V SYSTEMS: Blockchain Database and Apps Platform

Sunny King

Kate Shan

Rob Zhang

Scott Nadal

Background

Technology is forever evolving. The birth of the Internet, arguably one of the most revolutionary event in history, took place only around 30 years ago. In a very short span of time, nonetheless, it has evolved so much and moved from giant computers to tiny smart phones in the hands of billions around the globe. The benefits and impact that it brings need no explanation. Other technological areas like Artificial Intelligence and Quantum Supremacy, have also witnessed significant growth over the years. And despite the differences among these technology inventions, all of them have been a target of a wide variety of criticism before reaching massive adoption or earning substantial development resources.

Satoshi Nakamoto's announcement of Bitcoin [Nakamoto 2008] is no different. There are constant skepticism surrounding the token - its black market association or the highly fluctuated valuation are just some of the many examples. Yet, Satoshi's brilliant creation of blockchain has gradually picked up momentum over the years. Almost every major corporation around the world has in some way involved with blockchain technology, be it incorporating them into current business model or investing in related companies. This is a testimony to how valuable and revolutionary this technology is, and also how much ahead of his time Satoshi was.

Blockchain, in general, should be viewed as a distributed database system. This implies that a significant portion of the world's data could be stored on blockchain, just as they do in traditional relational databases and the comparatively recent cloud databases. With the massive potential that blockchain could bring, however, the world has yet to witness the true materialization of the technology. In light of this, Sunny King, creator of the Proof-of-Stake mechanism, devises a brand new consensus mechanism, Supernode Proof-of-Stake (SPoS), to not only tackle the rising energy consumption owing to the Proof-of-Work mechanism first explored in Bitcoin, but also refine the Proof-of-Stake mechanism. With this mission imprinted in the project, we envision to push forward a new economic era.

Introduction

Since Bitcoin was not designed for general data usage, attempting to use the Bitcoin style blockchain for data storage has proven to be difficult and expensive. Bitcoin protocol limited legitimate data usage to the scale of 100 bytes per transaction - although this limit changes over time, the magnitude stays essentially the same. This limitation was deliberately put in place at the creation of Bitcoin, as the accommodation to data usage is a conflicting goal to the system performance. It has been a prolonged battle and drama to raise Bitcoin's

maximum block size limit, by which evidently reflects that inherent scalability limitation of the technology. The scalability issues stem from the fact that, unlike previous distributed databases, Bitcoin is an extremely redundant system. Each full node of the Bitcoin network has a complete dataset of the Bitcoin blockchain, and must also validate the blockchain in its entirety. To promote data usage, it would cost even more consumption of the already-limited storage resources, and reduce the maximum transactional throughput of the system. The high cost associated with such extreme level of redundancy and resource straining discourages the scaling of blockchain.

Over the years, there have been many attempts to make blockchain more scalable. For instance, Bitcoin initially tackled the redundancy issue via a system called light-weight validation, which cleverly organized transactions in a merkle tree data structure, such that users can still follow the blockchain consensus in a decentralized fashion by only using light-weight nodes. This technique was able to significantly lower the redundancy level of the Bitcoin network. Currently, the number of light-weight nodes far exceeds the number of full nodes in the Bitcoin network.

Blockstream later suggested that applications may be offloaded to sidechains [Back 2014]. In order to maintain a Bitcoin-centric world, a pegging system to Bitcoin was proposed in this scheme.

Besides from that, Ethereum proposed to tackle the redundancy level via sharding. Sharding is a distributed database technique to divide a large database into smaller 'shards', which is stored in different nodes. However, due to the lessening redundancy, this system introduced a risk of reduced shards availability. To counter this, Ethereum would likely require the existence of several highly-available full nodes storing its whole blockchain.

V SYSTEMS Platform: Re-architecting Blockchain Technology

There are tens of thousands of blockchain project happening around the world. But due to the many flaws and inherent scalability issues, the world has yet to witness a massive adoption of this technology. It is time to tackle the core issues of blockchain and reinvent the technology to bring a truly scalable, stable, and global blockchain platform that is easy to use and is compatible with billions of system. By doing so, enable the widespread of blockchain adoption and push forward a whole new era.

