International Journal of Advanced Educational Research
www.multidisciplinaryjournals.org
ISSN: 2455-6157
Received: 01-06-2023, Accepted: 16-06-2023, Published: 01-07-2023
Volume 8, Issue 3, 2023, Page No. 1-7

Considerations for blockchain technology: Approaches, architecture and use cases

Kapil Bakshi[1], Kiran Bakshi[2]
[1] Department of Americas Division, Cisco Systems Inc, United State
[2] Department of Americas Division, Microsoft Corp., United State

Abstract
Blockchain is a new technology, and innovators are just starting to identify the wide-reaching applications and possibilities for businesses and governments. The industry is familiar with public blockchains, the underlying technology powering cryptocurrencies like Bitcoin. At its core, blockchain is a shared ledger of transactions that is decentralized, secure and immutable. With the introduction of decentralized applications and smart contracts, the possibilities for blockchain have expanded far beyond cryptocurrencies. This paper will discuss several aspects of block chain technology and components including, smart contracts, use of peer to peer networks, shared general ledger, security with immutability, proof of work based consensus and programmability. Also concepts of transactions, blocks, mining, and consensus, which lead to various possible blockchain projects. This paper also explorers open source, business blockchain framework, called Hyperledger Fabric. Additionally, the paper will discuss the current state of block technology, with industry use cases. Potential aerospace and aerospace supply chain, applications for enterprise blockchain will be discussed

Keywords: Blockchain technology, underlying technology, blockchain overview, transaction scripts

Introduction

History and Definition

Blockchain is essentially a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable, and updateable only via consensus or agreement among peers. [1] Blockchain can be defined as a platform whereby peers can exchange values via transactions in a distributed fashion without a central trusted arbitrator. Additionaly, Blockchain can be thought as a distributed shared ledger. Blockchain can be considered a shared ledger of transactions. This allows blockchain to conduct consensus mechanism ina decentralized fashion, without a central authority. A block is a set of transactions bundled together in order to organize them logically. The transaction are ordered and grouped into blocks. Hence the term Blockchain.

Blockchain was introduced with the advent of bitcoin in 2008 and implemented in 2009. Bitcoin is a digital currency which has been in limelight for past few years. It is important to review Bitcoin as its motivation is tied to Blockchain technology. Bitcoin has started a revolution with the introduction of the very first fully decentralized digital currency, which addresses the distributed, secure and stable aspect of Blockchain. This has also initiated interest in academic and industrial research areas. Since its introduction in 2008, bitcoin has gained much popularity and is currently the most successful digital currency in the world with billions of dollars invested in it. It is built on decades of research in the field of cryptography, digital cash, and distributed computing.

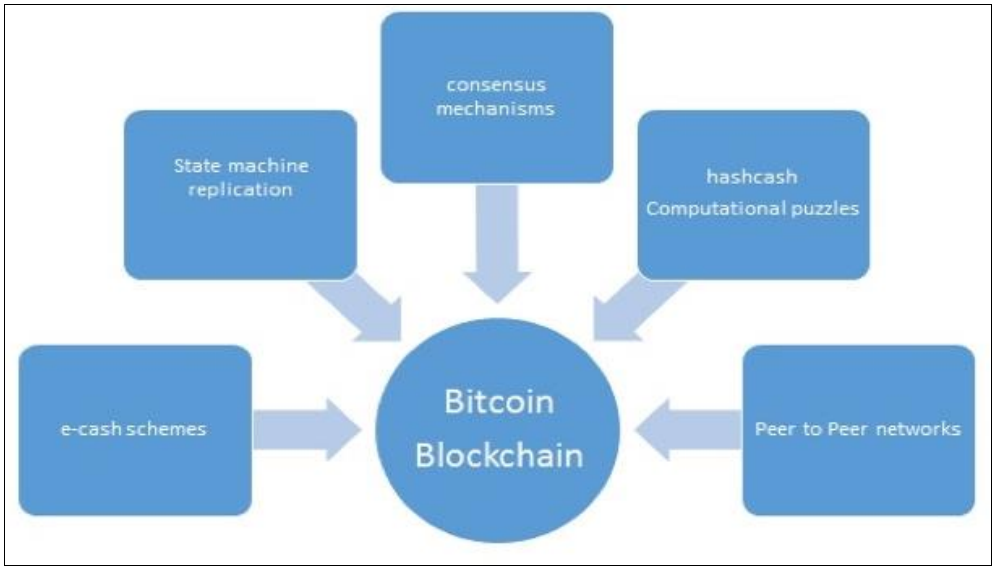

Fig 1: Topics of Bitcoin and Blockchain [1]

As part of bitcoin development, several technical aspects of blockchain were developed and considered. Including, e-cash schemes, state machine replication, consensus mechanism, has hcash computational and peer to peer network. All these topics will be discussed in this paper. Finally, Blockchain has many applications in various industries, some of these use cases will be discussed later in the paper.

