PUND-IT™
INVESTIGATE - INTERPRET - INFORM

Marketplace Update

August 2017

- ## Ensuring Secure Enterprise Blockchain Networks: A Look at IBM Blockchain and LinuxONE

  By Charles King, Pund-IT, Inc.

Pund-IT, Inc.
Hayward, CA
U.S.A. 94541

Contact:
charles@pund-it.com
Ph: 510-909-0750
www.pund-it.com

Ensuring Secure Enterprise Blockchain Networks

A look at IBM Blockchain and LinuxONE

By Charles King, Pund-IT, Inc.

Introduction: The Security Landscape and Cyber Threats

Many organizations and business people feel overwhelmed by today's digital threat landscape. Along with longstanding problems, like fun-loving hackers attempting to breach companies' firewalls, there are also well-funded and well-organized cybercriminals to contend with, many of them supported by hostile states and government agencies.

Sometimes working separately, sometimes in collusion, these groups target tangible assets that can deliver immediate financial gain. But they also seek out less tangible secrets, intellectual property and anything connected to achieving strategic or competitive advantage.

However, those are just the problems lurking outside the gate. Inside, along with managing honest workers who can't keep their network credentials straight or curiosity in check, companies face acts of corporate espionage, the accidental corruption or destruction of information assets and partners who nose around on the sly for tidbits of valuable data.

Secure blockchain solutions

How can organizations best protect themselves? Seemingly overnight, a new class of technology – generically called blockchain – has emerged as *THE* solution for establishing and managing digital trust among parties that would normally require trusted third parties to conduct safe and secure business transactions.

The advanced encryption and hashing algorithms at the heart of blockchain promise to radically improve numerous well-known interactions, such as trade settlements along with new business opportunities, like the trusted provenance of diamonds. In fact, some think that blockchain may have solved central, crucial security problems due to the inherently decentralized architecture of its prototype application, Bitcoin whose Core network has not been violated.

However, while one can applaud blockchain's success against attacks to date, it is also important to acknowledge up front that no product or service can guarantee absolute security. That is because by their nature, network connected solutions supporting individual and team interactions incorporate features and functions that act as common attack vectors.

That includes impressive emerging technologies, such as blockchain networks. But at the same time, examining those risks and what vendors are doing to address them reveals that some IT offerings are better than others for security-minded organizations.

High among those are private blockchain networks such as the IBM Blockchain Platform, based on IBM's LinuxONE platform, and the Linux Foundation's Hyperledger Project. This report will consider some of the most common reasons for and modes of cyberattack that businesses currently face, along with how networks built on IBM Blockchain, supported by IBM's LinuxONE, can help stymie and even thwart those attacks.

Cyberattack modes and motivations

Let's start by considering how and why attacks occur. Generally speaking, there are two common modes or vectors for cyberattack; *attacks on the network* and *one-on-one attacks*.

Attacks on the network can be launched from anywhere, and typically involve the misuse of stolen network credentials by individuals or groups outside the organization or by privileged insiders. *One-on-one attacks* typically occur internally and are launched by individuals or groups with access to legitimate credentials.

So far as motivations for network attacks, monetary gain leads off the list with tangible assets, like bank and credit card accounts that can be manipulated for cash payments or purchases among the highest profile targets. In fact, the IBM X-Force Threat Intelligence Index 2017 report found that the financial services industry was targeted most frequently by cyber hackers in 2016 with more than 4 billion records leaked worldwide.

That exceeds the combined total of records leaked from the two previous years, making it likely that blockchain adoption in that sector will be robust. But cybercriminals also target intangible assets, including contracts, legal agreements and intellectual property whose value relates to the strategic or competitive advantage they can provide. These points also motivate attacks by nation states that steal defense-, trade- or politically-related data which can provide long term benefits.

However, the desire for monetary or competitive gain is also common "inside the firewall" where bent, greedy employees may be looking to exploit opportunities for the corporate equivalent of "stealing the silver." The same motivation is also sadly present among some presumably "trusted partners" and, in fact, may motivate blockchain network participants who attempt to spy on one another.

