Next Generation Secure, Scalable and Interoperable Dualchain Network Architecture

Alex Lightman, Eric Gu, Ken Huang, Chen Hao
Table of Contents
DISCLOSURE............................................................................................................................. 5
Overview ......................................................................................................................................... 6
 What is DNA Chain ? .................................................................................................................... 6
 Five main problems existing with current public chain addressed by DNA............................... 6
 1: Identity: ..................................................................................................................................... 6
 2: Security: .................................................................................................................................. 6
 3: Reliable data source: .................................................................................................................. 7
 4: Performance and scalability: ....................................................................................................... 7
 5: Interoperability: ....................................................................................................................... 7
 DNA Technology Stack — Delivering Performance & Interoperability ............................................ 7
 What is the Dualchain Network Architecture? .............................................................................. 8
 How does the DNA chain interact with the Metaverse Blockchain? ................................................ 8
 What is KrawlCat’s role within the DNA technology stack? ............................................................ 9
 Key points to note re: DNA technology stack .............................................................................. 9
 Security and Digital Identity ......................................................................................................... 10
 Current Problems and Challenges with Identity and Identity Management Systems (IDMS).......... 11
  Managing Identities Is Overwhelming ....................................................................................... 11
  Identity Is Broken ........................................................................................................................ 11
  Current Options Have Real Costs .............................................................................................. 12
  Social Media Users Do Not Control Their Identities ................................................................ 12
  Private, Centralized Identity Platforms Are Not Secure .............................................................. 12
  Where have centralized systems failed our personal identities? ............................................... 13
  What is a Sovereign Identity? ...................................................................................................... 14
  How can Blockchain Safeguard our Digital Identities? .............................................................. 16
  The Metaverse Avatars – the Future of Blockchain Identity Management ................................. 17
 Security ......................................................................................................................................... 18
  Overview of Security Challenges ............................................................................................... 18
  DNA Approach to Security ........................................................................................................ 21
 Oracles and Reliable Data. ............................................................................................................ 23
 Performance, Scalability and Interoperability. ............................................................................. 25
 Internet Design: Building a Platform Featuring Scalability and Interoperability ......................... 25
  The Design Philosophy of the Internet ...................................................................................... 27
CONCLUSION

Appendix

Advisors

Team

DNA Roadmap, Long Term Goals, Milestones, and Relevant FAQ.

Roadmap overview

Selected Long-term goals:

Milestones:

Marketing, Outreach and Development Strategy and Tactics

FAQ on Selected Details of Roadmap and Token Sale

Conclusion

APPENDIX

Dualchain Network Architecture

Consensus

Three Node Structure

Lightning Network and Channel Building

Data feeds

Applications

DEX (Decentralized Exchanges)

eSports and Massively Multiplayer Online Games (MMO)

Dualchain (DNA) Token

Staking

Fees

Anti-spam
DISCLOSURE

Neither the delivery of this document at any time, nor any sales hereunder, shall under any circumstances create an implication that the information contained herein is correct as of any time subsequent to its date. Offers and sales will only be made to persons who are permitted to do so by appropriate local legislation in relevant jurisdiction, have the knowledge and experience to evaluate the merits and risks of the investment and who have the economic means to afford the illiquidity of the currencies offered hereby.

This White Paper is not intended to provide the sole basis of any investment or other evaluation involved legal entities and should not be considered a recommendation for further investigation. Each recipient is urged to determine its interest in investing based upon such investigations as it deems necessary for such purpose. Relevant legal entities and individuals will not be responsible for the consequences of any failure by any proposed investor to make such investigation or for any reliance by any proposed investor upon any statement contained in the White Paper.

All investments involve risk and may lose money.

The information set forth herein is believed by the Company to be reliable. It must be recognized, however, that predictions and projections as to the Company's future performance are subject to a high degree of uncertainty and no warranty of such projections is expressed or implied hereby. No representation, expressed or implied, is made by relevant legal entities or its directors with respect to the completeness or accuracy of the content of, or any other matter set forth in the White Paper. Updated versions of this White Paper will be available on the DNA website.

All discussions regarding DNA and its projects are to be considered confidential. Interested parties may not disclose to others (unless required to do so by law) that they are engaged in any evaluation of these or related projects. All communications, inquiries and requests for information relating to DNA should be directed to the address and phone numbers listed in the Contacts section of this document.
Overview

What is DNA Chain?

DNA Chain is an open-source public blockchain creating a decentralized ecosystem of digitized assets and identities. Through Blockchain as a Service (BaaS), it provides enterprises and individuals access to customized, convenient, and secure blockchain services.

