Hewlett Packard Enterprise

Blockchain Platforms: Today and Tomorrow

Evolution to enterprise ready performance and scale

Technical white paper

"Technology is a word that describes something that doesn't work yet."
(Douglas Adams, Author)

An Introduction to Blockchain

Douglas Adams might be a little harsh, but apt in describing the comparatively immature and evolving Blockchain - an emerging technology predicted to be the next internet. Concepts such as disintermediated transactional networks, trust though consensus and on-demand transparency promise to disrupt the today's business models in a major way – the exact nature of disruption being still unknown. However, the impending change in status quo in the value-exchange process and the role of intermediaries is becoming apparent even with early use cases.

At its core, however, the technology is underpinned by three simple concepts:

1. A decentralized peer-to-peer network of market participants
2. A shared ledger that is constantly kept in sync across nodes
3. An economic incentive model manifested by a consensus algorithm

The Evolution of Distributed Ledger Technologies

The evolution of these concepts from Satoshi Nakamoto's 2008 whitepaper conceptualizing Bitcoin [1] to the current state of B2B disruption has been nothing short of remarkable. Permissioned networks, private ledgers and smart-contracts have the potential to enable businesses to 'tame' the public Blockchain. As these networks grow in size and become interoperable, we will see the emergence of public ledgers as the transactional backbone of the Internet of Things (IoT)

Gartner [2] postulates that Blockchain is at the top of the technology hype cycle, a theory validated by a very fragmented platform landscape. While the financial services industry has been leading from the front, it is still undecided between general purpose Blockchains like Ethereum and targeted implementations of the technology like R3 Corda and Ripple. Most companies have split their Proof-of-Concept dollars between multiple platforms as they continue uncovering layer after layer of challenges to practical implementations of a Blockchain solution. This is evident from the fact that hundreds of proof points have yet to yield real-world applications running at significant scale [3].

Still, the increasing number of Pilots and Proof of Concepts indicate the benefits out weighing the challenges. In the near future industry collaboration and production implementations will establish standards and 'best practices' that accelerate adoption (EEA [8] for example) – this is a simple function of maturity.

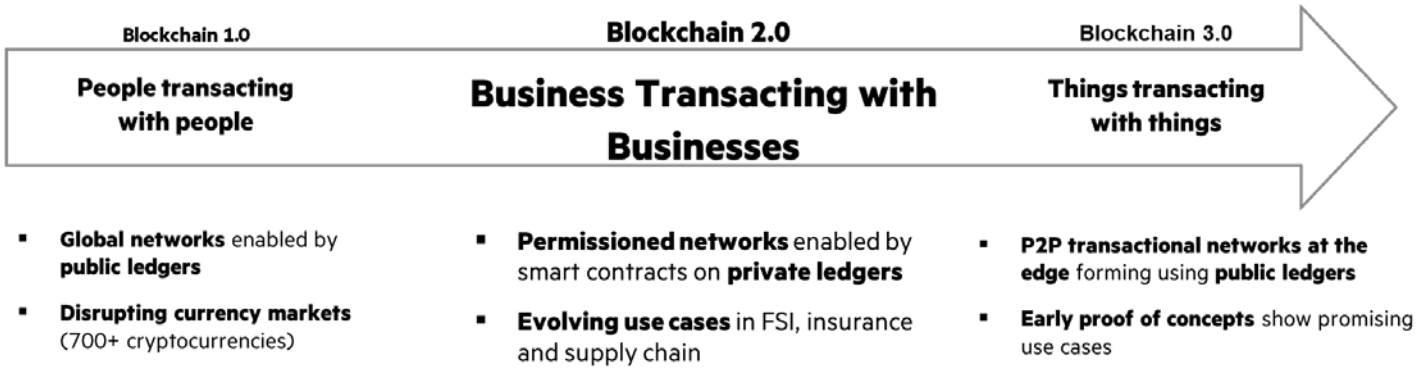

Figure 1: The Evolution of Blockchain Technology

Fundamental Challenges in Deploying a Blockchain

Enterprises do not like uncertain outcomes, and there is a quite a bit of uncertainty when it comes to Blockchain. While both platforms and businesses are evolving to solve some of the most critical challenges [4], there is clearly a 'last-mile' problem when it comes to enterprise adoption. We characterize this problem along three dimensions:

1. Capability Gaps in Blockchain Platforms

Resilience of Miners/ Notaries: While decentralization of Blockchain networks means that there is no single point of failure, miners or notaries have a special purpose for a particular market participant (e.g. a credit card processor or regulator). Until Blockchain reaches the level of maturity and predictability, these nodes are Mission-Critical.

Transaction Throughput: Customers indicate that a 10x improvement in performance is required to support next-generation payment networks. We expect IoT networks of tomorrow will require orders of magnitude that level. While innovative consensus algorithms and Software-level optimization with concepts like Sharding [10] have already shown proof-points for better performance, they are still approaching a ceiling. Moreover, storing the digital asset in conjunction with the Blockchain induces further drag on transaction throughput.

Hosting the Key Value Store (KVS) storage media and enabling digital asset storage on faster media enables orders of magnitude lower latency in transaction processing. Unless a business case exists for expensive high memory footprint nodes, the best available media today is NAND flash. A new tier of Non Volatile Memory technologies [6] by Micron, Samsung and SK-Hynix amongst others provide the perfect media for storing keys and digital assets. The catch, however, is that the core Blockchain virtual machine needs to be re-programmed to recognize and exploit the performance benefits of non-volatile memory.

Some of the resource-intensive hashing [7] computations can be run directly on an FPGA (Field-Programmable Gate Array) programmed to optimize the specific workload. When done strategically for the mission critical miner/ notary nodes, this accelerates the cryptographic hash at a node level and reduces total block time. Moreover, this provides a way to self-contain efficient bytecode execution so it doesn't unnecessarily get disrupted by external factors. At the same time, it opens the doors for faster and more secure consensus algorithms (like Intel's Proof of Elapsed Time)

In local networks native to the IoT world, smarter routing of peer-to-peer transactions between the local and World Wide Web networks will lower the load on Client/Server communication. This removes network bottlenecks expected to limit the growth of next-generation IoT networks.

The Performance Challenge

The only Blockchain deployed at scale today is Bitcoin, which has a block-time of 600 seconds. This means that you have to wait 10 minutes from when you post the transaction to the time it is 'finalized'. While this is a great replacement to settlement processes that take several days, they are a far cry from what you expect payment networks.

Ethereum has taken an exceptional stride to bring this down to 16-18 seconds with a theoretical floor of 12 seconds. This is still an order of magnitude slower than what is needed for high-volume use cases like Real-time payments and IoT.

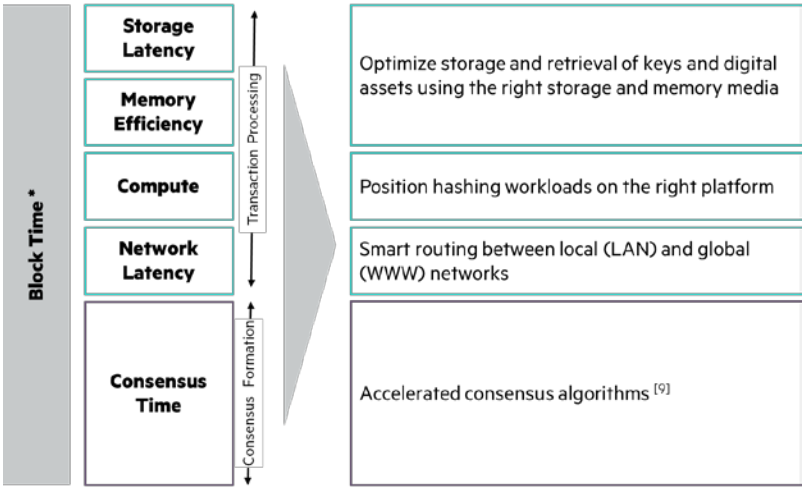

Figure 2: Accelerating Transaction Rates (*conceptual representation, not to scale)

Security – Key management: Key management is the one of the biggest barriers to enterprise readiness of Blockchains. This layer needs to accommodate different account level security (e.g. RSA, Lamport). While current Blockchain implementations have acknowledged the importance of this function, none has brought together a holistic solution to the problem.