Security Breaches: Beyond cui bono

However, cui bono – "for whose benefit?" (or more popularly, "Follow the money") doesn't fully address all motivations for cyberattacks. For example, attackers can be driven by abstract or subjective goals, like animal rights activists who target researchers and organizations with whom they disagree. Attacks can also be politically-inspired to enhance the fortunes of specific individuals or parties, disgrace their opponents or inflict damage on a government target's systems, data legitimacy.

Business attacks can be similarly motivated. Disgruntled workers have disabled or damaged their employers' IT infrastructures. In another vein, politically-minded insiders, like Edward Snowden and Chelsea Manning famously stole and publicly exposed information in what they considered acts of conscience but it would be a mistake to think they were the first or will be the last such individuals.

Finally, accidental or unintentional breaches can be just as severe as those that are carefully planned. Since networks are incapable of determining whether an internal breach occurred purposely or accidently, resulting investigations are often a costly waste of time and effort that increase the workload and stress of already overextended IT staff.

In addition, unintentional breaches can be every bit as damaging as planned attacks. Consider, for example, what might occur if business agreements or records of employee disciplinary actions were accidently publicized. Inadvertent destruction or alteration of docu-

ments and files may also expose a firm to compliance violations, penalties and legal actions.

In short, the growing variety and complexity of cyberthreats behooves organizations to learn as much and do as much as they can to protect themselves.

Why blockchain?

Blockchain originally emerged as a way of securely enabling public bitcoin cryptocurrency transactions but since then its core Distributed Ledger Technology (DLT) has rapidly matured as a platform for business processes and applications. How is that progressing? Primarily through the Linux Foundation's Hyperledger Project, a rapidly growing commercial blockchain development resource supported by over 40 IT vendors.

There are other blockchain platforms, like Ethereum which was initially developed in early 2014 by a Swiss company, Ethereum Switzerland GmbH. Launched publicly in July 2015, Ethereum enjoys great mindshare among cryptocurrency advocates but the platform has been subjected to four hard forks, including one in June 2016 following a successful cyberattack on The DAO, which utilizes Ethereum for investment capital governance.

That event highlights how, even using innovative blockchain designs and technologies, organizations would be foolish to believe that these solutions are entirely invincible. No product or service can guarantee absolutely unbreakable security. Keeping that in mind, blockchain networks can still support approaches to and methodologies for managing complex trades and transactions that are superior to most traditional processes.

Permissioned DLTs

In the Linux Foundation's Hyperledger Project, blockchain is used to implement shared ledgers that approved participants can use to examine and interact with a DLT, and seamlessly integrate new blockchain transactions within an existing "system of record." Thus, these "permissioned" DLTs are capable of supporting the frictionless trade of high value tangible and intangible assets.

Permissioned DLTs support four key capabilities:

1. **Collaboration**—enables interested parties to easily organize systems of record
2. **Constraint**—leverages "permissioned" designs that only allow verified participants to read, write or validate transactions
3. **Consensus**—utilizes agreement protocols for vetting, admitting and removing network members, and enforcing policies agreed upon by all members
4. **Consistency**—uses protocols to prevent temporary deviations or "forks" in blockchain data that can lead expose participants to faulty or incorrect information

As a result, permissioned DLTs enable transactions and processes to be accurately maintained and managed efficiently. That does not mean that DLTs are immune to abuse. In fact, they are vulnerable to the same sorts of attack vectors as traditional workloads. However, those issues can be partly or largely addressed with platform-based security features and solutions.

An effectively secured permissioned DLT can qualify as a "central authoritative source of truth" since participants can transparently access and audit all transactions entered into

the ledger. That, in turn, allows blockchain network participants to certify the integrity of transactions and the entire ledger, and to agree to the ledger's trustworthiness. Along with securing business transactions, it also removes the costs and complexities of employing third party intermediaries, such as banks and legal counsels as keepers of trust.

