Blockchain - What is it good for? Where should you run it?

An IBM Systems Point of View

Daniel Kohen
Nick Dudeney
Richard Gamblin

Version 1.2 – 27 Oct 2016

Executive Summary

Blockchain is a disruptive technology that will transform cross-business interactions in the coming years. Its core principles are to simplify and secure the transactions within a business network, based on a distributed digital ledger. IBM already has a proven track record with blockchain technology, making the largest contribution to the Hyperledger project and offering consultancy in its implementation.

IBM recently introduced a unique set of blockchain offerings, both for cloud-based and on-premises applications. The **High Security Business Network (HSBN)** is a new cloud offering, designed to exploit the high performance, enhanced security and high resilience characteristics of **IBM LinuxONE**. For organizations wishing to exploit these same qualities of service in-house, IBM offers an on-premises hosting platform with **IBM LinuxONE** and **Linux for z Systems**.

In this paper, we introduce blockchain and its use-cases and position the unique elements of IBM's blockchain solutions and how they exploit the secure, resilient and high performance characteristics of IBM z Systems.

Background

Businesses don't exist in isolation. They are connected to customers, suppliers and partners and operate across geographies and regulatory boundaries in a business network. Goods and services flow within and across networks in what we commonly call a market. Within these networks, assets are exchanged and value is created through transactions governed by contracts.

Throughout history, instruments of trust emerged to allow the exchange of value, including minted coins, paper money, letters of credit and banking systems. Important innovations, which have helped overcome distance and inefficiency include data communication, credit card systems, the Internet and mobile technologies.

Even so, many business transactions remain inefficient, expensive and vulnerable. For example, the participants in a real estate transaction (banks, property owners, auditors, attorneys, title companies, governments and insurance companies) each keep their own records updated with their transactions. The individual networks have complex silos that require reconciliation and are prone to tampering. This introduces expense due to duplication of effort and the need for third party validation or the presence of intermediaries. It is clearly inefficient, as the contract is duplicated by every participant. It is also vulnerable because if a central system is compromised, it affects the whole business network. Incidents can include fraud, cyber-attack or a simple mistake. This depletes trust, prevents automatic verification or authentication of assets, and increases costs.

Blockchain is a technology that implements a shared ledger allowing participants in a business network to see and interact with the "system of record", also called **Distributed Ledger Technology (DLT)**. Blockchain enables new business models based on the frictionless trade of high-value tangible assets (e.g. houses, diamonds) and intangible assets (e.g. mortgages, contracts). It does this with enhanced connectivity between participants in a business network including customers, suppliers, banks, & partners. By sharing a common ledger, inter-business transactions and processes can be managed more quickly and efficiently (see fig 1)

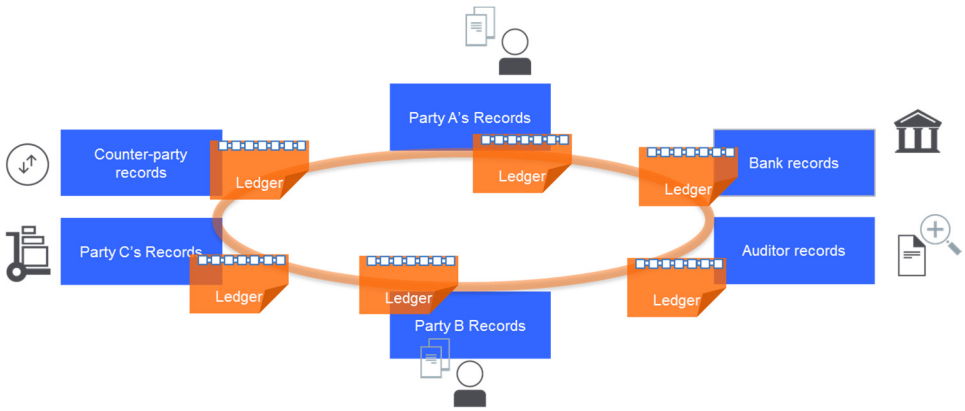

Figure 1: anatomy of Distributed Ledger Technology in a business network

Most models for transacting business today are built on the guarantee of a central, authoritative source of truth, where disparate parties that do not necessarily trust each other can at least trust a central authority. Each party typically owns a part of the process, and there can be overlap between the data retained by each party, within their individual company systems. With blockchain, cryptography and consensus replace third-party intermediaries as the keeper of trust, and all blockchain participants certify the integrity of the whole.

