CLABBY ANALYTICS

Research Report

Why Blockchain/Hyperledger Belongs on LinuxONE

Executive Summary

This report assumes that the reader has a basic understanding of the Blockchain, a distributed ledger database, and some knowledge of the evolving distributed ledger standard known as Hyperledger. This report also assumes that your enterprise has made a strategic commitment to Blockchain and Hyperledger – and is now looking to implement a transaction processing environment based on these technologies.

Two Implementation Choices

From our perspective, there are only two implementation choices: 1) host it; or, 2) turn to a service provider.

1. If your enterprise chooses to host Blockchain/Hyperledger services, the biggest challenge your information technology (IT) organization will face is security. Your other challenges will involve performance tuning to handle large volume transaction processing, and improving governance.
2. If your enterprises chooses the service provider route, it will need to ensure that your service provider can deal satisfactorily with security, performance and governance challenges.

> ***For enterprises that choose to host their Blockchain environment, we strongly recommend deploying Blockchain solutions on IBM LinuxONE servers. For enterprises that go the service provider route, we strongly recommend that the service provider services be based on LinuxONE architecture.***

Three Reasons Why We Chose LinuxONE for Blockchain/Hypervisor Implementations

The reason that we recommend deploying Blockchain on LinuxONE architecture is based upon three factors:

1) LinuxONE offers the strongest system/application-level security in the industry;
2) LinuxONE is 2.3 times faster than its “industry standard” Intel competitors; and,
3) IBM has started to integrate its Watson cognitive computing technology with Blockchain and Hyperledger technologies – making it possible to automate and streamline certain transaction handling processes. Over time, we expect that Watson cognitive computing will become an integral part of advanced Blockchain/Hyperledger implementations.

In this *Research Report*, *Clabby Analytics* takes a closer look at the security, performance and cognitive advantages offered by IBM’s LinuxONE architecture. We conclude that there is no other architecture on the market like LinuxONE. With huge advantages in security and performance – and with Watson cognitive computing facilities – we expect LinuxONE to become the preferred implementation for large scale Blockchain/Hyperledger deployments.

Background

Blockchain is a transaction processing scheme originally designed to process cryptocurrency. The way it works is that maintains a list of records (blocks) that are linked (chained) to one another to create a transaction flow. Blocks in the transaction are timestamped, and can be viewed by all the intermediaries involved in the transaction. By linking and time-stamping these blocks a transaction can be initiated, recorded, viewed and approved – with money or value being exchanged at the end of the transaction. The beauty of this "open ledger" Blockchain approach is that the data in blocks cannot be modified – and transacting parties have a fully transparent view of the progress of the transaction. When mutual consensus (using pre-arranged contracts) is reached by all parties, and all deliverables along the flow of the transaction have been met, the transaction is concluded. Money or value is exchanged at the completion of the transaction.

> ***Think of blockchain as a immutable, transparent database that can help enterprises improve the security of their transactions while making transaction processing far more efficient. Blockchain helps reduce fraud, eliminate middlemen, streamline process flow and speed delivery and payment. It is a next generation transaction processing environment that has the potential to tremendously improve transaction process flow while significantly lowering transaction processing costs.***
>
> ***In other words, it changes the way that transactions will be handled in the future by not requiring a centralized authority to handle all the steps of conducting a transaction – instead, all the elements needed to conduct the transaction (such as contractual and payment information) becomes locked in a public record to a series of steps known as the Blockchain. Using this approach, computers can verify the validity of each transaction and create an immutable (untamperable, if there were such a word) record of a transaction's flow. Say goodbye to bills of lading; to courier services; to other middlemen; to various contractual services and to other time- and cost- consuming overhead (such as bank payment delays) related to processing today's transactions.***

Hyperledger is an open source "umbrella project" that seeks to augment the Blockchain ledger with a series of open source blockchains and related tools. Hyperledger blockchains are being designed to server financial, technical and supply chain markets – each market with its own consensus, storage and service models. Typically, these open source blockchains provide identity services, access control and contract agreement/administration facilities.