Blockchain Overview

In order to understand Blockchain technologies, some basic background and foundational aspects need to be discussed. Including, distributed systems, CAP Theorem, Byzantine General Algorithm and Consensus mechanism.

Background Concepts

Distributed Systems understanding is essential to architecting Blockchain because it is a decentralized distributed system. In a distributed systems two or more nodes work with each other in a coordinated fashion to achieve a common outcome and it's modeled as a single logical platform. A node can be defined as an individual player in a distributed system. All nodes typically connected to each other via a network and can send and receive messages from each other.

One of the challenges in distributed system is coordination between nodes and fault tolerance. In a system, in case of a node or network outages, the distributed system should tolerate it and should continue to function as a system in order to achieve the desired outcome. This has been an area of research and several algorithms and mechanisms has been proposed to address this topic.

The Consistency, Availability, Partition (CAP) Theorem states that with consistency, availability, and partitioning tolerance, only two can be optimized at any time. Consistency is a property that ensures that all nodes in a distributed system have a single current copy of data. Availability means that the system is functional, accessible, is accepting incoming connections and responding as required. Partition tolerance ensures that if a group of nodes fails the distributed system still continues to operate correctly. Hence there are additional techniques used to address CAP Theorem. For example, fault tolerance is solved by using replication. This is a commonly used method to achieve fault tolerance. Consistency is achieved using consensus algorithms to ensure that all nodes have the same copy of data via state machine replication. Blockchain addresses aspects of state machine replication.

In terms of nodes attributes, it can be faulty, or malicious and have their own memory and processor. A Byzantine node exhibits, intentional malicious, which is could be damaging to the operation of the network. The Byzantine Generals Problem describes the scenario, where more than two generals need to agree on a time to attack their common enemy. The added complication here is that one or more of the generals can be a traitor, meaning that they can lie about their choice. [2] Hence, the Byzantine Generals Problem is a term from the computer science description of a situation where involved parties must agree on a single strategy in order to avoid complete failure, but where some of the involved parties are corrupt and disseminating false information or are otherwise unreliable. Blockchains are decentralized ledgers which, are not controlled by a central authority. Hence the value stored in these ledgers, bad actors have huge economic incentives to try and cause faults. Byzantine Fault Tolerance solution, and thus a solution to the

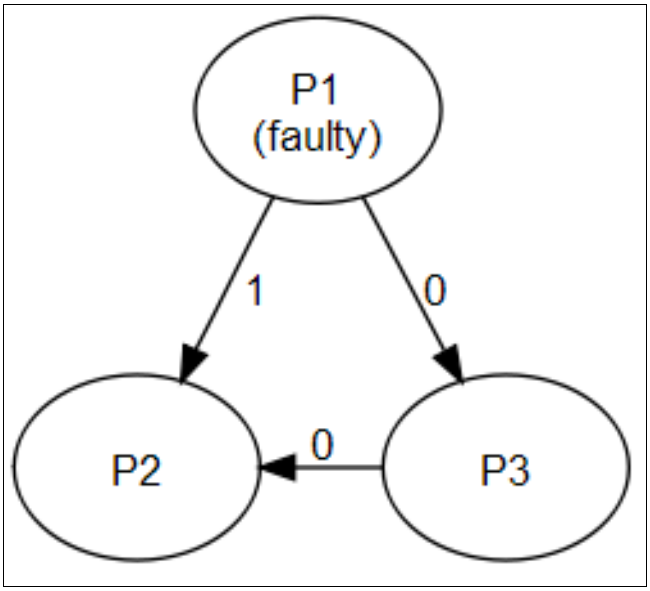

Fig 2: Byzantime Problem Explained [2]

Byzantine Generals' Problem for blockchains is considered and implemented. In the absence of BFT, a peer is able to transmit and post false transactions effectively nullifying the blockchain's reliability. To make things worse, there is no central authority to take over and repair the damage. When Bitcoin was invented, a probabilistic solution to the Byzantine Generals Problem as described in depth by Satoshi Nakamoto [2].

