A Survey on Blockchain for Enterprise Using Hyperledger Fabric and Composer

Dongcheng Li and W. Eric Wong*
Department of Computer Science
University of Texas at Dallas
Richardson, USA
e-mail: {dxl170030,ewong}@utdallas.edu

Jincui Guo
School of Mechanical Engineering and Electronic Information
China University of Geosciences (Wuhan)
Wuhan, China
e-mail: guojc888@vip.sina.com

***Abstract*—The potential of blockchain technology is immense and is currently regarded as a new technological trend with a rapid growth rate. Blockchain platforms like Bitcoin are public, open, and permission-less. They are also decentralized, immutable, and append-only ledger; those ledgers can store any type of data and are shared among all the participants of the network. These platforms provide a high degree of anonymity for their users' identity and full transparency of the activities recorded on the ledger while simultaneously ensuring data security and tamper-resistance. All nodes on the network collectively work to validate the same set of data and to achieve group consensus. Blockchain platforms like Ethereum have the ability to develop smart contracts and embed business logic. This allows the use of blockchain beyond cryptocurrency as a business management solution. Besides the issues of scalability and the expensive nature of most blockchain systems, many attributes of traditional public blockchain are not desirable in a business or enterprise context such as anonymity, full transparency, and permission-less. Permissioned blockchain platforms like Hyperledger Fabric are designed and built with enterprise and business in mind, retaining the desirable qualities of blockchain for enterprise while replacing the qualities of blockchain that are undesirable for the enterprise. In this paper, we present a comprehensive review on the Hyperledger enterprise blockchain technologies.**

Keywords-component: Hyperledger Fabric; Hyperledger Composer; Blockchain; Chaincode

I. Introduction

The emergence of blockchain is a disruptive technology in asset trading and information sharing sectors with the capability to change numerous businesses, professions, enterprises, industries, and even facets of life. Its potential usage in other industries apart from the financial sector is considered probable. The focus of this paper is to provide a detailed literature review on blockchain for enterprise using Hyperledger Fabric and Composer. It will also delve into the technologies, challenges, and applications of this disruptive technology. The organization of this paper is as follows. In section 2, we present a high-level overview of the blockchain technology. We introduce various frameworks and tools hosted by the Hyperledger greenhouse that aim to facilitate the development of enterprise blockchain in Section 3. In Section 4, we explain the taxonomy and architecture of Hyperledger Fabric and Composer as an enterprise solution in detail. Then, in Section 5 we review and evaluate the applications of Hyperledger Fabric and Composer in recent researches. Finally, we draw the conclusion of the paper and elaborate on potential future works.

II. The Overview of Blockchain

In order to understand blockchain technologies for enterprise, it is important to first understand the basics, the categories, and the benefits of blockchain.

A. What is Blockchain?

Blockchain is a peer-to-peer, decentralized platform with an architecture that is distributed and assigns its assets to all nodes, working collectively to make approval decisions on behalf of the network. In a decentralized system, there is no central node acting as an agent or middleman for all communications. However, every node has the permission to perform peer-to-peer capabilities identified as transactions [1]. Besides being distributed, the blockchain ledger is append-only, utilizing cryptographic methods that ensure that as soon as a transaction has been added and verified in the ledger, it cannot be modified, changed, or deleted and happens on each and every instant [2].

B. Types of Blockchain

According to Rajput et al [3], there are two types of blockchain models: permission-less and permissioned. To obtain discretion, security, and other requirements, permission-less and permissioned blockchains are significant in the blockchain society [4].

1) Permission-less Blockchain: Permission-less blockchain is often referred to as a public blockchain network system. In this kind of blockchain technology, the real-world identification of participants are pseudonymous, and each member participating may add another block to the ledger. Bitcoin, which is an open platform, is an excellent example of a permission-less blockchain [4]. Every individual or company can decide to run a node for the blockchain and participate in transaction approval with the mining algorithm. Ethereum is another example of a permission-less blockchain framework that allows an individual to make and implement the program on the platform [5] .

978-1-7281-6057-3/19/$31.00 ©2019 IEEE
DOI 10.1109/DSA.2019.00017

2) Permissioned Blockchain: The permissioned blockchain is created to license an individual, an enterprise, or a group of companies to move data and record transactions proficiently. Permissioned blockchain comes with an extra layer of privilege to choose who can take part in the transactions within the network, with the identity of every member known to all members [3]. In the permissioned blockchain network framework, the member does not get an opportunity for extortion as their identity is known to the administration server.

C. Why Blockchain?

One of the significant aspects of blockchain entails establishing trust across a business or enterprise network through the blend of smart contracts, a distributed ledger, cryptographic algorithms, and the element of consensus. The ledger holds the present state of assets as well as the past records of all transactions, and there is always a secure connection between the two adjacent transactions so they cannot be effectively disrupted. The immutability nature of blockchain enables the record to be the single source of truth for questions about the business processes which span across multiple organizations.

The most grounded uses for blockchain involves business networks, which include trust via the properties of consensus, immutability, provenance, and finality. Immutability implies that the historical record of transactions cannot be changed. Finality provides ease of mind since every member is guaranteed that their copy of the ledger matches every single other copy and that transactions contained in the blockchain have been truly committed. Provenance implies that the start of any assets held in the ledger is known. Alterations to the ledger need approval by members, as indicated by an agreed-upon endorsement policy. This objective is accomplished through consensus, in which members of the system endorse that the transaction is legitimate and concede the refreshed state of the ledger [6].

Furthermore, implementing blockchain in an organization can provide clarity and insight into business processes. By reducing costs and overall complexity of the business network, it improves the discoverability and traceability for information, and by automating shared processes across organizations, blockchain creates a trusted library of business processes. Figure 1 shows the side-by-side comparison between a traditional business network model and a blockchain business network model.