> ***Think of Hyperledger as an open source project that seeks to enrich Blockchain with the kinds of tools and facilities needed to serve enterprise-class customers while further streamlining process flow.***

With all of the benefits that Blockchain and Hypervisor deliver, there remain a few technical challenges with these technologies (see this blog by Peter Evans-Greenwood for further details). In short, blockchain performance is determined by network performance because networks limit the number of transactions in a block (becoming congested if block sizes are too big – and a chain of blocks can get very large); and they need to regulate the time between blocks (dwell time). Evans-Greenwood explains that there are several approaches being evaluated to workaround network shortcomings such as playing with parameters, reducing the size of transactions, packing more transactions into block, offloading some of the work from the main Blockchain – and so on. But in the end, *he argues that the "sweet spot" for Blockchain is in "low volume, high value exchanges"* – for instance in tracking diamonds through their supply chain as we describe in this blog, or in handling expensive disputes, also described in this blog.

> ***But what if these shortcomings could be mitigated by a specially designed system architecture? IBM's LinuxONE features an extremely large communications subsystem that can off-load a tremendous amount of communications processing from the central processor; it has very fast processors and accelerators that can speed up blockchain processing; it has the strongest cryptosecurity in the industry; and it has been designed to handle variable transaction workloads as compared with static workloads (Blockchains are variable workloads).***

Why Deploy Blockchain/Hypervisor on IBM's LinuxONE Server Environment as Compared with x86 Servers?

Why deploy Blockchain/Hypervisor on LinuxONE? The quick answers are: 1) superior performance; and, 2) unmatched security.

The Performance Advantage: It Has to Do With the Processor and a Superior Systems Design

Last year, *Clabby Analytics* wrote a report on LinuxONE architecture (found here) that described some of the major advantages this server environment has over x86-based servers. In short, those advantages include:

- A different type of processor that is extremely well suited to processing Linux workloads. LinuxONE is better at processing variable workloads than x86 servers due to significantly more cache and a concept known as "stacking";
- The LinuxONE processor can process certain workloads more quickly than x86 processors (currently LinuxONE processors can operate at 5GHz – Intel's 64-bit processors generally operate in the 2-3 GHz range – see this list);
- The LinuxONE environment has a huge communications subsystem (up to 667 dedicated cores) that can support up to 8,000 virtual machines;
- LinuxONE configurations can exploit up to 10TB of main memory; and,
- LinuxONE has accelerators for blockchain hashing and security.

> ***All of these design advantages lead to faster performance when processing variable Linux workloads, such as blockchains.***

IBM business partners are reporting impressive results when running the same containers and Linux database workloads on LinuxONE as compared to x86 architecture. For instance, it has been reported that Docker containers run on average 2X better than on Intel Haswell-based systems; MongoDB has been reported to run 2.4X faster when compared to x86 servers; and the Spark DB is seeing 50% better performance on LinuxONE as compared to traditional x86 architecture.

The Security Advantage: Crypto Hardware

A few years back, *Clabby Analytics* described the alarming worldwide situation in computer fraud (see this report). We described fraud as one of the world's largest businesses. We claimed that "bad guy" individuals and organized crime organizations defraud enterprises and individuals of almost $3.5 trillion in revenue and saving each year – and this number is growing (it currently represents about 5% of the world's total gross national product). We also observed that these bad guys are well financed; they are not regulated; they are innovative and creative – and they only have to get one intrusion sequence right in order to defraud others (whereas enterprises and individuals cannot afford a single intrusion).

Cyber fraud has reached such an alarming rate that U.S. Army General Keith B. Alexander (the director of the National Security Agency [NSA] and chief at the Central Security Service [CSS]) has called cybercrime: "the greatest transfer of wealth in history" (see this article for more of Alexander's assessment of the worldwide fraud situation).

Implementing a Blockchain/Hyperledger transaction environment can help thwart cybercrime. Blockchain, by its very design, prevents tampering by disallowing modification of blocks. But much can be done on the systems and software infrastructure side to also reduce exposure from internal and external tampering.