Blockchain Projects from Inception to Production

While the business benefits of shared IT systems are easy to understand, it can be a huge leap to get from the original concept for a new blockchain application to a working production system. Blockchain is still a relatively new technology, and implementation requires a new set of skills and capabilities. As a thought-leader in blockchain technologies, IBM has the appropriate experience and investment in blockchain to ensure that many of the pitfalls of managing a complex multi-party IT project can be avoided.

IBM is a leader in Open Source projects and the single largest contributor of the **Linux Foundation's Hyperledger** project with our own implementation of blockchain. The consortium of companies comprising this initiative elected an IBM executive as its chairman early in 2016. IBM has pledged significant resources to the development of Hyperledger. In addition, IBM is a leader in blockchain consultancy with a focused services team in our Financial Services Sector. IBM's global digital agency iX is also able to engage with clients to assist with the design of new use cases for blockchain. Furthermore, IBM Bluemix Garage, associated with Design Thinking method for use cases identification accelerate development of Blockchain applications. In combination with IBM's years of experience in delivering major IT projects, we provide the full range of capabilities to ensure success in all stages of a new blockchain project.

Skilled IBM practitioners are working today with many businesses worldwide who are prototyping and delivering new blockchain systems. The key to success is to have trust in each member of a blockchain consortium, and in the technology which will deliver the production system.

IBM's Blockchain Initiative

The Hyperledger Project, backed by IBM, Cisco, Intel, the Linux Foundation, and others, has created a standards-based, open-sourced blockchain platform to accelerate adoption and the development of surrounding services. The Linux Foundation's Hyperledger initiative is intended to make blockchain real for business. IBM has made available 44,000 lines of code to the Linux Foundation open source

project and is an active member in promoting blockchain fabric for business applications.

IBM is particularly focused on security, and is working within the Linux Foundation's Hyperledger Project to ensure that the Hyperledger fabric itself is designed to be self-verifying, immutable and corruption resistant. Furthermore, IBM is focusing its offerings on the subset of blockchain implementations that are limited to known and trusted partners who have been verified through an identity server. That is why Hyperledger adopts consortium/private distributed ledger technology (DLT) which is more suitable for business network than public DLT.

Blockchain fabric's base functions include Shared Ledger as a single source of truth, Smart Contracts for business logic, Security (cryptography) to make it tamper proof and Digital Assets as a Record repository. The IBM Blockchain, through Hyperledger project initiative, plan to add the following functions that improve significantly its ability to cover business needs including:

- Permission (Participants Identity)
- Private (un-linkable identity)
- Auditability (identity & ownership)
- Choice of Consensus method (Modular protocol)
- Confidentiality (permission control)
- Scalability through architecture and platform long term experience

The Linux Foundation's Hyperledger is intended to provide the most secure and available implementation of blockchain, suitable for major enterprises and their partners to build new trusted systems on.

The New Cloud Services for Blockchain: High Security Business Network (HSBN)

Hyperledger fabric is now available both as an IBM public cloud offering and as an on-premises self-managed technology that can be deployed on Linux (see fig. 2)

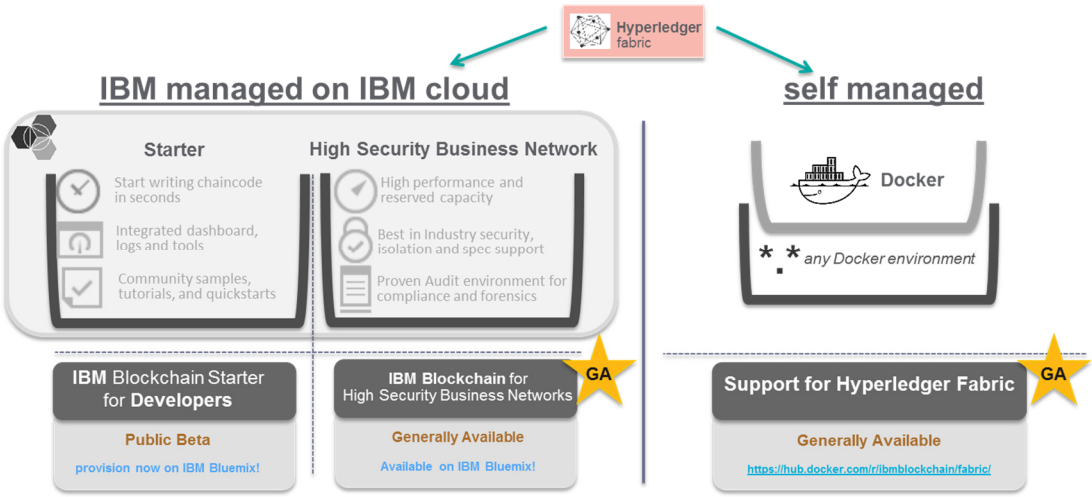

Figure 2: IBM Blockchain Offerings, all running Hyperledger fabric

IBM has two offerings that allow blockchain applications to run in a public cloud infrastructure, based on IBM Bluemix.