It is a blockchain project that provides a foundational infrastructure for social and enterprise needs. Our goal is to construct a universe where digital assets and digital identities (Avatar) build the basis for asset transactions with the help of a value intermediary (Oracle), thus establishing a new blockchain ecosystem that will transform human society and allow us to enter the New Reality.

Five main problems existing with current public chain addressed by DNA

DNA chain is trying to solve 5 main problems existing with current public chain.

1: Identity:
DNA builds the Identity (Avatar) at the core of the DNA design. Indeed, self sovereign identity built at the core of a public chain is essential for wider use of public chain due to the needs to build reputation score for the identity, the needs of KYC/AML, the needs to having a token economy model based on the ownership of data and assets and the needs to protect privacy of users.

2: Security:
Defensive in depth approach is needed in designing a public chain. It is not just consensus algorithm security (although it is one of the most important parts of public chain). Ensuring safety is also about smart contract security, wallet security, and node security. DNA leverages hybrid consensus algorithm (POW+POS+DPOS) for better consensus algorithm security. DNA uses template based smart contract (instead of full Turing complete smart contract) to limit security vulnerabilities. For wallet security and node security, DNA will also design security controls needed.
3: Reliable data source:
In order to implement real world application using public chain. It is necessary to provide reliable data source to avoid garbage in and garbage out problem. DNA leverages Avatars and Oracles for reliable data source.

4: Performance and scalability:
Main limiting factors for scalability is the network bandwidth, computational power of participating nodes, and storage. DNA uses child chains to partition the network bandwidth, nodes, and storage.

5: Interoperability:
At present, separate blockchains exist in isolation. A party transacting with an ERC-20 token on the Ethereum network may not send that asset to a different chain, like EOS. To build a truly inclusive blockchain ecosystem, interoperability needs to be built-in to multiple protocols.

DNA Technology Stack — Delivering Performance & Interoperability
Although blockchain in its current form has been around for more than a decade, there remain several sticking points which many protocols have struggled to overcome. The most pressing issues generally center around handling a high number of requests, leading to delays and rising fees, and communicating between chains.

For example, the Bitcoin protocol, launched in 2009, has almost 10,000 full nodes on its network and maintains a high level of security and decentralization, but inadequate transactions per second or TPS. This issue has become known as ‘scalability’, the ability of a blockchain protocol to handle high volume of transactions at once, which many experts believe is essential for building a functioning ecosystem of decentralized applications and smart contracts.

On the other hand, many private chains claim to offer TPS in the millions and therefore a high degree of scalability, although they have just a few federated node operators. As a result, they lack adequate decentralization and therefore compromise on security and parity. The quest to strike a balance between these desirable traits has often driven new innovations in the blockchain space, such as the Lightning Network and Segwit in Bitcoin and the planned implementation of sharding on Ethereum.
The Dualchain Network Architecture, or DNA blockchain protocol, deploys a novel and highly sophisticated technology stack to solve the problems of scalability, security, and decentralization. However, the processes which go into making the DNA and Metaverse protocols work are complex, with many different technical aspects. Here, we look at the technology behind the DNA protocol and its foundational structure.

What is the Dualchain Network Architecture?
The Dualchain Network Architecture, or DNA, is a chain that runs in parallel to the original Metaverse ETP chain to facilitate higher transaction speeds and enable the use of Lightning channels. Inspired by the layered design of the internet, the DNA Dualchain focuses not on solving the blockchain trilemma in a single monolithic protocol, but instead by introducing two separate layers for performance and interoperability.

Named the Performance Layer (DNA-PL) and the Interoperability Layer (DNA-IL), this layered approach allows issues of interoperability or scalability to be approached and solved separately, rather than in a single chain.

So, why is this approach needed? Essentially, while other projects have attempted to solve interoperability and scalability on one chain and then encountered performance issues when both solutions are needed, DNA approaches these problems in parallel. This allows the DNA blockchain to scale without affecting interoperability and likewise allows interoperability without compromising on scalability.

How does the DNA chain interact with the Metaverse Blockchain?
The Metaverse mainnet, a hybrid PoW and PoS protocol, serves as DNA’s base chain. In other words, DNA is built on top of the Metaverse blockchain. It’s important to note however that the DNA protocol is designed as a standard, which will enable it to be used and applied across a range of other public or private blockchains. Like Lightning networks in other chains, DNA allows for a high TPS without delays on the main Metaverse blockchain. But unlike Lightning networks, DNA allows participants to transact without pre-establishing a dedicated payment channel. Instead, DNA features prebuilt channels between 23 Super Nodes and 529 Regular Nodes. If participants have an open channel to any one of those nodes, their transactions will be lightning fast.

