The IBM Advantage for Implementing the CSCC
Cloud Customer Reference Architecture for
Blockchain

Table of Contents

Executive overview .................................................................................................................. 2
Introduction .............................................................................................................................. 3
Industry expertise .................................................................................................................... 4
Blockchain method .................................................................................................................. 5
Hyperledger ............................................................................................................................... 6
IBM Blockchain offerings ...................................................................................................... 7
IBM Blockchain Platform ....................................................................................................... 7
Services .................................................................................................................................. 8
Summary ................................................................................................................................. 8
Blockchain reference architecture ......................................................................................... 9
Public network ........................................................................................................................ 11
  Edge services ......................................................................................................................... 11
  Users ................................................................................................................................... 11
Cloud network ........................................................................................................................ 12
  Blockchain applications ........................................................................................................ 12
  Blockchain platform ............................................................................................................ 13
  Systems integration ............................................................................................................... 17
  IBM Blockchain Platform ................................................................................................... 17
  Transformation and connectivity ......................................................................................... 23
Enterprise network ................................................................................................................ 23
  Enterprise user directory ..................................................................................................... 23
  Enterprise applications ......................................................................................................... 24
  Enterprise data .................................................................................................................... 25
Blockchain foundational services ......................................................................................... 26
  Governance ........................................................................................................................ 26
  Security ................................................................................................................................ 27
    Secure system design, development, and management ...................................................... 27
    Securing and isolating the software and data .................................................................. 28
    Support from z System cryptography ............................................................................. 31
Blockchain network management ......................................................................................... 31
Context and options ............................................................................................................. 32
Permissions options .............................................................................................................. 32
Blockchain storage options ................................................................................................. 33
  Ledger storage ...................................................................................................................... 33
  Data storage ......................................................................................................................... 34
Executive overview

A January-March 2017 IBM survey of 3,000 C-suite executives revealed that on average, 33 percent of organizations across all industries and regions are already considering or are actively engaged with blockchain. This number includes organizations that are already experimenting with or piloting blockchain implementations (33 percent in the banking and financial market industries). Successful blockchain adoption offers a number of benefits, including removing friction, allowing better flow of capital, or simply providing a trust level that couldn’t be achieved outside of a blockchain business network.

Because blockchain is an emerging and foundational technology with the potential to impact so many industries and business processes, its adoption comes with challenges. These challenges are related to the business model and governance of the blockchain business network, the technology and access to skilled developers, and the legal implication for smart contracts.

IBM® is uniquely positioned to be a partner with blockchain adopters.

- The IBM Blockchain Founder Accelerator program brings together like-minded innovators who can share best practices and get access to technology and skills.
• The IBM Cloud Garage's blockchain services provide a way to identify an optimal use case, quickly deliver a blockchain-first project, and scale to production.
• IBM is a founding member of and contributor to the Linux Foundation's Hyperledger project.
• The IBM Blockchain Platform offers blockchain as a service in IBM Cloud with the platform and tools required to develop, govern, and operate business networks.
• IBM Blockchain offers the convenience and speed of the cloud, including the proximity of other cloud services required by a blockchain-based solution, and the resiliency, security, and scalability of the IBM LinuxONE platform.

Introduction
This paper describes the advantages and benefits of working with IBM when implementing the open standard CSCC Cloud Customer Architecture for Blockchain. We provide a high-level overview of IBM Blockchain offerings and differentiators. We discuss the different aspects of the reference architecture and relate the IBM capabilities for specific aspects of the architecture. Our goal is to describe to business and technical executives, influencers, and practitioners how IBM is uniquely positioned to be your partner of choice for blockchain initiatives. The paper is organized as follows:

• Introduction
• Industry expertise: Explains how industry expertise is required to apply blockchain to a specific use case.
• Blockchain method: Lists proven practices and processes for blockchain success.
• Hyperledger: Introduces this open source collaborative initiative.
• IBM Blockchain offerings: Gives a high-level overview of IBM offerings.
• Blockchain reference architecture: Recaps the CSCC paper with details of IBM advantages for each of the components of the architecture.
• IBM Blockchain Platform: Describes the IBM Blockchain as a Service full-stack offering.
• Blockchain foundational services: Provides a detailed look at IBM differentiators for governance, security, and network management.
• Context and options: Describes additional concepts and components that are common in blockchain environments.
• Runtime flow: Describes a supply chain scenario that uses the Hyperledger Fabric blockchain implementation.
• Cloud deployment considerations: Lists things to consider in deploying a blockchain solution.
• Summary
• Appendix A: Blockchain fundamentals
• Appendix B: IBM Cloud offerings mapped to reference architecture
Blockchain technology has the potential to radically alter the way enterprises conduct business and the way institutions process transactions. Blockchain technology, at its core, features an immutable distributed ledger—a decentralized network that is cryptographically secured. Participants can share a ledger through peer-to-peer replication, which is updated every time they agree to commit a block of transactions.

The technology can reduce operational costs and friction, create transaction records that are immutable, and enable transparent ledgers where updates are nearly instantaneous. It can also dramatically change the way workflow and business procedures are designed inside an enterprise and can open up new opportunities for innovation and growth.

Blockchain technology can be viewed from business, legal, and technical perspectives:

- From a business perspective, blockchain is an exchange network that facilitates transfer of value, assets, or other entities between willing and mutually agreeing participants, ensuring privacy and control of data to stakeholders.
- From a legal perspective, blockchain ledger transactions are validated, indisputable transactions that do not require intermediaries or trusted third-party legal entities.
- From a technical perspective, blockchain is a replicated, distributed ledger of transactions with ledger entries referencing other data stores (for additional information related to ledger transactions). Cryptography is used to ensure that network participants see only the parts of the ledger that are relevant to them, and that transactions are secure, authenticated, and verifiable, in the context of permissioned business blockchains.

Industry expertise
A 2017 Harvard Business Review publication titled “The Truth About Blockchain” states that blockchain is not so much a disruptive technology as it is a foundational technology. We believe blockchain can have as much impact on trusted transactions as TCP/IP had on information. Because blockchain is a foundational technology that can be applied to many business problems, in its early days some saw it as a technology looking for a business problem to solve. This technology-first approach doesn’t work. Instead, we discuss blockchain in the context of a use case, its business network, a specific business asset or assets, and their associated business transactions.
Industries each have their own set of opportunities, challenges, and constraints for use cases. For example, in the US, insurance is regulated by states. Having both the industry expertise and the expertise of how blockchain technology can be applied in the industry is a critical success factor for effective blockchain projects. This knowledge is critical at the beginning of a project when multiple use cases are proposed and one must be selected. It is also important throughout the lifecycle of the blockchain initiative when governance, business, legal, and technology models must be developed.

We are witnessing the rise of industry blockchain consortia like R3 (banking) or B3i (re-insurance). These consortia of companies are competitors in their industry but are evaluating the impact of blockchain and are defining the business models and standards required for industry-wide blockchain adoption. In parallel, organizations are experimenting with blockchain outside of the industry consortia. These organizations leverage existing client or partner relationships to found blockchain business networks, to quickly pilot blockchain, to get value, and to scale. These blockchain business networks sometimes span industries—such as banking and retail, telco and banking, or supply chain and insurance.

IBM is uniquely positioned because of its large blockchain client base (400+ clients) and its experience with successfully delivering blockchain projects. IBM has blockchain consulting practices for different industries with business consultants who are experts in the industry. IBMers have deep technology expertise—architects and developers from our IBM Cloud Garage for blockchain implementations and IBM developers who contribute to Hyperledger every day. IBM contributes to the standardization of blockchain with other companies through groups like ISO. The IBM Cloud Garage Blockchain Workshop provides the framework for IBM clients to get access to this expertise and to quickly realize value.

**Blockchain method**

We stated that blockchain technology is both emerging and foundational. But these two aspects combined can stall your blockchain initiatives. Your challenges include: Where do I find blockchain developers? What is a good use case for my company? Should I join a consortium or wait?