Hence a consensus mechanism is required in a distributed system like Blockchain, where steps that are taken by nodes in order to agree on a state or value. Consensus mechanisms have recently come into the research again and gained much popularity with the advent of Blockchain. There are various considerations which provide the desired results in a consensus mechanism. Review some of these considerations are below: Termination: All functional nodes terminate execution of the consensus process and eventually reach a decision. Agreement: All functional nodes decide on the same value. Validity: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node. Fault tolerant: The consensus algorithm should be able to run in the presence of malicious nodes (Byzantine nodes). Integrity is where by no node makes the decision more than once. The nodes make decisions only once in a single consensus cycle.

There are several types of consensus mechanism. To reviews two of them briefly. First Byzantine fault tolerance-based consensus, with no compute intensive operations such as partial hash inversion, this method relies on a simple scheme of nodes that are publishing signed messages. Eventually, when a certain number of messages are received, then an agreement is reached. Second, leader-based consensus mechanisms, where nodes to compete for the leader-election and the node that wins is the final leader. There are several practical implementations of consensus mechanism. For example, Paxos, where nodes are assigned various roles such as Proposer, Acceptor, and Learner. Nodes or processes are named replicas and consensus is

achieved in the presence of faulty nodes by agreement among a majority of nodes. As new consensus models are constructed, we should keep these in mind and understand how they can apply to distributed ledger technologies.

Architecture Components (Elements) Overview

Blockchain can be conceptually constructed by layers of a distributed peer-to-peer network on the Internet, as can be seen below in the figure. It is analogous to OSI (Open System Interconnection). This is shown in the following diagram:

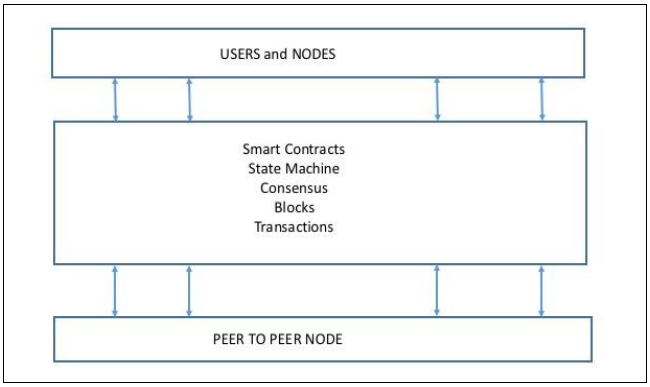

Fig 3: Network view of Blockchain

Blockchain, in layman terms, can be seen as a platform whereby peers can exchange values using transactions without the need for a central trusted arbitrator. This allows Blockchain to be a decentralized consensus mechanism where no single authority of the database. A block is a collection of transactions bundled together and organized logically. The transactions and size are variable depending on the type and design of the Blockchain in use. A reference to a previous block is also included in the block unless it's a genesis block. A genesis block is first block in the Blockchain that was hardcoded at the time the Blockchain was started. The structure of a block is also dependent on the type and design of a Blockchain, but generally there are a few attributes that are essential to the functionality of a block, such as the block header, pointers to previous blocks, the time stamp, nonce, transaction counter, transactions, and other attributes. A general depiction of a block is shown in a block diagram as in Figure 4.

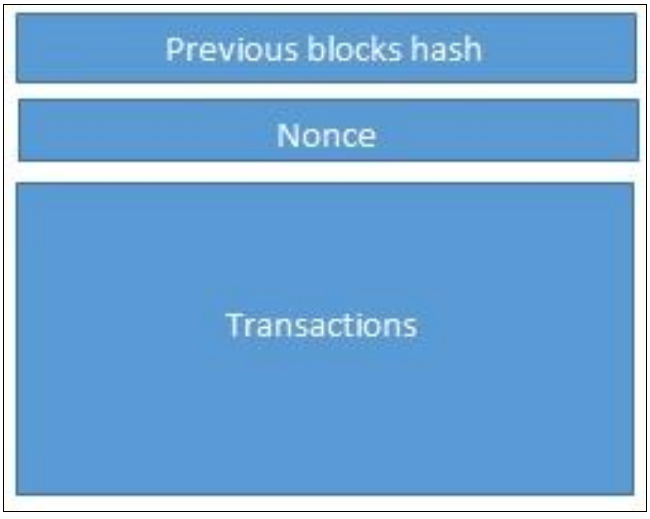

Fig 4: The structure of a block.

