Internet Scale Blockchain Architecture

Akamai Technologies – Akamai Labs

A Technical Paper prepared for SCTE•ISBE by

Akamai Labs
Michael Fay et al.
Akamai Technologies, LLC
150 Broadway Cambridge MA
mifay@akamai.com

Table of Contents

List of Figures

Introduction

Blockchain has quickly become a disruptive technology enabling whole new business models and ecosystems including the rise of cryptocurrencies such as Bitcoin and Ethereum. It is changing how people think about recording interactions, transparency and auditability.

Applications can extend beyond just providing an auditable ledger for tracking payments, financial services transactions, digital assets and currency balances. Blockchain can be leveraged for proof of existence and proof of integrity for data and/or state and establish provenance via an auditable trail of interactions. This could be applied to many industries ranging from insurance, advertising, health care, shipping and logistics, commerce and defense.

However, many popular blockchain implementations have real challenges and limitations around scalability, performance, reliability and security. A new blockchain architecture is required to address enterprise and institutional use cases that need scale and speed.

Content

1. An Overview of Blockchain

A simple definition of blockchain is a digital record of interactions added over time and protected from alteration. A more detailed definition would be a permanent, append-only distributed ledger that addresses data provenance and provides transparency and auditability by embodying the canonical history of transactions leading up to a given exchange of value. Essentially, its a database that enables sharing authority amongst participating entities and only allows information to be written once, preventing deletions and modifications.

So what’s so special and useful about a blockchain? Since the information in a blockchain is not centralized and cannot be altered, it provides a great mechanism for use cases that require a tamperproof record. Examples of popular applications for blockchains include providing an auditable ledger for tracking payments, financial services transactions, digital assets and currency balances. In these cases, a blockchain can represent and manage real value and/or digital assets and thus a transaction includes both the clearing and settlement phases of a financial transaction. Another popular blockchain application is the use of Smart Contracts to provide asset custodianship services and scripted policy execution. Other potential applications include using blockchain to provide auditable trails of transactions including, everything from parts to repairs to medical records to warranties to insurance claims.

Blockchain is built upon several key principles, which include decentralized authority, transparency, and immutability. The first principle is that there is no central authority to approve transactions or set rules. Authority is distributed through consensus across multiple participants, usually represented by various networked computers. Transparency means that the records in the blockchain are self- verifiable, containing all information required for auditing by any participant. Lastly, immutability refers the inability to alter or forge data once it has been committed to the blockchain.

Many of these applications are served by a centralized database, so what additional advantages does a blockchain provide? With centralized databases, clients must depend on the trustworthiness and reliability of the database operator. Database records are not inherently transparent, immutable, tamper-proof or self-verifiable. In addition, the cryptographic foundations of blockchain provide superior reliability and security in the face of failures or adversarial conditions.

In order to achieve these advantages, blockchains employ cryptographic techniques as a foundation of their design. At regular intervals, a decentralized group of nodes (networked computers) add a new block to the ledger. Each block contains a sequence of transactions organized into a tree of cryptographic hashes called a Merkle Tree. The root hash of the tree is recorded in the block header, and the hash of the block header uniquely identifies the block. Each block is cryptographically linked to its predecessor by including the previous block hash in its header, forming a "chain". Clients of the blockchain submit transactions to the network that must be digitally signed by a valid private key. This digital signature makes the transaction computationally intractable to forge or alter. Furthermore, the use of cryptographic hash functions in the block structure make it intractable to modify any block. Therefore, both transactions and blocks are tamper-proof. This property makes blockchains applicable to many use cases that require trustworthy exchanges between multiple, independent parties (e.g,, auditable records that are shared between insurance and medical providers and their patients). The first block in the chain is called the "genesis block". Each block has a link to a single previous block. Following these links and verifying each of the transactions within a block allows any eligible party that has a copy to independently verify the entire blockchain.

2. Challenges and Limitations of Blockchain

Blockchain systems are typically limited by some of these characteristics: **scalability**, **performance**, **reliability** and **security**. These limitations are a barrier to leveraging blockchain for use cases that require a high-performance solution to quickly, securely, and efficiently process transactions with almost limitless scale.

