

the *Availability Digest*

www.availabilitydigest.com
[@availabilitydig](https://twitter.com/availabilitydig)

How HPE is Making Blockchain Resilient¹

July 2017

Blockchain. Oh, no! Another new technology about which I know nothing. That statement summarized my feelings about blockchain until I heard a presentation from HPE's Matt Riesz at the May 2017 NYTUG meeting in Berkley Heights, New Jersey (USA). Matt is a superb speaker. His clear, concise explanation of how blockchain works elevated my understanding from total ignorance to a "not nearly as dumb as I thought I was" level. This article is based on Matt's presentation.



Matt also explained how HPE has partnered with R3, the provider of the Corda open-source distributed ledger technology (DLT) platform, to bring resilience and scalability to DLT applications. R3 leads a consortium of more than 70 of the world's largest financial institutions in the research and development of blockchain database usage within financial systems. It was the consortium's efforts that brought Corda into fruition.²

At the recent HPE Discover conference in Las Vegas, R3 demonstrated Corda, now in public beta, running on Integrity NonStop.

What Is a Blockchain?

A blockchain is a secure, append-only distributed database that is created by a collection of untrusted or semi-trusted parties. The distributed nature of a blockchain allows parties to engage in transactions without a trusted central authority. A copy of the blockchain is made available to all involved parties.

Transactions are organized into *blocks*. Each block contains a timestamp and a link to the previous block. A checksum in each block header is calculated based on the block contents and on the checksum of the previous block. Thus, blockchains are inherently resistant to modification of the data within a block. Once recorded, the data in any given block cannot be altered retroactively without the alteration of checksums in all subsequent blocks. This makes blockchains suitable for the recording of transactions that must maintain their integrity. Oftentimes, users will ignore new transactions until several new blocks have been appended to the blockchain to ensure that the transactions they are accessing are secure.

Blockchain systems assume that some parties engaged in a transaction may be dishonest. These systems only need a majority of participants to be honest. Any party involved in a blockchain may create a new block to be added to the chain. However, all parties involved in the blockchain vote on any new block that is to be added. If a majority of the parties do not agree that the block is valid, it cannot be added.

¹ This article was originally published in The Connection and is republished here with the kind permission of The Connection.

² R3 has explained that Corda, although inspired by blockchain architecture, is itself not a traditional blockchain platform.

Marc Andreessen has said that the blockchain's distributed consensus model is the most important invention since the Internet itself. Marc is the co-author of Mosaic, the first widely used Web browser, and the co-founder of Netscape.

Others have said that the blockchain will transform value exchange as profoundly as the Internet transformed information exchange.

The First Blockchain Use – Bitcoins

Blockchains were introduced with *Bitcoins*. Bitcoin is a cryptocurrency. No physical bitcoins exist. Rather, transactions take place directly between users without an intermediary. The transactions are recorded in a public distributed ledger, a blockchain. Since the system works without a central repository, bitcoins are the first decentralized digital currency.



Bitcoins are stored in a digital wallet, which may be either in the cloud or on someone's computer. Bitcoins are totally anonymous. There is no need for either the buyer or the seller to provide identification. Only the digital wallet ID is exposed. People can transfer bitcoins with each other via their digital wallets using either mobile apps or their computers.

Bitcoins can be bought and sold on bitcoin exchanges. The largest bitcoin exchange, Mt. Gox, went belly-up in 2014 after hackers stole almost a million bitcoins from it.

Bitcoins currently move about USD \$185 million via 220,000 transactions a day. The total value of all outstanding bitcoins is approximately USD \$10 billion.

Blockchain's Rapid Evolution

Blockchain is effectively a Distributed Ledger Technology (DLT), and DLTs are transforming business models in the Financial Services Industry (FSI). FSI is making significant investments in proof-of-concepts to support blockchain business cases.

However, current DLT vendors cannot support scalable, enterprise-grade solutions. Their implementation models have proven to be too slow for rapidly evolving business and technology demands. They also are not mature enough at this time to meet the enterprise and governance requirements of security, risk, manageability, and performance, among other prerequisites. DLT technology must meet the pace of change required by an organization.

Hurdles to DLT Adoption

What is required is an open and modular application framework for the development of blockchain applications rather than the fragmented set of platform providers and point solutions that exist today. Performance, scalability, and resiliency are below enterprise standards with high numbers of single points of failure. These challenges must be met by robust blockchain foundational services such as accelerated smart contract virtual machines and highly available environments such as HPE NonStop servers. There is no blockchain-specific infrastructure or reference architecture at this time that provides a fault-tolerant environment to run blockchain workloads at scale.

What's more, the small startups that currently dominate the blockchain market do not integrate well if at all with existing technologies and standards. As such, it has been difficult to engage business units, partners, the industry, regulators, and others for support and funding.

The R3 Consortium

A major player in the blockchain world is R3. R3 is a distributed database technology company that leads a consortium of more than 70 of the world's largest financial institutions in research and development of blockchain database usage in the financial system.

The consortium's efforts have created an open-source distributed ledger platform called *Corda*. Corda is a distributed ledger in that the ledger is distributed across multiple platforms and shared with other participants. Each participant has at least the part of the ledger in which it has participated, and the participants collectively could assemble an entire ledger.

Corda is geared towards the financial world as it handles more complex transactions and restricts access to transaction data. Although it is inspired by blockchain databases and has many of the benefits of blockchains, it is not a blockchain. The aim of Corda is to provide a platform with common services to ensure that any services built on top of it are compatible with the network participants.

How HPE Can Help

One of the interesting aspects of blockchain is that it is by its very nature resilient to faults. If a node fails for any reason, all of the other nodes have a copy of the chain so it never goes away.