The structure of a generic Blockchain is depicted with the of the following figure 5:

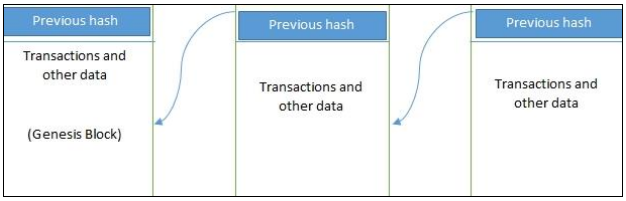

Fig 5: Generic structure of a Blockchain

Salient Elements of a Blockchain

In this section, the key elements of Blockchain architecture are discussed.

Block

A block bundling of multiple transactions and other objects like previous block hash (hash pointer), timestamp, and nonce.

Transaction

A transaction is the fundamental unit of a blockchain. A transaction represents a transfer of value from one address to another.

Peer-to-peer network

This is a network topology where all peers can communicate with each other and send and receive messages.

Address

Senders and recipients are denoted by a notion of addresses, they are unique identifiers that are used in a transaction on the Blockchain. An address is a public key or derived from a public key. Addresses themselves are unique identifier, but can can be reused by the same user. A user may not use the same address again and generate a new one for each transaction. This newly generated address will be unique. In a Blockchain implementation like Bitcoin, users are usually not directly identifiable but some research in de-anonymizing bitcoin users have shown that users can be identified successfully. In practice, users generate a new address for each transaction in order to avoid linking transactions to the common owner, thus avoiding identification.

Transaction scripts

Transaction scripts are predefined sets of commands for nodes to transfer tokens from one address to another and perform various other functions. Also, any computer can take any program and run it just verbatim, then that system (Turing Complete) and the software program also fall under this topic.

Nodes

A node is an end point on a Blockchain network which performs various tasks based on the role it takes. This is done by following a consensus protocol. Nodes can also perform tasks such as payment verification, validators, and many others functions depending on the type of the Blockchain used and the role assigned to the node. A node can propose and validate transactions and perform mining to facilitate consensus and secure the Blockchain.

Virtual machine
A virtual machine allows Turing complete programs to be run on a Blockchain, whereas a transaction script can be limited in its operation. Virtual machines are not available on all Blockchains; however, various Blockchains use virtual machines to run programs, for example Ethereum Virtual Machine (EVM) and Chain Virtual Machine (CVM).

State machine
A Blockchain is also a state transition mechanism where a state is modified from its one form to the another and to a state as a result of a transaction by the nodes.

Smart contracts
Smart contract run on top of the Blockchain and form the business logic when certain conditions are met. The smart contract feature is not available in all Blockchains but is now becoming a very desirable feature due to the flexibility and power it provides to the Blockchain applications.

Blockchain Architecture
Blockchain Platform architecture is depicted in the Figure 6. The platform supports key capabilities for blockchain solutions in a blockchain network. Blockchain provides a platform to run smart contracts. These are automated autonomous programs and run business logic. This is indeed a key feature of Blockchain as it allows flexibility, programmability, and much desirable control of actions that users of Blockchain need to perform according to their specific requirements.

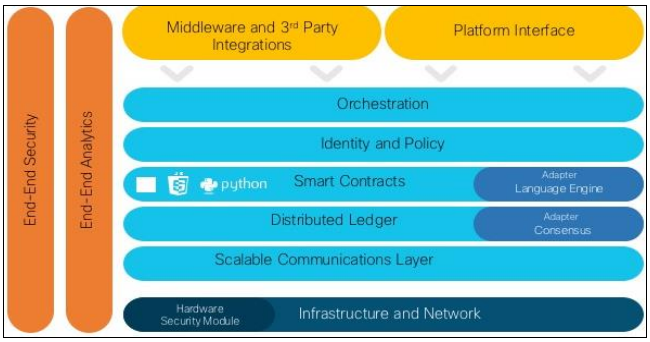

Fig 6: Blockchain Platform Architecture [7]

Capabilities of a Blockchain
Let review Blockchain architectural functions below. [4]

Distributed Transactions
Distributed consensus is the major feature of a Blockchain. As a result Blockchain can present a single version of truth that is agreed upon by all parties without the requirement of a central authority. Any transactions posted from nodes on the Blockchain are verified based on a predetermined set of rules and only valid transactions are selected for inclusion in a block. This also enables Blockchain to transfer value between its users via tokens (structure to carry values).