Why IBM Blockchain and IBM LinuxONE?

Let's consider IBM's interest and involvement in blockchain, including its related solutions and services. Along with over 40 other vendors, the company supports the Linux Foundation's Hyperledger Project, contributes a significant amount of code to the effort and has representatives on the Project's technical steering committee.

Why is IBM so enthusiastic about blockchain? For both practical and strategic reasons. In a nutshell, the business and trade processes that can be supported with blockchain DLTs are squarely within IBM's enterprise business transaction sweet spot. In other words, IBM has the history and expertise needed to implement successful blockchain DLTs and numerous customers ready for those solutions.

But IBM also has something other vendors lack; the LinuxONE mainframe, a platform that seems as if it were designed for blockchain implementations.

What is it that makes IBM Blockchain, running on LinuxONE, ideal for blockchain DLTs? Introduced in 2015, LinuxONE was the first IBM mainframe solution designed from the bottom-up for Linux workloads. Though the company has supported Linux on mainframe systems since 2000, those workloads typically ran on dedicated Integrated Facility for Linux (IFL) co-processors supported by the z/OS operating system and z/VM virtualization.

In contrast, LinuxONE systems can be ordered with Red Hat, SuSE or Canonical Ubuntu operating environments, and support both z/VM and KVM virtualization. Along with delivering the same business-critical reliability, availability and scalability (RAS) capabilities that made the IBM mainframe an essential platform for thousands of enterprises.

Additionally, blockchain is an exemplary cloud workload. While Microsoft Azure and Amazon AWS both offer blockchain-as-a-service, only the IBM Blockchain Platform delivered by IBM Cloud incorporates unique technologies that specifically close key blockchain vulnerabilities. In short, IBM Blockchain on LinuxONE delivers mainframe-class hybrid and private blockchain cloud workloads. By building its IBM Blockchain Platform on LinuxONE servers, IBM Cloud offers customers the most secure platform for blockchain networks.

LinuxONE offers features that bolster the performance and security of IBM Blockchain networks, including;

- **Multi-tenant separation/isolation:** Since systems can host multiple blockchain networks, it's critical that participating entities' data and activities are kept separate and secure so they can only see and participate in approved activities. IBM achieves this isolation with logical partitions (LPARs) that support EAL5+ security, the highest commercially available security standard. The company's LinuxONE platform is the only blockchain platform that supports EAL5+.
- **Security against external attack:** A special form of IBM LPAR – the Secure Service Container – helps protect blockchain implementations against external attack by encapsulating all software in a secure, signed, trusted appliance-style container, sealed and vali-

dated against tampering. That protects blockchain DLTs against malware, misuse of privileged user credentials and deliberate or unintentional leakage of information. Because Secure Service Container support is driven all the way into the LinuxONE firmware, it is virtually impossible to defeat.

- **Cryptographic key safety:** IBM's LinuxONE further enhances security by encrypting all data in the blockchain container. In addition, encryption keys are stored in dedicated, tamper responsive Crypto Express5S cards which prevents privileged users from creating snapshots of blockchain data. As a result, IBM LinuxONE blockchain solutions can achieve the highest standard of security compliance for a Hardware Security Manager (HSM) – FIPS 140-2 level 4.
- **Integrated protection:** Some other blockchain vendors are beginning to talk about adding HSMs into their networks but following a piece-part approach to security leaves exposures unclosed. For example, if an administrator compromises the blockchain code, they could still invoke an HSM and decrypt sensitive data without actually seeing the keys. In stark contrast, combining Secure Service Container and encryption key protections puts IBM Blockchain on LinuxONE several steps ahead of the rest of the pack.

Given the inherent business value of blockchain networks, it's easy to see why IBM believes the technology is a critical strategic imperative for itself and its customers. In addition, taking the key features and capabilities of the IBM Blockchain Platform into consideration, it is difficult to see why enterprises serious about implementing maximally secure blockchain DLTs would use any other platform.