From a security perspective, LinuxONE features:

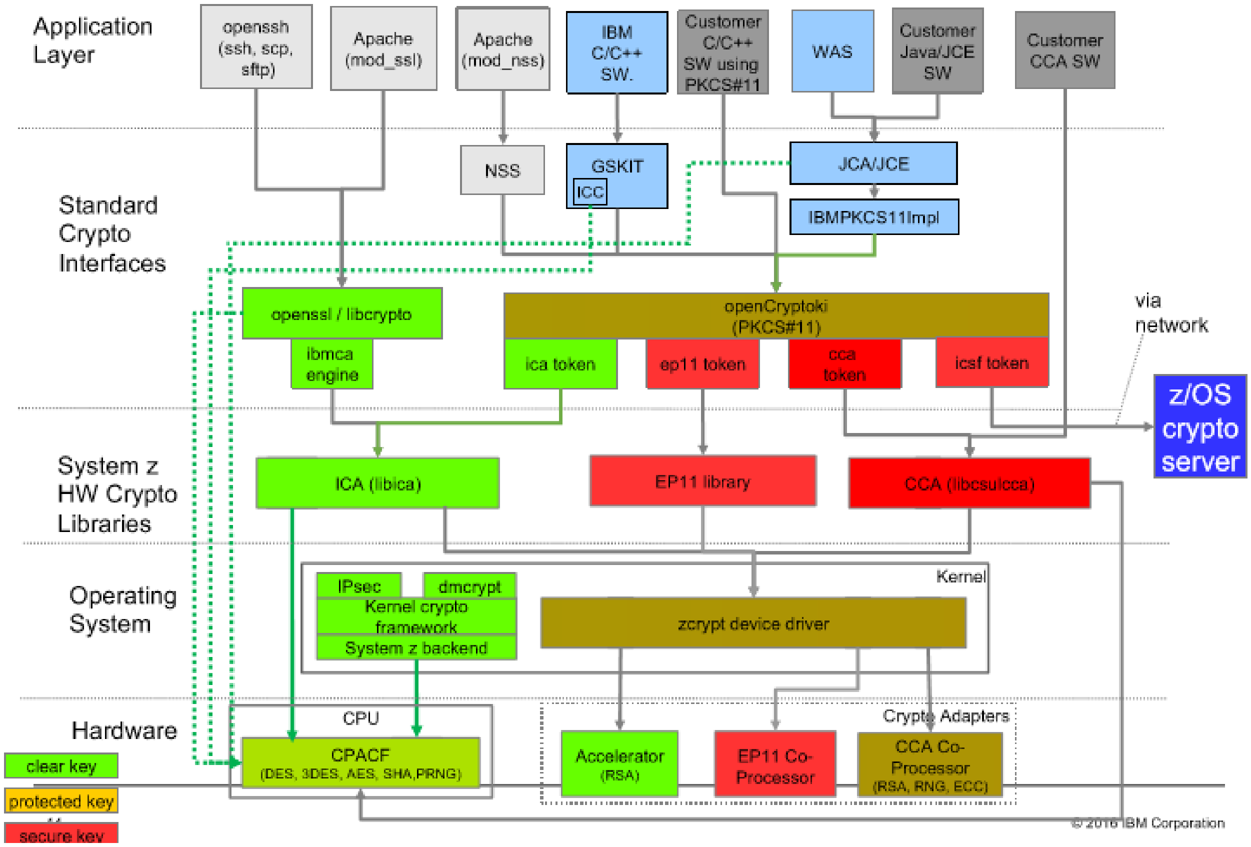
- Security level EAL Level 5+ – a security certification rating by Common Criteria based upon an international standard for hardware security. This rating is the highest rating of any commercially available system in the industry.
- FIPS 140-2, level 4 compliance – the highest compliance for cryptographic modules. No other platform in the industry has this compliance certification.
- Elliptic curve cryptography – an approach to securing public keys that greatly speeds security processing;
- Extensive Hardware cryptography – the processor in IBM's LinuxONE features logic that speeds security and hashing processing using CP Assist for Cryptographic Functions (CPACF) at the CPU level. Additionally, add-on Crypto Express 5S co-processor adapter cards protect secure key cryptography; and,
- Extensive software cryptographic features – LinuxONE offers an extensive array of software security features which can be found in the operating system, throughout the infrastructure, in crypto libraries, and at the application layer (see Figure 1 – next page).

It is important to note that as part of the security features of LinuxONE, security keys are placed into protected memory and placed into hardware secure modules in order to prevent access and tampering. IBM does not make it possible for code to take control of secured modules, and focuses on encryption protection to prevent administrative abuse. IBM's Secure Service Containers help protect code throughout the blockchain process flow – effectively encapsulating the blockchain into a virtual appliance, denying access even to privileged users

The benefits derived by using LinuxONE security as compared with typical Intel server designs include large costs savings (because security can be off-loaded from expensive CPU cycles); faster processing thanks to co-processor hardware accelerators; pre-certification to deal with regulatory requirements; and special functionality to deal with industry specific functions such as certain secure keys required in banking and financial applications.