Blockchain as a Database

The major breakthrough that blockchain technology brought was decentralization. Logically, one of the keys to adopting blockchain lies within the migration from traditional database structure to this new decentralized framework.

In general, traditional user accounts can be substituted by public-private keys and addresses in blockchains. Traditional databases are subject to strong access control, almost all data is restricted to authenticated

accounts. Moreover, account creation is also of a centralized model in traditional databases, by which a database administrator grants the user an account for access. With blockchains, conversely, key pairs are generated freely by anyone, without the need for centralized administration. Much of the data is then considered public access, unless it is stored in encrypted form on the blockchain. This applies even for private blockchains within an organization's own LAN, unencrypted data should still be considered as publicly accessible, due to the unavoidable breach into the LAN. Instead, privacy is protected by the anonymity of the virtual identities. This is in fact arguably a stronger privacy protection compared to a centralized model, where the loss of customer data happens often due to hacking.

For applications that require some form of central administration, it is achievable through the business logic inside the client/node software. Privileged key pairs known as administrators can be built into the client software. Administrators can then choose to mark those key pairs in violation of the service agreement as violators. Administrators can also mark specific data for censorship. The data of the violators or specific data that is inappropriate or illegal can then be disregarded by the node software. However, it is worth noting that this type of central censorship is of a weak form, since the violator data is still allowed to enter the blockchain, it is just not recognized by the official node software.

As for customer identification, it is typical for applications to require users to pass an identity verification at the account opening process before the account is activated for use. This can be achieved as well inside the client/node software. A whitelist of public keys that have passed the identity verification will be introduced, and only data from this list of public keys are recognized by the software.

With the above concepts in mind, a significant portion of the world’s databases in use today are suitable for migration to blockchain databases. Elements of a traditional database can have a new interpretation as objects in a blockchain environment. The followings are examples of basic objects:

- Public Key: the public part of a key pair generated by users
- Address: an abbreviated form of public key
- Virtual Identity/Avatar: long term use identity, as compared to public key, which can be for temporary use
- Organization: an identity associated with and managed by multiple virtual identities/avatars
- Fungible: virtual asset/token of a fungible nature, such as currency and share etc.
- Account: a container of fungibles for an identity, like a bank account. Not to be confused with user account of traditional databases

The followings are examples of basic relations:

- Ownership: relations between identities and objects
- Creation: relations between objects and identities who create them

- Issuance: relations between token issuer and fungible

The followings are basic user database operations:

- Create database
- Insert object
- Update object
- Delete object
- Create index
- Query by index key value

Objects, in the form of JSON objects, are pretty powerful data structures to represent structured data. Key-value pairs can be considered a simple example of objects. A key in a key-value pair should not be confused with public key of a virtual identity. This term is sometimes also referred as name-value pair to avoid confusion. Keyspace or namespace scope in the database can either be local to the user or global.

Under an ownership type of data model, the data object may be regarded as "owned" by the identity who inserted it, meaning it can only be modified or deleted by this owner. For global namespace, there is a global namespace resolution problem. This can be understood as global uniqueness constraint problem. When a user attempts to insert a key-value pair, an observer sees the key or name in the broadcast and then makes a competing insert of the same key or name, which may get confirmed into the blockchain instead of the original insert. Namecoin introduced a protocol to deal with this issue. The idea goes like this:

- User sends a pre-insertion reservation transaction, where the key/name of the insertion is hidden via hashing. The protocol understands that the reservation transaction reserves the insertion of the given key for some period.
- Wait for the pre-insertion reservation transaction to confirm.
- Then broadcast the actual insertion transaction to the network. The insertion transaction should include a link/reference to the reservation transaction to pass protocol validation that the insertion and the reservation match each other.