Therefore, like Lightning networks, the DNA protocol operates separately to the Metaverse blockchain — facilitating payments and then communicating with the Metaverse blockchain once payment channels are closed, in order to update the blockchain.
Exchanging data between these two chains, for actions such as smart contract creation, dApps, and complex transactions, is essential. This is the impetus for Metaverse’s and the DNA protocol’s strategic partnership with KrawlCat, which enables cross-chain transactions and brings real-world data on-chain.

**What is KrawlCat’s role within the DNA technology stack?**

Distributed ledgers are open and transparent stores of data and value, as most blockchain enthusiasts will know. In simple transactions of value, for example where Alice sends one Bitcoin to Bob, there is little in the way of transactional data attached to that trade, as it is a peer-to-peer transfer of fungible assets between two parties.

However, when different digital assets are transferred between two parties, such as a non-fungible token pegged to the price of an ounce of gold, there are very few ways to actually verify that the underlying party has the tangible assets to back that digital token. Another example would be up-to-date pricing data from world foreign exchange markets or stock prices, which by itself a solitary blockchain has no outside knowledge of.

This is where Oracles providers like KrawlCat Generalized Oracle come in. Oracles bring off-chain data, some of which we’ve described above, onto the blockchain. We could think of this as migration of web 2.0 data into a web 3.0 environment, where data becomes integrated within the decentralized ledger, and can be used to inform many different types of transactions. This makes transactions on a blockchain truly ‘trustworthy’, as participants know that their transaction data has been verified by one or more third-parties.

KrawlCat is a generalized Oracle, which allows it to communicate across different blockchain protocols for true interoperability. Between the Metaverse blockchain and the DNA blockchain, the KrawlCat protocol acts as a bridge connecting the data of the two.

**Key points to note re: DNA technology stack**

The technology underpinning DNA, KrawlCat, and the Metaverse blockchain are all founded on a highly sophisticated technology stack, which is constantly evolving as the protocol matures. But what are the most important aspects to note regarding this innovative new approach to a blockchain protocol?
The defining feature of the DNA chain is that it is being built in layers. Like the layers which make up the internet, DNA is working to solve both interoperability and scalability at the same time, without compromising on the performance or integrity of either.

Equally important is the DNA protocol’s status as a blockchain standard. It’s worth remembering that once the DNA protocol’s solution grows in popularity, it can be deployed across multiple blockchains worldwide — finally solving the scalability and interoperability dilemma.

Security and Digital Identity

"Identity will be the most valuable commodity for citizens in the future, and it will exist primarily online."

Eric Schmidt - Google Chairman
Current Problems and Challenges with Identity and Identity Management Systems (IDMS)

Managing Identities Is Overwhelming
In today’s highly-digitized environment where the overlapping demands of healthcare, banking, education, commerce, entertainment, social media and regulation require consumers to manage a portfolio of identities and log-on credentials just to function in online and real-world environments. In fact, according to Dashline3, in the United States, the typical email address is now connected to 130 different accounts. And this number does not even take into account the additional “identities” associated with physical IDs, access badges, fobs and drivers licenses we all carry.

Identity Is Broken
Single sign-on/password management software has helped ease this pain, but time and again sophisticated hackers have proven themselves adept at cracking into these programs and quickly gaining access to user data. Popular password managers LastPass, Keeper, Dashlane and 1Password have all been hacked in recent years. Hackers also successfully attacked SSO provider OneLogin. Quoting relevant OneLogin Statement:

“On Wednesday, May 31, 2017, we detected unauthorized access to OneLogin data... OneLogin believes that all customers served by our US data are affected and customer data was potentially compromised” Such statements have become all too common, serving as another reminder that in today’s digital environment, no person or entity is immune. This “password pain” has driven many users to leverage their social IDs associated with their Facebook and Google accounts; however, many find this to be an intrusive process.”
**Current Options Have Real Costs**

Ironically, despite the widespread threat of ID theft, most consumers find it overwhelming to manage the myriad of passwords needed to gain entry into today’s multitude of digital passageways. As a result, many let down their guard or practice poor digital hygiene, rendering their ID credentials even more vulnerable to theft. A recent Janrain survey found:

- Passwords discourage 58 percent of consumers from signing up for a new account
- 75 percent of users report suffering from “password fatigue”
- 37 percent admit to forgetting their password weekly.
- A 2014 Gigya survey found that over 80 percent of consumers have abandoned online registration because they didn’t want to share their data.