There is no commercially available Intel Linux server design that offers as extensive security services combined with the huge communications subsystem of LinuxOne.

Figure 1 – LinuxONE Systems Crypto Stack



Source: IBM Corporation -- 2016

Watson for Cybersecurity

Human cybersecurity experts can no longer keep up with the volume, variety and level of sophistication of cyberattacks – whether those attacks come from external or internal sources. The sheer number of attacks are just too many; and the methods, approaches, scams and viruses are just too varied and are becoming even more sophisticated. Adding to this, data is now moving through amorphous clouds; or being accessed by mobile devices – making it even more difficult to protect data at rest or on the fly. And new technologies such as the Internet-of-Things (IoT) introduce new access points and vulnerabilities that can potentially be exploited by cybercriminals.

Given this backdrop, how can enterprises better secure data? The traditional approach has been to implement an enterprise security strategy that puts in place policies and procedures that ensure that data is handled in a secure fashion – and that puts in place measures (such as firewalls and data encryption) that ensure the integrity of the systems, networks and data. By putting in place policies that limit human errors, that help overcome social engineering exposures and that discourage the misuse of technology, security experts can better focus on the task of looking for and/or protecting against internal and external breaches.

The problems with the traditional approach, however, are:

- To keep up with the volume of internal/external cyberattacks, an army of highly skilled security experts are required;

- It's hard to find the deeply skilled individuals needed to fight cybercrime;
- Deep skill sets can be very costly;
- Humans may not be able to respond as quickly to vulnerabilities as systems; and,
- Humans may not find all vulnerabilities.

To address these problems, business communities around the world are collaborating – sharing attack and vulnerability information in an effort to catalog vulnerabilities and threats in real time. Security software vendors are also "analytics-enabling" their applications, making it possible for systems to analyze vast amounts of monitored data, looking for anomalies that can then be addressed by human security experts. And some security software vendors are starting to exploit machine learning and cognitive computing technologies that can take advantage of large "corpuses" of data to identify new threats or find new patterns – and, in some cases, recommending corrective actions.

Over the past year we've seen "cognitive computing" play an increasingly important role in security administration, and when combined with machine analytics, we see a new era of cognitive security evolving. In this new cognitive security era, humans will have an assistant – Watson for Cybersecurity. (Watson is IBM's moniker for its cognitive machine learning, reasoning, natural language processing environment that, when coupled with security analytics software, provides security administrators with the most potent set of tools on the planet for resisting incursion and protecting data).

The way that Watson for Cybersecurity works is that it taps into large corpuses of information (such as the 100,000 documented software vulnerabilities in the IBM X-Force Exchange database , as well as the 100,000 security research papers and 700,000 security blogs published each year) to derive new insights. Watson can understand, reason and learn about security terminology, topics, threats and more by analyzing structured and unstructured data (including data from security blogs, articles and reports) – and by formulating answers that can fill-in the gaps in the knowledge of even the best security administrators. Obscure data points that might not be recognized by humans can be found and analyzed. Watson's deep insights are presented to security administrators who determine the proper course of action to remediate situations or reduce exposure.

IBM has branded its security operations center/Watson for Cyber Security offering as the "Cognitive SOC". And it is within the Cognitive SOC that Clabby Analytics expects much of the groundbreaking security activity in the industry to take place over the next decade.

As we look back at IBM's efforts in the security marketplace over the past few years, we find that the company has led industry efforts to collaboratively tackle cybersecurity problems. IBM has led the industry trend toward analytics-enabling security software. IBM has invested heavily in building a next-generation cognitive computing environment that is making it possible for systems to assist security experts in the performance of their duties. Further, IBM has introduced several security Software-as-a-Service (SaaS) and managed service offerings that make it easier for enterprises of all sizes to more easily implement enterprise-class security. And IBM has worked inclusively with over four hundred 3rd party security vendors to help build a rich portfolio of security offerings.

One last thing on Watson as it relates to Blockchain. As transactions take place across various domains, they run into dozens or perhaps hundreds of regulations that must be addressed. Watson now offers a regulatory service that can help streamline the complicated problem of dealing with regulations. The Blockchain story – LinuxONE combined with automated Watson regulation services – will be difficult for other vendors to mimic and overcome.