We learned three principles from blockchain early adopters:

1. **Build instead of reading**: A blockchain research "paper exercise" is limited. To understand what it means for your organization, you need to experiment with blockchain in context by applying it to a meaningful use case. Industry expertise is a must. The cloud (such as IBM Cloud) can enable fast builds and experiments.
2. **Think big, start small**: To generate enough support in the organization, a blockchain use case must add significant business value by enabling a new source of revenue, removing frictions and reducing cost, or supporting improved flows of capital. This requirement typically means that the selected blockchain use case is ambitious—for example, international payments without intermediaries or insurance policy issuance. Having an ambitious goal gets people’s attention and helps secure funding. You need to scope a minimal viable business network quickly (the blockchain equivalent of a minimal viable product, MVP) that can be implemented in a short amount of time (typically two to three months).

3. **Scale and secure**: Impediments to productive use and growth beyond early experiments fall into three categories: technical, legal, and business. For example: What are the governance rules for operating the blockchain business network? What are the legal challenges and uncertainties? Can the blockchain platform support hundreds of transactions per second? Can I trust blockchain with personal and sensitive data? IBM launched the IBM Blockchain Founder Accelerator in June 2017 to help blockchain network founders bring their network to production by connecting them with other like-minded innovators and providing the assistance needed for technical, legal, and business challenges.

IBM Blockchain services are based on agile and IBM Design Thinking principles, and include specific blockchain practices that support rapid innovation. IBM provides both the physical locations and the method to go from inception, to use case selection, to minimal viable business network selection, to delivering the first project, to scaling the business network into production. Refer to the IBM Cloud Garage Method Architecture Center - Blockchain for details.

**Hyperledger**

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration hosted by the Linux Foundation® and includes leaders in finance, banking, Internet of Things (IoT), supply chain, manufacturing, and technology. With more than 140 members at the time of writing, Hyperledger is the fastest growing Linux Foundation initiative. IBM is a founding member and a contributor. Hyperledger code is governed by the Apache 2 license. Projects developed under Hyperledger (four frameworks and four tools to date) include Fabric, which provides foundational capabilities for a permissioned business network (identity, shared ledger, consensus, smart contracts). Privacy, scalability, and modularity were critical themes for the Hyperledger Fabric v1 release, making it an optimal platform for enterprise-grade business networks.
IBM Blockchain offerings
We mentioned the IBM Cloud Garage’s blockchain engagement services, the IBM Blockchain Founder Accelerator program and the IBM Cloud Garage Method Architecture Center - Blockchain. IBM also offers worldwide support for blockchain at both entry and elite levels. IBM Blockchain offerings bring together some of the world’s most advanced expertise, technology, and ecosystem to transform industries.

IBM Blockchain Platform
Built on Hyperledger Fabric v1 and Hyperledger Composer, IBM Blockchain Platform is the only fully integrated enterprise-ready blockchain platform designed to accelerate the development, governance, and operation of a multi-institution business network. It is built to meet the needs of the group, not just the individual member. The platform is a flexible software-as-a-service offering delivered through the IBM Cloud. It provides network members the ability to collaborate on developing, governing, and operating a network with the performance and security for even the most demanding use cases found across regulated industries. In record time, you and your ecosystem can:

- **Develop**: Explore and accelerate development time with tools that can ensure close alignment between business leaders and developers. **Hyperledger Composer Playground** is a collaboration tool for building blockchain business networks, accelerating the development of smart contracts and their deployment across a distributed ledger. You can try Composer online using the Composer Playground, hosted on IBM Cloud. You can develop and test with a complete development environment on your laptop, including Hyperledger Composer and Hyperledger Fabric. You can collaborate and share your running blockchain network in the cloud.

- **Govern**: Accelerate activation, customization, and management of your business network with democratic, multi-party governance tooling. Use the Policy Editor to collectively manage rules and policies for your network and prevent any one member from having exclusive control. Grow elastically as network members, channels, and transactions evolve.

- **Operate**: Deploy and operate always-on networks with production-ready enterprise performance and security for most demanding and regulated use cases in your industry. Start small and scale elastically. Perform seamless code upgrades without pausing the network. Experience a hardened security stack with 100% encryption available and no privileged access to blockchain data.

The cost of a blockchain network is shared across its members. IBM Blockchain Platform has multiple flexible membership plans based on each ecosystem’s unique needs for compute performance and isolation.
With IBM Blockchain Platform you get “Blockchain as a Service” available on IBM Cloud and provisioned in a secure and scalable IBM LinuxONE™ environment. You also get associated tools for developers to manage the business network. A starter developer network option is available.

If you prefer to host and manage your own Hyperledger Fabric implementation, IBM offers Docker images and scripts. These are Docker Compose scripts and images available at no charge from Docker Hub. IBM tested and signed these images. IBM offers support for a charge.

**Services**

IBM has worked with more than 400 clients globally and across industries. A great way to get started is with the IBM Cloud Garage Blockchain Workshop, which combines best practices from industry use cases, design thinking, and agile development to define the scope of your minimum viable business network. IBM can co-develop the minimum viable business network with you.

After you have experimented with blockchain, the next step is to expand your business network into production. The IBM Blockchain Founder Accelerator program is designed to take blockchain network founders from proof of concept or production pilot to production.

IBM has a large blockchain practice under IBM Global Business Services. IBM offers IBM Blockchain solutions, which are code accelerators for the typical capabilities required by blockchain solutions (in addition to blockchain itself). Solutions accelerators include a process engine, a member management, a secure document store, and a provenance engine. As of this writing, solutions are available through a services engagement.

**Summary**

IBM Blockchain offerings can be summarized as follows:

1. IBM Blockchain services and IBM Blockchain solutions provided by IBM Global Business Services
2. IBM Blockchain Workshop
3. IBM Blockchain Founder Accelerator
4. IBM Blockchain Platform (Developer, Entry, Enterprise, and Enterprise+ plans)
5. IBM Hyperledger Composer Playground (part of IBM Blockchain Platform)
6. IBM Hyperledger Docker Compose images and scripts (part of IBM Blockchain Platform) and IBM Premium Support for Hyperledger (support for the images)
Blockchain reference architecture

A blockchain is a *shared ledger* distributed across a business network in which all confirmed and validated transactions are permanently recorded in append-only *blocks*. All the consensually confirmed and validated transaction blocks are linked in a tamper-resistant *chain* starting from the genesis block to the most current block. Each block is linked to its previous block using the cryptographic hash of the previous block. The name *blockchain* derives from the fact that these transaction blocks are chained together.

A blockchain is a historical record of all the transactions that have taken place in the network since the beginning of the blockchain. The blockchain serves as a single source of truth for the network.

A blockchain network consists of a number of member *nodes* where each member typically belongs to a different organization. Each node maintains a local copy of the ledger, which is kept in sync with the copies maintained by other nodes through communicating and consenting on the contents of the ledger.

Figure 1 explores the typical capabilities needed for a node or an enterprise participating in the blockchain architecture. The reference architecture is expressed across three networks: public, cloud, and enterprise.

The location of capabilities in these networks is shown as a best practice, but any capability can be implemented in any network according to the needs of the blockchain solutions. While cloud computing is not required to support blockchain platforms, services, or networks, IBM recommends the use of cloud because of its elasticity, performance, and networking characteristics.
As shown in figure 1, the architecture can span from public to cloud to enterprise network. Users of the blockchain application normally access the blockchain through the application from a public network. While the public network includes users accessing it from the Internet, in a typical enterprise solution the access is from the enterprise’s intranet. Therefore, the public network represents both the Internet and an enterprise’s intranet.

The cloud network hosts the blockchain platform. It also typically hosts the blockchain applications, although the blockchain application can span across other networks, as in the case of a native mobile-based application on the public network. In addition to the blockchain platform, the cloud network can host infrastructure software such as security, monitoring, and intelligence tools. The details of the cloud network components will be discussed later.

Though there are blockchain applications that do not need to integrate with enterprise applications, most applications are expected to integrate with the adopter’s enterprise applications to enhance the blockchain solution. The blockchain adopters can leverage a blockchain platform to reduce the friction that existed in their business network with their existing enterprise applications. These enterprise applications are hosted on the enterprise network and interface with the blockchain platform in the cloud network. An event in the blockchain platform can
trigger an update to the enterprise data in the enterprise network. Alternatively, the enterprise application can trigger a blockchain transaction when a certain event occurs. The enterprise directory can be used to support authentication and authorization required to access the enterprise application.

**Public network**
The public network contains the wide-area networks (typically the Internet), peer cloud systems, and edge services.