III. Hyperledger Technologies for Enterprise

In the past decade, blockchain technology has gained popularity not only in the tech sector, but also in the academic and financial sector. That increase in popularity has drawn more interest and developers who have in turn advanced the blockchain idea to create more protocols suited for different tasks. Such protocols include Bitcoin, Ethereum, Hyperledger, Ripple Consensus Network, R3's Corda, etc. [8]. Of these protocols, the most popular include Bitcoin and Ethereum due to the high usage of their respective currencies. However, Hyperledger have in recent years been gaining acceptance in the software development sector as more participants realize its potential benefits. This paper will focus on the Hyperledger protocol and explore the different technologies it offers, as well as its associated challenges and trade-offs.

Hyperledger is understood as an open blockchain platform that was first released in December 2015 by the Linux Foundation [8]. The main goal of utilizing the Hyperledger protocol is to enhance reliability and performance of the ledgers. Given that the platform is open source, there is a huge emphasis on the participation of players from different industries so as to advance the blockchain technology. Linux Foundation has made efforts to create a good environment for collaboration by providing a modular framework that supports a wide array of components for different uses. The combination and interaction between those components will benefit the development of blockchain solutions for enterprise. Figure 2 shows various frameworks and tools under the Hyperledger project.

A. Hyperledger Frameworks

Since the inception of the Hyperledger project in 2015, the platform has undergone major improvements made true through collaboration with players such as Enterprise Ethereum Alliance (EEA), Microsoft's Coco, Cisco, etc. [8]. These improvements have resulted in development of various Hyperledger frameworks that include Sawtooth, Iroha, Fabric, Burrow, Besu and Indy.

1) Hyperledger Sawtooth: developed by the Intel team, it is used to develop, deploy, and implement distributed ledgers. The platform has a different consensus algorithm for use based on the magnitude of a network. Rasti and Gheibi [10] posits such algorithm to include the Proof or Elapsed Time (PoET) which helps with scalability. The Hyperledger Sawtooth provides versatility and support for permissioned as well as permission-less deployments.

2) Hyperledger Iroha: was developed through a collaborative effort from NTT Data, Soramitsu, Hitachi, and Colu. The team developed this framework with the goal of easing integration into projects that require distributed ledger technologies (DLTs). Unlike other Hyperledger frameworks, Iroha focuses on the development of mobile applications together with client libraries for both Android and iOS. Yewale [8] points out that the Iroha framework is highly preferred by developers using the C++ language.

3) Hyperledger Fabric: is an open-source, permissioned blockchain framework for industrial-grade applications [11]. Rasti and Gheibi [10] describes Hyperledger Fabric as a revolutionary framework due to its features that allow membership services and plug-and-play properties for blockchain solutions.

4) Hyperledger Burrow: was designed by Monax [12] and allows developers and architects to create an Ethereum virtual machine environment within the context of their Fabric and Sawtooth networks. It is a solution to leverage Ethereum functionality in conjunction with Hyperledger functionality.

5) Hyperledger Indy: was developed by the Sovrin Foundation [12]. It provides developers and solutions architects with a wealth of tools around identity management.

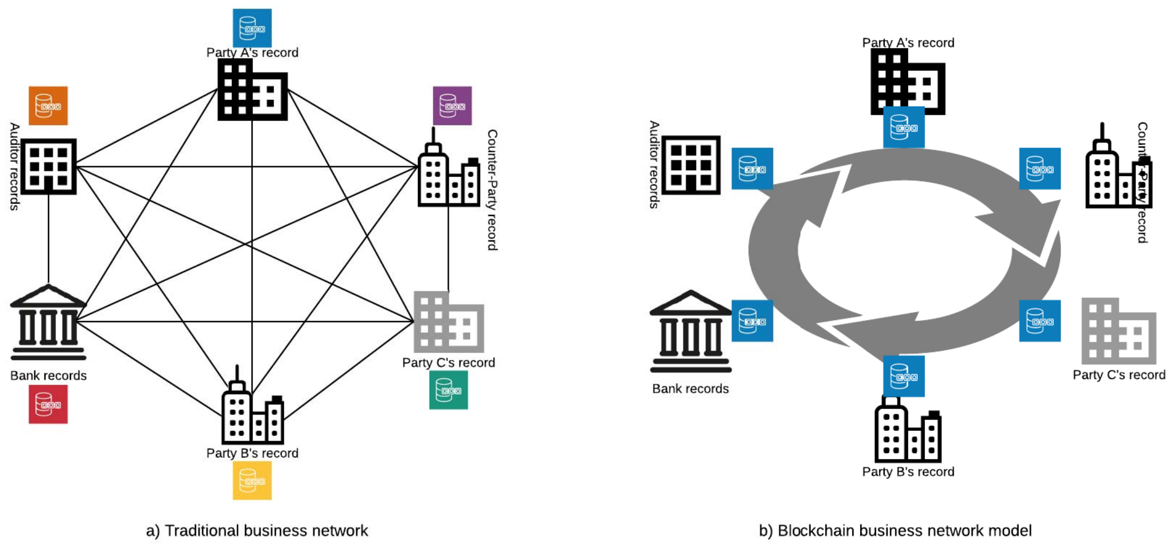

Figure 1. Side-by-side comparison between traditional business network model and blockchain business network model [7].

