A Comparative Analysis of Distributed Ledger Technology Platforms

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 25, 2019, accepted October 30, 2019, date of publication November 15, 2019,
date of current version December 3, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2953729

A Comparative Analysis of Distributed Ledger Technology Platforms

MOHAMMAD JABED MORSHED CHOWDHURY[1], MD. SADEK FERDOUS[2,3], KAMANASHIS BISWAS[4,5], (Member, IEEE), NIAZ CHOWDHURY[6], A. S. M. KAYES[1], MAMOUN ALAZAB[7], AND PAUL WATTERS[1]

[1]Department of Computer Science and Information Technology, La Trobe University, Melbourne, VIC 3086, Australia
[2]Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet 3114, Bangladesh
[3]Business School, Imperial College London, London SW7 2AZ, U.K.
[4]Peter Faber Business School, Australian Catholic University, North Sydney, NSW 2060, Australia
[5]School of Information and Communication Technology, Griffith University, Gold Coast, QLD 4215, Australia
[6]Knowledge Media Institute, The Open University, Milton Keynes MK7 6AA, U.K.
[7]College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia

Corresponding author: Mohammad Jabed Morshed Chowdhury (m.chowdhury@latrobe.edu.au)

ABSTRACT Distributed Ledger Technology (DLT) has emerged as one of the most disruptive technologies in the last decade. It promises to change the way people do their business, track their products, and manage their personal data. Though the concept of DLT was first implemented in 2009 as Bitcoin, it has gained significant attention only in the past few years. During this time, different DLT enthusiasts and commercial companies have proposed and developed several DLT platforms. These platforms are usually categorized as public vs private, general purpose vs application specific and so on. As a growing number of people are interested to build DLT applications, it is important to understand their underlying architecture and capabilities in order to determine which DLT platform should be leveraged for a specific DLT application. In addition, the platforms need to be evaluated and critically analyzed to assess their applicability, resiliency and sustainability in the long run. In this paper, we have surveyed several leading DLT platforms and evaluated their capabilities based on a number of quantitative and qualitative criteria. The comparative analysis presented in this paper will help the DLT developers and architects to choose the best platform as per their requirement(s).

INDEX TERMS Distributed ledger technology, blockchain, immutability, DLT platforms.

I. INTRODUCTION

The emergence of Distributed Ledger Technology (DLT), with strong support for data integrity, authenticity and provenance, has opened up the door of opportunities in different domains. One form of distributed ledger design is blockchain which records agreements, contracts and sales in a continually updated list. Although initially developed to support crypto-currency, this peer-to-peer system has come into prominence and gained popularity across a wide range of industry applications, as for example, supply chain, healthcare, education, finance, transport and governance. The inherent properties of DLT such as resiliency, integrity, anonymity, decentralization and autonomous control have fostered the early adoption of this technology in almost every application domain. Now, the experts and researchers all around the globe have been trying to explore the strengths and weaknesses of this game changing technology for the last couple of years.

With the increase in DLT application domains, the number of DLT platforms has also increased steadily. In addition to common DLT platforms, DLT developers and commercial companies have proposed and developed many application specific platforms that include capital markets, energy trading, digital supply chain, identity management, file sharing, and automated contracts. Some of them are in the early stages of development whereas others are currently in operation [1]. These platforms vary from each other in many ways such as their design, purpose, way of access, way of governance and so on. For example, anyone should be able to access Bitcoin [2], make transactions and be a validator whereas only authorized users can join in a Multichain [3] platform. Similarly, the block creation time, transaction rates, block

The associate editor coordinating the review of this manuscript and approving it for publication was Laurence T. Yang.

and transaction sizes play important roles in determining the performance of a DLT system which will vary for different DLT platforms. In a nutshell, it is important to understand the characteristics and capabilities of DLT platforms to select the most suitable platform for a particular application.

Towards this aim, we evaluate the feasibility of a number of DLT platforms. The selected platforms are: Bitcoin [4], Ethereum [5], Hyperledger Fabric [6], Hyperledger Sawtooth [7], Hyperledger Burrow [8], EOS [9], Multichain [3], R3 Corda [10], Cardano [11], IOTA [12], and WaltonChain [13]. The rationale for selecting these platforms are: i) the selected platforms represent the most well-established DLT platforms within the domain of private and public distributed ledgers and ii) the selected platforms cover a wide variety of application domains ranging from simple IoT (Internet of Things) use-cases to complex financial ecosystems.

A. STRUCTURE OF THE PAPER

The paper is organized as follows: Section II presents a brief overview of related works. A short introduction on the Distributed Ledger Technology (DLT) by outlining its different properties and types is presented in Section III. Section IV provides a technical synopsis of the selected DLT platforms. The evaluation criteria are detailed in Section V whereas the evaluation outcomes and critical analysis are presented in Section VI. Finally, Section VII concludes the paper.

II. RELATED WORK

In the past few years, many research have been conducted on reviewing the DLT technology, DLT platforms and DLT research frameworks [14], [15]. Here, we provide an overview of some of this recent research. A comparison of different DLT implementations has been presented in [16] that focuses on purpose, performance, governance mechanisms, consensus and security algorithms. Although the author summarizes some important aspects of several DLT platforms, there is no qualitative analysis presented in the report which is very crucial to understand the underlying capabilities of a DLT platform.

Chinmay et al. have presented a comparative analysis on Ethereum, Hyperledger and Corda platforms based on few basic evaluation criteria [17]. The paper also provides a comparison among five Hyperledger frameworks under the Hyperledger project. However, the major limitation of the paper is that it doesn't address most of the important performance metrics such as block size, block creation time, cost and energy consumption.

Another research on DLT platforms and their uses beyond bitcoin has been reported in [18] where the authors compared five different DLT platforms using several criteria related to usability, flexibility, performance and potential. All the platforms investigated in this paper are open source and therefore, only represent a particular domain of DLT systems.

Tien et al. have described an evaluation framework, Blockbench, for analyzing private DLTs [19]. Any private DLT can be plugged-in to Blockbench and benchmarked against different workloads generated through both real and synthetic smart contracts. In this paper, three major private DLTs have been evaluated through Blockbench to measure and compare their performance in terms of throughput, latency, scalability and fault-tolerance. However, this paper only helps to realize the performance gaps among private DLTs, not the public DLTs.

A systematic review on DLT platforms, especially focusing on healthcare or clinical informatics has been presented in [20]. The paper uses a systematic method to compare among DLT platforms and their technical features and also provides a reference for selection of suitable platform based on specific requirements for a healthcare application.

A recent research on DLT platforms is presented in [21] which evaluates a number of integrated platforms for IoT use-cases. The paper presents an evaluation framework that could be used to choose an appropriate DLT platform for IoT applications. However, the paper only evaluates the platforms that support integration of DLT to IoT and therefore, is not applicable to general use-cases.

III. DISTRIBUTED LEDGER TECHNOLOGY

Bitcoin [2], introduced in 2009, has emerged as the world's first widely used digital currency and has been used in a wide range of applications. It is underpinned by a novel mechanism called Distributed Ledger Technology, also known as blockchain technology, providing its solid technical foundation. Even though the terms blockchain and DLT are used interchangeably in the literature, there is a subtle difference between them which is worth highlighting. A blockchain is just an example of a particular type of ledger where data can be stored in a specific format. There are other types of ledgers with different data formats. When a ledger (including a blockchain) is distributed across a network, it can be regarded as a Distributed Ledger or simply a ledger.

Over the last few years, DLT has received widespread attention among the industry, the Government and academia. It is regarded as one of the fundamental technologies to revolutionize the landscapes of several application domains. At the center of DLT is the ledger itself. A distributed ledger is a ledger consisting of consecutive blocks chained together following a strict set of rules. The ledger is distributed and stored by the nodes of a P2P (Peer-to-Peer) network where each block is created at a predefined interval in a decentralized fashion by means of a consensus algorithm. The consensus algorithm guarantees several data integrity related properties in the ledger as described below.

Evolving from the Bitcoin ledger, a new breed of ledger has emerged which facilitates the deployment and execution of computer programs, known as smart contracts, on top of the respective ledger. Such smart contracts enable the creation of so-called decentralized applications (DApps), which are autonomous programs operating without relying on any system entity. Being part of the ledger makes smart contracts and their executions immutable and irreversible,

a sought-after property having a wide-range of applications in different domains.