**Edge services**
Edge services allow data to flow safely from the Internet into the provider cloud and into the enterprise. Edge services also support user applications. Edge services include:

- Domain name server (DNS)
- Content delivery networks (CDN)
- Firewall
- Load balancers

**Users**
Users are the parties of a blockchain who create and distribute blockchain applications and perform operations using the blockchain. These actors are consistent with the cloud computing actors and roles from International Standards Organization.

Users may include the following:

**Developers**
Blockchain developers create applications for users (client side) and develop smart contracts (server side) that interact with the blockchain and are used by blockchain users to initiate transactions. They also write code to enable the blockchain to interact with legacy applications. Developers can use Fabric Composer, which abstracts the details from blockchain platform, and makes it easy to develop blockchain applications and business networks and to integrate with existing systems.

**Administrators**
Blockchain administrators perform administrative activities related to the blockchain network and application such as deployment and configuration. Administrators use the tools available as part of the platform, such as byfn.sh, to build the blockchain network and to bring it up and down. These administrators
also use a cryptographic tool, cryptogen, to generate cryptographic material necessary for the blockchain network.

Operators
Blockchain operators are responsible for defining, creating, managing, and monitoring the blockchain network and application.

Auditors
Blockchain auditors are part of the business network and are responsible for reviewing the blockchain transactions or access control lists and for validating the integrity of those transactions from a business, legal, audit, and compliance perspective.

Business users
Business users operate in a business network and interact with the blockchain using an application. Often business users are not aware of the blockchain. This user set can be both human and non-human actors, such as other applications that interface with blockchain or an IoT device that interfaces with blockchain. IBM Cloud supports the development, securing, and scaling of the applications used by business users. These applications interact with the blockchain using the Hyperledger Fabric SDK.

Cloud network
Blockchain applications
Blockchain applications are used to present capabilities to users of the blockchain system. This is particularly important for business users, where capabilities must be presented in terms that relate to the particular application area, with concepts and processes familiar to those business users. Applications may also exist to serve other users with different roles, including administrators, operators, and auditors.

Blockchain applications can include web applications, with code centralized on a server closely associated with the blockchain node, or applications running on user devices, which are potentially connected to server-side application services.

The blockchain applications and services interface with the blockchain platform using the blockchain platform APIs. The applications may have access to other server-side resources, such as databases and services, to implement their capabilities.

Blockchain applications are built to benefit the business networks within specific industries including financial services, healthcare, insurance, energy and utilities, public sector, and retail. Blockchain can also enable cross-industry networks to help
revolutionize supply chains, secure and integrate Internet of Things (IoT) applications, and reduce cost and risk.

See Appendix C: Specific examples of blockchain applications.

Using **Hyperledger Composer**, which is a set of collaboration tools, business analysts and developers can rapidly develop blockchain applications. Composer enables developers to concentrate on solving business problems rather than the technical details of the blockchain. Composer offers business-centric abstractions that allow developers to define the business network in terms of its participants, assets, and transactions. After the network is defined, Composer generates the REST APIs that can be used to integrate with the application.

Developing and hosting blockchain applications on IBM Cloud lets you develop and test in a totally self-sufficient local development environment, including Hyperledger Composer, Hyperledger Fabric, CLI tools, IDE Extensions, REST Server, and app generator. The application can also take advantage of the vast catalog of services available on IBM Cloud. For example, blockchain applications invariably have a need for data services and the IBM Cloud environment provides a rich set of databases for the application to choose from, such as IBM Cloudant®.

**Blockchain platform**
The platform supports essential capabilities for blockchain solutions in a blockchain network node or enterprise. While each blockchain platform is set up and implemented differently, these core capabilities should be considered in blockchain platforms and solutions.
**Consensus**
Enables a consensus process used by the nodes within the blockchain network to agree on the validity and order of transactions appended to the ledger. The consensus process maintains a consistently replicated ledger within the network.

**Ledger**
A blockchain ledger holds both the current state of transactions (the world state) and a sequence of cryptographically linked blocks that contain transaction history.

**Membership services**
These services manage identity, privacy, confidentiality, and auditability on the network.

Membership only applies to permissioned blockchains. Permissioned blockchains only allow specific actors to access the data stored on the ledger, to submit transactions, or to validate the network. In a permissioned blockchain, the actors can 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 actors can equally submit transactions or attempt to accumulate them into acceptable blocks. There are no distinctions of roles.
Figure 2 – Hyperledger Fabric Membership Services

Figure 2 depicts the role of Hyperledger Fabric Membership Services, which represent a membership authority and its operations on issuing and managing Hyperledger Fabric membership credentials in a modular and pluggable way. The membership services allow for the co-existence of a variety of credential management architectures and for easy organizational separation in credential management and administration operations, according to business rules. Enrollment certificates (Ecerts) represent the long-term identity of the blockchain network participants. Hyperledger Fabric Membership Services are provided as part of the IBM Blockchain Platform.

**Transactions**
Transactions are records that are appended to the ledger. They can record the exchange of ownership for anything of value, such as stocks, bonds, commercial paper, diamonds, and more. Other use cases include changes to medical records or critical device status in an IoT example.

**Event distribution**
Events are notifications of significant changes or operations that occur in the blockchain network. For example, events result from execution of a smart contract
or the creation of a new block. Events are of interest to participants in the blockchain network.

Event distribution assigns listeners to receive the events from the blockchain. Events 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.

In an atomic broadcast, the sender in a blockchain network sends messages to all connected peer members in the same order of sending sequence. This concept is also termed total-order broadcast or consensus in the context of distributed blockchain network systems.

**Communication protocol**

This protocol is the mechanism by which participating computer systems communicate with each other in the blockchain networks. Typically, the participating computer network members use peer-to-peer protocols, such as gRPC, to communicate with each other in blockchain networks.

**Cryptographic services**

The cryptographic services component 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 are often used to protect the ledger from modifications. Any change to information 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. They also ensure that the transactions originated from senders (signed with private keys) and not imposters.

**Smart contracts**

Smart contracts, sometimes termed *chaincode*, are computer programs that execute in a secure environment within the blockchain platform of any node in the network. Smart contracts encapsulate business logic involving contract terms and conditions between agreeing participants.

The smart contract code determines what transactions are recorded into the blockchain and what information they contain. Smart contracts can be written in a programming language that depends on the blockchain platform.
A reference to the smart contract code and its signature is stored in the ledger. Transactions can invoke smart contract functions, which can be stateless or stateful, to perform business logic. If required, the code can access external information and systems through the system integration component.

Smart contracts help to make decisions and automate relationships. All possible outcomes of the contract must be explicitly specified in advance.

**Secure runtime environment**
During runtime, a blockchain transaction may invoke smart contract functions requiring a secure environment. A secure runtime environment is a hosting environment for server-side blockchain business logic.

An example is the use of the secure service 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 more.

**Systems integration**
Typical integration methods include application programming interface (API) adapters and enterprise service bus (ESB) connections between the blockchain platform and the enterprise systems.

**IBM Blockchain Platform**
IBM supports the capabilities described above in IBM Blockchain Platform, which is a full stack Blockchain as a Service (BaaS) platform with Hyperledger Fabric V1 tightly integrated and optimized, in a public cloud infrastructure based on IBM Cloud. IBM offers several plans for all stages of blockchain development and operation lifecycle. The Developer Sandbox plan is a lightweight private blockchain network designed for exploration and development of blockchain solutions. IBM Enterprise Plan includes several production-ready plans for pilots and live blockchain networks. It is designed to be a robust, highly available production platform with unparalleled security and compliance value for cloud-based blockchain production networks in single or multiple organizations, with flexibility in the deployment options of blockchain solutions.
IBM Blockchain Platform, as shown in Figure 3, offers the following unique features:

- Production-ready: available today as a self-service offering on IBM Cloud.
- Unique security features: across the entire stack, designed to have the strongest key protection, data protection, and trusted execution in the industry.
- Pervasive encryption: automatically encrypts all data saved in the blockchain. No changes to the Hyperledger Fabric or chain code are required for this feature. The encryption keys are saved in protected memory that is not accessible to human operators.
- High performance: based on optimized software, firmware, and hardware.
- Hardened configuration: minimized attack surfaces and optimized performance.
- Dedicated compute and high isolation: based on LinuxONE mainframe platform.
- Governance and management tools: dashboard and workflows to simplify tasks across multiple parties.
Distributed business networks

A typical blockchain business network, as shown in Figure 4, is comprised of multiple members. Each member of the network is responsible for provisioning peers and resources inside of its own IBM Cloud environment and paying for its resources. A shared consensus cluster—the ordering cluster—is hosted at the network level and is administered democratically by all members. All changes to the blockchain network occur according to defined and agreed upon governance policies. The Hyperledger Fabric v1 architecture is modular and allows pluggable consensus implementations. IBM Blockchain Platform provides support for managing the lifecycle of governance policies.

