Metaverse Dualchain

An Implementation of Next Generation Secure, Scalable and Interoperable Dualchain Network Architecture

Draft 0.6

By Eric Gu

Hao Chen

Ken Huang

May 22nd, 2019

Table of Contents

Issues that yet to be resolved

Struggles between Scalability and Decentralization

At present Bitcoin, with almost 10,000 nodes[1], is highly decentralized and censorship resistant but allows only 7 transactions per second and 1 million bytes every 10 minutes.

Private chains that maintain just 2-4 nodes, running Byzantine Fault Tolerance (BFT) consensus algorithms, are able to claim to achieve a million Transactions Per Second (TPS) and a great deal of storage space. However, they are at best federated databases, and not 'real blockchains', as they are neither decentralized nor censorship resistant.

Then, there are chains which compromise on these two extremes. EOS is one example, balanced at 21 nodes and tens of thousands of TPS. This makes it much faster than Bitcoin and Ethereum, while arguably maintaining certain degrees of decentralization - 21 nodes versus 3 to 4 nodes in private chain settings - or the many thousands of nodes seen in Bitcoin and Ethereum.

For the past 5 years, scalability has been a central concern of Bitcoin and blockchain more broadly. Bitcoin itself has gone through many changes (Segwit), forks (Bitcoin Cash), and addons (Lightning Network). Ethereum tried Casper (a kind of deposit-based security and authentication) as well. There are other proposals like Sharding or DAG which provide a temporary scalability solution. All of these are just tweaking the balance between decentralization and scalability, in a similar fashion to EOS.

Interoperability

Blockchains today exist as isolated islands: digital assets, digital identities, data, messages and smart contracts on one blockchain ecosystem aren't able to communicate or interact with

[1] https://bitnodes.earn.com/

other blockchains. Private chains and consortium chains generally lack transparency, and as such cannot be audited by any independent third party.

This lack of interoperability hinders adoption and the technology's progress, as any great improvement will generally be exclusive to one blockchain, and decentralized applications cannot be run across blockchains with different protocols.

Consensus

The most popular consensus algorithms today are still POW, POS, DPOS and variations of BFT algorithms. Blockchains maintaining POW at present include Bitcoin, BCH, Ethereum, Ethereum Classic and many others. Despite its track record in security, certainly as far as Bitcoin is concerned, POW is often criticized for wasting energy[2] and remaining prone to known attacks like 51% attacks, selfish mining attacks, and others.

The POS Consensus Algorithm does not yet have many great success stories to speak of. There are projects experimenting with different variations of POS, with NXT and Peercoin falling into that category.

Metaverse have already switched, and ETH also plans to switch to algorithms that are essentially combinations of POW and POS, aiming to significantly increase the cost of malicious attacks, thus ensuring far greater security.

The DPOS (delegated proof-of-stake) consensus algorithm was initially introduced by Daniel Larimer through the Bitshares Project, after which the EOS project developed DPOS into a system that operates on 21 masternodes. Despite EOS achieving thousands of transactions per second, it sacrificed decentralization and censorship resistance, which are two of the most celebrated features of blockchain.

[2] https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

Given the necessary tradeoffs in each consensus algorithm, a combination of two or more provides an opportunity to address the flaws in any consensus alone and to maximize performance in the trilemma mentioned above: decentralization, security and scalability.

Dualchain Network Architecture

Abstract

Dualchain Network Architecture is a combination of a decentralized, censorship resistant architecture and a scalable, programmable, fast architecture. It is a paradigm shift for the industry, aimed at addressing the specific issues present in modern blockchains as mentioned.

Instead of compromising scalability for decentralization or vice versa, the Dualchain Network Architecture (DNA) introduces an innovative, faster blockchain which runs parallel to the original mainnet. It is designed with the capacity to manage high transaction volumes on a per second basis. The introduction of a Dualchain structure optimizes scalability and decentralization by taking advantage of the benefits of different consensus algorithms, and for far greater interoperability when the protocol is adopted on other blockchains.

Consensus

In the Dualchain structure, multiple consensus algorithms drastically increase the cost of attacking the network interoperability between two chains and more generally, given the added complexity of attempting an attack on more than one consensus simultaneously.