Everledger – The case for IBM Blockchain and luxury goods

What does a blockchain DLT using I,the BM Blockchain Platform, anchored by LinuxONE, look like in real world applications? UK-based Everledger, a start-up that uses the IBM Bloackchain Platform to manage and track the provenance of diamonds is an example with a particularly high profile. The company has won numerous awards for the innovation and business value of its solutions, and Everledger CEO Leanne Kemp is a regular keynote presenter at industry trade shows, including IBM Edge 2016 and InterConnect 2017.

What are the problems that Kemp and Everledger are tackling? Illegal activities that reportedly cost the diamond industry billions of dollars annually, including misidentification of stones, upscaled valuations and the alteration of financial statements. In addition, despite the insurance industry spending hundreds of millions of dollars per year on prevention, nearly two thirds of fraudulent claims for stolen diamonds go undetected. The problem is that traditional paper-based diamond certification and ownership processes lack transparency, making it virtually impossible to verify and track the vast majority of transactions.

How does Everledger address this? By placing key information collected by certified diamond labs that constitutes a stone's "fingerprint" into its blockchain. That data includes the serial number and what are called the "four Cs) (cut, clarity, color and carat weight), plus 40+ pieces of meta data and high-resolution photos which are then linked to the laser inscription found on the girdle of the diamond. Along with uniquely identifying stones, the company also stores diamond identity, ownership and movement data on its global, digital ledger. To date, Everledger has digitized and certified over 1 million diamonds.

There are also thornier problems where Everledger's solutions provide significant value. Diamonds are among the most valuable and portable of the "conflict" or "blood" minerals mined and processed in countries, including Sierra Leone, Liberia, Angola, the Republic of Congo, Côte d'Ivoire, the Central African Republic, and the Democratic Republic of Congo. There, corruption and civil war have resulted in the enslavement of thousands of adults and children who are forced into mining work in unspeakable conditions.

The Kimberley Process, an international organization founded in 2000 to oversee the diamond trade and certify legitimate sales, has been plagued by counterfeiters whose fake certificates have been used to sell blood diamonds and fake stones. At IBM Edge 2016, CEO Kemp unveiled a new Everledger platform based on the IBM Blockchain Platform to digitally certify diamonds traced through the Kimberley Process.

While diamonds have provided rich ground for Everledger's initial success, it doesn't intend to limit itself to precious stones. Indeed, the company's blockchain DLTs can provide ideal platforms for certifying a wide variety of luxury goods, including art works, designer clothing, accessories and jewelry that are actively counterfeited. Over time, Everledger's IBM Blockchain Platfrom DLT environments could also be applied in pharmaceuticals, high end manufacturing and other areas where authenticity is critical for achieving and delivering expected results.

In other words, for Everledger and its CEO Leanne Kemp, diamonds aren't forever – they're just the beginning.

Final analysis: The Power of a Secure Blockchain

The continuing technological evolution of cyberthreats and the threat landscape can be both costly and potentially disastrous for targeted individuals and organizations. However, Everledger's example points to threats of a different nature, where traditional transactional processes are being twisted and gamed to benefit untrustworthy individuals at the expense of an entire industry, along with the thousands of adults and children enslaved in "blood" diamond mining.

The fact that blockchain DLTs can help address and correct these scenarios points to the remarkable power and flexibility of the technology. But a blockchain network is only as secure as the hardware and software that provides its foundation. Though numerous vendors and cloud providers offer blockchain solutions, the IBM Blockchain Platform based on IBM's LinuxONE and delivered by IBM Cloud offer unique features and technologies that make them the market's most secure blockchain offerings by virtually any measure.

Organizations interested in exploring the value of blockchain technologies, concerned about countering cyberthreats to key processes or determined to maximally secure their most valued assets would be well-advised to consider IBM's Blockchain Platform service on LinuxONE systems.

About Pund-IT, Inc.
Pund-IT™ (www.pund-it.com) emphasizes understanding technology and product evolution and interpreting the effects these changes will have on business customers and the greater IT marketplace.