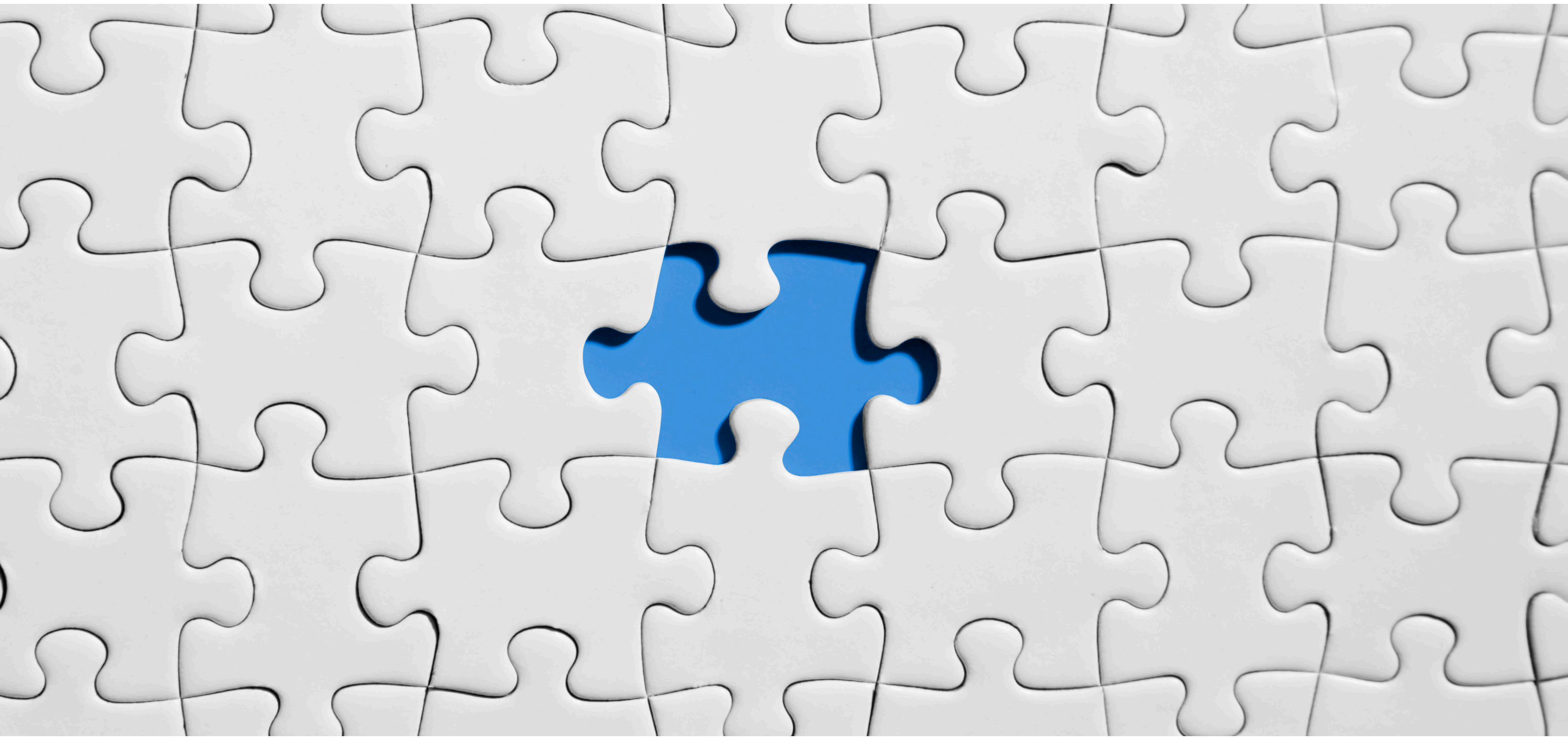
POWERCHAIN – BASED ON BLOCKCHAIN 3.0



Rajasekhar Nannapaneni
Sr Principal Engineer, Solutions Architect
Dell EMC
Rajasekhar.nannapaneni@dell.com

Knowledge Sharing Article
© 2020 Dell Inc. or its subsidiaries.

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

List of Figures

Glossary

Abbreviation	Full Form
BC	Blockchain
SC	Smart Contracts
DLT	Distributed Ledger Technology
IP	Intellectual Property
GPU	Graphics Processing Unit
CPU	Central Processing Unit
FPGA	Field-Programmable Gate Array

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Abstract

The evolution of Blockchain technology is turning into a revolution! We are unquestionably in the midst of a major drift carried by the Blockchain. A technology which started with crypto currencies has expanded into Blockchain 2.0 in the Enterprise space and is now evolving into the mobile and edge space as Blockchain 3.0.

Large enterprises are experimenting with this technology within the walls of their company. It is time to formulate solutions and products in the direction of Private Blockchain that could leverage the combination of use cases of public Blockchain and Blockchain on private enterprise infrastructures.

