoT, Security, Smart healthcare, Blockchain
An Application-aware QoS Routing Algorithm for SDN-based IoT Networking [8]	There is a massive amount of bandwidth required for the increasing number of IoT devices in use. This is leading to network congestion and degrading the quality of service (QoS).	The QoS problem is what drives the authors to propose an application-aware QoS routing algorithm known as AQRA, which is intended for SDN-based IoT networks. This routing algorithm finds the best fit paths that meet QoS requirements and dynamically adapts for better routing paths. This novel approach resulted in improved performance and shows promise in being applied in other SDN configurations.	June 28, 2018	IoT, QoS, SDN, Routing
P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking [32]	Security is one of the most challenging issues facing SDN. There are many attack vectors, namely packet parsing during file transfers.	A new blockchain enabled packet parser is proposed that retains blockchain security characteristics while supporting data processing functions. The architecture presented is built on top of Field Programmable Gate Arrays (FPGAs), to allow for faster processing speed and lower consumption of resources.	Jan 2020	SDN, Packet parser, FPGA, Blockchain, DoS, P4

TABLE III
ANALYSIS OF RELATED WORKS CONT.

3) Lack of set standards for implementing a Blockchain SDN solution: There is currently no convenient method for implementing a blockchain powered SDN. This makes it difficult when each and every academic implementation is different from one another. There is no set standard or starting point (aside from Amazon QLDB) for creating a decentralized SDN.

4) Scalability is still a challenge: All of the tests performed in the various research papers have only included several to several dozen nodes. With the rise of IoT already over billions of devices, these proposals lie largely unproven until proven at scale.

5) SDN Controllers still need to be managed: Despite various papers proposing ways of having a ledger be responsible for flow rules, SDN controller decisions still need to be made somewhere. A lot of the papers gloss over this detail, or fail to mention it entirely. In the situation where there is only one master SDN controller, this still yields a momentary lapse of failure in the event the master becomes compromised.

IV. LOOKING FORWARD

A survey of the papers analyzed shows there is still a lot of research to be accompmlished in this field. Potential areas of exploration include

- **Decentralizing the SDN controller with Ethereum Smart Contracts:** This is arguably the most difficult, but solves the issue of needing a centralized controller. With a decentralized SDN controller, the entire SDN can be decoupled and moved entirely into Ethereum smart contracts.
- **Establishing a set standard for north bound SDN APIs:** This would set a standard for developers to use that accelerates the development of Blockchain enabled SDN.
- **Further exploration on permissioned blockchains:** Understanding how we can limit access and prevent DDoS attacks by verifying the identities of entities accessing the blockchain is a lucrative ideology. More research is required to understand the feasibility of this methodology.
- **Explore blockchain-lite techonogies such as Amazon QLDB for SDN flow rule ledgers:** Because full blockchains are difficult to setup and maintain, a possible research oppurtunity is determining what can be accomplished using only Amazon Quantum Ledger Database or some other form of cryptographically verifiable ledger. Although this may not be a long term solution, it is far simpler and requires less overhead setup and resources to get working.

V. Conclusion

With the rise of Internet of Things (IoT) devices climbing into the tens of billions, it is important now more than ever to look at how we can leverage new technologies to keep up with demand. Using Software Defined Networks (SDN) in order to decouple legacy services into isolated data, control, and application planes, we now have a flexible and extensible networking paradigm. SDN alone will not solve the IoT scalability problem though, which is why this survey's exploration into how blockchain technologies can enable SDN to be more performant, secure, and available is so important.

This paper covers a multitude of different topics ranging from the backgroud of SDN, Blockchain, and IoT, to taking the deep dive into current research in this field. From the work surveyed, it can be concluded that blockchain enabled SDN shows a promising future for IoT applications. This paper also shows the strategic advantages of combining such technologies together and provides insights into future explorations on the topic. With future research, the world of blockchain enabled SDN for IoT is expected to show major promise and may even possibly be powering the world of tomorrow.

Declaration of Competing Interest

The author declares that there is no competing financial interest or personal relationships that could appear to influence the work reported in this paper.

Acknowledgement

The author thanks Dr. Dijiang Huang for his guidance as a research professor and insights into writing a well articulated technical survey.

References

[1] G. S. Aujla et al. "BlockSDN: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications". In: *IEEE Network* 34.2 (2020), pp. 83–91. DOI: 10.1109/MNET.001.1900151.

[2] S. R. Basnet and S. Shakya. "BSS: Blockchain security over software defined network". In: *2017 International Conference on Computing, Communication and Automation (ICCCA)*. 2017, pp. 720–725. DOI: 10.1109/CCAA.2017.8229910.

[3] Vitalik Buterin. *Ethereum Whitepaper*. 2013. URL: https://ethereum.org/en/whitepaper/.

[4] Rajkumar Buyya and Amir Vahid Dastjerdi. *Internet of things: principles and paradigms*. Elsevier/Morgan Kaufmann, 2016.

[5] Rick Cattell. "Scalable SQL and NoSQL data stores". In: *ACM SIGMOD Record* 39.4 (2011), pp. 12–27. DOI: 10.1145/1978915.1978919.

