November 19, 2016

REPORT: TREND

Protecting Private Distributed Ledgers

As Distributed Ledgers Evolve beyond Bitcoin, Security Becomes More Complex and More Subtle

Steve Wilson

Vice President and Principal Analyst

Content Editor: R "Ray" Wang

Copy Editor: Maria Shao

Layout Editor: Aubrey Coggins

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A whole new branch of Information and Communications Technology (ICT), Distributed Ledger Technologies, or DLTs, was spawned by the advent of blockchain. Designed at first in support of Bitcoin, blockchain has evolved rapidly beyond the original rarefied needs of cryptocurrency, to meet mainstream privacy and regulatory demands.

Data protection for private DLTs is more subtle and more complex than for public blockchains. This report outlines the major security factors for private DLTs – access controls, encryption and operational hygiene – so as to help businesses adopting these novel technologies make robust purchase or investment decisions.

This report assumes the reader is familiar with blockchain and DLTs, has arrived at a decision to implement them, and is now researching how best to build or buy DLT services. The previous Constellation reports "Beyond the Hype: Understanding the Weak Links in the Blockchain" and "How to Conduct Effective Blockchain R&D" address upstream blockchain evaluation and requirements analysis. And "How to Secure Blockchain Technologies" provides a more detailed security analysis.

Business Themes

 Safety and Privacy

 Matrix Commerce

 Technology Optimization

FROM CRYPTOCURRENCY TO MAINSTREAM BUSINESS

Distributed Ledger Technologies (DLTs) had a somewhat chaotic beginning. The original blockchain was expressly designed to solve a very special problem: how to avoid Double Spend of electronic cash without any digital reserve bank or other administrator. Normally, nothing stops digital data being copied and relayed, and so it's intrinsically hard to prevent electronic cash being spent twice. This problem was long regarded as unsolvable, so the emergence of blockchain proved inspirational for security professionals.

At the same time, a number of non-technical factors – blockchain's overt political themes, the mystery surrounding its creator Satoshi Nakamoto, and the promise that cryptocurrency might disrupt the banking industry – all fueled a broader enthusiasm for blockchain. Businesspeople have been genuinely attracted by blockchain's low infrastructure cost, low friction, and high resilience. And thus, we've seen a tremendous wave of innovation, with multiple blockchain variants and models, and a great many new algorithms coming out in just a few years.

The basic blockchain was premised on a few unusual conditions. They are:

- **Anonymity:** A design objective of Bitcoin is anonymity; the blockchain protocol is designed for cash transactions where payor and payee need to know nothing whatsoever about one another. On the other hand, most business payments demand some identification, for fraud control or regulatory purposes.

- **Complete Transparency:** All transactions executed on the blockchain remain publicly visible for all time so that the network can reach agreement on the state of the ledger. The stark lack of privacy matters little in the utopian world of pure crypto-currency because payments are taken to be anonymous. But for most other use cases, a ledger needs additional layers of encryption.

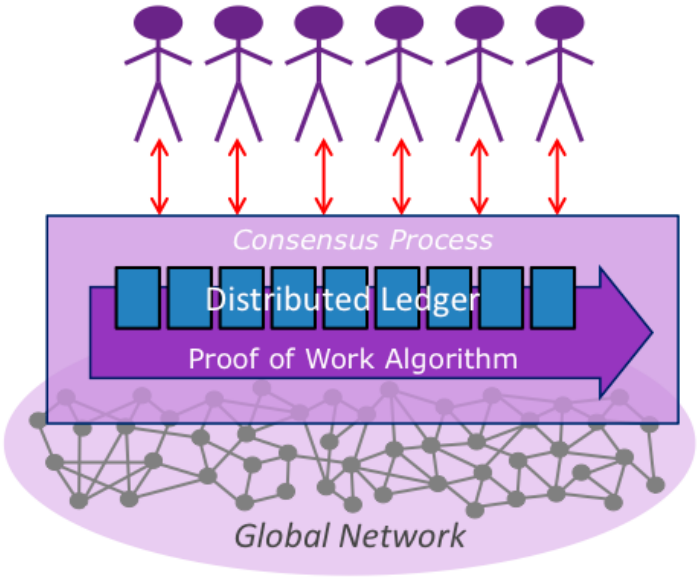
- **Being Permissionless**: No registration is required before one may start acquiring

and spending Bitcoin or establishing a Bitcoin mining node. There is no central administrator, much less a standardized Know Your Customer regime of conventional financial services. This is because Bitcoin is truly like cash; the only thing that matters is possession. Thus, the original blockchain is radically open. In a sense, it has to be, in order to foster the enormous scale needed to make it resistant to corruption. Yet, this is another fundamental feature at odds with most other use cases. The majority of private business needs private record keeping and privileged access for those who are authorized to write to the ledger.