Secure Transactions
The key challenge for secure transaction adoption by financial other industries is need for privacy and confidentiality of transactions. Blockchain addresses this aspect of security. Blockchain is based on cryptographic technology that ensures the integrity and availability of data. Confidentiality is not fully addressed due to the requirements of transparency. Confidentiality is not really requierment and transparency is preferred in the Blockchina implementation use cases. For example, in bitcoin confidentiality is not really required; however, it is desirable in some scenarios. Research in this area is in progress. Other security services such as nonrepudiation and authentication are also provided by Blockchain as all actions are secured by using private keys and digital signatures.

Immutability
This is key capability of Blockchain: records once added onto the blockchain are unchanged over time. There is the possibility of rolling back the changes but this is considered almost impossible to do as it will require an unaffordable amount of computing resources. For example, in much desirable case of bitcoin if a malicious user wants to alter the previous blocks then it would require computing for all those blocks that have already been added to the blockchain. This feature makes the records on a blockchain practically immutable.

Membership Services
Membership services manage identity, privacy, confidentiality, and auditability on the network. Membership only applies to permissioned Blockchains. Permissioned Blockchains allow specific users to submit transactions. In a permissioned Blockchain, the actors may be given different roles granting them permission to perform a specific set of operations. In a non-permissioned Blockchain, participation does not require authorization and all users can submit transactions.

Event Distribution
Notifications of changes or operations that occur in the Blockchain network are termed as events. An event resulting from execution of a smart contract or the creation of a new block could create a notification. Events will have event producers and event consumers. Producers publish events of interest to the Blockchain network, and consumers of events subscribe to events of interest and process the events as they receive them. Events are of interest to participants taking part in the Blockchain network. Event distribution capability connects listeners to receive the events from the Blockchain. In an atomic broadcast, the sender of messages in a Blockchain network sends messages to all connected peer members in the same order of sequence.

Communication Protocol
Protocol include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. The participating Blockchain computer network members use peer-to-peer protocols, such as gRPC, to communicate with each other in Blockchain networks.

Cryptographic Capability
The Cryptographic Capability provides the Blockchain with access to the necessary cryptographic algorithms, either directly or by providing an interface to hardware or software that implements the algorithms. Hash functions and digital signatures are examples of algorithms that are commonly used in Blockchains. Hash functions protect from ledger

modifications. Changes data in blocks hash in the ledger will result in a computed hash that is different from the hash that was previously computed and stored for the ledger. A new hash is computed each time a transaction is added to the ledger. Digital signatures ensure that the receiver receives the transactions without intermediate parties modifying or forging the contents of transactions, while also ensuring that the transactions originated from senders and not imposters.

Smart Contract

Smart contracts, also called as chaincode, software programs that execute in a secure environment within the Blockchain platform on a node in the network. As mentioned before, Smart contracts have the business logic involving contract terms and conditions between agreeing participants. The smart contract program determines the transactions and block data to be recorded in Blockchain Platform. Smart contracts are written in a programming language of the Blockchain platform. The smart contract program is stored in the ledger. Transactions can invoke smart contract functions, which can be stateless or stateful, to perform business logic. Smart contracts help to make decisions and automate relationships.

Data storage

There are several data storage considerations for Blockchain platform. Ledger storage is the physical storage where the transaction data in the Blockchain ledger is stored. Only a small amount of the data associated with a particular transaction is stored directly in the Blockchain ledger itself. Auxiliary data associated with the transaction, which is much larger, is stored independently from the entry in the Blockchain ledger, only referenced by the entry. This approach helps manage Blockchain ledger with large volumes of data. Data storage capability of Blockchain platform can support data other than the Blockchain ledger itself. For example, a database storage, either an SQL database or a NoSQL database. It can also take the form of an object storage service or a block storage service. The choice of which form of data storage is used depends primarily on the nature of the data objects themselves and the operations that need to be performed on them. Additionally, replication and backup of the data objects needs to be considered. For some data storage services, replication and backup are built into the service itself. In other cases, it is necessary to create replicas or backups through custom mechanisms.