A consensus algorithm is a fundamental component in any DLT system. By a consensus algorithm, a distributed ledger is synchronized across multiple nodes. There are many consensus algorithms introduced by the DLT platforms that are designed to meet specific goals. Bitcoin introduced the notion of the so-called Proof-of-Work (PoW) consensus [23] algorithm in which a block creator (miner), to create a block, must solve a cryptographic puzzle by producing a hash which satisfies certain properties. Solving such a cryptographic puzzle requires a lot of computation and thus consumes a lot of electricity. To solve this problem, another consensus method, called Proof-of-Stake (PoS) [24] has been put forward. The core idea of PoS evolves around the concept that the nodes willing to participate in the block creation process must prove that they own a certain number of coins at first and must lock a certain amount of its currencies, called stake, into an escrow account. The stake acts as a guarantee that it will behave as per the protocol rules. The node which escrows its stake in this manner is known as the stakeholder, forger or minter in PoS terminology. The minter can lose the stake in case it is found to misbehave. DPoS (or Delegated PoS) [25] is a variant of PoS in which a stakeholder delegates the stacking task to another entity.

A. DISTRIBUTED LEDGER PROPERTIES

A distributed ledger exhibits several properties that make it a suitable candidate for several application domains including digital evidence chain. The properties are discussed below.

- **Distributed consensus on the ledger state:** One of the crucial properties of any distributed ledger is its capability to achieve a distributed consensus on the state of the ledger without being reliant on any Trusted Third Party (TTP). This opens up the door of opportunities to build and utilize a system where every possible state and interaction are verifiable by any authorized entities.
- **Immutability and irreversibility of ledger state:** Achieving a distributed consensus with the participation of a large number of nodes ensures that the ledger state becomes practically immutable and irreversible after a certain period of time. This also applies to smart contracts which enable the deployment and execution of immutable computer programs.
- **Data (transaction) persistence:** Data in a distributed ledger is stored in a distributed fashion ensuring its persistency as long as there are participating nodes in the P2P network.
- **Data provenance:** The data storage process in any distributed ledger is facilitated by means of a mechanism called transaction. Every transaction needs to be digitally signed using public key cryptography (PKI) which ensures the authenticity of the source of data. Combining this with the immutability and irreversibility properties of a distributed ledger provides a strong non-repudiation instrument for any data in the ledger.
- **Distributed data control:** A distributed ledger ensures that data stored in the ledger or retrieved from the ledger can be carried out in a distributed manner that exhibits no single point of failure.
- **Accountability and transparency:** Since the state of the ledger, along with every single interaction among participating entities, can be verified by any authorized entity, it promotes accountability and transparency.

B. DISTRIBUTED LEDGER TYPES

Depending on the application domains, different ledger deployment strategies can be pursued. Based on these strategies, there are two predominate ledger types, Public and Private, as discussed below.

- **Public ledger**, also known as the non-permissioned ledger, allows anyone to create and validate blocks as well as to modify the ledger state by storing and updating data by means of transactions among participating entities. This means that the ledger state and its transactions along with the stored information is transparent and accessible to everyone. This raises privacy concerns for particular scenarios where the privacy of such data needs to be preserved.
- **Private ledger**, also known as the permissioned ledger, can be restricted unlike its public counterpart in the sense that only authorized and trusted entities can participate in the activities within the ledger. By allowing only authorized entities, a private ledger can ensure the privacy of ledger data, which might be desirable in some use-cases.

IV. DLT PLATFORMS

This section provides a brief description of selected DLT platforms highlighting their key features and functionalities.

A. BITCOIN

Bitcoin [4] is the seminal DLT system that introduced the first widely successful digital currency, colloquially known as crypto-currency. It is based on a public distributed ledger allowing anyone in the world to join the Bitcoin P2P network, participate in the process of updating the ledger state and to interact with other entities in the network. Being predominantly a payment system, Bitcoin enables anyone to transfer digital currencies from one entity to another entity via transactions. This showcases a crucial feature: how the right of a digital asset can be transferred successfully between entities in a network? Inspired by the technical innovation of Bitcoin, as well as its large-scale worldwide adoption, numerous crypto-currencies have been developed. Many of these crypto-currencies aim to address specific security and/or privacy bottlenecks of Bitcoin targeting specific business use-cases. Even so, Bitcoin remains the market leader in this domain.

In the heart of Bitcoin is a novel consensus algorithm, Proof-of-Work (PoW), also known as Nakamoto consensus. The algorithm is designed to solve a computationally

intensive crypto puzzle, that is required to generate a cryptographic hash with specific properties. It ensures that each block created periodically is valid and there is a distributed consensus among the participating entities on the order of the blocks within the ledger. This enables precision accuracy of the data stored in the ledger. The data on the ledger is mostly a series of transactions outlining how each Bitcoin currency, with its tiniest denomination, is circulated among entities. The immutability and irreversibility of the ledger states, thanks to its distributed consensus, guarantees that the ledger with its data remains accurate even though it is distributed among trustless entities, without relying on a trusted third party certifying its correctness.

B. ETHEREUM

Ethereum is the seminal smart contract empowered DLT system [5] featuring a virtual machine, called Ethereum virtual machine (EVM) whose state, along with the additional ledger data, is stored in the ledger. Like Bitcoin, it provides similar functionalities for a cryptocurrency payment network. In addition, the EVM in Ethereum allows smart contracts to be deployed and executed on a public ledger, thereby enabling the creation of immutable computer logic. A smart contract in Ethereum is deployed by means of a transaction by spending a certain amount Ethereum crypto-currency called Ether. Furthermore, the invocation and execution of smart contracts is bound by a pay-per-use model requiring to spend a certain amount of Ether to store, process and update data in the ledger via transactions.

Once deployed in the ledger, a simple model of the execution of a smart contract is as follows. A smart contract is invoked with some input data via a transaction. The EVM executes the smart contract using the input data and generates an output. This execution changes the state of the EVM, which is stored in the ledger along with the output data. A PoW consensus algorithm guarantees the updated state is accurately recorded in every node in the network. The public ledger ensures that the transfer of currencies and the EVM's change of state via transactions are completely transparent and verifiable by any participant.

C. MULTICHAIN

Multichain is an open source platform that enables us to create and deploy private distributed ledger applications either within or between organizations. Originating from Bitcoin blockchain, Multichain allows the end users to configure the maximum block size, target time for blocks, active permission type, mining diversity, mining reward, chain's protocol, permitted transaction type and metadata [21]. It also provides a simple, easy-to-interact application interface (API) and command line interface (CLI) to maintain and deploy DLT systems. In addition to functional and operational benefits offered by the Multichain platform, it covers a wide variety of use-cases such as connected health, KYC (Know Your Customer), insurance security, and food supply chain [22].

Although derived from the Bitcoin core software, Multichain solves the problems related to mining, privacy and openness via integrated management of user permissions. The DLT platform implements a hand-shaking process through which distributed ledger nodes connect to each other. In this process, every node has to present its identity as a public address on the permitted list and also has to verify that the other's address is on its own permitted list. For this purpose, each node sends a challenge message to the other node and the corresponding node sends back a signature of that message as a proof. The peer-to-peer connection is aborted if any of the nodes disagree with the results. Unlike Bitcoin, Multichain uses a distributed consensus among identified validators to restrict mining to a set of identifiable entities. To ensure a fair mining policy, the platform uses a randomized round-robin system for block-adders and implies a constraint on the number of blocks that a miner can create within a given window. Although, the transaction fee and block rewards are set to zero by default in multichain blockchain, one can configure the parameters as necessary. During the last year, multichain released a new version (Multichain 2.0 Beta) with smart contract support that allows custom rules to be defined regarding the validity of transactions or stream items.

D. EOS

EOS is the first and the most widely known DPoS (Delegated Proof-of-Stake) smart contract platform as of now [9]. In fact, DPoS mechanism was first invented by Daniel Larimer, the Chief Technology Officer of EOS. With the promise of greater scalability and higher throughput than any existing DLT platform, it raised 4 billion USD in the highest ever ICO event to date [23]. Even though, the initial EOS currency was created on the Ethereum platform, they later migrated to their own blockchain network. The DPoS consensus algorithm of EOS utilizes 21 validators, also known as Block Producers (BPs). These 21 validators are selected from a pool of BP candidates with votes by EOS token (currency) holders. The number of times a particular BP is selected to produce a block is proportional to the total votes received from the token holders.