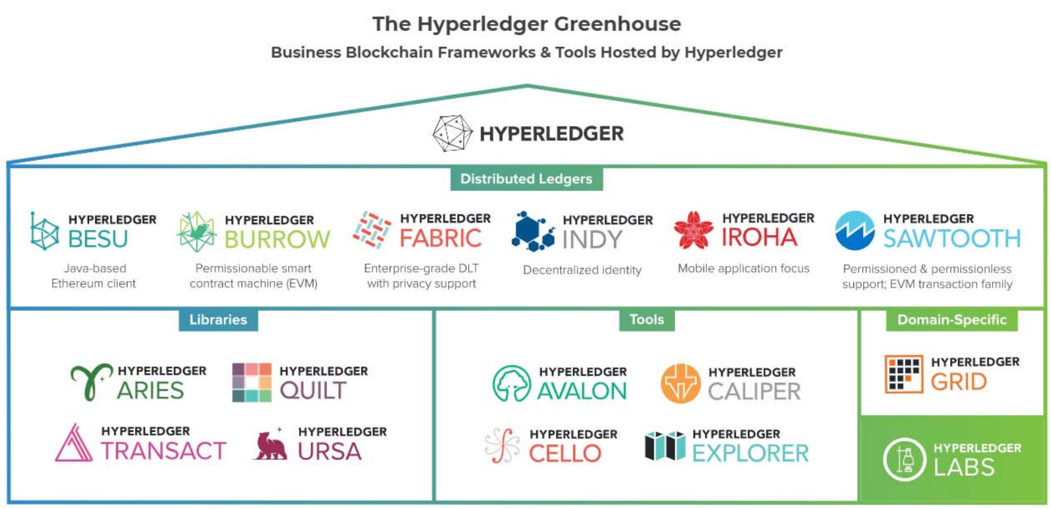

Figure 2. Hyperledger Enterprise Blockchain Technologies [9].

6) Hyperledger Besu: is the most recent project to join the Hyperledger platforms. As an open-source Ethereum client, it makes use of the Ethereum public network. In addition, it is written in Java [9].

B. Hyperledger Tools

Hyperledger tools refer to supporting software utilized to maintain and execute blockchains [13]. Also, these tools are utilized to monitor and explore information on the ledgers as well as design and make improvements in the blockchain networks. The common Hyperledger tools include Caliper, Cello, Composer, Explorer, and Avalon.

1) Hyperledger Caliper: is a benchmarking and performance monitoring tool for Hyperledger solutions [10]. It provides reliable metrics on network throughput, transactions per second, transaction volume, and more.

2) Hyperledger Cello: is designed to be a rich graphical user interface experience for Hyperledger solution. It allows administrators and the operations side of your organization to deploy and manage blockchain as a service [10], allowing them to quickly maintain and reconfigure Fabric and Sawtooth deployments.

3) Hyperledger Composer: a toolset that allows developers to quickly and easily define blockchain solutions [10], and then rapidly iterate through development cycles. However, the project has been deprecated since 29th August 2019, which means the support for program issues and updates for new features are foregone. This also causes incompatibility with the later version of Hyperledger Fabric. Since Hyperledger Composer is built on top of Hyperledger Fabric for calling the Fabric APIs, it is really optional in the process of developing blockchain applications with Hyperledger Fabric. Migrating from Composer to other tools or developing without it are all valid options. Hyperledger Composer is a well-developed project and can access the Fabric in an easy to use manner. It is sufficient and efficient for the purpose of creating a proof-of-concept business model.

4) Hyperledger Explorer: is a blockchain Explorer for Hyperledger solutions. It is similar to blockchain.info and etherscan.io used to view transactions and block information about blockchains [11]. In addition, it gives its user the functionality to scroll through and peruse data on the blockchain and collect metrics about data as it gets reported on blocks.

5) Hyperledger Avalon: is one of the newest projects to be included in the Hyperledger namespace. It was the result of Hyperledger, EEA, and cloud service provider ecosystems collaboratively working together. It allows computations to be handled off-chain while still maintaining trust and increasing transaction throughput without giving up privacy [14].

IV. Hyperledger Fabric and Composer as an Enterprise Solution

It is almost impossible nowadays for a viable business model to operate and be self-sufficient without dependencies on any other organizations or entities. One of the biggest problems that Hyperledger attempts to solve is providing truly shared infrastructure across multiple different organizations on a business network. Modern business network infrastructures are like the Traveling Salesman problem, whereas the number of participants (businesses) that joins the network increases linearly, the complexity of the entire business network increases exponentially [7]. By utilizing the network infrastructure of Hyperledger, integrating new businesses to an existing business network becomes easier.

In addition, Hyperledger Fabric provides a modular design with a demarcation of responsibilities between the nodes in the blockchain network, implementation of smart contracts also known as chaincodes, and configurable consensus and participant services. At the core of the system is a distributed ledger for the unchanging account of transactions happening in the system. Fabric architecture is intended to convey high degrees of privacy, versatility, adaptability, and scalability. In this section we will dive into the different elements that goes into the Hyperledger Fabric and Composer business solution.

A. Nodes

Hyperledger Fabric is often shortened as HF and is currently one of the significant and most mature permissioned blockchain structures in the Hyperledger namespace. Unlike Bitcoin or Ethereum which have only one node type in the network leading to great inefficiency and poor scalability, the Hyperledger Fabric Network comprises of several node types, client nodes, peer nodes, and ordering nodes, which each give different functionalities to an organization [3].

1) Client Node: is the node on the blockchain network that the client interacts with, and it initiates all transactions or Chaincode calls made on that Fabric network.

2) Peer Nodes: have two distinct types, Committing Peer and Endorsing Peer. The former keeps a redundant copy of the ledger, and the latter not only keeps a copy of the ledger but also executes the chaincode. In addition, there is a special kind of peer called an Anchor peer, which can be set for any single peer in every organization. It spans multiple channels or even multiple networks and is used to bridge these channels or networks together.