Since the squatter does not know what the key or name is at the time the reservation transaction is broadcasted, it would not be able to get in before the actual owner, unless a reorganization of the blockchain happens after the insertion transaction is broadcasted. However, this is still unable to prevent squatters from guessing what other people want and claiming them in advance, like in the domain name system.

Ownership can be transferred. During the transfer transaction, the owner of the object is modified. By default, only owners can modify or delete an object. However, other models which allow more flexibility are also considered. For example, a documentation or wiki application may not require ownership of each data record. Once the object is inserted, everyone is free to modify or delete them. Another possible way is to utilize a

whitelist of identities who are allowed to modify the object.

Advanced Database Features

The platform also plans to introduce advanced database query features. An object-relational query language such as those similar to MongoDB, is more flexible than the traditional relational query model, also known as SQL. Google's MapReduce also presents a new form of data processing.

Database Migration

Migration features are extremely important for a database. As a database scales, it would be more cost effective to migrate it to a separate blockchain of its own, so the blockchain fees can be lowered specific to the application itself. The platform plans to provide migration tools to move database from one blockchain to another.

Modularity Goals

Modularity is an important design goal to lower the system complexity and reduce future development and maintenance cost, not only for the platform itself but also for the individual blockchains running applications in the ecosystem.

Layers of protocol:

- Consensus management layer
- Block tree management layer
- Interchain processing layer
- Transaction processing layer
- Data format layer
- Peer-to-peer network layer
- Internet protocol layer

System components:

- Pluggable consensus models
- Pluggable business logic container
- Database management component
- Database operation component
- Database query component
- Shared peer-to-peer networking
- Full node with blockchain processing
- Smartphone based light-weight cold wallet
- Smartphone based light-weight hot wallet
- Browser based wallet

Consensus Systems

The original Proof-of-Work consensus used by Bitcoin is now the breakthrough where it all began. For more than eight years in running, Bitcoin's system has certainly proved its reliability.

However, the rising energy consumption and centralized mining pools have become targets of criticism. This is why Proof-of-Stake consensus was introduced in 2012 through Peercoin [King 2012]. The major difference between Proof-of-Work and Proof-of-Stake is that instead of allocating weight based on computing resource consumption as in the case of Proof-of-Work, Proof-of-Stake consensus systems allocate weight relative to the amount of coin holdings participating in the consensus activity, also known as block minting. This algorithm decouples the consensus security level from system energy consumption level and eliminates the requirement of energy consumption in order to reach consensus, thereby resolving the energy concerns over Proof-of-Work, while reducing overall system operating cost in the process. Proof-of-Stake consensus is a major breakthrough as it significantly lowers the cost of blockchain technology and thus the entry barrier, enabling a vastly diversified blockchain ecosystem.

Nevertheless, there are concerns over Proof-of-Work and Proof-of-Stake consensus mechanism, including the lack of incentives for nodes to perform hardware upgrades and the random process of block generation. These are proven to be major obstacles to scaling blockchain. And after careful evaluation, our team has devised the brand new Supernode Proof-of-Stake (SPoS) consensus, to both incorporate the goods and discard the bads with the old mechanisms. SPoS consensus will serve as the enabling technology for blockchain to reach a global scale.

Supernode Proof-of-Stake consensus mechanism dictates that elevated nodes (supernodes) act as minting pools while holders of VSYS coins, native currency of the blockchain, take up the role as minters through leasing their coins to supernodes. Interests will be paid to coin owners who leased their coins to supernodes for minting. This new incentive model does not only ensure the quality of the nodes, but also guarantee a truly decentralized ecosystem where VSYS coin owners have the actual power to govern the network. At the same time, the system also allows for contention to be supernodes at any moment through determining a winner among contenders by comparing their minting average balance. This innovative mathematical approach ensures the system carries enough stake liquidity while reduces busy contention attack. More detailed information regarding the Supernode Proof-of-Stake consensus mechanism is available in the SPoS whitepaper.