Blocks in EOS are produced in rounds where each round consists of 21 blocks. At the beginning of each round, 21 BPs are selected and then each of them gets a chance in a pseudo-random fashion to create a block within that particular round. Once a BP produces a block, other BPs must validate the block and reach into a consensus. A block is confirmed only when more than two-thirds majority (denoted with $+2/3$) of the BPs reach the consensus regarding the validity of the block. Once this happens, the block and its associated transactions are regarded as confirmed or final so that no fork can happen.

The EOS cryptocurrency is used to select the 21 BPs with voting as well as to reward the BPs for creating blocks and thus, securing the network. EOS had an initial supply of 1 Billion EOS tokens with an annual inflation of 5%. Among the inflated currencies, 1% is used to reward the block

producers whereas the other 4% are kept for future research and development for EOS. Currently, an EOS block is created in every 0.5s.

E. CARDANO

Cardano is regarded as a next-generation DLT system supporting smart contracts and decentralized applications without relying on any PoW consensus algorithm [11]. Instead, it utilizes Ouroboros, a provably secure PoS algorithm [24]. In Ouroboros, only a stakeholder can participate in the block minting process. A stakeholder is any node which holds the underlying cryptocurrency of the Cardano platform called Ada. Ouroboros relies on epoch, a predefined time period consisting of several slots. A stakeholder is elected for each slot to create a single block. The selected stakeholder is called a slot leader and is elected by a set of electors. An elector is a specific type of stakeholders which has a certain amount of Ada in its disposal. In each epoch, the electors select the set of stakeholders for the next epoch using an algorithm called Follow the Satoshi (FTS). The FTS algorithm uses a random seed to introduce a certain amount of randomness in the election process.

A share of the random seed is individually generated by all electors who participate in a multiparty computation protocol. Once the protocol is executed, all electors possess all the required shares which are then used to construct the random seed. The FTS algorithm utilizes the random seed to select a coin for a particular slot. The owner of the coin is then elected as the slot leader. Intuitively, the more coins a stakeholder possesses, the higher is its probability to be selected as the slot leader. Ouroboros is expected to provide a transaction fee-based reward to incentivize stakeholders to participate in the minting process. However, it is to be noted that unlike other DLT platforms discussed here, Cardano and its Ouroboros algorithm is still in developing phase. Therefore, how it will perform once deployed is yet to be seen.

F. HYPERLEDGER FABRIC

Hyperledger Fabric is the first major private DLT system originated from the Hyperledger ecosystem [25]. It has been designed with strong privacy in mind to ensure that different governmental agencies and business organizations can take advantage of a DLT system in different use-cases. A crucial capability of Fabric is that it can maintain multiple ledgers within its ecosystem. This is a useful feature, which separates Fabric from other DLT systems consisting of only one ledger in each of their domains. A key strength of Fabric is its modular design and pluggable features. For example, Fabric is not dependent on a particular format of ledger data, and thus, is useful for a number of use-cases. In addition, the consensus mechanism is fully pluggable, therefore different types of consensus algorithms can be used in different situations. Currently, Fabric supports SOLO and Kafka [26] and a SBFT (Simplified Byzantine Fault Tolerance) algorithm [27] is to be released soon. In addition to smart contract support, Fabric employs two layered architecture for enforcing privacy in the ledger.

- The first layer is the identity layer. Fabric utilizes a specific provider known as the Membership Service Provider (MSP), which is responsible for managing the identities of all participants in the ledger. Using this identity layer, it is possible to create security policies that dictate which entities can perform what actions within a specific ledger.
- The second layer is the channel layer. Fabric allows a channel to be created among a particular set of entities to segregate their interactions from other entities. Unlike any other DLT system, a ledger in Fabric is attached to a particular channel. This enables a ledger to separate its transactions and maintain its state without any interference or involvement of other entities. This channel-based mechanism allows Fabric to maintain multiple ledgers simultaneously as well as to exercise suitable privacy controls over each ledger.
- A smart contract in Fabric is known as a chaincode. It is a computer program deployed on the ledger allowing it to interact with the ledger data. Currently, such chaincode can be written in Go and Java with other programming languages to be supported in future.

Fabric utilizes a special entity called Orderer, which is responsible for creating a new block and extending the ledger by adding the block in the appropriate order. There are other entities known as endorsers. Each endorser is responsible for validating and endorsing a transaction where it checks if an entity is allowed to perform a certain action in a ledger encoded within the transaction. Figure 1 shows the generalized consensus mechanisms in all hyperledger platforms. A simple flow in Fabric is as follows.

- All required entities are registered in the MSP.
- A channel with a ledger is initiated. In addition, a policy is created containing the endorsement criteria as well as other security and privacy criteria.
- A chaincode is deployed in the ledger.
- When an entity wishes to invoke certain functions in the chaincode to read data from the ledger or to write data into the ledger, it submits a transaction proposal to all the required endorsers as dictated in the policy.
- Each endorser validates the proposal, executes the chaincode and returns a proposal response consisting of other ledger data.
- The proposal and its response along with the ledger data are encoded within a transaction and sent to the Orderer.
- The Orderer creates a block using the transaction and returns the block to the endorsers.
- Each endorser validates the block and if validated, extends the ledger by attaching the new block. This essentially updates the state of the ledger.

G. HYPERLEDGER SAWTOOTH

Hyperledger Sawtooth, initially developed by Intel, is a software framework for creating distributed ledgers suitable for

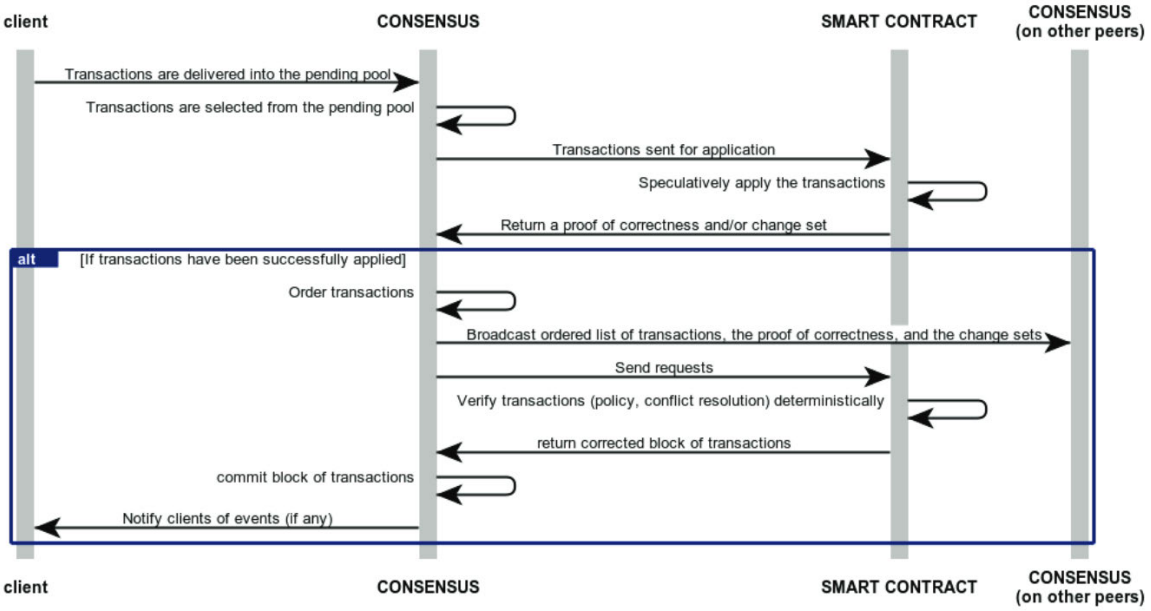

FIGURE 1. Generalized Hyperledger consensus process flow.

a variety of use cases [6]. Sawtooth utilizes a novel consensus algorithm called Proof-of-Elapsed-Time (PoET) which depends on Intel SGX (Software Guard Extension). Intel SGX is a new type of Trusted Execution Environment (TEE) integrated in the new generation of Intel processors. SGX enables the execution of code within a secure enclave inside the processor whose validity can be verified using a remote attestation process supported by the SGX.