3) Ordering Nodes: collectively make up the ordering service that keeps all the data in sync and prevents any data anomalies or mis-ordered transactions on the ledger.

B. Ledgers

The replicated ledger in Hyperledger Fabric create the failover mechanism and fault tolerance for the system. The histories contained in the Ledgers are immutable transactions and are used to show business participants how their assets grow, evolve, change, and die over time. There are two types of ledgers in Hyperledger Fabric: the transaction log and the world state database.

1) Transaction log: are the permanent append-only immutable ledgers in Hyperledger Fabric. Transaction log by default use the instance of level DB that had the update and delete functionality removed and are left with only the create and read operations [15].

2) World state database: stores the current state of all assets and information related to participants. It is the mutable storage (ledger) of Hyperledger Fabric, since it still has the update and delete functionality, and information in the database can be changed. By default, it is kept in an instance of CouchDB, which can perform complex queries and only shows the current state of the network [15].

C. The interplay between different types of nodes and ledgers

The process begins with a user inside the client application on a client node submitting a transaction. The client node broadcasts that transaction to all the endorsing nodes for a certain chaincode on the network. Then, each of those endorsing nodes execute the chaincode and create a read-write set, the "before" state and the "after" state around the transaction. Next, they independently send their read-write set back to the client application. The client application compares the result received from the endorsing peers against the definition in the endorsement policy. If the result passes, the network reaches consensus. Then, the client application sends that transaction to the ordering service for inclusion on the ledger before the ordering service broadcasts that transaction to all the endorsing and committing nodes. At this stage, the endorsing and committing nodes perform the checks again on the received transaction against the read-write set, which prevents the possibility of recording the wrong state of an asset due to transactions coming from different applications simultaneously. After the checks returns successfully, the transaction moves on to the ledger. This means a permanent record of this transaction has been added on the transaction log, and the world state database is updated to reflect the new current state of the affected assets and participants. Finally, the confirmation that this transaction has been successfully included on the ledger is sent back to the client node.

D. Membership Service Provider and Certificate Authority

The identity of each node on the Hyperledger Fabric System, which is issued by a certificate authority [16] and managed by the X.509 certificates as default, is generally identified by the membership service provider that corresponded with an enterprise. All nodes in the Hyperledger Fabric network have a uniqueness to the identities of all parties. The membership service provider answers the question "is this a valid user (node) in my organization?" Additionally, it gives the chance to use an agreement mechanism that is a lot lighter computationally than the mechanism of Proof of Work. Chaincode in HF. empowers members to execute complex transactions according to demarcated authorizations (permissions). Hyperledger Fabric additionally adds the capacity to fabricate trusted subnetworks, known as channels, that can create shared records with its own set of smart rules (Chaincode) to a distinct set of nodes. Endorsement Policies allow participants to define consensus among themselves and set up different consensus parameters for different channels.

E. Components in Hyperledger Composer

The Hyperledger Composer underpins the Hyperledger Fabric structure and runtime and facilitates a faster business network for the execution of applications [17]. The business network description is transferred as an archive (. bna file) when it is set to be deployed. The description of the network is comprised of four primary files: query, script, model, and access control, as seen in Figure 3.

1) The script file: describes the different transactions in the system. The file is coded using the JavaScript scripting language and works on the transaction logic.

2) The query file: outlines the structure and capacity of queries from this system.

3) The model file: is in charge of delineating the organization of the network. The model file has three major segments: transactions, assets, and participants, and assets and participants own different properties. In additional, there are also events.

a) Participants: are individuals, organizations, or systems who are going to interact with an asset.

b) Assets : are the items participants care about. They can be tangible or intangible and usually have a finite lifespan.

c) Transactions : are mostly the interactions between the assets and the participants.

d) Events : can be raised in chaincodes and is defined using the event keyword and, just like Transaction, does not require a unique identifier.

4) The access control file: outlines the particular extent of access clients have in the business network.

Hyperledger Composer also offer a web-based tool called Composer-Playground which is used to streamline the activity by aiding in the development, packaging, and testing of the ventures. Figure 4 shows the snapshot of the Composer-Playground tool.

F. Application Deployment Process

When the system is well-defined, it can be transferred as an archive file, copied, and installed on another computer. A network card is utilized to access the network. Network cards can appear as a member or an administrator. Member cards, by and large, have more controlled access to the system, while the administrator can perform all of the high-clearance tasks such as adding new members or removing members. This card type describes the node that uses the card to interface with the system and, consequently, describes what sort of responsibility the node has.

Hyperledger Composer incorporates the composer rest-server to create REST API automatically for the business network. In addition, Hyperledger Composer also makes extensive use of the Yeoman configuration tool. It is very easy to create new solution templates or Angular front-end against the REST API with a single command line using the Yeoman generation. The amount of time saved by leveraging various Hyperledger Composer tools is tremendous. Figure 5 shows the structure of the application using Hyperledger Composer.

V. Applications of Hyperledger Fabric and Composer in Research

There are several potential applications of Hyperledger Fabric in the modern world. Such applications include the automation of business contracts to increase trust levels, the creation of a loyalty reward platform, implementation of distributed storage to improve trust between individuals, and an asset depository whereby the assets are dematerialized to enable users to access different types of assets without going through a middleman [8]. A survey and review of real-life cases that have applied Hyperledger Fabric and Composer revealed that not only are such instances many, but also numerous research articles have been published about them. This section provides a review, analysis, and comparison of the cases that have applied Hyperledger Fabric and Composer to develop blockchain enterprise solutions.