This Knowledge Sharing article emphasizes Private Blockchain solution –termed as "PowerChain" for Enterprises. This solution is formulated using various Dell Technologies products and solutions in combination with some of the leading technologies that could pave way for a Hybrid Blockchain solution thereby addressing some of the unique use cases.

Introduction

One of the disruptive technologies in today's world, Blockchain is a standard and transparent distributed ledger technology which has become quite popular with crypto currencies as blockchain 1.0. This distributed nature of blockchain has not only made it popular but also applicable to quite a few use cases.

The advent of Ethereum has taken blockchain to the next level to private enterprises as blockchain 2.0 and the recent advances of Hyperledger has led to opportunities in edge computing. This article aims to bridge the gap between private and public blockchain technology.

What is Blockchain?

Blockchain is an immutable distributed ledger technology which can be used as legal proof of record. A blockchain contains information in the form of a chain of blocks. In 1991 this technique was developed to timestamp digital documents so that tampering will be impossible, and no one, i.e. a notary, can backdate them.

In 2009, Satoshi Nakamoto adapted blockchain to created Bitcoin, a digital cryptocurrency.

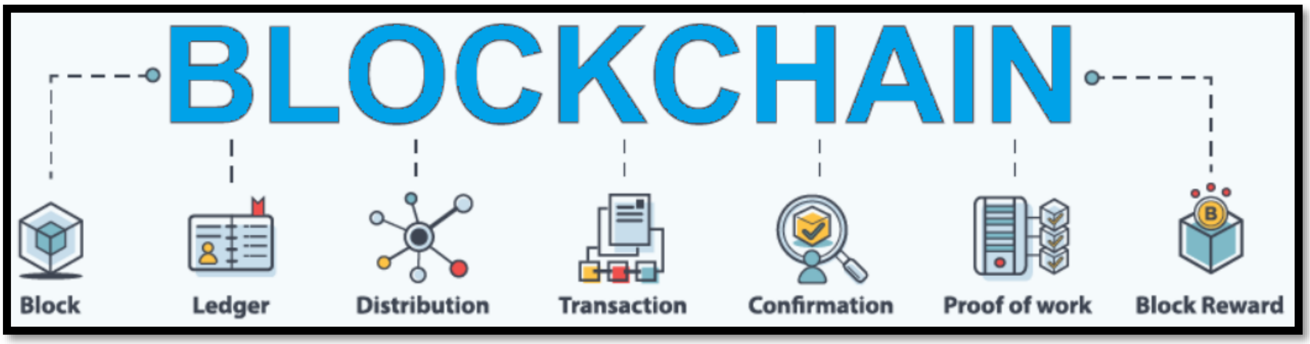


Figure 1: Blockchain

Blockchain components are illustrated in Figure 1.

Blockchain Internals

Each block in a blockchain contains data, the key (hash) of the previous block and the key (hash) of the current block. The type of the blockchain depends on the data stored in the blocks within the blockchain. For instance, the blockchain that handles bitcoins contains the information regarding the sender, receiver and transaction details with amount.

The key (hash) mentioned can be compared to a fingerprint. It is a unique entity whose contents in the block are identified. A key (hash) is always created as soon as the block is created and the key (hash) changes when the block is changed.

The changes in block directly relate to changes in key (hash) which means the change in fingerprint implies change in block. The previous block key (hash) helps maintain a chain-like relationship that provides security for blockchain changes.

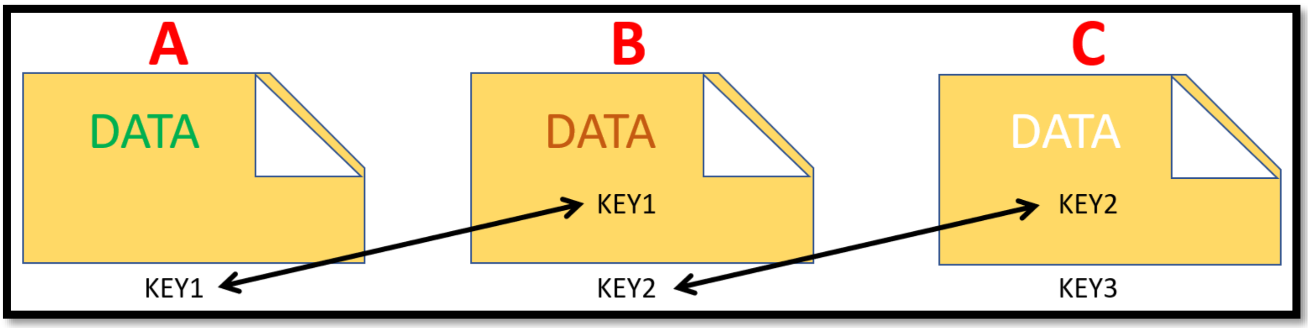


Figure 2: Chain of blocks

Figure 2 illustrates a blockchain with 3 blocks which details that it has current and previous blocks in every single block except the first one which is termed as genesis block. Thus, a chain-like relation appears when the hash of block C directs to block B and hash of block B directs to block A.