Here are selected relevant links

- [https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/](https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/)

**Social Media Users Do Not Control Their Identities**

In addition to privacy concerns, Facebook and Google account holders (among others) have had accounts disabled or closed with little explanation. Often, these closures occurred because users unknowingly violated the “terms of service” agreements these companies demand users abide by. Rightly or wrongly, most social media users are only one “inappropriate” post or comment away from being locked out of their accounts, with little recourse for recovery once an account is closed. The reality is that technology heavyweights such as Facebook, Google, LinkedIn and others control identity data — not the user. These companies are not accountable to users. They can deny access at any time, for any reason and are not required to provide explanation or recourse.

**Private, Centralized Identity Platforms Are Not Secure**

No link between the online and real worlds. Current digital identity solutions have another significant usage flaw — they are rarely applicable to real-world activities. Although vulnerable, online log-ins at least offer a convenient method to toggle from one website to another. But in real-world, brick-and-mortar environments, online logins have no use, forcing consumers to carry around a wallet full of physical IDs such as gym memberships, driver’s licenses, building access cards, etc.

One more example that illustrates the substandard state of today’s identity management system is the lack of security and consistency surrounding current username/password-based solutions. The massive 2017 Equifax breach demonstrates how easily an allegedly state-of-the-art
security network can be infiltrated and how traditional SMS-based, two-factor authentication (2FA) processes are ineffective and create a false sense of security at best.

At present it is almost impossible to live our day-to-day lives without transacting online or using the internet for our social interactions. As of 2019 there are over 4 billion active internet users – more than half the world’s population – and worldwide the average person spends 6 hours and 42 minutes online each day.

Our hyper-connected society provides for huge growth in productivity, easier social interactions, and a reduction in the effects that distance and borders have on communication and finance.

However, this connectedness has come at a heavy cost. Now more than ever our personal data – identities, financial information, addresses, life events – is freely available to be viewed or even leaked online. But just as technology has provided a multitude of new ways for criminals and companies to exploit our personal data, emerging technology is also helping in the fight for our data sovereignty.

**Where have centralized systems failed our personal identities?**

Many users think little of entering their personal data into websites like Facebook, Google, Amazon, or even smaller and less established sites. Although many of these sites are considered relatively safe, once a user consents to their information being used by third parties they have little control over how it is used and stored. Moreover, as data breaches can and do happen, our personal data can be stolen by criminals who may then use it to access our personal accounts.

This happens because the data stored on companies’ internal databases is most often siloed – stored in a single location and vulnerable to attack. At present, this ad-hoc approach to data and identity management is the best available solution to companies, as the internet in its current form lacks an adequate identity management layer.

This leaves our personal data open both to internal viewing by the staff of companies with whom we agree to share our data, and also at risk of being ‘leaked’ in a hack on the database. Similarly, there are many instances where websites themselves are dishonest in the way they use personal data. One of the highest profile cases in recent years was the Cambridge Analytica scandal, involving the social media giant Facebook.
In early 2018, it was discovered that UK-based research group Cambridge Analytica had been compiling sensitive information harvested from individuals’ Facebook profiles for use in politically motivated advertising.

This scandal prompted a huge resurgence in the anti-trust movement, casting serious doubt on the assumption that internet giants had the best interests of their users at heart when it came to their digital identities.

As a result, many lobbyists and politicians called for tighter data protection laws, and many members of the public were left questioning how they might keep their online identities safe. More importantly, however, it helped to shed light on the concept of a ‘sovereign identity’.

**What is a Sovereign Identity?**

Essentially, a self-sovereign identity is one in which a user retains full control over every aspect of their personal data and how it is controlled or shared. Instead of the siloed information users freely give to third-party sites at present, sovereign identity management solutions would verify an individual’s credentials without them needing to share all of their personal details.

This concept rests on the assertion that our digital identities are a valuable asset, over which we have fully sovereign ownership. As a result, the misuse or unauthorized use of our digital identities would constitute a violation of an individual’s self-sovereign property. Many companies walk a blurred line between the fair use of our digital data, and overstepping their usage rights.
In the European Union, stricter data protection laws such as the GDPR legislation introduced in 2018 have added greater protections to our personal information. Despite this, there are no widespread solutions in place to protect our digital identities online and as a result, companies, advertisers, and researchers take advantage of our identities as we navigate the web.