To support the execution of business logic (contract) on top of the ledger, Sawtooth implements a different approach compared to Ethereum or Hyperledger Fabric. Sawtooth has introduced a novel concept called *Transaction Family* that encapsulates the business logic. A transaction family consists of a data model encoding the state of the ledger and a transaction language which is used to change the state of the ledger. The key advantage of Sawtooth is that it is agnostic about the transaction family. This means that different types of transaction families can be accommodated, including:

- a transaction family consisting of a single type of transaction that is used to update the ledger state, similar to Bitcoin.
- a more complex transaction family consisting of Virtual Machine with specialized opcode supporting the creation of smart contract similar to Ethereum.
- In the current iteration of Sawtooth, three different types of Transaction Families have been included:
  - EndPointRegistry - A transaction family for registering ledger services.
  - IntegerKey - A transaction family used for testing deployed ledgers.
  - MarketPlace - A more expressive transaction family for buying, selling and trading digital assets. However, other transaction families, suitable for specific business use-cases, can be created by extending the supplied transaction families.

On top of the concept of transaction families, the PoET model is used to achieve distributed consensus among the participants. PoET, similar to the Nakamoto consensus algorithm in Bitcoin, relies on the concept of electing a leader in each round to propose a block to be added in the ledger. The difference is that other Nakamoto algorithms select a leader by a lottery mechanism, which utilizes computing power to generate a proof. However, PoET solely relies on the Intel SGX capability to elect a leader. During each round, every validator node in the network, requests for a wait time from a trusted function in the SGX enclave. The validator that is assigned the shortest waiting time is elected as the leader for that round. The winning validator then can propose a block, consisting of a series of transactions from the defined transaction family. Other validators can utilize a trusted function supported by SGX to assess whether a trusted function has assigned the shortest time to the winning validator and the winning validator has waited the specified amount of time. Furthermore, other validators verify the validity of the block before it is included in the ledger. The inclusion of the PoET as a consensus algorithm enables Sawtooth to achieve massive scalability as it does not need to solve a hard, computationally intensive cryptographic puzzle. In addition, it allows Sawtooth to be used not only for a permissioned ledger, but also for a public ledger.

Interestingly, there has been a project proposal on 'how Hyperledger Burrow (discussed in the next subsection) can be integrated as a transaction family into the Sawtooth domain to bring the advantages and flexibilities of Ethereum in Sawtooth platform' [7].

H. HYPERLEDGER BURROW

The latest entry to the Hyperledger umbrella is Hyperledger Burrow. This is a private (permissioned) deployment of the Ethereum platform [5]. It has been created and then deposited to the Hyperledger code-base by Monax Industries Limited. The core component in Burrow is a permissioned version of the EVM (Ethereum Virtual Machine) to ensure that only authorized entities can execute code. Two additional components have been added to Burrow: Tendermint consensus engine and the RPC gateway. The Tendermint consensus falls under the category of a Byzantine Fault Tolerance (BFT) algorithm which can be used to achieve consensus even under the Byzantine behavior of a certain number of nodes, e.g. nodes acting maliciously. The key feature of the Tendermint algorithm is that it does not require nodes to solve, unlike the PoW consensus algorithm of public Ethereum, any computationally intensive crypto puzzle to achieve distributed consensus. Burrow depends on a number of validators which are known (authorized) entities and are responsible for validating each block utilizing the Tendermint consensus algorithm. This algorithm allows consensus to be achieved in Burrow with 1/3 nodes exhibiting Byzantine behaviors, either acting maliciously or having been down due to network or system failure. Since Burrow utilizes the EVM, a wide-range of smart contracts and DApps could be deployed in this platform. Using the Tendermint algorithm with a set of known validators allows Burrow to scale at a much faster rate than Ethereum, while preserving the privacy of transactions by allowing only known entities to participate in the network. However, the current development state of Burrow is quite rudimentary. The lack of proper documentation makes it hard to investigate whether it is suitable for developing any proof-of-concept.

I. IOTA

IOTA is a distributed ledger designed for the Internet of Things. It provides secure communications and payments between IoT devices [12]. Unlike using a hashcash-like proof-of-work, it uses Tangle, a consensus-building data structure made of a Directed Acyclic Graph (DAG). Its transactions are fast, free of cost and scalable. IOTA uses Tangle to solve the double spending problem alongside solving both the scalability and transaction fee issues faced by most distributed ledgers, including Bitcoin. By requiring the sender in a transaction to perform approval of two transactions, IOTA turns its users into miners; hence, the act of making a transaction and verifying transactions are coupled on this platform. There are no dedicated miners; instead, those making transactions are the actors affecting the system.

Tangle is a consensus-building system that, instead of employing a blockchain, uses an orderly approach of verifying transactions to reach the consensus. Each network member in IOTA that submits a new transaction needs to verify two other transactions on the network before having its transaction verified. This approach ensures reaching the consensus out of a web of verifications.

Tangle makes IOTA network even more distributed than a distributed ledger network. With a blockchain, the network is distributed among the miners on the blockchain while with Tangle the network is distributed among every participating node. Scalability, fast transactions and the ability to validate an unlimited number of transactions simultaneously make IOTA suitable for the use-cases working with IoT devices. IOTA has the plan to introduce Qubic and this platform's smart contract will be capable of providing general-purpose, cloud or fog-based permissionless multiprocessing on the Tangle.

J. CORDA

Corda is a distributed ledger technology that aims to provide support for finance use-cases [10]. It is a permissioned network that constitutes the condition that all participants must have verifiable identities using public-key infrastructure. One of the primary differences between Corda and other mainstream platforms such as Bitcoin and Ethereum is the use of a blockchain. Corda is a distributed ledger but does not use a blockchain to record transactions.

Corda views the approach of broadcasting each transaction to the network an unnecessary dilution of privacy. It is instead designed to make those entities aware of transactions which are directly involved. For example, if a bank creates a transaction mentioning that it owes a customer a certain amount of dollars, only the bank, the customer, and relevant regulatory organizations will be able to know about the existence of the transaction.

Anonymous networks use proof-of-work to prevent attacks on the network. However, permissioned networks like Corda can skip proof-of-work because of the permission process that ties in-network identities to real-world identities. Corda advances a step further asserting that transactions are no longer necessary to be batched together into blocks; therefore, block-styled architecture is not used in this distributed ledger. Corda transactions operate using consumable states. For example, a state might be "Entity X is the rightful owner of Asset A". Entity X can spend this state to perform a transaction by creating a new state "Entity Y is the rightful owner of Asset A". Once the input state is spent, it no longer remains valid. In the above example, after the transaction, Entity X no longer owns Asset A. Consumable states are analogous to the latest entry of a blockchain ledger that can be used to validate a new transaction.

The consensus in Corda is reached at transaction level by involving relevant parties only and subject to transaction validity and transaction uniqueness. Validity is secured by checking for all required signatures and by assuring that any transactions that are referred to are also valid. Uniqueness concerns the input states of a transaction, particularly, it has to be ensured that the transaction in question is the unique consumer of all its input states.

One of the powerful features that make Corda different than some renowned financial networks such as Ripple and Stellar is its smart contract facilities. Corda acts as a financial

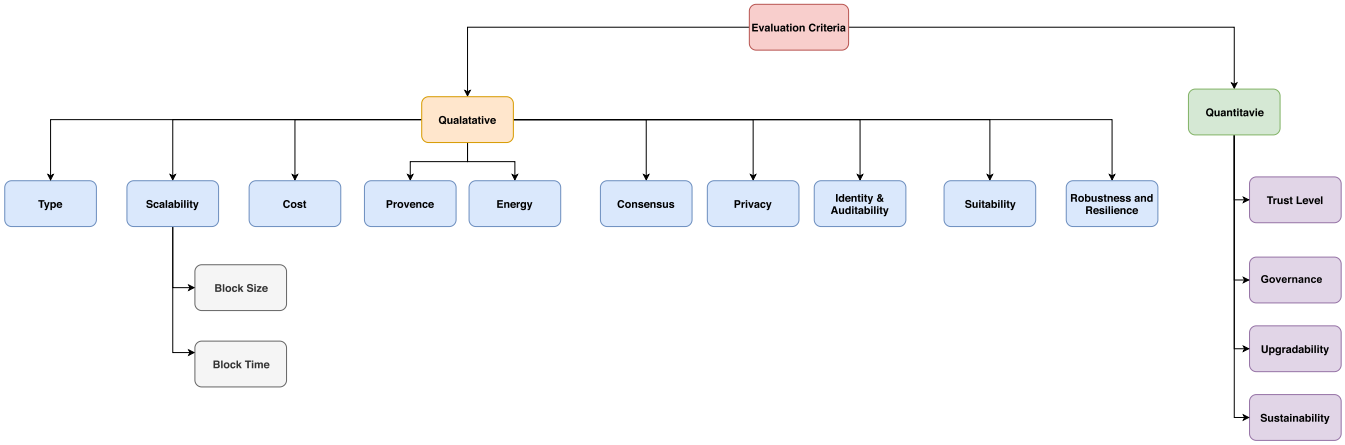

FIGURE 2. Taxonomy of evaluation criteria.

network as well as a platform enabling it to have the best of both Ethereum/Hyperledger and Ripple/Stellar domain. It has a large developer community who can write codes in Java and Kotlin to develop DApps in Corda.