[6] Zoran Cekerevac et al. "INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS". In: *MEST Journal* 5 (July 2017), pp. 15–5. DOI: 10.12709/mest.05.05.02.03.

[7] Luke Conway. *Blockchain Explained*. Nov. 2020. URL: https://www.investopedia.com/terms/b/blockchain.asp.

[8] Guo-Cin Deng and Kuochen Wang. "An Application-aware QoS Routing Algorithm for SDN-based IoT Networking". In: *2018 IEEE Symposium on Computers and Communications (ISCC)* (2018). DOI: 10.1109/iscc.2018.8538551.

[9] Published by Statista Research Department and Jan 29. *Global number of connected IoT devices 2015-2025*. Jan. 2021. URL: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.

[10] Nick Feamster, Jennifer Rexford, and Ellen Zegura. "The Road to SDN". In: *Queue* 11.12 (2013), pp. 20–40. DOI: 10.1145/2559899.2560327.

[11] *Fog computing*. Feb. 2021. URL: https://en.wikipedia.org/wiki/Fog_computing.

[12] Zach Herbert. *Why blockchains are the future of cloud storage.* Feb. 2017. URL: https://blog.sia.tech/why-blockchains-are-the-future-of-cloud-storage-91f0b48cfce9.

[13] Dijiang Huang, Ankur Chowdhary, and Sandeep Pisharody. *Software-defined networking and security: from theory to practice*. CRC Press/Taylor & Francis Group, 2019.

[14] E. Moges and T. Han. "DecOp: Decentralized Network Operations in Software Defined Networking using Blockchain". In: *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2020, pp. 225–230. DOI: 10.1109/INFOCOMWKSHPS50562.2020.9162978.

[15] Janakiram MSV. *All the Apache Streaming Projects: An Exploratory Guide*. July 2016. URL: https://thenewstack.io/apache-streaming-projects-exploratory-guide/.

[16] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Aug. 2008. URL: https://bitcoin.org/bitcoin.pdf.

[17] Arvind Narayanan. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[18] Michael Noll. Jan. 1994. URL: http://www.columbia.edu/dlc/wp/citi/citi517.html.

[19] C. Qiu et al. "Permissioned Blockchain-Based Distributed Software-Defined Industrial Internet of Things". In: *2018 IEEE Globecom Workshops (GC Wkshps)*. 2018, pp. 1–7. DOI: 10.1109/GLOCOMW.2018.8644520.

[20] A. Rahman et al. "DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium". In: *IEEE Access* 8 (2020), pp. 209594–209609. DOI: 10.1109/ACCESS.2020.3039113.

[21] A. Rahman et al. "DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management". In: *IEEE Access* 8 (2020),

pp. 140008–140018. DOI: 10.1109/ACCESS.2020.3012435.

[22] A. Rahman et al. “SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT”. In: *IEEE Access* 9 (2021), pp. 28361–28376. DOI: 10.1109/ACCESS.2021.3058244.

[23] M. A. Salahuddin et al. “Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare”. In: *Computer* 50.7 (2017), pp. 74–79. DOI: 10.1109/MC.2017.195.

[24] P. K. Sharma, M. Chen, and J. H. Park. “A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT”. In: *IEEE Access* 6 (2018), pp. 115–124. DOI: 10.1109/ACCESS.2017.2757955.

[25] P. K. Sharma et al. “DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks”. In: *IEEE Communications Magazine* 55.9 (2017), pp. 78–85. DOI: 10.1109/MCOM.2017.1700041.

[26] Amit Kumar Sikder et al. “A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications”. In: (Feb. 2018).

[27] Inc. Tesla. *Tesla, Inc. SEC Filing #0001318605*. Feb. 2021. URL: https://www.sec.gov/ix?doc=/Archives/edgar/data/1318605/000156459021004599/tsla-10k_20201231.htm.

[28] *Turing completeness*. Jan. 2021. URL: https://en.wikipedia.org/wiki/Turing_completeness.

[29] Gowthamy Vaseekaran. *Big Data Battle : Batch Processing vs Stream Processing*. July 2018. URL: https://medium.com/@gowthamy/big-data-battle-batch-processing-vs-stream-processing-5d94600d8103.

[30] Deutsche Welle. *Why does Bitcoin need more energy than whole countries?* Feb. 2021. URL: https://www.dw.com/en/why-does-bitcoin-need-more-energy-than-whole-countries/a-56573390.

[31] *What Are the Most Traded Cryptocurrencies?* URL: https://www.plus500.com/Trading/CryptoCurrencies/What-are-the-Most-Traded-Cryptocurrencies~2.

[32] Abbas Yazdinejad et al. “P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking”. In: *Computers & Security* 88 (2020), p. 101629. DOI: 10.1016/j.cose.2019.101629.

Austin Derbique received a Bachelor of Science in Computer Science from Utah State University, Logan, Utah, USA in 2017. Upon graduation, he began work as a cloud engineer for a global satellite communications company. As a certified solutions architect on Amazon Web Services, Austin is knowledgeable with compute, storage, and networking. He is currently pursuing a Master of Science in Computer Science at Arizona State University where his research primarily focuses on future blockchain applications.