Any block modified in the middle, such as block B, would result in a change of that block change which will in turn result in invalidation of all the following blocks from block C.

Though this mechanism provides security for the blockchain, the security provided by hash (key) is not enough as advanced computing might generate several hashes resulting in tampering the chain. Hence another concept, called proof-of-work, is introduced.

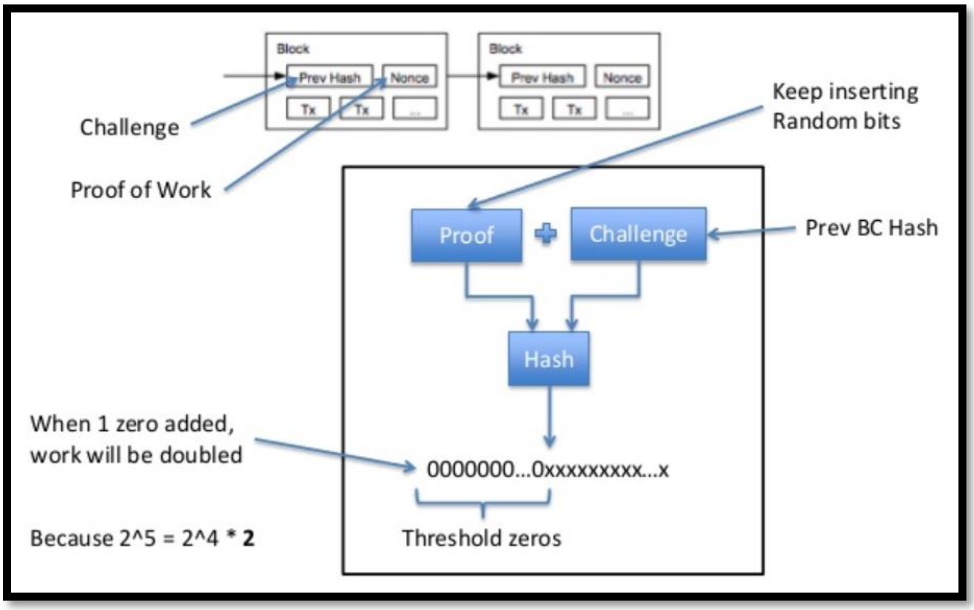


Figure 3: Proof-of-work

Proof-of-work recreates the blocks through figuring out the contents by block information, but it's a slow process. However, this process enhances the security mechanism and overcomes any tampering of block issues. This mechanism is detailed in Figure 3.

Besides having features like hashing and proof-of-work, blockchain also comes with an inherent advantage that it is distributed. The peer-to-peer nature of blockchain makes it to distributed rather than centralized which makes it open.

A full copy of the blockchain is sent to anyone who joins the network and a recheck is performed to validate the consistency of blocks every time someone joins the network.

The addition of new blocks to the network or to the chain creates consensus in all nodes in the network by distributing the updates. This process decides which blocks can be agreed and validated. This also means that this process rejects any invalid or tampered blocks.

In theory an entire blockchain can be tampered with only when more than 50% of distributed peers in the network are tampered with, which is impossible.

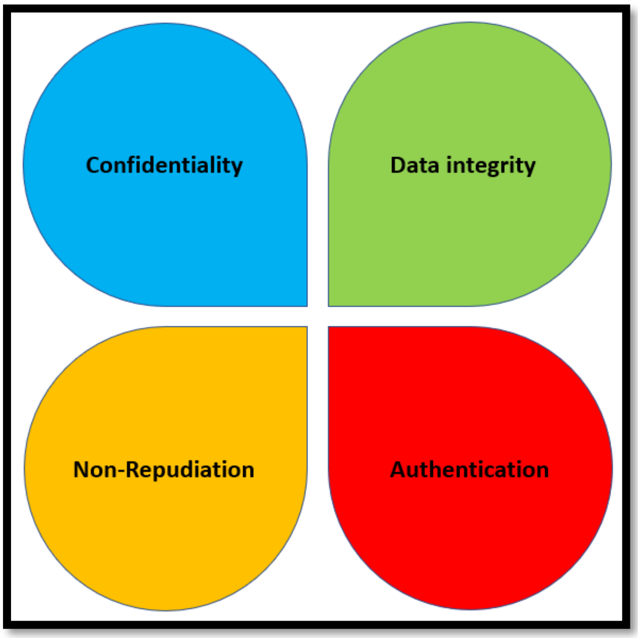


Figure 4: Information security

Blockchain works on peer to peer networks and due to the distributed nature of the peer to peer networks, information security is paramount. The main concerns of Information security which needs to be addressed are shown in Figure 4.

1) **Confidentiality:** When A sends a message to B, no one else should be able to read the message other than B.
2) **Integrity:** When A sends a message to B, no one else should be able to modify the message.
3) **Non-Repudiation:** When A sends a message to B, A can't refute the message validity.
4) **Authentication:** When A sends a message to B, it is ensured that it's not a forgery and that it is sent by A and not by anyone else.