Three Node Structure

The DNA architecture provides for three different node types with different functions: Child Nodes (unlimited), Regular Nodes (529) and Super Nodes (23).

Child Nodes delegate their staking power to Regular Nodes, Regular Nodes maintain full nodes of the blockchain ledger, receive DNA tokens as block rewards and distribute them to Child Nodes.

The 529 Regular Nodes vote for and elect Super Nodes, and then keep them accountable for the decisions they make. 23 Super Nodes make decisions on Requests for Changes, Improvement Proposals, and other major decisions.

All nodes participate in the staking process and receive newly minted DNA tokens and transaction fees as block rewards.

DNA Dual Chain Design

DNA's Dual Chain design is inspired by the layered design of the Internet.

The Internet utilizes a layered protocol architecture to address each functionality separately. Internet's interoperability is achieved when the Internet Protocol (IP) abstracted away the differences between different networking technologies. This layered abstraction design creates a common infrastructure for all sorts of different applications to connect and communicate despite the differences in the underlying network they use.

Similarly, instead of trying to tackle both scalability and interoperability in one big monolithic layer, DNA adopts a layered design addressing the two issues separately in two distinct layers – the Performance Layer (DNA-PL) and the Interoperability Layer (DNA-IL).

Dividing a system into multiple sub-layers gives each layer the flexibility to evolve separately and independently. As we've seen, this feature has allowed the Internet to be grow and scale at incredible speed as it upgrades from dial-up to fiber optic, 4G and 5G links. The speed of Internet's growth and the success of its interoperability would have been very difficult without its layered protocol architecture that addresses each functionality separately in different layers. Like the Internet, DNA's divided layered architecture will allow DNA-IL to improve Interoperability independently without affecting the performance of the DNA-PL layer. Similarly, DNA will be able to scale without damaging its compatibility and sacrificing its interoperability.

Lightning Network and Channel Building

The Lightning Network as it exists today allows for extremely fast transactions and significantly reduced fees. However, channels between the two transacting parties need to be pre-established in order for the payment routing to happen. As there is no clear incentive for transacting parties to create channels, the speed of adoption for the Lightning Network has been unsatisfactory.

In Dualchain architecture, channels amongst the 23 Super Nodes and the 529 Regular Nodes are already built due to the pre-existing delegating and staking processes. As long as both transacting parties have channels with any of the nodes, their transactions will be lightning fast and they pay only a fraction of the regular fee.

Data Feeds

Real world data like news events and stock prices are not automatically captured and included by blockchains. These data are often essential for smart contracts to function properly. In the DNA structure, Oracles which provide data feeds in a decentralized fashion become much more feasible as the scalability issue is addressed.

Applications

The **success of the Dualchain** is measured using the following criteria:

1. Number of assets created/exchanged in the system
2. Numbers of digital identities and smart contracts
3. Size of data feed and number of Oracles

DEX (Decentralized Exchanges)

Solving the scalability issue using Dualchain makes decentralized exchange not only possible, but essential. As the system is capable of handling tens of thousands of transactions per second, traders will come in to seek arbitrage opportunities, and thus provide liquidity.

Nodes and Super Nodes can act as brokerages to underwrite a new token offering, further driving liquidity.

Super Nodes may also issue derivatives like futures, options and warrants, thereby adding a protective hedging layer on the DEX.

Fees generated by the DEX are distributed through the staking process.

eSports and Massively Multiplayer Online Games (MMO)

MMOs by definition have large number of players with digital identities, and have their own internal digital economy with a variety of digital currencies, assets and messages. Value exchange in such an ecosystem can be achieved through smart contracts. The successful launch of a MMO based upon blockchain would have tremendous benefits to the large-scale adoption and proliferation of the technology.

Dualchain (DNA) Token

Staking

Proceeds accrued from staking are determined both by the number of DNA tokens and by the duration of staking.

Fees

The fees to send data feeds, tokens and smart contracts cross-chain are paid in DNA token.

Anti-spam

All transactions require DNA tokens to execute, making it more difficult for spammers to attack the system.