2. Implementation Challenges

As with any new technology, implementation architectures, tools and methodologies are still immature, new and evolving rapidly. This is further complicated by stakeholders spanning many domains (for example, legal, audit, information privacy and security).

In many ways, Blockchain is no different to many 'new style' workloads. But given the speed of evolution and the disruptive potential, agility is key through the service lifecycle of the implementation. Future favours the fast: Time to value has never been more critical. For many organizations the preference towards a proven waterfall approach extends well into implementation phase dependencies – traditional operating and provisioning models are not fast enough, neither are traditional platform offerings. The IT world needs to be agile to keep pace of business use case demands.

From a systemic perspective, the primary implementation challenge in any 'new style workload' is to meet the requirements today within acceptable service level and cost envelope and have the ability to scale with the business. Platform technologies are likely to change through phases of implementation. A Development environment is unlikely to have the same architecture as Production system. But consistency is necessary for services to migrate seamlessly and quickly across environments.

However, the unique nature of enterprise Blockchains is that they are expected to scale as a common backbone enabling multiple use cases and applications. This requires provisioning the correct resources for the core Blockchain workloads and the application overlay to provide predictable service levels as the application ecosystem grows.

In a somewhat fragmented platform landscape, a one size fits all model does not meet the steady service expectations of many clients. Expectations of scale, availability, serviceability and performance require 'scale up' as well as 'scale out' nodes. Hybrid IT, use of common infrastructure APIs and unified control planes for management provide platform agility that modern applications require. There are two strategies that help maximize efficiency of your hybrid IT:

1. Composability: Provisioning infrastructure through APIs allow Blockchain services to be provisioned on-demand, often on spare client capacity

2. Flexible Capacity: Use of capacity based pricing that aligns with the consumption of the business service enables robust pilots that can scale with transaction volume and the application ecosystem

3. Driving Business Value

In a global marketplace, organizations need a future vision and constant innovation to drive competitive advantage. This involves developing and integrating the right strategy, processes and leveraging emerging technologies such as 'Blockchain' as a pivotal value driver to:

1. Enable services or solutions in new or developing markets
2. Allow the creation and distribution of virtual assets
3. Reduce transaction processing times (from days to near real time)
4. Increase efficiency through the removal of overheads associated with intermediaries
5. Remove a central authority or intermediary as a point of failure
6. Build a trust mechanism between parties or IoT devices
7. Enable traceability and immutability of records so reducing the risk of collusion and tampering

When considering a program using Blockchain technologies, six 'domain' areas need to be considered, assessed and managed to increase the chances of a successful outcome:

1. Industry readiness – Do Blockchain technologies represent new opportunities or cause 'disruption' to the existing business models in the organizational and its industry
2. Strategic plan – A clear articulation of the opportunities and threats with a clear strategic plan and roadmap around the use of Blockchain technologies
3. Management framework – Appropriate program, project management and governance models are in place to manage, escalate, control, review and assess the readiness and implementation of Blockchain technologies
4. Workload evaluation – A Blockchain solution will need to handle the (projected) workloads, interface with legacy systems and work within regulatory and compliance constraints and as such assumptions and dependencies need to be understood and impacted and factored in
5. Minimal Viable Products (MVP) – Due to the relative immaturity of Blockchain technologies an 'agile' approach should be used to split and sequence the implementation in to a number of MVP's and sprints to realize the benefits, gain learnings, constantly improve and adjust the direction of travel
6. Culture and Staff – The use of Blockchain technologies represents a mindset change, impact the existing business model as well as a new technology as such it is important to consider the human 'change' aspect

By analyzing the direct, indirect and new business value Blockchain technologies bring to the identified use cases an organization can formulate an execution roadmap through the use of Minimal Viable Products (MVP's) to provide the highest benefit while lowering the barriers to execution.