These problems are addressed by Cryptography.

Smart Contracts

Blockchains are evolving with new features and smart contracts is one of the latest developments. These contracts are stored on a blockchain which are simple programs that exchange coins automatically on certain agreements.

In 1997, Nick Szabo came up with smart contracts long before the introduction of the now-popular bitcoin. They are completely digital unlike contracts in the real world and are stored on a distributed ledger.

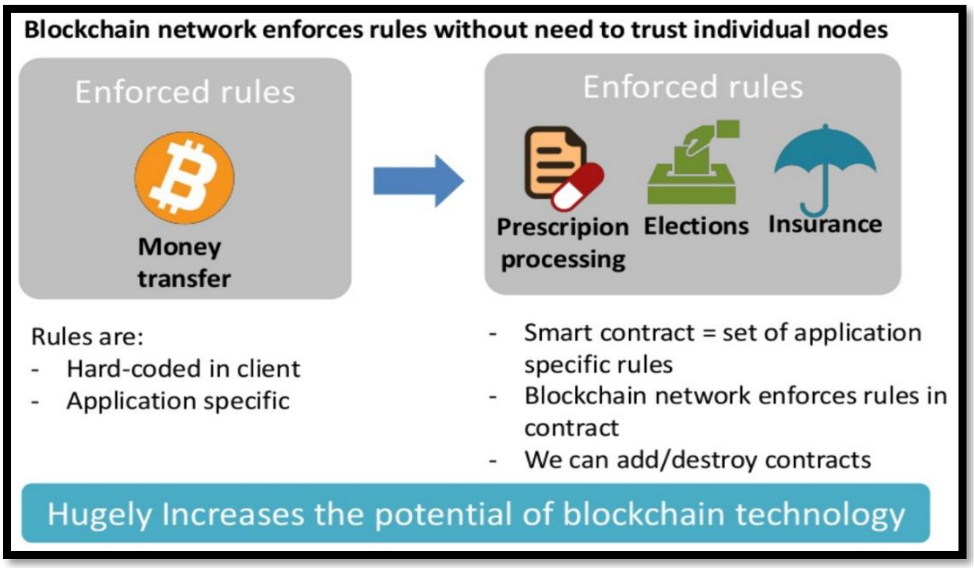


Figure 5: Smart Contracts

Smart contracts are small programs which can be trusted since they are distributed on a blockchain. They leverage the advantages of blockchain such as they are immutable which means they can't be changed once stored on the blockchain. This in turn means that the contracts can't be tampered with and anyone on the blockchain can identify the invalidity if tampered. Hence, it's impossible to tamper with the smart contracts.

Several applications exist for smart contracts. One such use case is for payment on delivery systems in postal companies. It could also be used for claim processing by insurance companies. Payment systems can be automated for loans by banks by using smart contracts. Ethereum is one of the blockchains that supports smart contracts which is the biggest.

Application of blockchain

One of the popular applications of blockchain are bitcoin and other cryptocurrencies. Currently there are about 1600+ cryptocurrencies and they facilitate the public to transact with one another directly without the interference of banks.

Besides cryptocurrencies, automobile odometer tampering can also be avoided using blockchain technology. A tampered odometer leads to fraudulent transactions with customers buying previously owned cars. A replaced smart odometer can avoid such frauds by updating data online over internet. Bosch's IoT lab is already developing this for car fleets.

The patents and IP can be tracked online via blockchain technology – like a notary – and can all be covered legally. Another use case is digital voting which can leverage blockchain technology for storing votes that have been cast. This will create a tamper-free voting process thus increasing trust in elections.

Food-borne diseases can be tracked back to the source of the food production or distribution if they are integrated with blockchain technology to quickly identify food contamination.

Other applications of blockchain that can be easily implemented include notary, tracking packages, medical record storage, streaming service contracts, and more.

Types of blockchain

Blockchain can be considered a specialized type of database when you look at it from a basic level. In general, the databases within the organization tend to be called centralized databases while the data in blockchain is distributed. The moment it is called distributed, one would question trust, fault tolerance, etc. However, to the contrary, the distributed nature itself would bring in those features of trust and fault tolerance due to its security and distributed features.

Centralized databases within the organization might have some drawbacks such as not allowing simultaneous writes from various users or might be a single point of failure. The uniqueness of blockchain among several distributed databases is that its records are kept distributed.

Blockchain architecture can be categorized as permissioned and permission-less blockchains.
Bitcoin and Ethereum are some of the popular public blockchains. When it comes to permissioned blockchains, Hyperledger is popular.

Figure 6 highlights the details and differences between permission blockchain and permission-less blockchain.