Media of exchange

The DNA token acts as the media of exchange between other assets cross-chain.

Collaterals

DNA can serve as the asset collateral for smart contracts.

Voting for Nodes

The number of DNA tokens weighted by the duration of staking dictates the voting power in the elections of nodes.

Security

Security is paramount for any blockchain project. DNA adopts a multi-layered approach towards security, set out as follows:

- Node security: Providing hardened OS settings to Child, Regular and Super nodes, such as disabling unused OS accounts, closing unused IP ports, applying latest security patches, etc.
- Consensus algorithm security: The POW algorithm has been battle-tested and has delivered impressive security to date. Various POS-based algorithms have seen varying degrees of security. DNA's BaseChain, the Metaverse mainnet, uses a POW/POS hybrid consensus to maximize security. For the DNA Chain, an additional consensus algorithm such as DPOS can be employed to increase security, and permissioned nodes can be deployed if necessary.
- Wallet security: DNA plans to use a wallet/account security approach similar to that of EOS. First, multisignatures (multi-sig) are a proven method in the blockchain world for signing a transaction by multiple parties, which is often required with certain wallets, accounts and particularly smart contracts. DNA allows assigning permissions to accounts that have a public and private key pair. Users also have an account name that consists of 12 characters. Each DNA account therefore, has two authorities:

owner and active, where the former can add or remove permissions to other authorities as a type of parent-child relationship. In DNA, an account name can be managed by a person or a group of people with different permission levels. So it is not just one person who manages these decisions, instead the action must be approved by several parties to the same account. This feature is very useful in escrow accounts, where the sender and recipient each have one of the public keys and a third party also has access to the account. This setting has real world utility, for example, in disputes or commercial contracts.

- The base chain uses secured Built In Smart Contract (BISC), a built in hardened template that has so far been deployed and used without security breaches. With DNA Chain, we allow both BISC and the flexibility of general purpose Smart Contracts which can support greater utility and features, but introduce complexity and security issues. To counter these additional risks, the result from the execution of general purpose Smart Contracts must be recorded on the Base Chain.
- Distributed Denial of Service attack (DDOS) protection is needed for protecting Regular and Super Nodes. The DNA project team will recommend relevant DDOS vendors when DNA goes live.

In addition to implementation of the above security measures, the DNA team will seek third party auditors to validate our security approach, audit the codebase, and perform penetration testing. We are in discussions with a number of blockchain security companies and will publish updates once there is a formal agreement.

Governance

23 Super Nodes make the key decisions on Requests for Changes, Improvement Proposals and other major decisions.

529 Regular Nodes vote for and elect Super Nodes, and keep them accountable for the decisions they make. All nodes will participate in the staking process and receive newly minted DNA tokens and transaction fees as block rewards.

Large numbers of Child Nodes delegate their staking power to Regular Nodes. Regular Nodes keep full nodes of the blockchain ledger, receive DNA tokens as block rewards and distribute these to their delegating Child Nodes.

Conclusion

Herein we have described an implementation of Dualchain network architecture on the Metaverse blockchain. By adding a DPOS blockchain with an extremely fast block time and using a multi-level super node structure to propagate lightning network channels, enabling lightning fast transaction speed and close to zero fees alongside the original POW/POS Metaverse Blockchain, the DualChain system drastically increases transactions per second and allows for much more data on-chain while safeguarding its decentralization and censorship resistance. The DNA protocol itself is a standard, meaning it can be applied to other public permissionless blockchains or permissioned consortium chains alike, and can establish standard APIs and protocols that allow messages, data, assets, digital identities and smart contracts from different blockchains to interact. As a result, decentralized applications (DAPPs) can be deployed across multiple platforms, with high confidence in security and scalability. Permissioned (private/consortium) blockchains can also benefit from the improved transparency provided, as they can easily be audited by third parties upon implementing this protocol.

References

[1] Satoshi Nakamoto “Bitcoin A Peer to Peer Electronic Cash System” 2008.

[2] Joseph Poon and Thaddeus Dryja “Lightning Network White Paper” 2016.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.