After reviewing the research publications on blockchain technologies, several cases of application of Hyperledger Fabric and Composer were identified. The cases were distinct from each other as they spanned multiple industries. Some of the cases were theoretical, while others reported findings after practical applications. Theoretical cases refer to those that

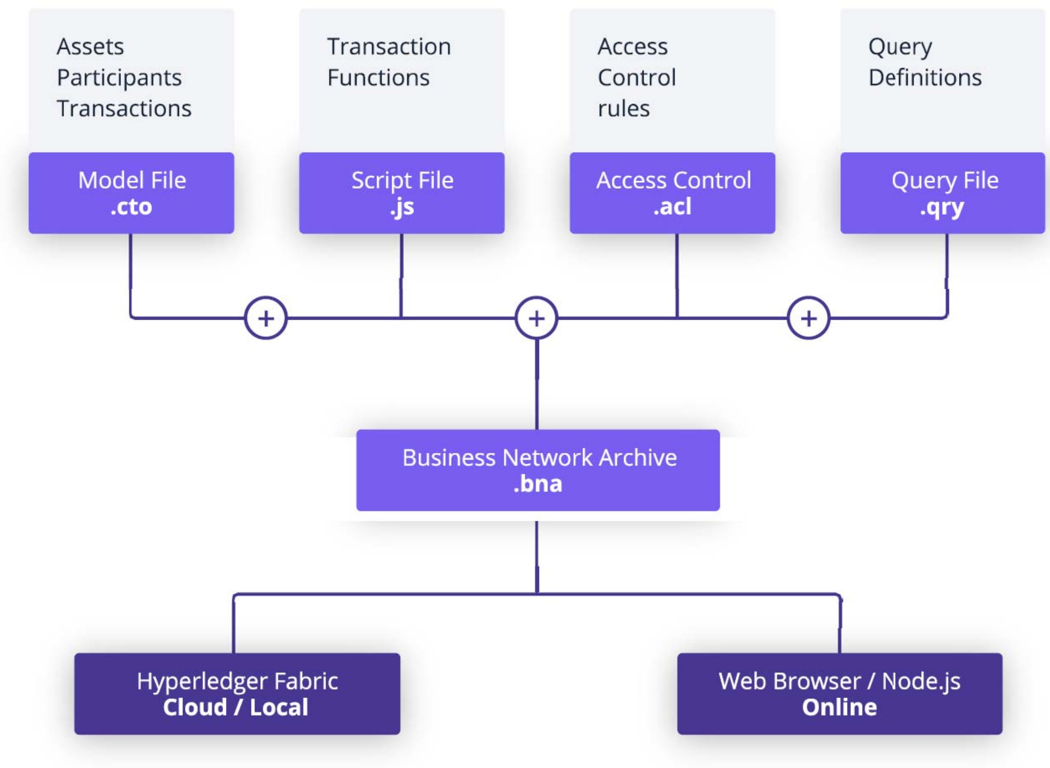

Figure 3. Hyperledger Composer Architecture [18].

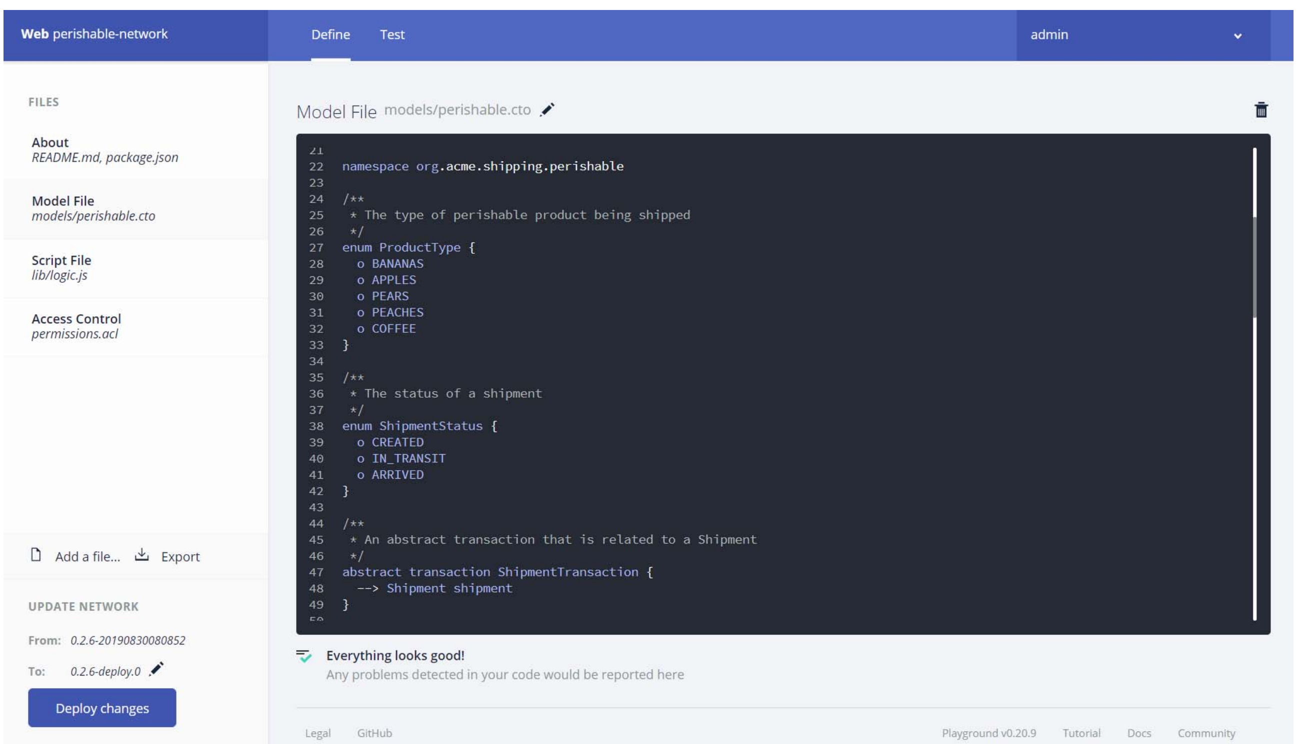

Figure 4. Hyperledger Composer Playground Web Interface [19].