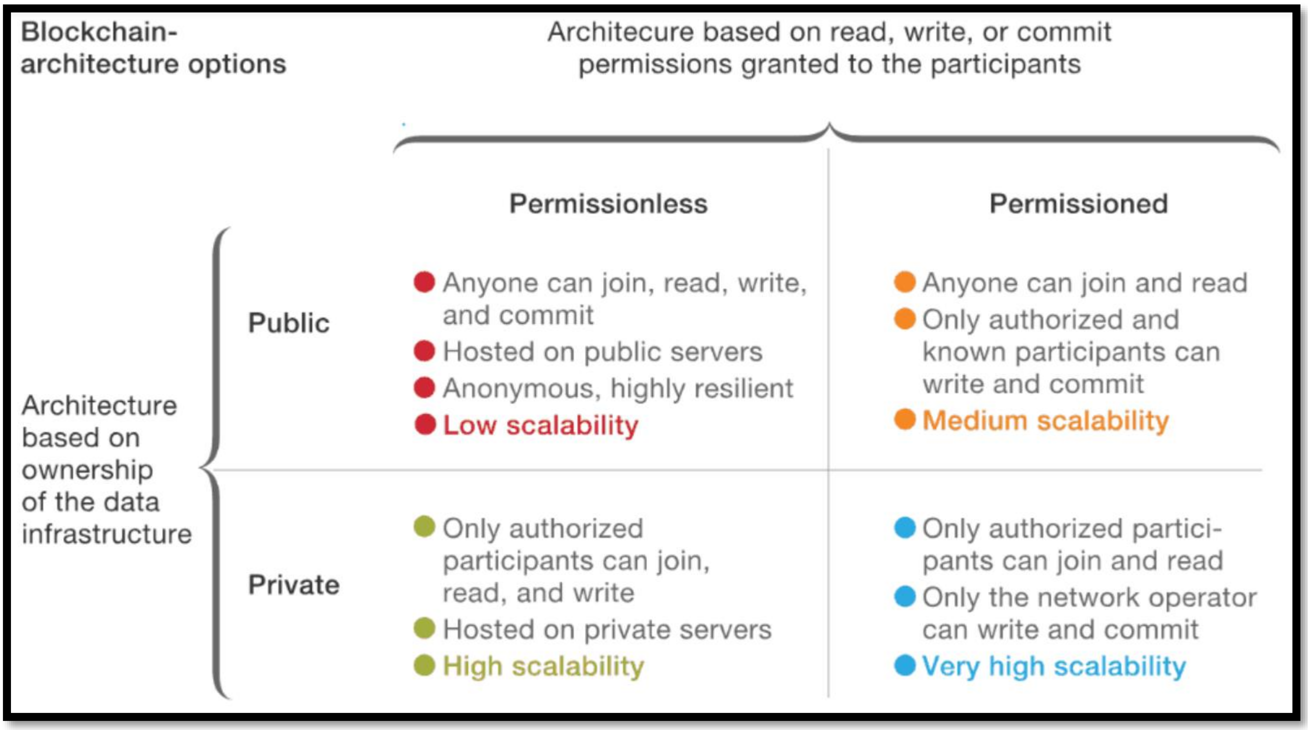


Figure 6: Blockchain architectures

Blockchain for enterprises

The advent of Ethereum has exploded the Decentralized applications (DApps) and thereby spread its wings into enterprises. DApps and data on Ethereum has read access to the public and thus, have true capabilities for decentralization and are open.

The nature of public read access to Ethereum also limits the type of information that can be floated around publicly, especially for enterprises. Hence, permissioned blockchains such as Hyperledger came into existence which provides trust-based access.

Blockchains can be categorized into blockchain 1.0 which is primarily used by cryptocurrencies on public networks where interaction is between public and blockchain 2.0 which works on private networks between enterprises based on predetermined transaction privacy.

The most recent blockchain can be categorized as blockchain 3.0 which is primarily focused on edge and Internet of Things (IoT). It works on both private and public networks. Figure 7 illustrates the 3 categories of blockchains.