Smart property

Blockchain has enable the capability to link a digital or physical asset to the Blockchain in an irrevocable manner. The asset cannot be claimed by anyone else and in users control. This capability has far-reaching implications especially in Digital Rights Management (DRM) and electronic cash systems where double spend detection is a key requirement. The double spend problem was is addressed in bitcoin implementation.

Runtime Environment

During execution, a Blockchain transaction may invoke smart contract functions requiring a secure runtime. A secure runtime environment is a hosting environment for server side business logic. An example is the use of a secure container that contains a set of signed runtime components such as a secure operating system, libraries for Blockchain supported programming languages, their respective runtimes, and secure capabilities.

Access and Control

There two kinds of access and controls in place for a Blockchain network, based on permissions. Permissionless networks are open to any participant and transactions are verified with policy and rules of the network. Any participant can view transactions on the ledger, even if participants are anonymous. Bitcoin is the most familiar example of a permissionless network. Permissioned networks are limited to participants within a given business network. On permissioned blockchains, participants are allowed to view only the transactions relevant to them and are only allowed to perform operations for which they have permission.

Foundational Services

The Blockchain Platform offers foundation services to integrated and function the transactions together. The procedures and policies that govern the operation of the blockchain network are known as governance. The Blockchain network participants agree upon these policies. Security refers to the security policy and standards that are in place to secure the Blockchain platform. [5] Security and privacy in Blockchain deployments must address both information technology (IT) security as well as operations technology (OT) security elements. Blockchain protocols architecture relies on public-key cryptography. Monitoring and Intelligence services include monitoring, analytics, and automation tools that are used to respond to changes in the platform and environment. The network management service provides visibility of the network operations including business process metrics and performance and capacity data. It also provides a management interface used to change configurations and other parameters.

Hyperledger Frameworks

Hyperledger is emerging as the standard for enterprise Blockchain platforms. Through open source and open governance, it features innovative new capabilities hardened for use by businesses. Hyperledger Fabric is an open source enterprise-grade distributed ledger technology (DLT) platform, designed for use in enterprise, that delivers some key capabilities over other distributed ledger or Blockchain platforms.

Hyperledger began in 2015 when many different companies interested in Blockchain pooled their resources and create open-source Blockchain technology that anyone could use. Hyperledger was established under the Linux Foundation, which has started many open source projects that grow strong sustaining communities and thriving ecosystems. Hyperledger is governed by a diverse technical steering committee, and the Hyperledger projects by a diverse set of maintainers from multiple organizations. It has a development community that has grown to over 35 organizations and nearly 200 developers since its earliest commits. [3] Hence it enables, highly modular and configurable architecture, enabling innovation for a range of use cases.

Hyperledger is a distributed ledger platform to support smart contracts authored in general-purpose programming

languages such as Java, Go and Node.js. Hence, enterprises already have the skill set needed to develop smart contracts, and no additional training to learn a new language is needed. The Fabric platform is also permissioned, unlike with a public permissionless network, the participants are known to each other, rather than anonymous and therefore fully untrusted. A key capability of Hyperledge Fabric platform's is its support for pluggable consensus protocols that enable the platform to be more effectively customized to fit particular use cases and trust models. Fabric can leverage consensus protocols that do not require a native cryptocurrency. Avoidance of a cryptocurrency reduces some significant risk/attack vectors, and removal of cryptographic mining operations implies that deployment with roughly the same operational cost as any other distributed system.

There are several projects under Hyperledger. Some of the them are listed below. [3] Hyperledger Fabric, is the foundation for developing applications with a modular architecture, Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play. Hyperledger Sawtooth is a modular platform for building, deploying, and running distributed ledgers. Hyperledger Sawtooth includes a key consensus algorithm called Proof of Elapsed Time (PoET), which targets large distributed validator populations with minimal resource consumption. Hyperledger Iroha is an easy to use, modular distributed Blockchain platform with its own unique consensus and ordering service algorithms, rich role-based permission model and multi-signature support. Hyperledger Burrow is a permissionable smart contract machine. Burrow provides a modular blockchain client with a permissioned smart contract interpreter built in part to the specification of the Ethereum Virtual Machine (EVM). Hyperledger Indy is a distributed ledger, for decentralized identity. It provides tools, libraries, and reusable components for creating and using independent digital identities rooted on Blockchains or other distributed ledgers for interoperability.