To bring blockchain technology into the mainstream, there has been rapid acceptance of the need for *permissioned* blockchains and *private* blockchains (or private DLTs).

But marrying blockchain with conventional security measures is easier said than done. To a large extent, the founding assumptions of blockchain are also its core requirements because the security of blockchain – especially its redundancy and immutability – depends on its reaching a very large scale. So it has proven difficult to separate the properties of anonymity and transparency – they are inherent to the early algorithm and its pure e-cash use case. Furthermore, subtle side

Figure 1. The Original Blockchain Focused on Bitcoin



Source: Constellation Research

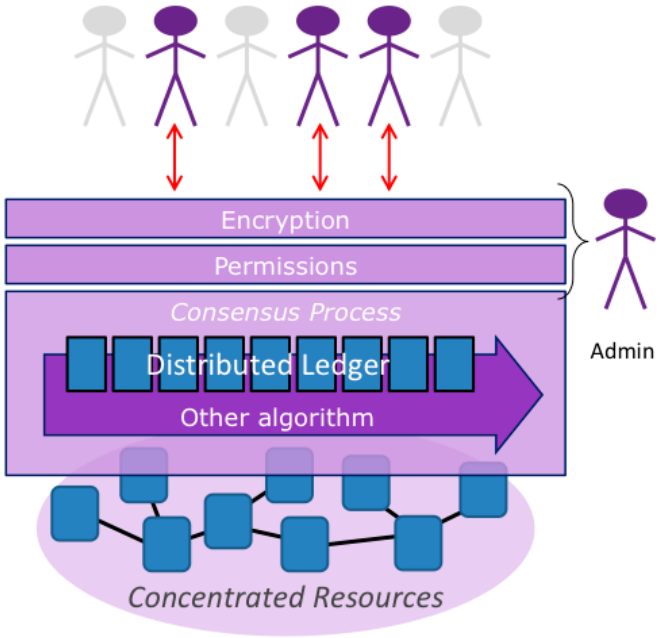
effects arise when permissions processes or key management structures are folded onto the public blockchain.

A clear lesson of the past three or four years is that advanced DLT research and development demands great care. Constellation has concluded that, for the majority of businesses seeking to deploy blockchain or Distributed Ledgers, the best course of action is to work with the big "ledger labs". As IBM's Global Head of Blockchain Aron Dutta told the Constellation Connected Enterprise conference in October 2016, "mistakes will be made" as DLTs continue to evolve.

SUBTLETIES IN PRIVATE DLTS

In more complex private (or permissioned) DLT applications, the interactions between security layers and the underlying consensus algorithm are subtle, and great care is needed to manage side effects. Indeed, security needs to be rethought from the ground up, with key management for encryption and access control matched to often new consensus methods appropriate to the business application. With private ledgers, the computation is still distributed, similar to the original public blockchain, but tends to be more concentrated,

Figure 2. Permissioned Distributed Ledger for Business



Source: Constellation Research

often using resources controlled by a DLT service provider.

Here are some important security points to consider:

Permissions and Access Controls

When deployed for private business, a DLT must implement access controls – including an identity manager – to determine who has the appropriate privileges to write to the ledger. The benefit of the original distributed blockchain architecture is diluted when third parties are required to oversee aspects of the end-to-end security. Private ledgers can bring single points of failure, which need to be managed through traditional defense-in-depth strategies. Constellation also advises that second- and third-generation consensus algorithms may be better suited to permissioned ledgers than the earlier "Proof of Work" developed for Bitcoin.

Encryption

When sensitive data needs to be masked, then an additional key distribution and management layer is required. Encryption key management must not be underestimated. In effect, it requires a foundation of trust (or trusted administrative processes) of the sort that Bitcoin functions without, thanks to the massively distributed Proof of Work algorithm. So again, when off-chain processes are factored into a private DLT, more attention to the consensus core is required.