1) the starter plan, based on IBM Softlayer, our multipurpose cloud offering;
2) the new cloud service for blockchain, **High Security Business Network (HSBN)** that was originally announced as a beta on July 14th and made generally available on October 20th.

HSBN offers unique security and compliance value for cloud based production environments, and flexibility in the options for getting started with deployment of blockchain PoCs.

HSBN is based on IBM LinuxONE (see Fig. 3), that provides a unique set of features for blockchain applications, including:

- Isolated and highly secured environment, distinguishing HSBN from other cloud-hosted offerings;
- Operating system, fabric, and nodes which all exist in an IBM **Secure Service Container;**
- Delivery of performance optimization for peer-to-peer communication, availability, scalability, and encryption.

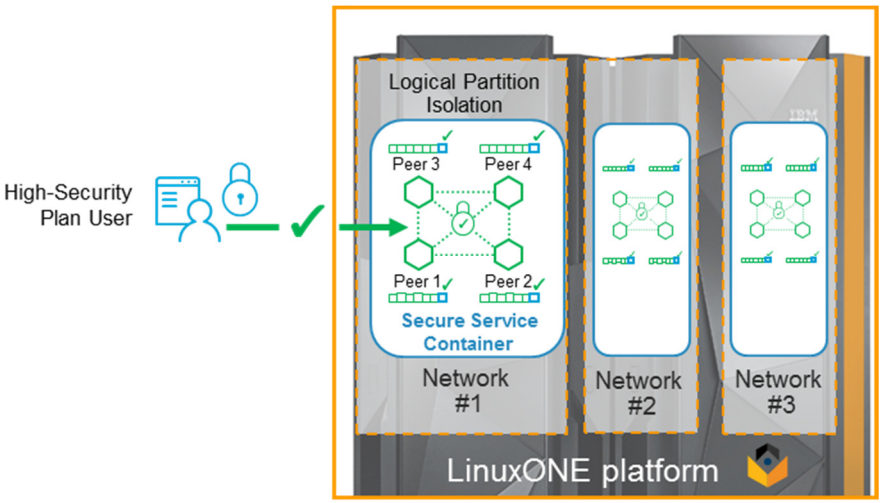

Figure 3: HSBN on IBM LinuxONE running isolated Blockchain networks in a multi-customers topology

Consequently, IBM clients can test their 4-node + certificate authority blockchain network in a high-security cloud environment that simulates a production deployment.

The blockchain HSBN cloud services offering has been Generally Available since October 20th 2016. Later in 2016 an on-premises version will also be made available.

The self-managed, on-premises version of Hyperledger, shipped in a Docker container and supported by IBM, was also made Generally Available on October 20th 2016.

LinuxONE or Linux on z Systems to Run Blockchain Applications On-Premises

Blockchain implementations require stringent qualities of service, particularly related to security, but also performance, resilience, scalability, and integration with existing systems. It is therefore no surprise that LinuxONE and z Systems have been chosen to deliver our premier offerings in this space. 71% of Fortune 500 companies use z Systems for their most trusted core systems, and the significant development effort that has gone into the platform can now be unleashed for new business critical applications.

Security

The protection of a blockchain service against tampering, and protection of the data against misuse, is directly relevant to its shared network business model. If the integrity of the blockchain is compromised, then that model falls apart.

IBM's LinuxONE has been designed to deliver the highest level of protection for blockchain implementations that depend on the level of trust that participants place in the deployment.

Separation between entities

A blockchain network consists of various independent entities hosted in a multi-tenant configuration. The first level of protection required, is the protection of the entities against each other – ensuring that there are no vulnerabilities between tenants.

If two competitors are both members of the same permissioned blockchain, it is imperative that their information be kept separate so they can only see and participate in activities in which they have common interest.

Certification of a platform's capability to maintain horizontal security between guests, is described by the Evaluation Assurance Level, or EAL standard. Most platforms rely on software-based isolation which can be compromised, so most operating systems and virtualization managers are only at EAL4; a moderate to high level of security.

IBM's LinuxONE takes isolation a step further, enforcing separation through firmware and hardware This technology, called logical partitioning (LPAR), delivers security at the **EAL5**, one of the highest commercially available certifications.