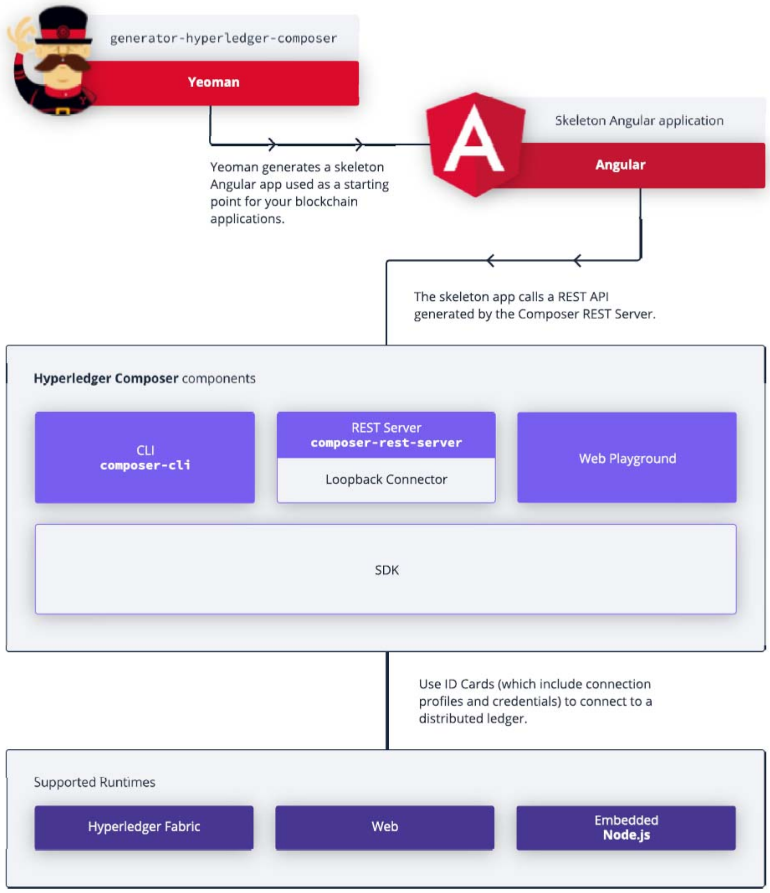

Figure 5. Layers in the Hyperledger Fabric and Composer Solution [18].

only proposed the blockchain solutions on paper and had not actually implemented them in real life or tested their feasibility or effectiveness. After analyzing the cases, the applications of Hyperledger Fabric and Composer were categorized into three groups. These groups include applications in medical services, applications in supply chain and business transactions, and applications in cybersecurity and fraud prevention. This section reviews the various applications for each sector while providing a comparison of the individual cases in that category.

A. Medical services

As indicated by Jamil et al [15], the yearly business loss of US pharmaceutical enterprises is roughly $200 billion because of prescription forging and medication counterfeiting. Duplicating isn't simply the principle reason; rather, when contrasted with conventional medications, these fake drugs produce diverse symptoms to human wellbeing. It is hard to recognize fakes in light of the fact that these medications go through various complex disseminated systems, a process that opens doors for fakes to enter the bona fide store network. As such, the safety of the pharmaceutical inventory network has become a significant worry for the wellbeing of the general public. Jamil, Hang, Kim and Kim [15] proposed a novel drug supply chain management solution that utilizes Hyperledger Fabric and Composer to handle secure medication inventory network records. The proposed framework resolves this issue by directing medical record transactions on a blockchain to make a medicinal ecosystem with a drug supply chain. The scholars did various investigations so as to show the ease of use and effectiveness of the planned stage. Finally, they utilized Hyperledger Caliper as a benchmarking apparatus to lead the presentation of the planned framework.

Similar to Jamil, Hang, Kim, and Kim's [15] publication, Munoz, Constantinescu, Asenjo, and Fuentes [20] published their findings after implementing a blockchain-based solution to address a healthcare problem. Their solution focused on addressing the challenge of universal access to health records. As the world increasingly becomes connected, known as globalization, there will be increased need for universal access to every patient's health records so as to connect the health care services. That would help to eliminate the redundancy and high costs that characterize emergency medical conditions. In this view, Munoz, Constantinescu, Asenjo, and Fuentes [20] developed the ClinicAppChain, which is a low-cost and cross-platform blockchain solution that allows users to participate without the need for cryptocurrencies.

There has been an emergence of general-purpose blockchain frameworks that are used to establish healthcare applications. One of the challenges faced by health information technology (HIT) is the security breach of medical records data. It is imperative to ensure that the medical records data has been safeguarded because they are central to the diagnosis and treatment regimens of the patients [13]. In Agbo and Mahmoud's paper, they compared the common general-purpose blockchain frameworks to the requirements for healthcare systems in order to help guide other researchers and practitioners of health informatics when selecting the right platform for establishing and experimenting with blockchain-based healthcare applications.