Today, many of the limitations of blockchain implementations are around **scalability** and **performance**. These two characteristics are closely related and highly dependent on the architecture and implementation of the system. Some of the impacting factors include the number of nodes, the number of users, the number of transactions, and the number of connections or network traffic.

In terms of **scalability,** many implementations have limitations to volume and rate of transactions processed. A decentralized permissionless network (such as Bitcoins) has challenges with **scalability** (or transaction volume). This type of implementation usually encompasses a large geographic area, potentially resulting in unpredictable latencies and unreliable timing assumptions and therefore is difficult scale horizontally (adding more machines does not increase performance, but rather may deteriorate performance). Even current implementations of permissioned networks haven't achieved high transaction volumes in terms of scalability.

While permissioned networks, without the burden of resource intensive computation, would seem to scale, they have not yet achieved the scale required. In addition, they have the disadvantage of limited geographic presence as compared to a distributed platform.

Performance limitations are primarily related to the latency in confirmation time or the time required to commit a transaction. To support massive numbers of users and transactions, considerations must be made for the nodes and the connections. Adding more nodes with more connections and traffic between nodes can negatively impact scale and performance (or confirmation times) because propagation times for both transactions and blocks will increase. This is a critical factor in why large decentralized permissionless implementations such as Bitcoin have slow block creation and transmission

Reliability is challenged by availability as it relates to distribution. Adding more nodes can increase reliability. While systems like Bitcoin are highly reliable, they suffer scale and performance issues as previously mentioned. Controlling the number of nodes and connections by centralizing them in few data centers will reduce the reliability of the system because the nodes are less distributed.

Lastly, **security** and trust has been limited by unproven trust models and key management at scale. Decentralized permissionless approaches are protected against a single point of failure but have inherent risk due to lack of security and governance in the participating machines. Conversely, a permissioned approach has secure access and governance, but usually introduce a single/limited points of failure in terms of an attack surface.

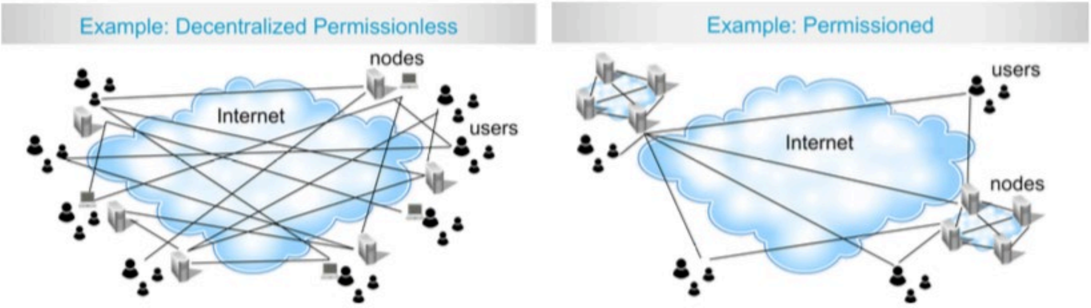

Figure 1 – Examples of Decentralized Permissions and Permissioned

3. A Blockchain Architecture for Scale & Speed

Akamai has built a new unique high-performance blockchain architecture that will enable institutions and enterprises to quickly, securely and efficiently process transactions with almost limitless scale. Akamai has focused on significantly improving the **scalability** and **performance** weaknesses of existing blockchain implementations, while maintaining and improving the **reliability** and **security** characteristics. Akamai's blockchain system is capable of processing 10M+ onchain transactions per second, with each transaction committed and confirmed in the system in under 2 seconds*.

So what is unique about Akamai's approach and the potential benefits? The Akamai blockchain architecture combines innovations in blockchain technology with Akamai's globally distributed platform. It provides the benefits of decentralization (geographic and network diversity) with a permissioned approach, offering improved scalability, reliability, performance and security. Akamai's globally distributed platform enables fast and secure access from anywhere around the world to provide a solution for enterprise customers that is superior to permissionless networks (like Bitcoin) and current permissioned network implementations. In addition, Akamai's globally distributed platform provides inherent critical security features to protect the blockchain network against a variety of attacks, including DDoS.