Sample Use Cases

Aerospace and Supply Chain

Most of leading manufacturing, include aerospace manufacturing industry have enterprise resource planning (ERP) and supply chain management software. Yet despite this huge investment in supply chain infrastructure, most companies have only limited visibility and insight into where all their products are at any given moment. Asset tracking addresses several issues not generally seen in ledgers. For example, asset tracking requires handling diverse data types, including composite format required for telemetry and environmental sensing. Blockchain Platform accommodates both domain-specific data and the transaction families that operate on it, including data constraints such as verifying the calibration of a sensor. Hence, Blockchain provides benefits for cross-industry traceability. It can help establish a community of participants and an authoritative record of provenance. The Blockchain's decentralized fault-tolerance enables updates from a wide range of nodes.

Healthcare

Blockchain is posed for innovation in preventative care and community-based healthcare models. The capability of distributed ledger technology for ensuring data integrity while sharing between parties can ensure success, which is vital to the improvement of health. Blockchain can integrate team-based healthcare, and payment with the care provided along with it. The inherent properties of cryptographic public and private key access, proof of work and distributed data, creates a capability of integrity for healthcare information. Blockchain technology also makes it simple to track a drugs and medicine as it moves from the manufacturer to the patient. This improves the traceability of a drug as it moves across the supply chain, and addresses drug counterfeiting. Blockchain provides ease of collaboration, by smart contracts and authorization to access all electronic health data. Its transaction layer can enables access to a diverse set of standardized, anonymous and non-patient identifiable information. Transparency and automation can lowers administration costs. It is a phased approach rather than an instant overhaul of systems, and hence is suited to healthcare sector.

Financials

There are several use cases in financial industry, include know your customer (KYC), Payments and Trade Finance. [6] Know your customer (KYC) requests can cause delays of days and weeks to banking transactions. The KYC blockchain enables structured information to be recorded, assessed and shared across this network using cryptography. With the customer's consent, banks will be able to collect, validate and share data efficiently and accurately. The existing international payment system routed through banks and central banks. Blockchain can speed up money transfers, also help banks to operate continuously. Decentralizing the payments queue and consolidating the payments used to expose details to third parties in the settlement process. Blockchain can address this challenge. The trade finance business includes multiple trading partners and manual records handling. This creates delays, duplication and fraud and high levels of inefficiency. Blockchain digitizes sales and other legal contracts, allow the location of goods to be monitored and facilitate settlement in close to real time. This provides a mechanism to link all constituents like banks, importers, exporters, government agencies, shipping companies, transport operators and insurers.

Summary

The paper takes a survey of Blockchain technology, architecture and use cases. Blockchain, is rapidly gaining broad acceptance. Industries and research institutions are investigating in ways to use Blockchain to increase trust across their business value chains and address challenges around complexity, transparency, and security. The innovation of Blockchain is its ability to automate trust among the parties using it. Transactions are settled in a collective fashion and recorded on a distributed ledger, which removes the need for an established third party to create a trusted relationship. Participants can directly use the Blockchain as the source of truth. This trust allows consumers, enterprises, and governments to automate how they manage any transactional relationship. However, to unleash its full potential, it needs to be based on an established set of standards that meets the complex needs of the enterprise. In addition, today's organizations are seeking industry specific solutions to transform their business processes and need the ability to build Blockchain networks that are interoperable.

References

1. Bashir M. Mastering Blockchain. USA: Packt Publishing Inc, 2017.
2. O'Dowd A, Ramakrishna V, Novotnv P, Gaur N, Desrosiers L, Baset S. Hands-on Blockchain with Hyperledge. USA: Packet Publishing Inc, 2018.
3. Hyperledge: Linux Foundation. (August 2018). An Introduction to Hyperledger. https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf
4. Arold T, Gaur N, Manicka S, Perepa B. Cloud customer Architecture for Blockchain, 2017. Object Management Group. https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-Blockchain.pdf
5. Prusty N. Blockchain for enterprise. USA: Packt Publishing Inc, 2018.
6. Dill B, Smits D. Zero to Blockchain. IBM: Redbooks, 2017.
7. Jagadeesan R. PSODGT-1001, 2018.
8. Enterprise Blockchain. Cisco Blockchain Platform. Cisco Live: Orlando, 2018.