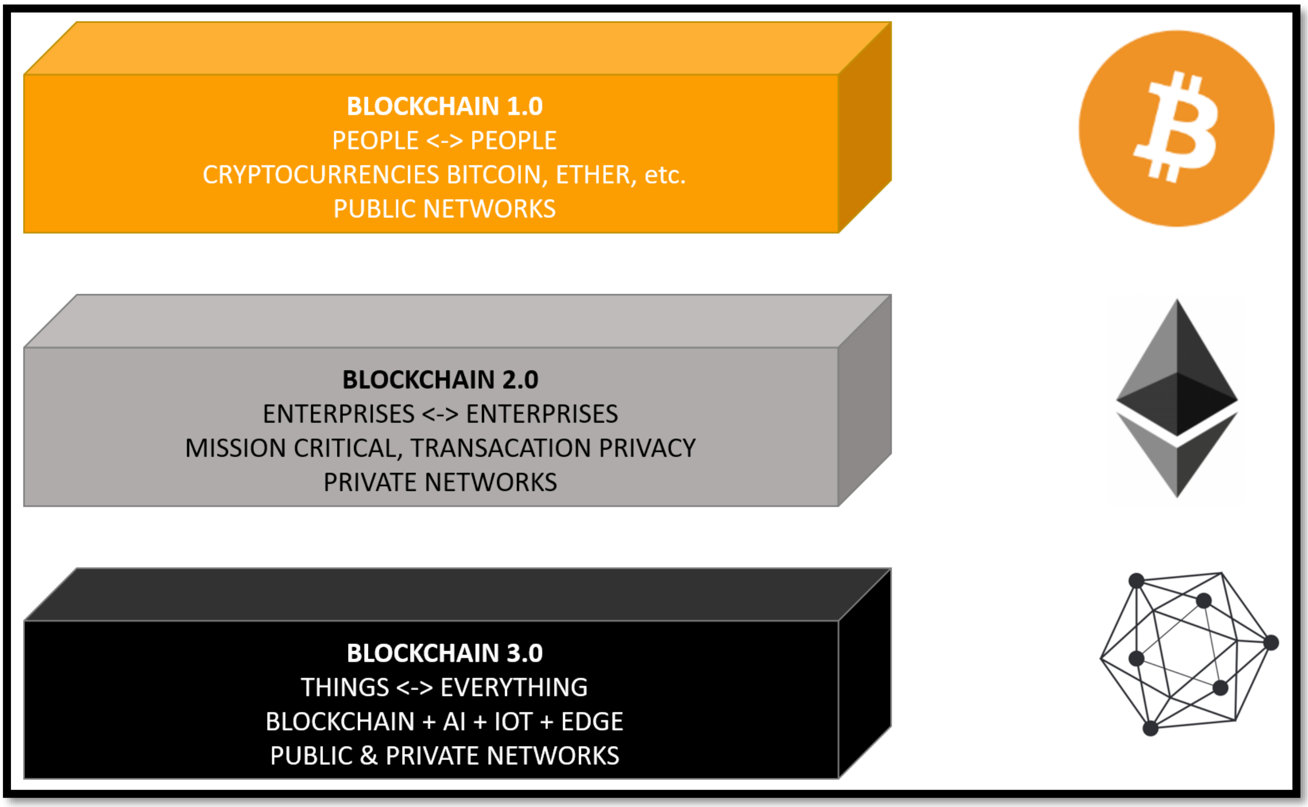


Figure 7: Blockchain categories

Distributed storage

In the world of distributed computing, the need for distributed storage is pivotal, especially for the storage that will be in permissioned blockchain infrastructures. The storage arrays that are in the enterprise datacenter receives data from blockchain-based applications and the arrays provide security to the data and also need to update blockchain with the transactions for distribution.

The data from blockchain applications will be received in two formats, one in format of the data itself and another in the format of the hash of the data. The typical architecture of distributed storage in permissioned blockchain infrastructures will send the data to the storage array while the hash of the data which acts as a transaction will be sent to the blockchain.

This process of data storage architecture, shown in Figure 8, ensures that the data stored in the storage array is secured and private while the hash of data is distributed. This distributed storage is leveraged in private datacenters and at edge locations in blockchain 3.0.