Enterprise plan (EP)
EP enables one to bootstrap a working enterprise grade network, spanning multiple stakeholders, in a matter of minutes. A suite of tools for management and operation of business networks offers built-in monitoring and support functions, allowing easy lifecycle management. It also includes distributed governance tooling to set democratic policies for lifecycle tasks, and workflow tools such as signature collection.

EP is based on IBM LinuxONE systems, which provide a unique set of features for blockchain applications, including:
• Isolated and highly secured environment, distinguishing EP from other cloud-hosted offerings.
• Operating system, fabric, and nodes which all exist in an IBM Secure Service Container.
• Performance optimization for availability, scalability, and encryption.
• Pervasive encryption.

**Open platform**
Hyperledger is a Linux Foundation-managed umbrella project, a global open source collaborative effort created to advance cross-industry blockchain technologies. Fabric grew out of the IBM Open Blockchain project, which was donated to Hyperledger.

As an open collaborative effort, the project has the following key attributes:
• Open governance: the project is managed by a large group of cross-industry and non-profit members, safeguarding transparent governance and broad applicability of the Fabric in the business world.
• Open standards: Fabric is designed to adhere to established industry standards, ensuring interoperability with other blockchain and systems through open, published interfaces and services.
• Open source: the source code is publicly available and anyone can inspect and validate it, leading to high quality and fitness for purpose.

**Performance**
EP provides high performance for systems requiring high transaction rates, very fast consensus calculation, fast and scalable blockchain blocks read and write capabilities, and cryptographic acceleration.

LinuxONE delivers the high capacity scale-up and scale-out processing required by blockchain applications. It is engineered so that high volumes of data can be delivered and processed through its scalable I/O system, very large memory, the fastest commercial microprocessor in the industry, and the largest cache. Communication between peers takes place over a high-speed network where communication is highly secure with no data leakage.

Hyperledger Fabric heavily uses cryptographic algorithms for secure communication, block calculation, and consensus. EP provides hardware accelerators for blockchain encryption and hashing, using accelerators that speed encryption up to 32x ratio compared to software encryption. LinuxONE provides pervasive encryption to all blockchain data, with no changes required to blockchain applications, software, or chaincode.

**Availability**
In a blockchain network, an outage of a peer required to participate in consensus and ledger replication can impact the entire network. While a failing peer may be recovered, it is better to ensure high availability than to rely on recovery.
LinuxONE systems are designed to be the most available servers on the market. Their unmatched design points allow:

- prevention of errors through built-in redundancy for all the critical system components and extensive testing and failure analysis.
- exhaustive error detection and correction capabilities that can isolate problems.
- non-disruptive installation, upgrades, and maintenance of hardware and firmware to help avoid outages.
- automated failover capabilities that can speed recovery and minimize system impact.

Blockchain nodes are deployed in multiple logical partitions (LPARs) to provide high availability. Typically, three or more LPARs forming a cluster with dedicated hardware resources, are used so that the downtime of any one of the LPARs does not affect the availability of the blockchain network. A cluster has assigned dedicated hardware resources such as network or cryptographic cards so that its configuration meets high availability and isolation requirements.

For the IBM Blockchain Platform Enterprise Plan, the LinuxONE and data storage units are configured with hardware redundancy. Redundant switches and other network infrastructure are used to provide high network availability.
**Tenant isolation**

![Diagram of IBM LinuxONE - Tenant isolation](image)

LinuxONE supports multiple layers of isolation as shown in figure 5. Not only is there isolation at the LPAR level, but each set of Docker containers is running a specialized Isolated Docker. Isolated Docker combines the benefits of containers with the security of virtual machine isolation. It provides a standardized container format with small footprint and overhead. The containers are isolated, yet they share the underlying OS kernel and rely on Linux namespaces for isolation.

An ordinary container is started as a task in its own namespace. On LinuxONE, an Isolated Docker container is started as a KVM virtual machine. The virtual machine has no operating system or services, but simply a kernel and minimal initialization to execute the container task. A network is configured via the virtualization, and the container filesystem contents are passed through to the guest.
This level of isolation prevents the threads from rogue software running within the containers such as rogue chaincodes.

**Transformation and connectivity**
This capability enables secure connections to enterprise systems and the ability to filter, aggregate, or modify data or its format as it moves between cloud and blockchain components and enterprise systems (typically systems of record).

Within the blockchain reference architecture, the transformation and connectivity component sits between the cloud network and enterprise network. However, in a hybrid cloud model these lines might become blurred. The transformation and connectivity component includes the following capabilities:

- **Enterprise secure connectivity**: integrates with enterprise data security systems to authenticate and authorize access to enterprise systems.
- **Transformation**: transforms data going to and from enterprise systems.
- **Enterprise data connectivity**: enables cloud provider components to connect securely to enterprise data. Examples include VPN and gateway tunnels.

**Enterprise network**
The enterprise network is comprised of the enterprise user directory, enterprise applications, and enterprise data.

**Enterprise user directory**
The enterprise user directory stores user information to support authentication, authorization, or profile data related to the enterprise applications. The transformation and connectivity services use this to control access to the enterprise network, enterprise services, or enterprise-specific cloud provider services.
In a previous section, we described the Hyperledger Fabric Membership Service. The Membership Service Provider API is a pluggable interface that supports a range of credential architectures. It provides user authentication, credential validation, signature generation, and optional credential issuance. As shown in Figure 6, the default implementation calls Fabric-CA and Hyperledger Fabric also supports “bring your own identity” (external certificate authority).

**Enterprise applications**
Enterprise applications are created or used by an enterprise that is interacting with the blockchain network. The enterprise applications may interact with the smart contracts on the blockchain. A smart contract may obtain data from the enterprise application, send data to the enterprise application, or request services from the enterprise application.
Figure 7: How applications interact with Blockchain

Figure 7 shows how the blockchain application interacts with the Hyperledger Fabric blockchain. Developers create an application and one or more smart contracts. The smart contracts are deployed to peers on the network. The blue box on the diagram represents a peer. The application uses the Hyperledger Fabric SDK to interact with the blockchain. It submits payloads to the smart contract or queries the state of the ledger. Note that a ‘put’ or ‘delete’ command will go through consensus (starting with smart contract execution) and then be added to the blockchain. A ‘get’ command can only read from the world state but is not recorded on the blockchain.

**Enterprise data**

Enterprise data includes metadata and systems of record for enterprise applications. Enterprise data can flow directly to data integration or the data repositories providing a feedback loop in the analytical system for blockchain systems. Enterprise data that relates to blockchain includes:
• **Transactional data**: Data about or from business interactions that adhere to a sequence or related processes (financial or logistical). This data can come from reference data, master data repositories, and distributed data storage.

• **Application data**: Data used by or produced by enterprise applications functionally or operationally. Typically, the data has been improved or augmented to add value and drive insight.

• **Log data**: Data aggregated from log files for enterprise applications, systems, infrastructure, security, governance, and others.

**Blockchain foundational services**

**Governance**
The procedures and policies that govern the operation of the blockchain network are known as governance. A key challenge to initiating and governing a decentralized network is to create a network management experience that offers all participating members some control, while preventing any one member from being exclusively in control. Initiating and governing a blockchain network across a group of members once it is operational can require significant coordination, time, and effort. The ability to properly govern a blockchain network is often overlooked or underestimated. Proper governance ultimately ensures the network is in compliance, removes uncertainty and risk of your business obligations (embodied in the smart contracts), ensures privacy and confidentiality of different classes of transactions (embodied in channels), and eliminates the introduction of bad-actors as network members.

Key advantages of IBM Blockchain Platform include:

• Democratic management tools that allow the decentralized network to be managed collectively and under the governance policies set by the network members.

• A dynamic management environment that allows the network to start small (with a couple of smart contracts and network members) and grow elastically as new smart contracts and network members become available.

• Pre-built tools and policies that enable faster onboarding, customization, and activation.