Vertical protection

LPAR technology will protect two entities from each other, but the network also needs protection from cybercriminals. One of the most serious vulnerabilities today

is the threat of attack through privileged user accounts. In this sort of vertical attack, all-access credentials granted to many IT staff are used to illegally access data or manipulate processing.

Blockchain implementations on LinuxONE are protected from vertical attack with technology that builds on LPAR. **IBM's Secure Services Container** (see fig. 4) is a special LPAR that encapsulates all software in a secure, signed, trusted appliance-like container.

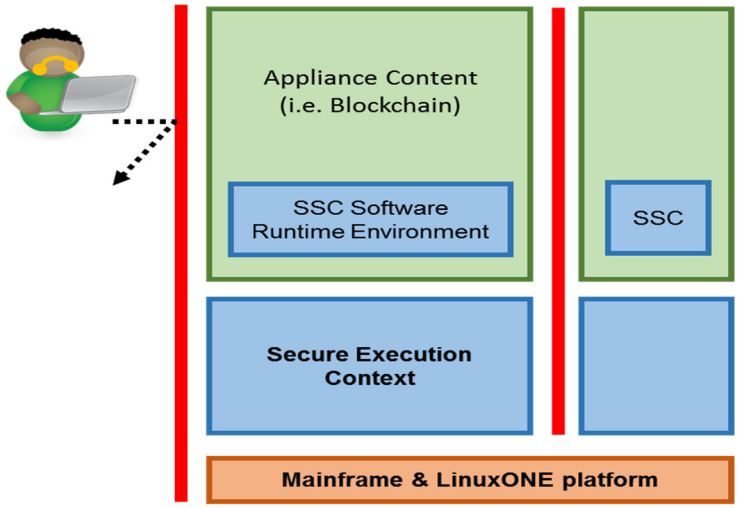

Figure 4: Secured Service Container partition anatomy on LinuxONE or Linux on z Systems

Firmware is used to validate that the software has not been tampered with, and prevents access to the partition once running. It is virtually impossible to manipulate a blockchain environment when installed in a Secure Services Container.

Secured Service Containers offers most advanced security features that allow:

- **Protection against misuse of privileged user credentials**: Blockchain operating environment and data are protected against access and abuse by root users, system administrator credentials and other privileged user access
- **Protection against malware** being installed
- **Protection of peers from one another** to prevent deliberate or unintentional leakage of information from one party's environment to another
- **Key safety**: identity, communication and data privacy are safeguarded in SSC. For our general availability release, key security will be enhanced by implementing "secure key" using our tamper resistant crypto card (See next section)

Protection of encrypted data

IBM z Systems LPAR technology protects against horizontal manipulation, and Secure Services Container technology protects against vertical manipulation. But it might still be possible for a privileged user to snapshot the data in a blockchain container. This data is encrypted and useless unless that user can access the encryption keys. Protection of these keys is therefore the lynchpin of a successful overall security scheme.

To deliver the highest level of security for cryptographic keys, LinuxONE uses dedicated, tamper-resistant crypto cards (Crypto Express5S card) that store the encrypted keys in a secure enclave within the hardware. This allows the IBM solution to achieve the highest standards of security compliance (certified to highest level FIPS 140-2 level 4)

IBM z Systems Provides Other Key Attributes for Blockchain Applications (Performance, Integration, and Availability)

Enabling Blockchain applications to be completely secure is critical but other service level considerations also need to be addressed, including performance, scalability, availability and integration with other applications.

Performance

Blockchain implements a new type of "system of record" but it shares many of the attributes required by transactional applications: high transaction rates up to hundreds of transaction/second; very fast consensus calculation; fast and scalable blockchain blocks read and write capabilities; cryptographic acceleration.

IBM's LinuxONE offering and Linux on z Systems specialty engines (IFLs) deliver the high capacity scale-up and scale-out processing required by large applications. It also ensures that high volumes of data can be delivered and processed through its scalable I/O system, very large memory space of 10 TB, with the fastest commercial microprocessor in industry, and the largest cache (z runs Open Source software 2x-3x faster than Intel-based platforms). It also leverages platform hardware with the **built-in on-chip accelerators** for blockchain encryption (hashing) and blockchain cryptography.

In addition, LinuxONE servers provide on chip hardware acceleration with CPACF (CP Assist for Cryptographic Functions) and SIMD (Single Instruction Multiple Data) that allow acceleration of encryption up to 32x ratio compared to software encryption.