Concentration

Private DLTs become much more concentrated compared with pure blockchains and, therefore, need careful system administration to protect against insider threats and to control fraud. The nodes of a private blockchain, as devoted to enterprise applications, will demand greater security attention than is required with public blockchains. Tamper resistance and immutability are more easily compromised, for it simply becomes easier for an attacker to take

control of a majority of the nodes in the smaller underlying private networks.

To protect private DLT nodes, Constellation recommends Hardware Security Modules (HSMs) certified to Common Criteria EAL4+ or FIPS 140 level 3+. All cryptographic algorithms in use should be explicitly included in the HSM certification. Commensurate personnel security standards are needed at private DLT service providers to mitigate against insider attacks.

CHOOSE YOUR DLT SERVICE PARTNERS WISELY

It's still early in the DLT evolution and there are significant risks for any organization that tries to go it alone on its blockchain journey. For this reason, Constellation recommends that most enterprises seeking to use Distributed Ledgers should partner with large DLT research labs with the security skills and resources to deal with the unfolding complexity.

The first-generation blockchain was devoted to an atypical use case - pure anonymous cryptocurrency. Security was baked entirely into the original Bitcoin protocol. But the emerging private DLT fabrics involve many more dimensions. Bank-grade hosting and hardware security will be essential to ward off attack from outsiders, insiders, and potentially malicious code introduced into hosted blockchain elements. Early adopters must look for distributed ledger hosting environments that support the highest-grade node security and key management available. Above all, the best DLT partners will have the expertise to refine the consensus algorithms as the use cases become more and more mainstream compared with the ideal world of the first-generation blockchain.

CONSTELLATION RESEARCH PANEL

We gratefully acknowledge the following reviewers of this report:

- Paul T. DiMarzio, IBM, Worldwide Portfolio Marketing Manager, z Systems Analytics, Cognitive, IoT & Blockchain
- Mance Harmon, Ping Identity, Head of Architecture

Steve Wilson

Vice President and Principal Analyst

Steve Wilson is Vice President and Principal Analyst at Constellation Research, and leads the firm's work in Digital Safety and Privacy. A 20-year veteran in cyber security, Wilson is one of the world's most original thinkers in digital identity.

Wilson is a researcher, innovator and R&D leader with 30 years of experience in information technology. Since 1995, he has been dedicated to digital identity and privacy, responsible for numerous breakthroughs in smart technologies, identity management, privacy enhancing technologies and national identity frameworks. Wilson has been awarded nine cyber security patents, and is currently undertaking a Ph.D on the evolution of identity ecosystems.

Wilson advises Chief Information Security Officers, Chief Privacy Officers, strategists and ICT architects seeking to optimize data protection in complex digital systems. He provides Privacy Impact Assessments, builds robust security strategies, and helps architect identity for Big Data, Internet of Things and cloud rollouts.

His coverage areas include: Digital Safety and Privacy, Data to Decisions and Consumerization of IT.

@Steve_Lockstep | www.constellationr.com/users/steve-wilson

https://au.linkedin.com/in/lockstep

ABOUT CONSTELLATION RESEARCH

Constellation Research is an award-winning, Silicon Valley-based research and advisory firm that helps organizations navigate the challenges of digital disruption through business models transformation and the judicious application of disruptive technologies. Unlike the legacy analyst firms, Constellation Research is disrupting how research is accessed, what topics are covered and how clients can partner with a research firm to achieve success. Over 350 clients have joined from an ecosystem of buyers, partners, solution providers, C-suite, boards of directors and vendor clients. Our mission is to identify, validate and share insights with our clients.

Organizational Highlights

- Named Institute of Industry Analyst Relations (IIAR) New Analyst Firm of the Year in 2011 and #1 Independent Analyst Firm for 2014 and 2015.
- Experienced research team with an average of 25 years of practitioner, management and industry experience.
- Organizers of the Constellation Connected Enterprise – an innovation summit and best practices knowledge-sharing retreat for business leaders.
- Founders of Constellation Executive Network, a membership organization for digital leaders seeking to learn from market leaders and fast followers.

www.ConstellationR.com

@ConstellationR

info@ConstellationR.com

sales@ConstellationR.com

San Francisco | Belfast | Boston | Colorado Springs | Cupertino | Denver | London | New York | Northern Virginia
Palo Alto | Pune | Sacramento | Santa Monica | Sydney | Toronto | Washington, D.C

constellation RESEARCH