K. WALTONCHAIN

Waltonchain is a new DLT platform for the IoT industry [13]. The platform is named thus in order to commemorate and recognize the contribution of Charles Walton, the inventor of RFID (Radio Frequency Identification) technology and to advance his vision for the ubiquitous deployment of the RFID technology in the form of IoT. With this motivation, Waltonchain would like to disrupt the current IoT industries by integrating the transparency, accountability and provenance properties of a distributed ledger with RFID-enabled IoT hardware. Indeed, the core platform consists of RFID hardware (both RFID tags and reader), the Waltonchain public DLT platform and the software platform that interfaces the hardware with the distributed ledger. Hence, it can be considered as a novel fusion of hardware and software providing an ecosystem for multi-organization network integration in the form of supporting multiple different distributed ledgers, data sharing and value transfer between them.

The ultimate goal is to create a novel service delivery model called Value IoT (VIoT) which will be suitable for a wide range of IoT applications such as supply chain tracking, product authentication, identification, food and drug traceability and so on. The Waltonchain platform has a layered architecture consisting of six layers with different layers having different functionalities including hardware, network and application development management. The Waltonchain platform introduces a hybrid consensus algorithm called WPoC (Waltonchain Proof of Contribution). WPoC is a combination of three different consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS) and Proof of Labor (PoL). Waltonchain presumably (as not explicitly specified in their whitepaper) will consist of two types of network: public and private. A public network controls the parent public distributed ledger whereas there could be different public/private child chains for maintaining different child chains, each for a specific industry or use-case.

V. EVALUATION CRITERIA

This section presents a brief description of different DLT evaluation criteria. The selected criteria have been classified in two major categories: Quantitative and Qualitative (Figure 2). Each category and the relevant criteria are presented below.

A. QUANTITATIVE

Within the scope of this paper, we classify those criteria as quantitative that either exhibits a quantifiable property, or which can be assessed objectively. Each criterion belonging to this category is discussed below.

- **Type** indicates the type of ledger the particular system utilizes: public or private.
- **Scalability** is used to indicate how much data a system can process within a certain period of time. A highly scalable system has better chance to be adopted in different scenarios. It is predominantly determined by the combination of the following two parameters:
  - *Block size* indicates the maximum allowed size of a block in a DLT system. A higher block size indicates a higher data processing capability for a particular DLT system.
  - *Block creation time* specifies the average block creation time for a particular system. It is, in turn, dependent on the consensus algorithm utilized by the system.
- **Cost** outlines the associated cost incurred, if any, for any transaction to process or store data in the ledger. A system in which it is rather expensive to process and/store any data might face the risk of being omitted in favor of others. Cost is often referred as ‘‘transaction fee’’ in blockchain domain.

TABLE 1. Quantitative evaluation of selected DLT platforms (Part A).

Platform	Type	Scalability		Cost	Energy	Consensus
		Block Size	Block Time			
Bitcoin	Public	1MB	10m	Y (using Bitcoin)	High	PoW
Ethereum	Public	Implicit restriction	15sec	Y (using Ether)	High	PoW
EOS	Public	1 MB, dynamically configurable	0.5 sec	Y	N	DPoS
Cardano	Public	∼1 MB	20 sec	Y	N	Ouroboros
Fabric	Private	Configurable	0.5-2 sec	N	Very low	Using orderers and endorsers
Sawtooth	Private	Configurable	NA	N	Very low	PoET using Intel SGX
IOTA	Private	Configurable	Configurable	No fees	Very low	Tangle
Multichain	Private	Configurable	Configurable	Y (Enterprise version)	Very low	Distributed consensus among identified validators
Corda	Private	Configurable	0.5-2 sec	No fees	Very low	Notaries
Waltonchain	Public & Private	225 TX	30 sec	Y	Low	WPoC

- **Energy consumption** denotes if the consensus algorithm utilized by a system consumes any electrical energy during the mining/block creation process.
- **Consensus** algorithm that is used to achieve distributed consensus in a DLT system. This directly impacts the block creation time and the energy consumption of any DLT system.
- **Privacy** analyses the privacy mechanism for any DLT system. A system having built-in privacy preserving feature has higher probability for wide-scale adoption.
- **Identity and Auditability** can be used to analyses how each entity is identified and the consequence of such identification with respect to auditability.
- **Suitability** indicates if a system is suitable for different data types, sizes and/or volumes. If a system supports multitude of different data types, sizes and volumes, it has better chance for any large-scale adoption.
- **Robustness & Resilience** analyzes if a system is resilient and robust against different types of attacks and unprecedented errors.

B. QUALITATIVE

In the absence of a concrete measurable property/objective argument, the criteria that tend to align towards the boundary of subjective argument are classified within this category. Each criterion belonging to this property is described below.

- **Trust level/public confidence** analyzes the level of trust or public confidence of a system in terms of its adoption in different domains.
- **Governance** explores the governance mechanism of a DLT system. A democratic and open governance mechanism can, in a way, instill public confidence in a system which ultimately can boost the level of trust for that system.
- **Upgradability** is a desirable feature, either to add useful novel features or to rectify unforeseen errors in a system. Therefore, every system should support practical upgradability features with backward compatibility to ensure seamless integration.
- **Sustainability** explores if the ecosystem of maintaining a system is sustainable over a long period of time, which is needed for a continuous wide-scale adoption.

VI. EVALUATION AND DISCUSSION

This section presents our evaluation of the selected DLT platforms against the chosen evaluation criteria. In addition, we also synthesize the evaluations of the chosen DLT systems. The evaluation of the selected systems using the quantitative and qualitative criteria are presented in Table 1, 2, 3 and 4 respectively. For carrying out the evaluations, we have investigated the respective documentation for each platform, blogs and several other online sources. For each criterion within the quantitative group, either a corresponding value has been provided (if exists) or an explanation is provided to clarify the criterion. For the qualitative evaluation, we have added explanatory/evaluative remarks.

Public DLT systems such as Bitcoin and Ethereum are fueled by a powerful consensus algorithm along with a robust P2P network and are widely adopted. These features contribute to their formidable security, where data stored in the ledger becomes practically immutable after a certain period of time. Ethereum adds a computing layer on top of the ledger enabling the support for deploying immutable computer programs via smart contracts. These are both open source platforms and the governance mechanisms are mostly democratic where general users and miners have final say regarding how the DLT systems may evolve. Both systems support the notion of accountability and transparency. Due to all these positive attributes, there is a strong level of trust and public confidence on both systems and they have been extensively utilized to disrupt the traditional approaches in several application domains.

A few examples of such applications are DNS-like decentralized naming system (Namecoin [28]), decentralized

TABLE 2. Quantitative evaluation of selected DLT platforms (Part B).