Another publication by Rajput, Li, Ahvanooey, and Masood [3] presents a case of how Hyperledger Fabric and Hyperledger Composer can be used in the healthcare sector to better manage personal health records (PHRs) and improve patient care. The motivation for this project stems from the uncertainty on the functions of PHRs during emergencies. In many health care settings, a patient cannot give consent to emergency medical practitioners to access their medical records. Rajpu, Li, Ahvanooey, and Masood [3] point out that many emergency care settings do not have a secure approach of managing and tracking the patient's health records. Personal health records contain critical information about the patient and such information should be confidential and secure. To address these problems, Rajput, Li, Ahvanooey, and Masood [3] proposed an emergency access control management system (EACMS) that is blockchain based and utilized Hyperledger Fabric and Hyperledger Composer.

The operation of EACMS begins with the initialization of rules for gaining access to the emergency control management of the PHR. After the patient saves their health information in the blockchain solution, it can be accessed by multiple individuals. However, the blockchain system only allows the PHR data to be visible to the EMTs which typically have universal access rights in accordance with the patient's rules. One outstanding feature of this solution is that it monitors and keeps track of all the transactions in the network hence improving the management of health data. Unlike other proposed solutions earlier, Rajput, Li, Ahvanooey, and Masood [3] conducted experimental tests of the solution to evaluate its feasibility and efficiency. The results of the tests confirmed that EACMS enhances the security of a patient's PHR and introduces efficiency by reducing time delays in accessing necessary information by emergency care providers.

B. Supply Chain and Business Transactions

A study by Silva, Guerreiro, and Sousa [21] revealed that a lack of trust, control and traceability are common issues in many industries. Those issues occur due to the high number of business joint efforts between partners in different domains. To address the issues related to traceability and trust in business processes, Silva, Guerreiro, and Sousa [21] developed a blockchain solution using Hyperledger Composer. The researchers combined the concepts of DEMO, an enterprise ontology that maps human interactions and business transactions in an organization, and Hyperledger Composer and then applied the concept developed in a context of food supply and distribution. In particular, the scholars used a case study of a big banana retailer with a large supply chain in the United Kingdom. Using the Hyperledger Composer, the artifact was validated. The results of the test showed that two participants could submit orders that upon effective completion, and the status of the order was changed. The blockchain solution enabled the participants to monitor and track the order, increasing trust levels in the process.

On the other hand, literature by Sinclair, Shahriar, and Zhang [22] provides evidence that Hyperledger Composer has several potential applications in various supply chains, especially the drug supply chain. Recently, the Food and Drug Administration (FDA) introduced a new set of regulatory requirements, the Drug Supply Chain Security Act (DSCSA), to control illegal behavior in drug supply chains. Before DSCSA, many businesses encountered problems related to fraud prevention and payment authentication. After the enactment of the legislation, businesses must now run effective and seamless operations to avoid problems with the law. However, Sinclair, Shahriar, and Zhang [22] established that many enterprises face an uphill task in complying with the regulations. To address this challenge, Sinclair, Shahriar, and Zhang [22] developed a blockchain prototype to enable compliance with the requirements of DSCSA. The scholars used the Hyperledger Composer to implement the prototype by modeling different entities in the supply chain. Based on their experiences with the Composer, Sinclair, Shahriar, and Zhang [22] reported that the tool not only allows rapid development of blockchain prototypes, but also makes it easy to integrate them with a supply chain.

C. Cybersecurity and Fraud Prevention and Detection

According to Chua, Li, and He [23], blockchain technologies are most popular in the development of immune networks from intrusion and fraud. Chua, Li, and He [23] assert that although there are several technologies with the potential to improve operational efficiency, many businesses are reluctant to adopt them. Such technologies include the EPCglobal Network that is used to share data about a product between trading partners. Chua, Li, and He [23] further opine that despite the potential benefits of the EPCglobal Network, many players are put off by the huge financial and manpower investment required to implement and maintain its standards, notwithstanding security, storage, and computation issues. To address these challenges, Chua, Li, and He [23] proposed a blockchain solution that uses Hyperledger Fabric to act as a link between trading partners. The scholars assert that the solution complies with EPCglobal Network standards and allows the participants to enjoy benefits like elimination of the need to maintain electronic product code information services (EPCIS) and the provision of discovery services.

In a review of an article by Gabriela, Karim, and Lepoint on cyber insurance systems that are blockchain-based, the authors develop a system that uses a Hyperledger Composer blockchain framework to solve an existing problem. According to Lepoint et al. [24], conventional providers of insurance are gradually shifting to the growing sector of digital insurance. Given the developing state and condition of that sector, they are utilizing manual processes and models that they have created for other (physical) areas. The article argues that the distinctive nature of cyberspace, a profoundly connected and inter-dependent system of software and hardware that works at sub-second speeds, needs computerized techniques and a framework to be able to build up a feasible insurance environment. Such an insurance framework consists of numerous partners from various entities with no trustworthy third party, therefore a (locally) distributed and safe framework interface is needed. To address these problems, Lepoint et al., [24] proposed BlockCIS, a blockchain-based system for digital insurance. They set up BlockCIS by employing the Hyperledger Composer structure and demonstrated how such a platform can execute a safe, distributed setup for evaluating the digital threat for enterprises. Lepoint et al., [24] portrayed some innovative features such as incorporating selective disclosure of information into BlockCIS. They indicated that their future work consists of deploying the blockchain-based system in a working domain, attempting to evaluate how precisely the computed digital threat score demonstrates the probability of an assault or breach, and appropriately structuring the motivations of a BlockCIS launch [24].

After reviewing the available literature on Hyperledger Fabric, Composer, and other blockchain technologies, it is true to say that the application of such technologies to improve the security of transactions is the most researched field within this topic. The emphasis on and the high number of publications applying Hyperledger Fabric and Composer to enhance cybersecurity is attributed to the exponential growth of communication technologies and the emergence of the Internet of Things [25]. Currently, a majority of Internet of Things platforms have centralized architectures which make them vulnerable to single point-of-failure and cyber-attacks. In this view, Hang and Kim [25] propose a blockchain-based platform that emphasizes data integrity, ease of access, and real-time monitoring using Hyperledger Fabric.