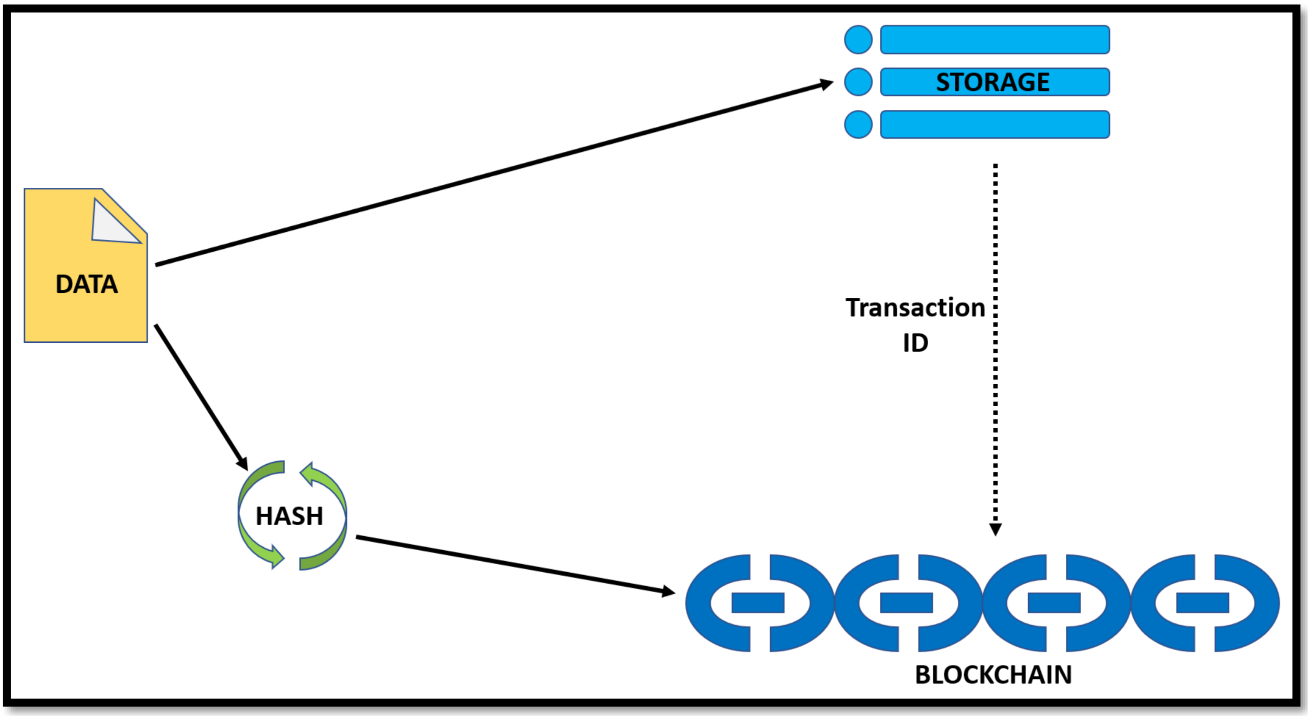


Figure 8: Distributed storage

Blockchain 3.0 Topology

The blockchain for enterprises has extended itself to private datacenters, public clouds and edge computing IoT devices as blockchain 3.0.

A Hyperledger fabric can help integrate the permissioned and public block chain infrastructures. The hash generated from the blockchain applications in the datacenter is sent over to the public distributed network with the Hyperledger fabric.

The public cloud infrastructure that hosts certain blockchain applications can easily maintain distributed ledgers in the public blockchain. The same applies to edge computing devices which can send the transactions to the public blockchain.

The overall blockchain 3.0 topology is shown in Figure 9 which indicates that the hash and transactions are stored in public blockchain while data resides in permissioned blockchain.

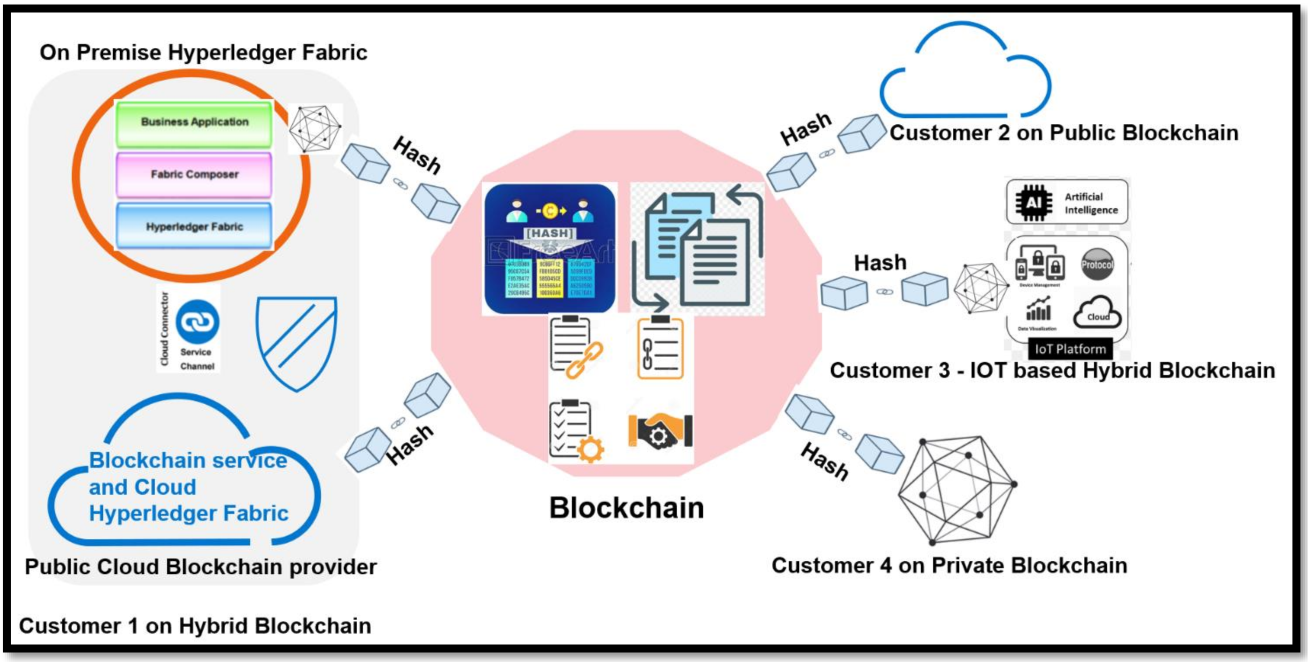


Figure 9: Blockchain 3.0 Topology

PowerChain

In this article, the blockchain 3.0 solution is proposed with a mixture of Dell Technologies products and solutions and termed as the PowerChain solution. This solution highlights the private datacenter permissioned blockchain capabilities using various Dell Technologies products.