The Blockchain Service Provider Route

Several previous sections have described the benefits of deploying Blockchain/Hyperledger on LinuxONE architecture. In our opinion, due to the communications subsystem and security extensions of this architecture – and due to current and forthcoming Watson extensions – we believe that it should serve as an essential building block for building the blockchains of the future. Accordingly, we believe that if an enterprise takes the service provider route to build blockchains, the underlying infrastructure that that service provider should use should be based on LinuxONE.

Last month, IBM introduced “Blockchain Services for Hyperledger Fabric v 1.0 on IBM Cloud” – a blockchain service that makes use of the open source Hyperledger Fabric to provide blockchain services to its customers. Deployed on an IBM public cloud, this offering represents the first commercial deployment of Blockchain/Hyperledger as a service.

With this service as an underpinning, developers can quickly build production blockchain networks – using underlying LinuxONE secure servers as a basic building block. As expected, the new Hyperledger functionality focuses on helping enterprises build enterprise-grade blockchain networks that can quickly scale as new members join their blockchains. Transaction rates of greater than 1,000 transactions per second are now being reported – as Clabby Analytics expects this number to greatly accelerate over the next few years with new hardware introduction by IBM.

Note that the IBM Cloud was first-to-market with High Security Business Network services for regulated environments. Customers running Blockchain on the IBM Cloud now include Everledger, Walmart, the Bank of Tokyo-Mitsubishi UFJ and Northern Trust.

The reason that IBM’s secure cloud implementation is important is that Blockchains are, to quote IBM, “only as safe as the infrastructures on which they reside. IBM's High Security Business Network offers the world’s most secure Linux infrastructure that integrates security from the hardware up through the software stack, specifically designed for enterprise blockchains.”

IBM’s secure cloud environment helps protect Blockchains from insider attacks – and takes advantage of LinuxONE security to prevent the leakage of information from one party's environment to another; protect encrypted data for storage of cryptographic keys; and offer a highly-auditable operating environment.

Enterprises considering going the Blockchain/Hyperledger service provider route should look closely at the Blockchain/Hypervisor LinuxONE-based services offered by IBM via its secure cloud environment.

Summary Observations

There is a natural inclination by IT managers to gravitate toward Intel architecture when deploying Blockchain. Probably 90% of all Linux on servers has been deployed on Intel-based architecture. Plus, most of the blockchains built to date have been run on distributed Intel servers processing micro crypto transactions.

But Blockchain is moving into a new marketplace – a higher end, higher value marketplace that requires extremely high reliability, scalability and super strong security. And these requirements dictate that a more powerful, more secure, more scalable, more reliable and faster architecture be deployed to support lengthy and complex, high-volume blockchains.

It is quite possible to build a high-volume, Intel-based blockchain environment. But LinuxONE would likely outperform that environment by a factor of at least 2:1. And all of the extra work needed to offer as secure an environment as LinuxONE could cost tens of thousands to hundreds of thousands of dollars – while also opening the door to new vulnerabilities due to a plethora of access points.

When it comes to deploying Blockchain/Hyperledger, enterprises have a few choices to make: 1) build their own blockchains on Intel architecture and subject themselves to lesser performance and less security; 2) contract blockchain services from a service provider that operates it on Intel servers (again subjecting themselves to lesser performance and security); 3) build on a turn-key LinuxONE environment; or, 4) buy services on a LinuxONE-based cloud.

> ***With a huge communications subsystem; with best-in-class security; with Watson cognitive computing extensions; with a strong commitment to the open source Blockchain/Hyperledger effort; with industry leading performance; with a Blockchain/Hypervisor service delivery mechanism based upon IBM's secure cloud – all based on IBM's LinuxONE architecture – Intel-biased IT executives should have a hard time justifying the deployment of blockchains on Intel server hardware.***

Clabby Analytics
http://www.clabbyanalytics.com
Telephone: 001 (207) 239-1211

Clabby Analytics is an independent technology research and analysis organization. Unlike many other research firms, we advocate certain positions — and encourage our readers to find counter opinions —then balance both points-of-view in order to decide on a course of action. Other research and analysis conducted by Clabby Analytics can be found at: www.ClabbyAnalytics.com.