Platforms	Privacy	Identity and Auditability	Suitability	Robustness and Resilience
Bitcoin	Transactions are linked via pseudonymous identifiers. Transactions and other data are visible to everyone.	Pseudonymous identification via public key. Being a public ledger, it has strong support for auditability and accountability in case the proper identity of entities can be verified.	Can be used to store a short amount of data (around 80 bytes) using OP_RETURN opcode. There is no support provided for smart contracts to process on-chain data.	Robust P2P structure. Strong resiliency against data immutability, thanks to its consensus algorithm and wide-spread adoption.
Ethereum	Transactions are linked via pseudonymous identifiers. Transactions, smart contract code and other data are visible to everyone.	Pseudonymous identification via public key. Being a public ledger, it has strong support for auditability and accountability in case the proper identity of entities can be verified.	Can be used to store arbitrarily large amount of data, however might incur huge cost. Supports smart contract to write immutable logic which can be used to process on-chain data.	Robust P2P structure. Strong resiliency against data and code immutability, thanks to its consensus algorithm and wide-spread adoption.
EOS	Transactions are linked via pseudonymous identifiers. Transactions, smart contract code and other data are visible to everyone.	Pseudonymous identification via public key. Being a public ledger, it has strong support for auditability and accountability in case the proper identity of entities can be verified.	Can be used to store arbitrarily large amount of data, however might incur huge cost. Supports smart contract to write immutable logic which can be used to process on-chain data.	Robust P2P structure. Resiliency is less than Ethereum because of its usage of only 21 validators with the possibility of collusion and corruption among the validators. If the BPs perform as per the rule, it can provide resiliency against data and code immutability.
Cardano	Transactions are linked via pseudonymous identifiers. Transactions, smart contract code and other data are visible to everyone. Privacy features are not defined yet.	Pseudonymous identification via public key. Being a public ledger, it has strong support for auditability and accountability in case the proper identity of entities can be verified.	Smart contract not supported yet. Planned to be released in the future version.	Robust P2P structure. Resiliency depends on the number of electors. If the number of electors is less, there is a possibility of collusion and corruption. If the electors follow the protocol diligently, it can provide resiliency against data and code immutability.
Fabric	Strong privacy support using the private ledger for authorized users Utilizes a concept called channel which allows to maintain privacy among a subset of peers within the network.	PKI-based identification requires every entity to be registered and issued with the required keys. Strong support for auditability and accountability.	Can be used to store arbitrarily large amount of data. Supports smart contract which can be used to process on-chain data.	Robust P2P network whose resiliency will depend on the number of endorsers and the number of orderers.
Sawtooth	Strong support for privacy using the private ledger where only known entities can participate.	Verifiable identity via public key cryptography. Strong support for auditability and accountability.	Can be used to store arbitrarily large amount of data. Supports smart contract using transaction family which can be used to process on-chain data.	Robust P2P network whose resiliency will depend on the number of validators.
IOTA	Pseudonymous	Pseudonymous	Suitable for IOT data	Robust P2P structure with large number of nodes.
Multichain	Privacy support through integrated management of user permissions	Verifiable identity via public key cryptography. Strong support for auditability and accountability	Can be used to store arbitrarily large amount of data (1GB per item off-chain data). Version 2 supports smart contract that allows custom rules to be coded for validating transactions or data.	Robust P2P structure with richer data stream support Resiliency depends on the number of validators
Corda	Privacy support through integrated management of user permissions	Pubic Key Infrastructure	Financial data	Robust P2P structure whose resiliency depends on the number of validators
Waltonchain	RFID tag	Pseudonymous	IoT Data	Robust P2P structure with large number of nodes.

immutable time-stamped hashed record (Proof of Existence [29]), decentralized PKI (Certcoin [30]) and so on. Similarly, Ethereum has been used in a variety of domains, including: energy (Electron [31]), finance and banking, sports, IoT (Slockit [32]), naming service (ENS [33]), healthcare (Patientory [34]), and crowd-funding (DAO and Initial Coin Offerings).

However, Bitcoin, Ethereum, and many other public DLT systems, suffer from serious shortcomings in several aspects including scalability, energy consumption, privacy, identity and cost. They are not even close to the current traditional approaches in handling a large amount of financial transactions. Their consensus algorithms are energy intensive and lead many to doubt their sustainability over time. Furthermore, data stored in these ledgers are visible to any participant and therefore not suitable to handle sensitive data. All entities are identified via cryptographic pseudonyms that makes it hard to audit and are open to Sybil attacks [35]. Data that can be stored in Bitcoin is quite limited, whereas Ethereum is much more flexible in this regard where different types of data can be stored via any smart contract. Storing data incurs expense and is therefore infeasible to store a large amount of data in both ledgers.

On the other hand, the other public DLT systems presented in this paper (EOS, Cardano, IOTA and Waltonchain) aim to tackle some of the major limitations of Bitcoin and Ethereum, most notably the issue of scalability and energy consumption. These DLT platforms have a higher transaction rate and consume almost negligible energy. This has been possible because of their utilization of different model of consensus algorithms such as DPoS, Ouroboros (PoS), Tangle and WPoC (Waltonchain Proof of Contribution) respectively. Also, all these platforms have support for smart contracts to facilitate different types of applications. However, IOTA and Waltonchain have been specifically designed for the IoT domains.

An interesting aspect in the selected public DLT systems is their corresponding governance mechanism. All of them are open source and with a little bit of difference how improvements are carried out. Bitcoin, Ethereum, and Cardano allow anyone to submit improvement proposals which are then approved by different mechanisms. However, it is not clear how this is carried out in IOTA and Waltonchain.

These public DLT systems are upgraded based on a mechanism called fork which can be of two types: hard fork and soft fork. A soft fork creates backward-compatible version

TABLE 3. Qualitative evaluation of selected DLT platforms (Part A).

Platforms	Trust Level	Governance	Upgradability	Sustainability
Bitcoin	High	• Open source • Improvement proposal via Bitcoin Improvement Proposal (BIP) • Code-base developed and maintained by a group of developers • Adoption of new features depending on users and miners	• Upgrade of ledger is carried out via soft and hard fork	• The electricity consumption of PoW algorithm is unlikely to be sustainable in future • No concrete action plan to rectify this problem can be found
Ethereum	High	• Open source • Improvement proposal via Ethereum Improvement Proposal (EIP) • Code-base developed and maintained by a group of developers • Adoption of new off-chain features depending on users and miners • On-chain governance is maintained dynamically via the miners	• Upgrade of ledger is carried out via soft and hard fork • smart contract is not upgradable	• The electricity consumption of Proof of Work algorithm is unlikely to be sustainable in future • Plan to move towards a Hybrid Proof of Work and Proof of Stake solution has been proposed to ensure sustainability
EOS	Medium	• Open source code-base • Governed by ECAF (EOS Core Arbitration Forum) • On-chain governance rule must be approved by the (+2/3) majority of, i.e. 15/21 BPs and the approval must be maintained for 30 consecutive days • Once new rule enforced by code upgrade, this also must be approved by (+2/3) majority of BPs and the approval must be maintained for 30 consecutive days	• Upgrade of ledger is carried out via soft and hard fork • Every single user-deployed smart contract can be upgraded without forking the blockchain	• The electricity consumption is almost negligible because of its DPoS consensus algorithm • EOS is gaining popularity among different application domains because of its high scalability, specifically high throughputs However, many still are skeptical about its security because of its utilisation of only 21 BPs to achieve consensus
Cardano	Low, because it is still in the development phase and many features are not available yet	• Open source code-base • Improvement proposal via Cardano Improvement Proposal (EIP) • This proposal must be selected by every ADA stakeholder using a weighted voting mechanism depending on how much ADA the corresponding stakeholder holds	• Upgrade of ledger is carried out via soft and hard fork • It is not clear yet if a smart-contract can be upgraded	• The electricity consumption is almost negligible because of its PoS-based Ourobors consensus algorithm • As many of its features, particularly smart contract facility, are not implemented yet, currently it has low popularity. It is yet to see how it functions and how much popularity it can gain once all of its features have been properly implemented

of a distributed ledger whereas a hard fork is not backward compatible. Any major feature in a distributed ledger is upgraded via a hard fork whereas minor changes are carried out via a soft fork.

Smart contracts in Ethereum lack any upgradability feature, thereby making it difficult to update any smart contract in case a new feature needs to be added or a bug needs to be corrected. Since a smart contract can potentially hold a large amount of Ether (e.g. when they are used for crowd-funding via ICOs), any bug in the smart contract code can be exploited, risking the theft of crypto-currencies. We have experienced two major cases involving DAO which accounted for 60 million of Ether [38] and Parity multi-sig wallet which accounted for around 6.1 million [39]. In the case of DAO, the Ethereum had to be hard-forked to invalidate the stolen crypto-currencies, yet the stolen Ether in the Parity attack remained unrecoverable without a hard-fork. Both attacks were made possible due to a bug in the corresponding smart contracts, meaning that the Ethereum protocol remained secure. For this reason, the confidence in Ethereum remains high and the price of Ether and market capitalization of Ethereum has also increased. Interestingly, EOS has a built-in smart contract update capability without creating any fork of the ledger. Public blockchain is often criticized for lack of governance when it comes to cyber crime [36], [37], money laundering [38] and drug trading [39].