By comparison, Corda, being a SQL database, does have some possible fault-tolerant issues. For instance, if a node dies, so does its portion of the distributed ledger.

Enter HPE NonStop, which has both a highly resilient and high-performance database, SQL/MX, and a continuously available platform. HPE has announced that it has entered into a partnership with R3 to bring Corda to Mission-Critical HPE Systems.³ HPE and R3 will bring Distributed Ledger Technology to workloads that must run at enterprise scale. A proof of concept created in collaboration with HPE Labs, HPE Mission Critical Systems, and R3 has demonstrated R3 Corda running on the HPE Integrity NonStop platform, delivering the resiliency and scalability enterprise customers need as they bring their DLT applications into production.

Via such partnerships, HPE can accelerate the selection of blockchain applications based on business demands. It can enable Line of Business leadership to incorporate DLT solutions that will address enterprise business goals. As with any new technology, there are risks; but HPE is well-positioned to evaluate the challenges of a blockchain approach and to propose viable risk mitigations.

From the R3 perspective, HPE Integrity NonStop offers a proven reference architecture, one that delivers reliability, performance, and scalability improvements as compared to other platform implementations. HPE offers educational, advisory, and implementation services augmented by Blockchain-as-a-Service offerings. In addition to R3, it maintains a multi-platform ecosystem with partners such as Ethereum and Microsoft.

Ethereum is a full distributed blockchain implementation backed by a tradeable cryptocurrency. It offers availability with predictable performance and resilience. It uses accelerated cryptography, shared memory, and an enterprise-grade support ecosystem.

The Corda Distributed Ledger

HPE NonStop with R3 Corda uses an enterprise-grade message bus (HPE NSMQ) and a persistent data store (SQL/MX). It provides linear scaleout and is suitable for physical and virtual NonStop platforms.

³ [Just in – Exciting news about HPE and Blockchain](https://community.hpe.com/t5/Alliances/Just-in-Exciting-news-about-HPE-and-Blockchain/ba-p/6967334#.WVVnahPyui4)
<https://community.hpe.com/t5/Alliances/Just-in-Exciting-news-about-HPE-and-Blockchain/ba-p/6967334#.WVVnahPyui4>

Corda provides the fundamental services of a blockchain but is not itself a blockchain. A blockchain involves a specific architecture for implementing distributed ledgers. Corda has a different physical implementation. The storage method for Corda is ANSI SQL rather than blockchain. This allows the ledger to be queried with common query tools, though the data in the Corda ledger is encrypted. One would need the encryption key in order to query the data in Corda.

Corda does not require each state change to be broadcast to all nodes. Unlike blockchains, it is designed from the beginning as a distributed ledger to offer more robust and flexible storage of complete smart contracts.

With Corda, there is no unnecessary global sharing of data. Only those parties with a legitimate need to know can see the data within an agreement. Corda explicitly links human-language legal prose documents to smart contract code for choreographed workflow between firms without a central computer. It enables regulatory supervisory observer nodes. Transactions are validated by parties to the transaction rather than by a broader pool of unrelated validators.

A Corda smart contract is an agreement automated by computer code working with human input and control. The rights and obligations of the contract are legally enforceable, ensuring that the financial agreements are rooted firmly in law.

A Summary Comparison of Blockchain and Corda

The following table summarizes the comparative attributes of blockchain and Corda:

Property	Private Blockchain	Corda
Data replication	Broadcast to all bitcoin miner nodes	Only participant nodes hold data.
Data protection	Cryptographic chain of blocks	Cryptographic chain of records
Data structure	Flat/unstructured	SQL/structured
Reliability – platform	Transparent node failure	Node failure disruptive/outage
Reliability – data	Data corruption transparent	Avoided if using RAID
Scalability	Scale-up; no real scale-out	Scale-up and scale-out
Parallelism	Not fully used	Fully used
Transaction consistency	Eventual - BASE	Immediate – ACID
Consensus	BFT ⁴ & variations – system wide	BFT & variations – private
Transaction validation	Bitcoin miners	Notary and participants
Smart contracts	Add-on to architecture	Built into architecture – Java VM
Performance	Can be burdened by miner time	Potentially better than blockchain
Cryptocurrency	Bitcoin or other	None

Distributed Ledger Technology has applicability in several areas, including:

- Financial – funds transfers, clearing/settlement, brokerage, mortgage.
- Medical – record keeping/sharing.

⁴ BFT – Byzantine Fault Tolerance, the characteristic of a system that tolerates the class of failures known as the Byzantine Generals' Problem for which there is an unsolvability proof.

- Insurance – claims processing, document handling, liability insurance.
- Government records – property transfers, titles, licenses, elections/voting.
- Retail – gift cards, loyalty programs.
- Legal – digital notarizations, certificates, smart contracts.
- Education – records, grades, curriculum/course registration.
- Transportation – document tracking, digital signatures, fraud prevention.
- Energy – opportunities at electrical ‘grid-edge.’
- Libraries/documents/publishers – document handling and tracking, ties to payments.
- Smart contracts – two-party/multi-party.
- Controlled permissions – broad or restricted permissions for different party members.
- Provenance of creative assets – publicly verifiable registry (music, arts, patents).

Summary

R3's Corda is designed specifically for the Financial Services industry, a major consumer of Integrity NonStop's ability to quickly scale resources for real-time, high-volume transactions. R3 brings to the new partnership its expertise in distributed ledger and blockchain technologies. What it relies on from HPE is NonStop's acclaimed fault-tolerant environment, an impressive suite of HPE and partner solutions, and a large customer base that looks to HPE for assistance as new DLT applications are brought into production.

We once again want to thank HPE's Matt Riesz for use of his blockchain slide presentation as the foundation of this article.