Scalability

Sizing a future blockchain application can be a challenge: the number of peers will depend on the number of internal and external partners involved in the network and will also on the project maturity step. The consensus algorithm and cryptographic needs will impact resource consumption. In addition, the peak period may well be unpredictable due to transactions running outside the classic prime shift and so differ from typical office open hours.

IBM's LinuxONE offering as well as Linux on IBM z Systems provide unmatched scale-up capabilities that allow growth of applications with virtually limitless scale. With up to 141 core engines, 10 TB memory and 640 dedicated I/O processors LinuxONE can handle even the most demanding workloads. Increases of capacity can be

implemented without disruption and activated by microcode through Capacity on Demand (CoD).

Availability

Blockchain applications rely on a shared ledger that allows distributed workload on multiple nodes. However, as all peers participate in the network with consensus and ledger replication, a peer outage may impact the entire network (e.g. consensus may not be possible anymore), or, when recovering, a peer node may not be able to recover the shared ledger. While a node may be rebuilt this can take time and processing power, and during that period service levels may be impacted. As a result, it is far more preferable to ensure high availability than to rely on recovery.

IBM's LinuxONE and Linux on IBM z Systems offerings provide 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 isolate problems
- non-disruptive installation, upgrades, and maintenance of hardware and firmware avoiding outages
- automated failover capabilities that speed recovery and minimize system impact. This results in leading business continuity and disaster recovery solutions (GDPS) that ensure automated, reliable, and rapid recovery and enable planned site switches

With these capabilities, LinuxONE and IBM z Systems can enable the delivery of blockchain systems that require 24 by 7 availability.

Integration

Client networks of different ledgers must be able to call existing applications and refer to transactions on other Systems of Record. Examples might be SCM or ERP systems based on transactional middleware such as CICS, IMS, DB2, or batch systems.

On IBM z Systems, blockchain can be co-located with existing applications which are critical to each individual business in a network. Blockchain and current business processes can be optimally integrated through this co-location and through the exploitation of new technologies such as APIs and micro-services.

Co-location of a blockchain peer node with data and transactions on an existing z/OS system can reduce the latency of access to z/OS data by 20%, and increase throughput by more than 100%. Hipersockets and Shared Memory local communication provides the lowest latency communication between blockchain chain code/smart contracts applications and existing workloads on z/OS. Use of Hipersockets can also eliminate the need to encrypt traffic between blockchain and z/OS.

Conclusion

IBM's LinuxONE and Linux for z Systems offer the perfect platform for ultra-secure, flexible and adaptable blockchain applications that ensure trust and cooperation between business partners, and the confidence of their customers. z Systems have a proven track record for trusted IT systems in organizations across multiple industries.

IBM's High Security Blockchain Network is available as a cloud service, directly exploiting the advanced hosting characteristics of LinuxONE, and significantly lowering the entry price for new blockchain systems. Organizations have the choice of starting with this cloud offering, or implement blockchain applications on premises with LinuxONE or Linux on z Systems.

IBM is uniquely able to help you deliver successful blockchain implementations, based on extensive contribution to the Hyperledger project; consultancy expertise across multiple industries; and now with both cloud-based and on-premises solutions for blockchain application hosting.

Blockchain is the new wave – let IBM help you catch it.

Authors

Daniel Kohen, Executive Architect, WW zChampion Blockchain workgroup leader
Nick Dudeney, zClient Architect, WW zChampion Blockchain workgroup leader
Richard Gamblin, Digital Transformation Architect - European Technical Leader – WW zChampion API/Mobile workgroup leader

Thanks to the following people for their contributions to this project:

Andrea Corbelli, zSystems and LinuxONE Technical Sales Manager
Iain Neville, Executive IT Specialist IBM z Systems
Paul DiMarzio, Worldwide Portfolio Marketing Manager, z Systems Analytics, Cognitive, IoT & Blockchain
Bryan Gobin, Special Situations Strategist and Blockchain SME
Thomas Shepherd, Executive IT Specialist - IBM Certified Thought Leader - IBM zChampion - Mobile on z Systems Lead
Shuhichi Hayashi, zChampion, zCA (zClient Architect)
Kentaroh Ishimatsu, zChampion, IT Architect, IBM Systems HW Sales
Karsten Johannsen, Senior Manager Solution Sales - BDE Systems HW Solutions
Nigel Williams, API enablement and security IT Specialist, z Systems
Eric Phan, IT Specialist z Systems
Guillaume Hoareau, IT Architect, Blockchain and Mainframe Security