The private storage array that can be leveraged in PowerChain would be Dell EMC PowerMax 2000/8000 which provides enterprise storage capabilities with All Flash disk storage. The frontend of this storage will be NVMe fabric with 32Gbps connectivity to hosts.

The hosts in this solution can be Dell EMC PowerEdge servers C4140 or R940xa which has the capabilities of NVMe backend, FPGA and GPU support for high performance computing. The VMware ESXi will provide the operating environment for the blockchain applications.

This solution is integrated with Hyperledger fabric which is a permissioned blockchain in the datacenter and can easily interact with public blockchain based on permissions.

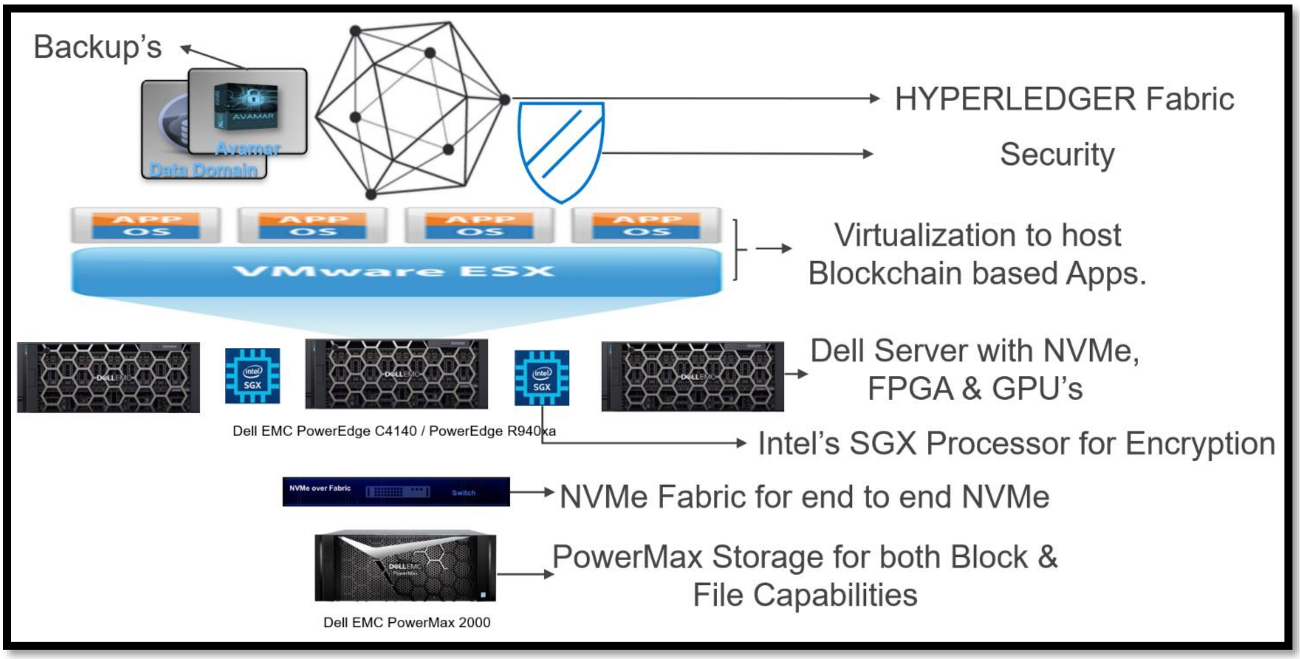


Figure 10: PowerChain Solution

Conclusion

Blockchain technology is truly a disruptive technology across all verticals. This article examined concepts and internals of this technology along with applications of blockchain in several domains.

The types of blockchain, both public and permissioned blockchain along with concepts of distributed storage which facilitates the next generation blockchain 3.0 technology were discussed.

The blockchain 3.0 technology for private, public and edge networks was proposed to be formulated with Dell Technologies products to create an overall PowerChain solution aimed to revolutionize the next generation blockchain applications that span private enterprise datacenters, public clouds and edge computing IoT devices.

References

[1] "Buterin, V. (2013). Ethereum White Paper: A next-generation smart contract and decentralized application platform, retrieved from https://github.com/ethereum/wiki/wiki/White-Paper"

[2] "F. Daniel and L. Guida, "A Service-Oriented Perspective on Blockchain Smart Contracts," in IEEE Internet Computing, vol. 23, no. 1, pp. 46-53, 1 Jan.-Feb. 2019. doi: 10.1109/MIC.2018.2890624"

[3] "Karamitsos, I., Papadaki, M. and Barghuthi, N. (2018) Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security, 9, 177-190. doi: 10.4236/jis.2018.93013"

[4] "K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016. doi: 10.1109/ACCESS.2016.2566339"

[5] "K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," in IEEE Access, vol. 7, pp. 10127-10149, 2019. doi: 10.1109/ACCESS.2018.2890507"

[6] "Nakamoto, S. (2018) Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf"

[7] "Nick Szabo, " Smart Contracts: Building Blocks for Digital Markets”, 1996, retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html"

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” DELL TECHNOLOGIES MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.