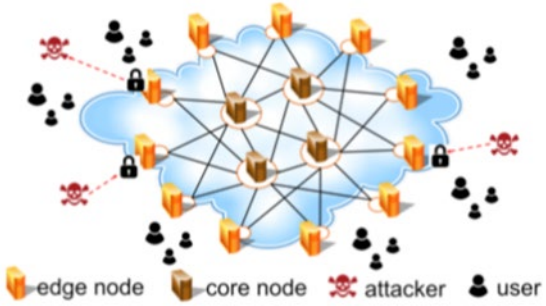

Figure 2 – Tiered Architecture

Akamai has architected a tiered approach for integrating blockchain technology with its globally distributed platform. Incoming transactions are accelerated and secured by the globally distributed Akamai platform (edge tier), then handed off to a highly secure set of network nodes executing the blockchain transactions (the core blockchain tier). Combining an Internet-scale core blockchain tier with advanced content acceleration and security capabilities in the edge tier, makes the architecture unique in providing an end to end flexible, performant and secure blockchain platform.

** Adaptable, represents end-to-end latency in a user generated payment processing transaction.*

3.1. Core Tier

The core tier provides unparalleled scale and speed for transaction processing, at the same time, adhering to all of the blockchain principles such as transparency, immutability, reliability, and self verifiability. To achieve scale, Akamai has applied years of experience in Internet-scale distributed computing into each node that processes transactions in the core. Other approaches to scale blockchains employ off-chain (or layer 2 approaches) to achieve scale. While these approaches have their merits, a system that processes and commits all transactions on-chain adhere better to the core blockchain principles. The layer 2 approaches could in fact be leveraged to scale the Akamai architecture even further. An innovative consensus algorithm powers the high speed transactions and block processing, with all nodes participating actively in finalizing transactions. In addition, the core tier provides high reliability, leveraging a node deployment that spans multiple, disparate data centers and geographies, combined with resilient network connectivity to handle disruptions.

3.2. Consensus

Akamai's unique consensus protocol is far more efficient in terms of scale, performance and cost than both current blockchain and traditional consensus mechanisms. The protocol ensures that node selection for block generation is both unpredictable and non-influenceable while remaining self- verifiable. In addition, current block propagation and finalization mechanisms have inherent limitations in scalability and resilience. To achieve block and transaction finalization at high speed, the Akamai protocol features configurable quorum requirements, with automated resolution in response to network partitions and attacks to overcome these limitations. In short, Akamai's innovative consensus protocol lays the foundation for a robust blockchain architecture suitable for Internet-scale adoption.

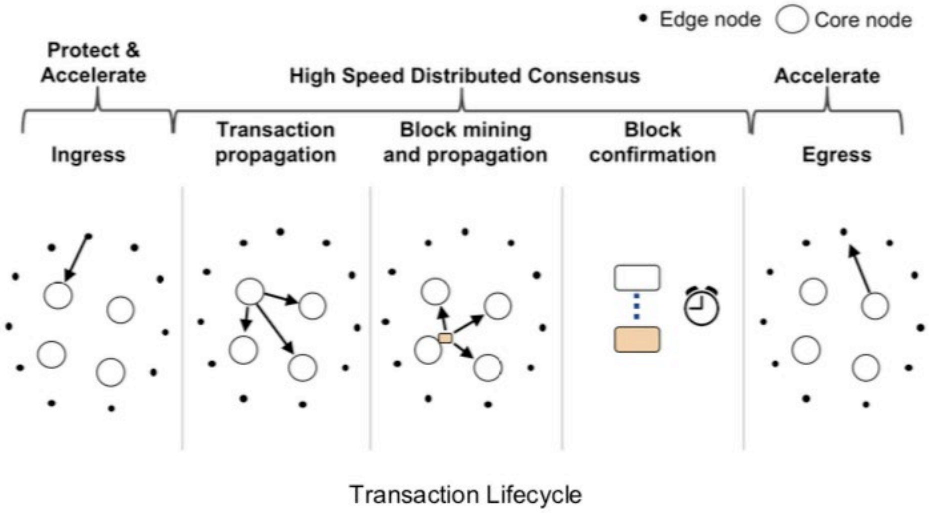

Figure 3 – Transaction Lifecycle

3.3. Edge Tier

Akamai's globally distributed intelligent platform forms an integral part of the the blockchain architecture serving as its edge tier. This tier provides sophisticated capabilities by ensuring content is accelerated across the internet, solving for issues such as congestion, unreliable connectivity and sub-optimal routing. The blockchain architecture leverages these capabilities to ensure that transactions are ingested close to their origination and reliably accelerated to the core tier for further processing.