Private DLT systems such as Fabric, Sawtooth, Burrow, Multichain and Corda have been created to resolve the issues of public DLT systems. They do not rely on an energy-intensive consensus algorithm. They can process transactions much faster than any public DLT system. The identity of each entity within the network is verified, thereby enabling auditability and accountability. This also acts as a mechanism for protection against Sybil attacks.

Private DLT systems afford federated access to data in the ledger, ensuring privacy by only allowing authorized entities to access any private and sensitive data in the system. There is no appropriate context-aware access control mechanism in these systems to control who can access what data. The classical context-aware access control systems [40] can be used to improve data sharing, considering different requirements, such as context-specific authorization for data access [41], context-specific data sharing, relationship-specific data access [42], situation-specific data sharing [43], and data access and sharing according to the imprecise contextual conditions [44]. In today's IoT-driven environments, we can integrate both access control and blockchain

TABLE 4. Qualitative evaluation of selected DLT platforms (Part B).

Platforms	Trust Level	Governance	Upgradability	Sustainability
Fabric	Emerging	• Open source code-base • Governed by the Hyperledger foundation charter • Code-base maintained by a committee • Anyone can participate in the development process	• Upgrade of the core software is carried out via Fabric committee member • Chaincode is upgradable using the version property	• Sustainability will depend on the commitment of the committee member of Fabric in the Hyperledger foundation and desire by different organisations to adopt it in different use-cases.
Sawtooth	Emerging	• Open source code-base • Governed by the Hyperledger foundation charter • Code-base maintained by a committee • Anyone can participate in the development process	• Upgrade of the core software is carried out via Sawtooth committee member • Transaction family is upgradable using the version property	• Sustainability will depend on the commitment of the committee member of Sawtooth in the Hyperledger foundation and desire by different organisations to adopt it in different use-cases.
Burrow	Low	• Open source code-base • Governed by the Hyperledger foundation charter • Code-base maintained by a committee • Anyone can participate in the development process	• No information available	• Sustainability will depend on the commitment of the committee member of Burrow in the Hyperledger foundation and desire by different organisations to adopt it in different use-cases.
Multichain	Moderate	• Open source code-base • Governed by Coin Sciences Ltd • Code-base maintained by the Multichain Development Team • The development team is working to include several high-end features for enterprise edition	• Upgrade of the core software is carried out by the Multichain development team	• Sustainability of Multichain will depend on client's satisfaction. Multichain is showing its potential as it has partnered with 86 companies.
IOTA	Moderate	• Open source code-base • Governed by the IOTA Foundation • Code-based maintained by the IOTA Development Team	• Upgrade of the core software is carried out by the IOTA development team.	• Highly sustainable. Only the energy consumption for validating two transactions is required for each participating node to get a transaction confirmed.
Corda	High	• Governed by a private company called R3. • Code-base maintained by R3 who releases versions on a regular interval. As of writing, V4.1 is the latest version available to use.	• Upgrade of ledger is carried out via soft and hard fork • It is not clear yet if a smartcontract can be upgraded	• Sustainability of Corda depends how clients use this DLT. Around 300 companies have been using it for financial use-cases.
Waltonchain	Moderate	• Open source code-base • Governed by Waltonchain • Code-based maintained by the Waltonchain Development Team	• Upgrade of the core software is carried out by the Waltonchain development team.	• Sustainability of Waltonchain will depend on the use of the RFID tags used in the industry.

technologies to implement more advanced context-aware access control systems working towards future implementations of blockchain-based access control for maintaining data sharing between different parties. In addition, there is no notion of cost in these systems, enabling any type and amount of data to be stored following their corresponding algorithms. Both fabric and Sawtooth support the upgradability of smart contracts, which can be vital when new logic needs to be incorporated or a bug needs to be fixed. All these properties make the private DLT systems suitable for scenarios that need to deal with highly sensitive data, such as digital evidence with high assurance and without undesirable restrictions.

However, one important aspect to note is that private DLT systems cannot provide the same amount of security regarding the immutability of data and code in comparison to public DLT systems. This is because compromising the integrity guarantee in any DLT systems would require corrupting or colluding with the majority of validating nodes (the so called 51% attack). It would be much more difficult, if not impossible, to control these many validating nodes in a public DLT system, consisting of thousands of miners/stakeholders compared to a private DLT system where there might only be a handful of validators. Even with this restriction, a satisfactory level of security can be achieved, as the participating nodes are trusted. Furthermore, the adoption level of private DLT systems is much less than public systems. This will arguably change as private systems are evolved and adopted by different organizations for use-cases in different domains.

Among five selected private DLT systems, our evaluations have found that Hyperledger Burrow lacks thorough documentation and is currently in the process of being migrated to the Hyperledger project. Because of this, we do not consider it to be a suitable candidate for this proof of concept. In between Fabric and Sawtooth, Fabric is more favorable as its strong privacy support using the notion of channels, as well as its flexible support for writing complex smart contracts using popular programming languages such as Java and Go. On the other hand, Sawtooth may provide a higher guarantee of security than Fabric because of its use of the SGX component. However, this is also a restriction of Sawtooth as it might be difficult to adopt in legacy systems which do not support Intel SGX technology. Multichain has potential to be a main competitor in this space, however, the development process of this private blockchain is relatively slow compared to other candidates. The summary of quantitative and qualitative assessment of different DLT platforms are presented in the above tables (1 – 4).

VII. CONCLUSION

Although the DLT is considered potentially disruptive in many ways, there is a lack of basic understanding how to use this emerging technology effectively in different domains.

It is evident that many startup companies have failed to select the right development platform for their blockchain applications which resulted in severe difficulties while developing the system. This paper aims to provide a comprehensive comparative analysis of different blockchain platforms that would help to realize the properties of both private and public DLT platforms. In addition, the quantitative and qualitative evaluation of these platforms will provide a reference for selection of a best-fit DLT platform for a given application.