IBM Blockchain Platform introduces the first set of integrated tools to allow teams to enforce change management of the network across cohorts through customizable democratic policies. Tools include the following:
• Activation tools to spark a new network and join additional member organizations, smart contracts, and transaction channels as they become available.
• Policy Editor to define flexible, democratic policies to govern changes to the network for membership, smart contract, and transaction channels.
• Multi-party workflow tool with member activities panel, integrated notifications, and secure signature collection for policy voting.

Security
Security refers to the security policy and standards that are in place to secure the blockchain platform. Security and privacy in blockchain deployments must address both information technology (IT) security and operations technology (OT) security elements. Blockchain protocols architecture relies on public-key cryptography.

IBM LinuxONE is an ideal platform for operating a secure blockchain. The inherent security of the LinuxONE platform is legendary, and it can be used to maximum effectiveness with Hyperledger Fabric to secure the software, the data, and the users, and bring it all together with IBM Blockchain Platform.

Secure system design, development, and management
IBM Blockchain Platform on IBM Cloud has layered security controls across the network and infrastructure. It helps ensure security readiness by adhering to security policies that are driven by best practices in IBM for systems, networking, and secure engineering. These policies include practices such as source code scanning, dynamic scanning, threat modeling, and penetration testing. It follows the IBM Product Security Incident Response Team (PSIRT) process for security incident management. Figure 8 summarizes the scope of these security features and practices.
Securing and isolating the software and data

IBM Blockchain Platform uses a number of technologies to ensure that the blockchain software and data can be trusted, and to ensure that the customer data is secure. Four technologies work together: LPAR, KVM, Isolated Docker Containers, and Secure Services Containers (SSC).

Logical partition (LPAR) is the built-in facility for hardware-enforced partitions which each act as a separate machine. Each LPAR runs its own operating system and has its own hardware resources. The separation is certified under Common Criteria at level EAL5+. Control of LPARs is provided by the PR/SM (Processor Resource/System Manager) layer.

KVM is the kernel-based virtual machine technology that is part of the Linux operating system. It provides strong isolation between virtual machines using a combination of hardware and software.

Isolated Docker Containers package software in a container that has everything needed to run an application. All components are tested to work properly, then packaged into a deployable container. Isolated Docker technology adds the use of a
KVM virtual machine to provide robust separation between multiple instances of the packaged code, or between that code and other applications running on the server.

**Secure Services Container (SSC)** is a technology developed by IBM to encapsulate an application and operating system into a secure and well-controlled appliance. The appliance is provided as a single image that is encrypted using a key generated on your IBM LinuxONE machine so that it cannot be used on any unauthorized system. A secure boot process validates the image, decrypts it, and loads it for execution. This process ensures that no malware or modified software can be inserted into your IBM Blockchain Platform system. In addition, all blockchain customer data is encrypted in storage using keys that are held securely in the SSC appliance and protected using the cryptographic techniques that protect the appliance itself.

LPAR, KVM, and SSC are combined for the IBM Blockchain Platform as shown in Figure 9.
Figure 9: Blockchain appliance architecture overview

The bottom of the diagram shows the PR/SM resource manager. Above that are multiple LPARs that each contain a SSC image. The green box shows the SCC running in the LPAR and above that are multiple KVM virtual machines. Each KVM contains a Docker image that is a single blockchain peer, running in isolation from other peers in the machine. Within each peer, there are multiple chaincodes that implement the functions which can be invoked externally to operate on the blockchain.

The security begins with the protection of the SSC itself. The SSC is a complete pre-configured environment for an instance of blockchain, from the operating system through all levels of the Hyperledger Fabric software. It also includes all related components needed to operate the blockchain, including management and
monitoring tools. The loading process ensures that this package cannot be modified in any way. This provides assurance that the entire blockchain software environment is running with a fully-tested set of components that operate properly together and do not contain any malware or other modifications.

The only interaction that is possible with the blockchain is through a set of REST APIs that communicate directly with the trusted software running in the SSC container. No other access is possible, not even standard system tools like SSH. Thus, the only things any insider or outsider can do are those things implemented in functions accessed through the REST APIs. Even system programmers cannot gain access to the internals of the blockchain software, to the blockchain system, or to customer data.

**Support from z System cryptography**
Cryptography is at the center of blockchain security. z System uses a set of cryptographic hardware and software that work together to provide both high security and high performance.

At the heart of the secure infrastructure, the Crypto Express6S Hardware Security Module (HSM) provides cryptography and key protection designed to meet the stringent requirements of NIST FIPS 140-2 Level 4, the highest level defined. The HSM protects critical elliptic curve cryptography (ECC) private keys that are used in the IBM Blockchain Platform system.

The integrity and immutability of the blockchain is protected using hash functions. The z System CPACF (Central Processor Assist for Cryptographic Functions) is a high-performance, low-latency cryptographic engine that is integrated into each of the z System CPUs. IBM Blockchain Platform uses CPACF for the required hashing and for symmetric cryptographic operations.

The functions that use the ECC public keys do not have to be performed in an HSM, because those keys do not have to be kept secret. To achieve maximum performance, the ECC public key functions are implemented using specially-tuned software that relies on the unique z System SIMD (single instruction, multiple data) instructions that are designed for parallel processing.

Working together, these cryptographic features are designed to help IBM Blockchain Platform achieve the highest level of security, while still providing industry-leading performance.

**Blockchain network management**
The blockchain network management component provides visibility of the blockchain network operations, including business process metrics and performance and capacity data. It also provides a management interface used to change configurations and other parameters.
IBM Blockchain Platform allows an organization to deploy and operate decentralized networks with a production-ready, security-hardened service. Start small and scale your network elastically as your membership and transaction volumes increase.

Key advantages of IBM Blockchain Platform include:
- High security environment with many hardware, firmware, and software security features designed for scalability, resiliency, and availability.
- Always on operations means that the network just keeps running. Includes the ability to continue operation while the network is being updated.
- Optimized for performance and running on the world’s fastest Linux compute.
- Pervasive, automatic encryption of all blockchain data that requires no changes to blockchain software or applications.

IBM Blockchain Platform includes tools and capabilities to simplify administrative tasks for operating your part of your blockchain network:
- Hardened security stack with no privileged access, malware and tamper resistance, 100% encryption possible if required by the application, HSM key protection, and many more features for networks with sensitive data in regulated industries. These capabilities can help reduce compliance costs.
- Dashboards for monitoring and managing the resources on the network.
- Lifecycle management for seamless upgrades of the full code stack without pausing the network.
- 24x7 technical support integrated into the portal.

**Context and options**
This section describes additional concepts and components that are common in blockchain environments and can be helpful in understanding blockchain solutions and networks.

**Permissions options**
*Permissionless* networks are open to any participant and transactions are verified against the pre-existing 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 known participants with privileged access to the business network. This means that you must be a member of the network in order to participate. On permissioned blockchains such as Hyperledger Fabric, private transaction and data are supported and participants are allowed to view only the transactions relevant to them and are only allowed to perform operations for which they have permission.
IBM believes that permissioned networks are necessary in order to apply blockchain in the context of our industries—to use blockchain to conduct business. That is the reason that a core component of the Hyperledger Fabric architecture is the Membership Services Provider interface. This interface represents a membership authority and its operations on issuing and management of Hyperledger Fabric membership credentials in a modular and pluggable way. A key function of the Fabric Membership Services Provider interface is to manage participants’ enrollment certificates, which are needed for applications to invoke Fabric APIs. The modular and pluggable Fabric architecture approach allows for the flexibility of either using the default Fabric certificate authority or an external certificate authority.

In permissioned blockchains, the identity of the network participants is known. Knowing the identity of participants allows for more flexibility in the selection of the consensus algorithms, based on the level of trust in the network. Permissioned blockchains allow for the use of consensus algorithms with improved performance (transactions per second) and resiliency (network still operating in the event of node failures). For example, in the Fabric architecture, there is no mining or proof of work involved to reach consensus. Instead, consensus is reached using a number of steps that involve peers endorsing transactions, an order service creating blocks, and peers validating ledger updates. Another example is the Byzantine fault tolerant class of algorithms, which are resilient to node failures.