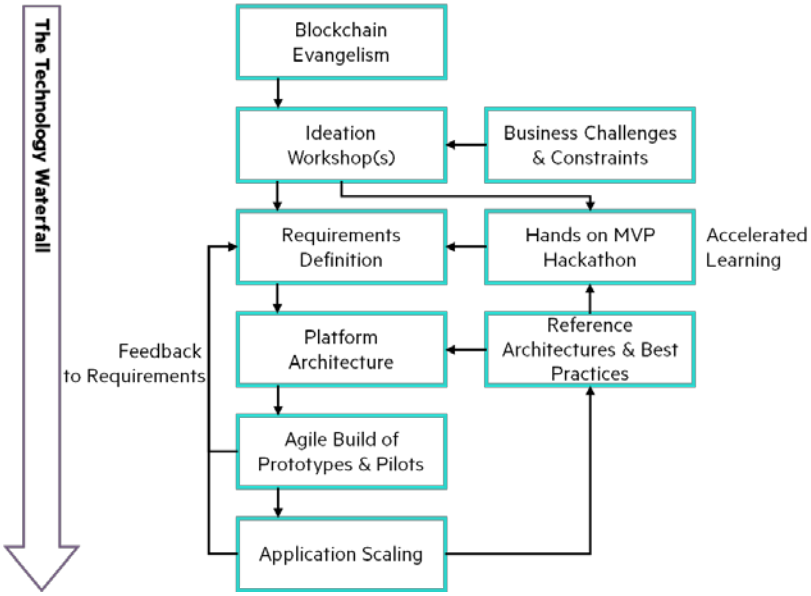

Figure 3: Approaching a Blockchain Initiative

How HPE can help

Hewlett Packard Labs is addressing some of the most pressing technology challenges facing enterprises in the Blockchain space. This leading edge innovation in platform infrastructure and next-generation performance with processor and memory technologies can accelerate Blockchain platforms to their next step of evolution. HPE can be the trusted advisor to our customers in their Blockchain incubation and transformation journey, bringing together the elements of a successful incubation:

1. Deliver the right platform from a broad portfolio of infrastructure products purpose built for enterprise workloads
2. Enable and support agile innovation and reduce time-to-value with HPE Pointnext's 50+ years of architecture design and implementation experience
3. Bring together development and delivery capabilities through ecosystem partners

References

[1] The original Bitcoin Whitepaper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” (Satoshi Nakamoto, 2008)
[2] Hype Cycle for Emerging Technologies (Gartner, 2016)
[3] Construct 2017 Day 2 Keynote - CoinDesk Developer Conference (CoinDesk, February 1, 2017)
[4] Blockchain technology: 9 benefits & 7 challenges (Deloitte Insights, 2016)
[5] Micron/ Intel 3D XPoint Technology
[6] Viking Technology Overview of Non-Volatile Memory
[7] StackExchange answer to cryptographic hash function used in Ethereum Virtual Machine (EVM)
[8] Enterprise Ethereum Alliance website
[9] Though we do not discuss Consensus in this document, it is a critical part of transaction throughput. KPMG’s Whitepaper puts together a comprehensive discussion on consensus methods
[10] To know more about Sharding, visit the Ethereum Wiki on Github

About the Authors

David Orwin is an Information Systems Architect in Hewlett Packard Enterprise Pointnext, focused on definition and delivery of technology solutions to solve business problems.

Justin Hibbard is the global Chief Technologist for Financial Services at Hewlett Packard Enterprise Sales (BEST) organization, responsible for enabling digital transformation and innovation for key customers

Sandeep Panda is the blockchain strategy lead at Hewlett Packard Labs, focused on technology strategy and incubation

Learn more about Hewlett Packard Labs

https://www.labs.hpe.com/

A00016578ENW, June 2017