VI. Conclusions

In this survey paper, we started our discussion with the basic concept of blockchain. Next, we introduced the Hyperledger greenhouse and its various frameworks and tools that aim to facilitate the development of enterprise blockchain. Then, we gave a comprehensive explanation on the taxonomy and system architectures of Hyperledger Fabric and Composer as an enterprise solution. Finally, we reviewed and discussed the applications and uses of Hyperledger Fabric and Composer in recent studies. We also evaluated the benefits and trade-offs of blockchain for enterprise. This survey is expected to serve as an effective guide to facilitate further understanding of the current blockchain technologies for enterprise, the application domains, and to explore potential research directions that could lead to exciting results in related fields. In summary, the use of blockchain in supply chain, healthcare, cybersecurity, and other industries is not a new idea and actually is one of the most favorable current research topics. However, blockchain for enterprise still has many issues that need further research and analysis to create more applicable and efficient applications that can fully benefit from the features of blockchain and achieve desired goals. In future works, a literature review and analysis on all researches about the newest version of Hyperledger Fabric without Composer will be composed, more enterprise blockchain platforms will be added into the comparison, and the performance of enterprise blockchain technologies and applications will be assessed in terms of throughput, scalability, and latency.

Acknowledgment

This work was supported by the USA National Science Foundation under Grant No. 1822137 and 1757828.

References

[1] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," IEEE Consumer Electronics Magazine, vol. 7, no. 2, pp. 18–21, 2018.

[2] S. Nakamoto *et al.*, "Bitcoin: a peer-to-peer electronic cash system," 2008.

[3] A. R. Rajput, Q. Li, M. T. Ahvanooey, and I. Masood, "EACMS: emergency access control management system for personal health record based on blockchain," IEEE Access, vol. 7, pp. 84 304–84 317, 2019.

[4] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, 2017.

[5] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in International Conference on Information and Communications Security, 2017, pp. 387–398.

[6] N. Zupan, K. Zhang, and H.-A. Jacobsen, "Hyperpubsub: a decentralized, permissioned, publish/subscribe service using blockchains," in Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos, 2017, pp. 15–16.

[7] "Global Blockchain Training & Certification." [Online]. Available: https://blockchaintrainingalliance.com/

[8] A. J. Yewale, "Study of Blockchain-as-a-Service Systems with a case study of Hyperledger Fabric implementation on Kubernetes," 2018.

[9] "The Hyperledger greenhouse." [Online]. Available: https://www.hyperledger.org/

[10] A. Rasti and A. Gheibi, "A coin marketplace implementation on blockchain using the Hyperledger platform," 2018.

[11] V. Dhillon, D. Metcalf, and M. Hooper, "The hyperledger project," pp. 139–149, 2017.

[12] T. Q. Ban, B. N. Anh, N. T. Son, and T. V. Dinh, "Survey of Hyperledger blockchain frameworks: case study in FPT university's cryptocurrency wallets," in Proceedings of the 2019 8th International Conference on Software and Computer Applications, 2019, pp. 472–

[13] C. C. Agbo and Q. H. Mahmoud, "Comparison of blockchain frameworks for healthcare applications," Internet Technology Letters.

[14] "Hyperledger Avalon: building the next wave of confidential applications." [Online]. Available: https://medium.com/iex-ec/hyperledger-avalon-building-the-next-wave-of-confidential-applications-54ba49dcd7e7

[15] F. Jamil, L. Hang, K. Kim, and D. Kim, "A novel medical bockchain model for drug supply chain integrity management in a smart hospital," Electronics, vol. 8, no. 5, p. 505, 2019.

[16] M. Bal and C. Ner, "NFTracer: a Non-Fungible token tracking proof-of-concept using Hyperledger Fabric," arXiv preprint arXiv:1905.04795, 2019.
[17] R. Wutthikarn and Y. G. Hui, "Prototype of blockchain in dental care service application based on Hyperledger Composer in Hyperledger Fabric framework," in 2018 22nd International Computer Science and Engineering Conference (ICSEC), 2018, pp. 1–4.
[18] "Hyperledger Composer." [Online]. Available: https://hyperledger.github.io/composer
[19] "Hyperledger Composer Playground." [Online]. Available: http://composer-playground.mybluemix.net/
[20] D.-J. Munoz, D.-A. Constantinescu, R. Asenjo, and L. Fuentes, "ClinicAppChain: a low-cost blockchain Hyperledger solution for healthcare," in International Congress on Blockchain and Applications, 2019, pp. 36–44.
[21] D. Silva, S. Guerreiro, and P. Sousa, "Decentralized enforcement of business process control using blockchain," in Enterprise Engineering Working Conference, 2018, pp. 69–87.
[22] D. Sinclair, H. Shahriar, and C. Zhang, "Security requirement prototyping with hyperledger composer for drug supply chain: a blockchain application," in Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, 2019, pp. 158–163.
[23] P. H. T. Chua, Y. Li, and W. He, "Adopting Hyperledger Fabric blockchain for EPCglobal network," in 2019 IEEE International Conference on RFID (RFID), 2019, pp. 1–8.
[24] T. Lepoint, G. Ciocarlie, and K. Eldefrawy, "BlockCIS—a blockchain-based cyber insurance system," in 2018 IEEE International Conference on Cloud Engineering (IC2E), 2018, pp. 378–384.
[25] L. Hang and D.-H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," Sensors, vol. 19, no. 10, p. 2228, 2019.