**Blockchain storage options**

When using blockchain to record transactions, there is often only a small amount of the data associated with a particular transaction stored directly in the blockchain ledger (“on chain”). Other data associated with the transaction, which might be much larger, is stored separately from the entry in the blockchain ledger but is referenced by the entry (“off chain”). Because the ledger is distributed between the network nodes and keeps track of all past transactions (the chain of blocks), this approach avoids overwhelming the blockchain ledger with large volumes of data. How much data should be on chain versus off chain is a matter of discussion and is a design choice that involves trade-offs.

As an example, a customer makes an order for goods from a supplier. The complete order could be a large document that includes a list of order items, quantities, prices, and ancillary information with details of the customer, delivery locations, and more. To record the transaction, the blockchain entry might reference an order number, a customer identity, and the total cost, plus a security token (such as a hash) relating to the complete order document (the PDF). The complete order document itself (the PDF) is stored separately in an off-chain database. Another example is the storage and administration of personal health records.

**Ledger storage**

Ledger storage is the physical storage where the transaction data in the blockchain ledger is stored.
**Data storage**

Data storage supports data other than the blockchain ledger itself and can take many forms, depending on the nature of the data. It can take the form of a database, either an SQL database (particularly for record-oriented data) or a NoSQL database (particularly for document-oriented data). 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. In some cases, multiple different forms of data storage might be used.

Separately, you must consider replication and backup of the data objects. For some data storage services, replication and backup are built into the service itself. In others, you must create replicas or backups through deliberate actions of the application.

No matter what your needs are, blockchain applications running in the IBM Cloud environment have many options to choose from. For relational databases, applications can choose from PostgreSQL, MySQL, or IBM Db2 Hosted. IBM Cloudant, MongoDB, RethinkDB, and ScyllaDB are some of the available choices for the applications if you require a document database.

Storing minimal amount of data related to the transaction in the ledger is typical. This might include a reference to other data stored externally. In our earlier example, the complete order document is probably stored externally. Blockchain applications running in IBM Cloud can take advantage of IBM Cloud Object Storage to store large objects associated with the transaction. Documents or objects stored in IBM Cloud Object Storage are dispersed across multiple geographic locations in a region or across multiple regions. IBM Cloud Object Storage encrypts the data at-rest there by alleviating the burden the application developer has on securing the data. In addition, globally distributed applications can benefit from easy access to the data from multiple endpoints. Blockchain applications can use S3 APIs to access the documents, as IBM Cloud Object Storage supports the most common subset of operations provided by S3 API.

**Interaction options**

There are several types of users in a blockchain ecosystem: developers, administrators, operators, auditors, and business users. There are several ways these users can interact with the blockchain. They can interact using command line interfaces and invoking shell scripts, using tools available as part of the SDK, or using collaboration tools like Fabric Composer to interactively build business networks and to create smart contracts and blockchain applications. Blockchain applications can also use the client SDK to develop their blockchain applications.
Command line interface (CLI)
Blockchain developers and administrators sometimes must interface with the blockchain network and perform activities such as import, export, manage accounts, monitoring, and more using a simple text command structure. The administrators can use a command line interface for these tasks.

Client SDK
The client SDK is a client-side programming library that features a set of APIs in the form of “methods” or “calls”, which client programs can use to access the capabilities and functionalities of the blockchain network. The client programs can be written in Java, Node, Python, or other supported languages. The SDK can also include development tools.

Software development kit (SDK)
SDKs for blockchain support communication and integration between blockchain applications and a blockchain platform. Blockchain application development involves developing, testing, debugging, and deploying the application.

The SDK is a set of tools that enables blockchain application developers to create and deploy the applications that interact with the blockchain network during the software development life cycle.

The Hyperledger Fabric Composer tool is an important feature of IBM Blockchain. With Hyperledger Composer, users can easily build the blockchain business network as well as create chaincode and the blockchain application. This allows the developers to focus on solving the business problem rather than dealing with the intricacies of the blockchain. Using Hyperledger Composer, business users can work with developers to define assets that are exchanged in the transactions, to define the business rules, and to define participants, their roles, and access control. The tool helps to model reusable components and helps to integrate with external enterprise systems. It also provides a playground for the developers to test their application. Some advantages of using Hyperledger Composer can be faster creation of blockchain applications, easier development cycle, and easier testing. This helps reduce the risk in delivering the application and business value.

Runtime flow
The technical implementations of blockchains vary depending on the type of blockchain that is chosen. They can use different methods to establish the network topology, manage participation, execute smart contracts, and manage growth.

The runtime flow below describes a supply chain scenario that uses the Hyperledger Fabric blockchain implementation. The scenario illustrates the movement of goods from an exporter at the port of origin to the port of destination using a selected
transporter. The transaction process is initiated by the importer and completed when the imported goods are cleared by custom officials.

1. A blockchain user accesses the blockchain platform to perform a transaction:
   a. A developer creates the blockchain application and deploys the application using an SDK and commands on a command line interface.
   b. An administrator sets up the blockchain network.
   c. An operator manages the day-to-day operation of the blockchain network.
   d. An auditor performs business-related audits.
   e. A business user uses a browser client to enable interaction. The various business users in this scenario include:
      • Importer
         i. The importer requests a Letter of Credit from its bank.
         ii. Following the receipt of the goods, the importer lets the bank know of the receipt.
• Importer’s bank
  i. Creates a Letter of Credit on behalf of the importer through the bank’s legacy system and publishes it on the blockchain through the system integration component.
  ii. Upon receipt of the goods by the importer, releases the payment to the exporter’s bank.
• Exporter’s bank
  i. Receives the Letter of Credit, publishes the receipt on the blockchain, and notifies the exporter.
  ii. Upon receipt of the funds from the importer’s bank, transfers the money to the exporter.
• Exporter
  i. The exporter readies the goods for shipment and requests export control authority for clearance.
• Export control authority
  i. Upon notification that the exporter is ready for shipping, the export control authority performs any necessary inspection on the goods and publishes the export certificate on the blockchain.
  ii. The export control authority notifies the shipping company.
• Shipping company
  i. The shipping company creates a Bill of Lading and publishes it on the blockchain.
• Departing port authority
  i. The departing port authority confirms the shipment by publishing the shipment on the blockchain.
• Arrival port authority
  i. The arrival port authority confirms the arrival of the shipment by publishing it on the blockchain.
• Customs authority
  i. The customs authority inspects the goods and, if passed, publishes the customs clearance on the blockchain.

The business users are likely to access the blockchain network through blockchain applications running on the cloud network. Other users may access the blockchain network from within the environment for administrative and operational purposes.
2. Upon receiving the request to access the blockchain network, edge services route the request to the security gateway.
3. Business users can access the application using a browser client that passes the request to the blockchain platform.
4. The request passes through the API SDK to the blockchain platform for authentication, authorization, and execution.
5. Hyperledger Fabric Membership Services, which provides security, privacy, and protection for blockchain users, authenticates the user and authorizes the action requested by the user based on their role.
6. Security services enable the Hyperledger Fabric Membership Services to establish the user’s identity and provide authentication, authorization, and integration capabilities.
7. A secure environment is spawned to execute server-side blockchain business logic.
8. Based on various triggers, smart contract business logic enforces contract terms between the stakeholders.
9. The validation of the smart contract might necessitate access to enterprise data. The request goes through the transformation and connectivity service, which transforms the data and ensures secure and reliable delivery.
10. External events can trigger a blockchain transaction, such as the creation of the Letter of Credit by the importer’s bank through its legacy systems.
11. Before the enterprise application performs any processing, the blockchain service instance can authenticate the user using the enterprise user directory.
12. The enterprise application can leverage data used by the client application as well as logs and context data for analytics. If the client application updates the data, then the enterprise application can process those changes.
   a. For example, the importer’s bank uses an enterprise application to approve a funds transfer through their legacy system, which subsequently sends a message through an interbank financial network.
13. Enterprise data is the data store for the enterprise application.

**Cloud deployment considerations**

Deployment considerations for a blockchain-based solution need to be made at two levels:

1. **The application**: The application includes the user interface and business logic for the solution. It is what users see and interact with. The application embeds the Fabric SDK and invokes Fabric APIs for smart contract
(chaincode) and ledger queries. Based on your needs and constraints, you must decide where the application runs—IBM Cloud, another cloud provider, or on premises. Running the application on IBM Cloud offers the advantage of having the required services (such as Node.js runtime and object store) in proximity of the blockchain services.