REFERENCES

[1] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ, USA: Wiley, 2016.
[2] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *J. Econ. Perspect.*, vol. 29, no. 2, pp. 213–238, 2015.
[3] (Sep. 2019). *Multichain*. [Online]. Available: https://www.multichain.com/
[4] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[5] C. Dannen, *Introducing Ethereum and Solidity*. Berkeley, CA, USA: Apress, 2017.
[6] (Sep. 2019). *Fabric Next*. [Online]. Available: https://github.com/hyperledger-archives/fabric/wiki/Fabric-Next
[7] (Sep. 2019). *Sawtooth*. [Online]. Available: https://www.hyperledger.org/projects/sawtooth
[8] (Sep. 2019). *Burrow*. [Online]. Available: https://www.hyperledger.org/projects/sawtooth
[9] (Sep. 2019). *Eos*. [Online]. Available: https://eos.io/
[10] (Sep. 2019). *Corda*. [Online]. Available: https://www.r3.com/platform/
[11] (Sep. 2019). *Cardano*. [Online]. Available: https://www.cardano.org/en/home/
[12] (Sep. 2019). *Iota*. [Online]. Available: https://www.iota.org/
[13] (Sep. 2019). *Waltonchain*. [Online]. Available: https://www.waltonchain.org/
[14] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, 2016, Art. no. e0163477.
[15] M. Risius and K. Spohrer, "A blockchain research framework," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 385–409, 2017.
[16] Z. Hintzman. (Sep. 2019). *Comparing Blockchain Implementations, Technical Paper*. [Online]. Available: https://www.nctatechnicalpapers.com/Paper/2017/2017-comparing-blockchain-implementations
[17] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, May 2018, pp. 1–6.
[18] M. Macdonald, L. Liu-Thorrold, and R. Julien, "The blockchain: A comparison of platforms and their uses beyond bitcoin," in *Proc. Adv. Comput. Netw. Secur. (COMS)*, 2017, pp. 1–17.
[19] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data*, 2017, pp. 1085–1100.
[20] T.-T. Kuo, H. Z. Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: A systematic review and healthcare examples," *J. Amer. Med. Inform. Assoc.*, vol. 26, no. 5, pp. 462–478, 2019.
[21] M. S. Ferdous, K. Biswas, M. J. M. Chowdhury, N. Chowdhury, and V. Muthukkumarasamy, "Chapter two—Integrated platforms for blockchain enablement," *Adv. Comput.*, vol. 115, pp. 41–72, 2019.
[22] G. Greenspan. (2015). *Multichain Private Blockchain-White Paper*. [Online]. Available: http://www.multichain.com/download/MultiChain-White-Paper.pdf
[23] (Sep. 2019). *icobench*. [Online]. Available: https://icobench.com/ico/eos
[24] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A prov-ably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2017, pp. 357–388.
[25] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project," in *Blockchain Enabled Applications*. Berkeley, CA, USA: Apress, 2017, pp. 139–149.
[26] N. Klaokliang, P. Teawtim, P. Aimtongkham, C. So-In, and A. Niruntasukrat, "A novel IoT authorization architecture on hyperledger fabric with optimal consensus using genetic algorithm," in *Proc. 7th ICT Int. Student Project Conf. (ICT-ISPC)*, Jul. 2018, pp. 1–5.
[27] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.* Cham, Switzerland: Springer, 2017, pp. 282–297.
[28] (Sep. 2019). *Namecoin*. [Online]. Available: https://namecoin.org/
[29] (Sep. 2019). *Proof of Existence*. [Online]. Available: https://proofofexistence.com.
[30] C. Fromknecht, D. Velicanu, and S. Yakoubov, "Certcoin: A namecoin based decentralized authentication system 6.857 class project," *Class Project*, to be published.
[31] (Sep. 2019). *Electron*. [Online]. Available: http://www.electron.org.uk/
[32] (Sep. 2019). *Slock*. [Online]. Available: https://slock.it/
[33] (Sep. 2019). *ENS*. [Online]. Available: https://ens.domains/
[34] (Sep. 2019). *Patientory*. [Online]. Available: https://patientory.com/
[35] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.
[36] C. Whyte, "Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise," *Studies Conflict Terrorism*, to be published.
[37] S.-H. Hong and M. Alazab, "Cybercrime and data breach: Privacy protection through the regulation of voluntary notification," Korea Legislation Res. Inst., South Korea, 2017, doi: 10.2139/ssrn.3042174.
[38] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the bitcoin ecosystem," in *Proc. APWG eCrime Res. Summit*, Sep. 2013, pp. 1–14.
[39] K. Hegadekatti, "Regulating the deep Web through controlled blockchains and crypto-currency networks," 2016, doi: 10.2139/ssrn.2888744.
[40] A. S. M. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization for cloud-based data resources," *Future Gener. Comput. Syst.*, vol. 93, pp. 237–255, Apr. 2019.
[41] A. S. M. Kayes, J. Han, and A. Colman, "ICAF: A context-aware framework for access control," in *Proc. ACISP*, 2012, pp. 442–449.
[42] A. Kayes, J. Han, A. Colman, and M. S. Islam, "RelBOSS: A relationship-aware access control framework for software services," in *Proc. OTM Confederated Int. Conf. 'On Move Meaningful Internet Syst.'* Berlin, Germany: Springer, 2014, pp. 258–276.
[43] A. S. M. Kayes, J. Han, and A. Colman, "An ontological framework for situation-aware access control of software services," *Inf. Syst.*, vol. 53, pp. 253–277, Oct./Nov. 2015.
[44] A. Kayes, W. Rahayu, T. Dillon, E. Chang, and J. Han, "Context-aware access control with imprecise context characterization through a combined fuzzy logic and ontology-based approach," in *Proc. OTM Confederated Int. Conf. 'On Move Meaningful Internet Syst.'* Cham, Switzerland: Springer, 2017, pp. 132–153.

MOHAMMAD JABED MORSHED CHOWDHURY received the dual master's degree in information security and mobile computing from the Norwegian University of Science and Technology, Norway, and the University of Tartu, Estonia, under the European Union's Erasmus Mundus Scholarship Program; and the Ph.D. degree from the Swinburne University of Technology, Melbourne, Australia. He is currently an Associate Lecturer in cyber security program with La Trobe University, Melbourne. He is also working with Security, Privacy, and Trust. He has published his research in top venues including TrustComm, HICSS, and REFSQ. He has published research work related to data sharing, privacy, and blockchain in different top venues.

MD. SADEK FERDOUS received the dual master's degree in security and mobile computing from the Norwegian University of Science and Technology, Norway, and the University of Tartu, Estonia, and the Ph.D. degree in identity management from the University of Glasgow. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh. He is also affiliated as a Research Associate with the Centre for Global Finance and Technology, Imperial College Business School. He has several years of experience of working as a Postdoctoral Researcher in different universities in different European and U.K.-funded research projects. He has published numerous research articles and book chapters in these domains in different books, journals, conferences, workshops, and symposiums. His current research interests include blockchain, identity management, trust management and security and privacy issues in cloud computing, and social networks.

KAMANASHIS BISWAS received the master's degree in computer science (specialization in security engineering) from the Blekinge Institute of Technology (BTH), Sweden, and the Ph.D. degree in ICT from Griffith University, Australia. Prior to his Ph.D., he worked as a Faculty Member with the Department of Computer Science and Engineering, Daffodil International University, Bangladesh, for about four and half years. He is currently a Lecturer in information technology with the Peter Faber Business School, Australian Catholic University - Strathfield Campus. He has published more than 20 research articles in various conferences, symposiums, and journals, including IEEE and Springer. He is a reviewer for many journals and international conferences. His research interests include blockchain technology, design and development of lightweight cryptographic schemes, energy efficient secure routing algorithms, intrusion detection systems (IDS), and clustering schemes in wireless sensor networks.

NIAZ CHOWDHURY received the bachelor's and master's degrees (Hons.) in computer science and engineering from East West University, Bangladesh, and the Ph.D. degree from the School of Computing Science, University of Glasgow, U.K. He is currently a Postdoctoral Research Associate with the Knowledge Media Institute (KMI), The Open University, U.K. His primary areas of research include the Internet of Things (IoT), blockchain, machine learning, data science, and privacy. He has diverse, yet well-connected research experiences gathered from three nations in the British/Irish Isles: Ireland, Scotland, and England. Prior to his current position at KMI, he completed another postdoc in the Department of Computing and Communication, The Open University, where he worked in the smart city project MK-Smart. Dr Chowdhury was a recipient of the Scottish ORS Scholarship in conjunction with the Glasgow University College of Science and Engineering Scholarship. He was also a research scholar at the School of Computer Science in Trinity College Dublin, where he received Government of Ireland IRCSET Embark Initiative Scholarship.

A. S. M. KAYES received the Ph.D. degree from the Swinburne University of Technology, Australia, in 2014. He is currently a Lecturer in cyber security with the Department of Computer Science and Information Technology, La Trobe University, Australia. His research interests include information modeling, context-aware access control, big data integration, the IoTs, cloud and fog computing, advanced data analytics, fuzzy computation, and security and privacy protection.

MAMOUN ALAZAB received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia. He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University. He is also a Cyber Security Researcher and a Practitioner with industry and academic experience. He organized and participated more than 70 conferences and workshops, seven as a General Chair. His research interests include cyber security, blockchain technologies, and digital forensics of computer systems, and particularly cybercrime detection and prevention. He has more than 100 research articles. He presented many invited and Keynotes talks at conferences and venues (22 events in 2018 alone). He is an Editor on multiple editorial boards, including an Associate Editor of IEEE Access, an Editor of the *Security and Communication Networks Journal* and a Book Review Section Editor: the *Journal of Digital Forensics*, *Security and Law*. He has been involved in past research work to support agencies, such as the Australian Federal Police, Attorney General's Department, and major banks in Australia.

PAUL WATTERS began his first R&D role in security, in 2002, joining the CSIRO's Networking Applications and Technologies (NAT) Group, and leading a programme in secure and distributed storage. In 2013, he took up a Professorship in IT at Massey University, New Zealand. In 2015, he became an Adjunct Professor at the Unitec Institute of Technology, the home of New Zealand's first Cyber Security Research Centre. He is currently a Professor and a Leading Expert in cyber security with the Department of Computer Science and Information Technology, La Trobe University, Australia. In recognition of his track record combating child abuse material online, he received an ARC Discovery grant, in 2015.