Mainchain-Sidechain Model

The platform introduces its own model for mainchain and sidechain. A blockchain S is called a sidechain of another blockchain M, the mainchain, if S satisfies:

- Awareness: full nodes of S are also full nodes of M and process the entire blockchain of M

- Synchronization: S observes abstract clock synchronization to M

Abstract clock synchronization deals with the ordering of blocks between the two blockchains. Imagine the blockchain as an abstract clock, whereof each block in the chain is a clock tick. It is called abstract as it has nothing to do with the local timestamps written into the blocks. Timestamps are local values that cannot determine the correct ordering of events globally. Instead, block number inside blockchain can determine a global time sequence. Observers can safely say events in a previous block always happen before events in a later block regardless of their timestamps.

When a sidechain block is generated, it links to the latest mainchain block as its mainchain parent. Multiple consecutive sidechain blocks are allowed to share the same mainchain block as their mainchain parent. This mainchain-sidechain parent-child relationship must also be order-preserving

This model of mainchain-sidechain allows us to develop a proprietary communication method between the two blockchains. Unlike Blockstream's proposal, our model does not require pegging on sidechains, thus giving sidechain projects much more freedom to innovate.

Cloud Features

The platform plans to provide toolsets to sets up blockchain for applications. Blockchain template preparation allows user to choose from different protocol parameters and pluggable components such as consensus model. Once the template and options are selected, the platform provides toolset to deploy a new blockchain for the application, possibly even before a specific business logic needed for the application is developed.

Smart Contracts

Smart contracts [Szabo 1996] allow parties to create binding agreements without a third trusted party. Bitcoin used a simple scripting system when validating a transaction. But this scripting system is quite limited, and for the fear of potential issues, Bitcoin restricted its use among standard transactions. Later, Ethereum [Buterin 2014] redesigned a new smart contract system with a Turing-complete programming language known as Solidity. It was a significant progression for blockchain technology, as it allowed autonomous and decentralized contracts to be realized for many application scenarios.

EOS recently proposed to implement another smart contract system utilizing WebAssembly, also known as wasm. Wasm is an emerging web standard for low level in-browser client side scripting. Wasm is typically developed via C or C++ and compiled to Wasm.

The platform plans to support compatible implementations of Ethereum and EOS style smart contracts. Virtual machines will be implemented in a modular fashion so that applications can choose to enable a preferred style of smart contracts. As more competing smart contract systems are developed by the industry, they would also be evaluated and considered.

Scalability

A great deal of effort has been put on solving the scalability limitations on a single blockchain. While some of them are notable, we believe that the ultimate future of scalability in the ecosystem is the result of an unlimited number of blockchains. We envision a world with possibly billions of blockchains operating at the same time. As a result, the platform will allow applications to be run in separate blockchains if necessary, achieving complete scalability isolation to other application systems in the same ecosystem.

Usability

Usability has long been a bottleneck for the general acceptance of cryptocurrencies. The platform plans to develop both browser based wallet and mobile light-weight wallet for smartphones, all while having modern user experience and high security in mind. Cold wallet should be easily used by everyone, allowing users to safeguard their virtual assets with a peace in mind, free from the threats from the dark corners of the web.

Conclusion

V SYSTEMS platform is aimed to significantly lower the cost of blockchain technology and massively increase the competitiveness of blockchain as a database platform compared to traditional database systems. It is our vision that the future of blockchain is not only in a few billion dollar worth of blockchains, but in billions of blockchains as well. This is a revolutionary change and we are excited to push forward a whole new economic era.

References

[Nakamoto 2008] Bitcoin: A Peer-to-Peer Electronic Cash System,
https://bitcoin.org/bitcoin.pdf

[Back 2014] Enabling Blockchain Innovations with Pegged Sidechains,
https://blockstream.com/sidechains.pdf

[King 2012] PPCoin: Peer-to-Peer Crypto - Currency with Proof-of-Stake,
https://peercoin.net/assets/paper/peercoin-paper.pdf

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

[Buterin 2014] Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,
http://www.the---blockchain.com/docs/Ethereum_white_paper---a_next_generation_smart_contract_and_decentralized_application_platform---vitalik---buterin.pdf