2. **The blockchain network**: By its nature, a blockchain network is distributed. The architect must decide how many nodes (participants) are in the network and where these nodes run (see Figure 4: IBM Blockchain Platform network diagram). Running all the nodes on the IBM Blockchain Platform (but in separate data centers) offers advantages for monitoring and managing the network. It is also possible to run some of the nodes in another cloud or on premises.

There are several other considerations that need to be evaluated when deploying a blockchain solution.

**Scalability and elasticity**
In a blockchain architecture, the number of transactions can be very large. Transformation and connectivity needs to provide scalable messaging and scalable transformation of data in the cloud for these data flows. Elasticity is the ability for a cloud solution to provision and de-provision computing resources on demand as workloads change.

Public clouds have a distinct advantage because they generally have larger pools of resources available. Customers also benefit by only paying for what they use. Private clouds and dedicated hardware can make up some of the difference with higher bandwidth data paths.

**Data bandwidth**
Public and private clouds need to be optimized for handling large data sets. Large cloud data sets requiring fast access benefit from processing components with fast and efficient data access. This can mean moving the processing to the data, or vice versa. Cloud systems can effectively hide the physical location of data and processing. You can perform tuning activities continuously with minimal impact on deployed applications.

**Data sovereignty**
The physical location in which data is stored might be regulated, with the regulations varying from country to country. This is particularly true for personally identifiable information (PII) and for sensitive data such as health data and financial records. The European Union has stringent regulations that apply to the PII of European citizens.

As a result, any blockchain system must consider data sovereignty rules, and must store and process data only in those locations permitted by the regulations. The
cloud service provider must allow the cloud service customer to control storage and processing locations, as well as backup locations.

**Resilience**
In blockchain systems, resilience and fault tolerance are very important. Blockchain systems should not depend on one single component at any point and should tolerate the failure of a single component. Components in the provider cloud should be made resilient through the use of multiple instances of programs and cloud services allied with data replication and redundancy on multiple storage systems.

The networks should also be resilient, for example using multiple paths and multiple providers in the public network. It is impossible to make the entire network available all the time but it should be highly available and resilient. It is important to ensure that the connectivity capabilities can support resilience.

**Security**
As more data about people, financial transactions, and operational decisions are collected, refined, and stored, the challenges related to information governance and security increase. Data privacy and identity management are incredibly important. The cloud generally allows for faster deployment of new compliance and monitoring tools that encourage agile policy and compliance frameworks. Tools that monitor activity and data access can actually make cloud systems more secure than standalone systems. Hybrid systems offer unique application governance features. Software can be centrally maintained in a distributed environment with data stored in-house to meet jurisdictional policies.

Enterprise blockchain provides a design avenue where transaction data, value, and state are inherently close to the business logic. A secure community process validates the security of the execution of business transactions, enabling a foundation of trust and the robust processing of transactions.

**Summary**
In this paper, we examined the standardized CSCC Cloud Customer Reference Architecture for Blockchain and described the advantages of working with IBM to implement this architecture. You can benefit from IBM’s industry expertise and experiences applying blockchain to your specific business use case. IBM Blockchain, however, is not just IBM. The reference architecture has been standardized with the Cloud Services Customer Council, vetted by many of its 600+ members, and submitted to standards organizations, including ISO TC307.

IBM Blockchain Platform is based on the Linux Foundation’s Hyperledger open governance model where the community is in charge of the code base. Hyperledger Fabric supports permissioned blockchain networks and private transactions within the context of the network. Hyperledger Fabric provides a modular blockchain
architecture that can adapt as the network grows or its trust level changes. Hyperledger Composer is a tool where developers or analysts can design business networks without coding. IBM Blockchain Platform is a fully integrated enterprise-ready blockchain platform designed to accelerate the development, governance, and operation of a multi-institution business network. It is designed to offer unrivaled security and scalability features.

With this and IBM's industry expertise, IBM is uniquely positioned to be your partner of choice to accelerate the development, governance, and operation of your network.

Acknowledgements
The following people contributed to this paper:
Writers: Petr Novotny, Todd Arnold, Subodh Manicka, Bertrand Portier
Reviewers: Arnaud Le Hors, Heather Kreger, Tim Richer, Gopal Indurkhya, Anshu Kak, Nitin Gaur, Donna Dillenberger, Stuart Jones
Images, Editing, PM: Glenn Daly, Susan Kruemcke, Robert Flaherty

Appendix A - Blockchain fundamentals
A blockchain is a shared ledger distributed across a business network. Business transactions are permanently recorded in append-only blocks to the ledger. All the consensually confirmed and validated transaction blocks are linked from the genesis block to the most current block with each block linked to its previous block using the cryptographic hash of the previous block—hence the name blockchain.

A blockchain is a historical record of all transactions that have taken place in the network since the beginning of the blockchain. The blockchain serves as a single source of truth for the network.

High-level view of a blockchain network
Figure 11 shows the basic components that comprise a blockchain and its environment. There are many variations on this basic conceptual design that add other features, but the diagram is a useful way to introduce how blockchains work.
In general, a blockchain system consists of a number of nodes, each of which has a local copy of a ledger. In most systems, the nodes belong to different organizations. The nodes communicate with each other to agree on the contents of the ledger and do not require a central authority to coordinate and validate transactions.

The process of gaining this agreement is called consensus, and there are a number of different algorithms that have been developed for this purpose. Users send transaction requests to the blockchain to perform the operations that the chain is designed to provide. When a transaction is completed, a record of the transaction is added to one or more of the ledgers and can never be altered or removed. This property of the blockchain is called immutability.

Cryptography is used to secure the blockchain itself and the communications between the elements of the blockchain system. It ensures that the ledger cannot be altered, except by the addition of new transactions. Cryptography provides integrity on messages from users or between nodes and ensures operations are only performed by authorized entities.

The authority to perform transactions on a blockchain can use one of two models, permissioned or permissionless. In a permissioned blockchain, users must be enrolled in the blockchain before they are allowed to perform transactions. The enrollment process gives the user credentials that are used to identify the user when he or she performs transactions. In a permissionless blockchain, any person
can perform transactions, but they are usually restricted from performing operations on any data but their own.

Most business-oriented blockchains include the ability to use **smart contracts**, sometimes called **chaincode**. A smart contract is an executable software module that is developed by the blockchain owners, installed into the blockchain itself, and enforced when pre-defined rules are met. When a user sends a transaction to the blockchain, it can invoke a smart contract module which performs functions defined by the creator of that module. Smart contracts usually have the ability to read and write to a local data store which is separate from the blockchain itself and can be updated when transactions occur. The business logic contained in a smart contract creates or operates on business data that is contained in this persistent data store.

In a simple blockchain, every node is identical and every copy of the ledger is identical. However, more complex blockchains allow differences in the nodes and the ledgers. Some blockchains support the concept of **subchains**, which are sometimes called **channels**.

Subchains are logically separate chains that occupy the same physical blockchain. Each subchain can be owned by a different entity and can be accessible by a different set of users. Nodes may be set up so that some nodes participate in certain subchains and not in other subchains. The result of this configuration is that the ledger on some nodes will contain transactions for that subchain while the ledgers on other nodes will not. Another variation on the basic blockchain is one in which nodes are assigned specific purposes instead of being identical in their function. This configuration may be used to optimize performance because the system can be faster if every node does not have to perform every operation required for a transaction on the chain.

**Key characteristics of a blockchain network**

There are several characteristics that apply to blockchain systems that affect their architecture and implementation:

- **Cryptography**: Blockchain's transactions achieve validity, trust, and finality based on cryptographic proofs and underlying mathematical computations between various trading partners.
- **Immutability**: This term means that blockchain transactions cannot be deleted or altered.
- **Provenance**: In a blockchain ledger, provenance is a way to trace the origin of every transaction such that there is no dispute about the origin and sequence of the transactions in the ledger.
- **Decentralized computing infrastructure**: These computing infrastructures feature computing nodes that are capable of making independent processing
and computational decisions irrespective of what other peer computing nodes may decide.

- **Distributed transaction-processing platform**: This platform handles a range of transactions, including exchanging value, assets, or other entities.

- **Decentralized database**: Each participating partner has access to a distributed database in its entirety at all times. No single party controls the database, which every party can verify or regenerate if required without having a central intermediary.