In addition, advanced security capabilities such as a cloud based distributed firewall provide attack resilience from a myriad of attacks on the Internet, including DDoS. Such advanced capabilities add a critical layer of protection for the core blockchain tier and ensure its security. Moreover, end to end content security and strong cryptography for the core blockchain tier is ensured by leveraging Distributed Key Management Infrastructure (KMI) features in the edge tier.

Apart from these market-leading capabilities leveraged by the most prominent brands on the Internet, the edge tier has innate flexibility to adapt the blockchain platform for varied use cases, by providing configurable workflows and data processing capabilities as part of the transactional flow. Further, the edge tier provides flexibility for applications with robust APIs and the ability to host application logic, close to transaction origination.

The capabilities of the edge tier are renowned in the industry as part of Akamai's current services, serving a large portion of global Internet traffic. The Akamai blockchain architecture builds upon years of battle-tested capabilities to create a robust end-to-end blockchain platform for institutional and enterprise consumption.

4. Blockchain as a Service

The Akamai blockchain architecture anticipates supporting multi-tenancy, allowing it to safely host multiple customers on the platform. Akamai's globally distributed platform is multi-tenant and currently supports thousands of mission-critical customer properties. In addition, given Akamai's global network deployment, instantiating unique blockchain networks for different needs, addressing privacy and locality requirements is now achievable.

The combination of these capabilities allows Akamai to offer blockchain as a service, thereby unlocking tremendous potential for hyper-scale blockchain applications. Building, deploying, maintaining and securing a blockchain platform can be risky, time consuming and costly. The complexity and challenges of DIY blockchain deployments may be cost prohibitive and difficult to scale. As a service company, the value of Akamai's globally distributed platform offers any business or organization an on-demand service for security, delivery, acceleration and now blockchain.

5. Benefits

Akamai's blockchain architecture provides substantially improved benefits over other implementations. First, in terms of **scalability**, Akamai has chosen a highly concurrent scalable distributed node architecture. For **reliability**, Akamai's distributed platform provides superior reliability with diversity in geographies/networks with nodes that have smaller standard deviations in terms of compute/connectivity. To address **performance**, Akamai has innovated on a low latency distributed consensus, which lowers computation overhead and reduces confirmation time. Lastly, **security** leverages Akamai platform and expertise to improved risk mitigation. . In addition, Akamai reduces security and operational risks with its robustness via its round the clock NOCC, heterogeneity of network architecture, secure servers, and global reach. Finally, Akamai benefits from a virtualized management layer that manages deployment of and, communication between nodes and provides API that hides the complexity of managing network of blockchain nodes.

Conclusion

Akamai has built an innovative blockchain design, from ground up, that leverages years of distributed computing principles in each node of its network, with nodes deployed in heterogeneous networks to provide fault tolerance. Moreover, the system also implements an innovative consensus algorithm to ensure that key blockchain principles aren't sacrificed for scale or speed. This system inherently leverages Akamai's market leading advanced security and performance capabilities to enhance its robustness. The results in terms of **Scalability** have shown that Akamai's blockchain system is capable of processing 10M+ on chain transactions per second. In terms of **performance** transactions are committed and confirmed by Akamai's blockchain system in < 2 seconds*. Akamai has demonstrated **reliability** by coupling it highly available blockchain network with Akamai's global edge platform**.** Lastly, in terms of **security**, Akamai's blockchain transactions are protected by strong cryptography, and our platform network is protected by our cloud security.

Abbreviations

CDN	Content Delivery Network
tps	Transactions Per Second

Bibliography & References & Copyrights

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access and video delivery solutions is supported by unmatched customer service, analytics and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published September 2018.