- **Shared and distributed accounting ledger**: These ledgers can be public, private, or semi-public/private. Ledgers can be shared amongst participants with privacy. In permissioned blockchains, participants can see the transactions fully with permission and still maintain anonymity. These transactions are final and irreversible because each transaction is linked to every preceding transaction in the ledger. The ledger entries are time ordered and are computationally and cryptographically architected to ensure permanence, and the ledger itself is widely replicated.

- **Software development platform**: A software development platform makes use of APIs, peer-to-peer networks, and public, private, or hybrid networks. Transactions are programmable since the underlying ledger is digital in nature, which leads to intelligent and programmable contracts and contract enforcements.

- **Cloud computing**: Blockchain systems frequently involve the use of cloud computing platforms. Cloud computing platforms offer the potential to use large amounts of resources in relation to data storage and also the ability to bring flexible and scalable processing resources to the analysis of data.

- **Peer-to-peer network**: In these networks, participating nodes communicate with each other directly and without a central or intermediate node or entity.

- **Wallet**: A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, and encryption keys.

Blockchain network implementations strive for scalability and concurrency, ensure no single point of failure, and include pluggable components like databases and other consensus mechanisms. Successful implementations support multi-level confidentiality and privacy, which is achieved through multichannel or subchain communication, multiple sub-ledgers, and multiple stakeholders for transaction visibility based on a need-to-know-basis.
## Appendix B: Blockchain Reference Architecture with IBM offerings

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DEFINITION</th>
<th>IBM PRODUCT</th>
</tr>
</thead>
</table>
| Peer provider cloud        | This service can be for wallet capabilities or a vendor cloud provider hosted blockchain network. | • Apple  
• Amazon  
• Microsoft  
• Google  
• PayPal  
• Third-party wallet/cloud provider |
| Edge services              | Provides network capability to deliver content through the Internet (DNS, CDN, firewall, load balancer). | • IBM Cloud platform  
• Fastly  
• Vyatta  
• Third-party services |
| Security gateway           | Network point that acts as an entrance to another network.                    | • IBM DataPower Gateway  
• IBM Security Access Manager  
• IBM Cloud platform  
• IBM Security Directory Suite  
• IBM Single Sign On  
• Application security |
| Provider cloud portal service | This service facilitates human users to connect to cloud provider.          | • IBM Cloud - Public  
• LinuxOne Community Cloud Portal |
| Server runtime             | Server runtimes host blockchain native applications on a server-side hosting environments. Server-side applications are deployed to server runtimes and are running as chaincode applications on blockchain networks in a hosted environment. | • IBM Cloud service  
  ▪ Public  
  ▪ Dedicated  
  ▪ On-premises  
  ▪ Hybrid  
• LinuxOne Community Cloud Portal |
<p>| API SDK                    | The SDK enables applications to interact with blockchain by invoking the Hyperledger APIs. | • Hyperledger Fabric SDK Design Specification v1.0 |</p>
<table>
<thead>
<tr>
<th>Service Type</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blockchain service</strong></td>
<td>This service is responsible for getting the blockchain network instantiated for blockchain applications to be deployed and consumed.</td>
<td>• IBM Blockchain Platform Sandbox for Developers&lt;br&gt;• IBM Blockchain Platform Entry Plan&lt;br&gt;• IBM Blockchain Platform Enterprise Plan&lt;br&gt;• IBM Blockchain Platform Enterprise+ Plan&lt;br&gt;• Hyperledger Composer Playground on IBM Cloud</td>
</tr>
<tr>
<td><strong>Blockchain admin and operations services</strong></td>
<td>Provides the ability to create, change, and monitor blockchain components. The services are part of the blockchain cloud service.</td>
<td>• IBM Blockchain Platform on IBM Cloud</td>
</tr>
<tr>
<td><strong>Blockchain system integration</strong></td>
<td>Responsible for integrating blockchain bi-directionally with external systems. The service is not part of blockchain service but used with it.</td>
<td>• IBM API Connect&lt;br&gt;• IBM Integration Bus</td>
</tr>
<tr>
<td><strong>Transformation and connectivity</strong></td>
<td>Provides secure connectivity between services running in the cloud and data or applications running on-premises or in other clouds.</td>
<td>• IBM API Connect&lt;br&gt;• IBM Integration Bus&lt;br&gt;• IBM Aspera&lt;br&gt;• IBM DataPower Gateway&lt;br&gt;• IBM InfoSphere</td>
</tr>
<tr>
<td><strong>Enterprise data</strong></td>
<td>Includes systems of record and metadata about the data for enterprise applications.</td>
<td>• IBM Db2&lt;br&gt;• IBM InfoSphere Master Data Management&lt;br&gt;• IBM BigInsights&lt;br&gt;• Hbase&lt;br&gt;• Spark</td>
</tr>
<tr>
<td><strong>Enterprise applications</strong></td>
<td>Includes applications that accomplish business goals and objectives that may interact with cloud services. All the EIS systems to which blockchain network need to connect to for delivery of smart contract capability and contract enforcement.</td>
<td>Enterprise-specific JEE, Messaging, EIS (SAP, Siebel), or such applications. Data and business logic involved in mainframes, CICS systems, MVS systems, and IBM zOS platforms.</td>
</tr>
</tbody>
</table>
| Enterprise user directory | Provides storage for and access to user information to support authentication and more. | • IBM Security Directory Suite  
• IBM Directory Server  
• IBM Security Manager  
• IBM Single Sign On  
• LDAP |
| Governance | | • IBM WebSphere Service Registry and Repository  
• IBM API Connect |
| Infrastructure security | | • IBM X-Force  
• IBM IDS/IPS Suite |
| Security monitoring and intelligence | Security monitoring and intelligence provides security and visibility into cloud infrastructures, data, and applications by collecting and analyzing logs in real time across the various components and services in the cloud. It provides real-time risk analysis of the workloads hosted in the cloud against the myriad of known vulnerabilities and alerts against zero day attacks. It includes problem and information security incident management and responding to expected and unexpected events. | • IBM QRadar  
• IBM Security Trusteer for security intelligence |
Appendix C: Specific examples of blockchain applications

There are many use cases for blockchain applications. Some well-understood examples include:

- **Letter of credit (LOC):** Blockchain provides a common ledger for letters of credit that allows banks and all counter-parties to have the same validated record of transactions and fulfillment of conditions. Smart contracts, also referred to as chaincode, define the conditions for payment and LOC fulfillment.

- **Trusted supply chain:** Blockchain provides an agreed-upon, shared record of the asset information—as it transverses the supply chain—recording who owns what, and when and where an asset is in the supply chain.

- **Healthcare payments:** Clinical attachments in healthcare claims involve a lot of actors, information, and records, where successfully associating information is a complex task. The matching of clinical versus payment data involves complex information requirements and can be very costly and time consuming. Blockchain can simplify this complicated relationship and automate the information collection and sharing.

- **IoT to Economy of Things:** Blockchain functions as a distributed transaction ledger for IoT transactions, helping to enable autonomous device coordination and peer-to-peer messaging.

- **Commercial paper:** Blockchain connects corporate treasuries with global advisors for investment advice, with subsequent execution through to clearing and settlement.

- **Contract management:** Blockchain is used as a shared repository of the legal documents and their approval histories. The business process or workflow of document handling is enabled by chaincode. When there are multiple related documents (such as a master service agreement, service contract, invoice, and others), chaincode automatically checks the consistency of these documents to reduce errors.

- **Manufacturing provenance:** Blockchain holds complete provenance details of each component part, accessible by each manufacturer in the production process, such as aircraft owners, maintainers, and government regulators.

- **Vehicle registration and maintenance:** Government regulators can create a vehicle template on blockchain that is updated by the manufacturer on transfer to the dealer, initial owner, and future owners. This could be augmented with other information, such as records of maintenance or vehicle theft. Use blockchain as a shared ledger of vehicle history, detailing usage, maintenance, warranty work, and replacement parts.

- **Livestock registry:** Blockchain provides a common ledger for the government, farmers, slaughterhouses, and cattle markets. All parties have access to validated records of livestock, including transactions and movements. Smart contracts define the conditions of transactions and movements according to animal type.
- **Equipment records**: Use blockchain as a shared ledger of equipment history, detailing usage, maintenance, and warranty work and replacement parts.
- **Food safety provenance**: Secure documentation is added to raw material and consolidated onto packaging with aggregation for shipment. Blockchain provides real-time visibility of the food supply chain to distributors, consumers, retail buyer, auditors, and regulators.