However, blockchain is putting power back into the hands of users and restoring their control over their own digital identities. Dulachain DNA blockchain technology is empowering users to take back control of their online personal identities, starting with the flaws extant in current identity management infrastructures.
How can Blockchain Safeguard our Digital Identities?

A self-sovereign digital identity is a concept made possible through blockchain-based identity management, although to date there have been few projects to successfully deploy such solutions. Using the cryptographic principles underlying blockchain technology, we can for the first time prove ownership of a user’s digital identity through mathematical proofs.

In practice, it means that a digital identity stored on a blockchain cannot be forged, as it would not be validated by other network participants. Likewise, as each user holds the private key to their digital identity on the blockchain, no personal data can be sent or shared without its rightful owner signing the related transaction.

It may at first be difficult for the average user to envisage their digital identity being stored in a single address on the blockchain. Instead, it’s easier to use a concept many users are already highly familiar with – digital avatars.
Avatars are ubiquitous on digital platforms – a digital representation of a particular person or entity. These avatars are often tailored to look like their owner in real life, but even if they are not visual in nature, avatars serve as personal data repositories which can interact with their digital world.

Now, through blockchain technology a new type of avatars can be proposed – one which uses an individual’s digital identity to hold assets. To provide a symbol of users’ online identities, Metaverse has created the ‘Metaverse Avatar’. These digital representations of real individuals can act as self-contained digital identities, enabling interactions with blockchain based services and assets.

For example, an Avatar on the Metaverse blockchain may represent a single real person, an individual machine in an IoT system, or a corporate entity.

Although blockchain protocols like Bitcoin have provided a pseudonymous way to transact online, the reality is that most real-world companies require some data on their users or customers in order to provide their services and comply with regulations.

With a blockchain-based identity solution such as the Metaverse Avatar, an individual’s data is protected through zero-knowledge proofs and encryption, which allows the Avatars to reveal
certain required information only with the explicit approval of the individual themselves and without sharing unauthorized personal data.

In conclusion, blockchain-based identity management solutions like the Metaverse Avatars will allow individuals to manage every aspect of their personal data with ease and confidence, delivering a long-awaited functional identity layer to the internet for the first time and facilitating a self-sovereign model of digital identity.

Security

Overview of Security Challenges
Blockchains can provide security advantages to a variety of applications by removing or reducing the need for trusted third parties. Second layer protocols can add more flexibility and may help better scalability, privacy, and interoperability. These foundational building blocks can provide enhanced integrity and resiliency. However, blockchains do not solve all security issues, and careful examination of the risks and challenges of blockchain usage is needed.

Some of these issues and associated mitigations are discussed below.

Private Data Leak:
When a user shares personal data with a relying party, the relying party may share that data outside of the context of the IDMS. This is a significant problem for any identity management system where user personal data is shared. However, this can be minimized by the use of
minimal presentation disclosure mechanisms. For example, zero-knowledge protocols may be utilized to share presentations that contain only the necessary information for a given interaction to relying parties rather than full credentials.

Separately, architectures that put less data on-chain may in general be more privacy preserving, but it depends on the exact architecture being used and how that data is being stored (e.g., unencrypted, encrypted, pointers to outside repositories, or hashes). Finally, vulnerabilities may be found in the authentication and messaging protocols used by a given system to support peer-to-peer data transmissions.

**Metadata Tracing:**
Pattern analysis techniques may be applied by attackers to on-chain metadata and possible interceptions of messages between parties. They may look at, for example, the time that transactions or credentials were submitted to the blockchain, which issuers signed them, or the IP addresses that they were broadcast from. This information may be leveraged by attackers to compromise the confidentiality of Personally Identifiable Information (PII). This correlation risk can be minimized by decoupling users from a unique persistent identifier through the use of pairwise pseudonymous identifier (or more advanced identifier unlinkability techniques).

Zero-knowledge proofs may also be used to obfuscate the details of blockchain transactions.

**Replay Attacks and Impersonation:**
A rogue relying party can attempt to collect user credentials and presentations in the aim of fooling another relying party into believing that they are that user. This kind of man-in-the-middle attack can be mitigated through relying parties using certain challenge response protocols and encrypted tunnels such that the subjects must always prove their identity (that they know the private key for the identifier associated with the transaction).

**Private Key Compromise:**
In most IDMSs, knowledge of a private key for an identifier is equivalent to owning the identifier. Thus, preventing the compromise of private keys is essential. Keys can be compromised due to errors in key generation, storage, or use, or can be stolen by malicious actors. Human errors can be mitigated through well-designed tools for key management and secret sharing (typically that is a user-friendly identity wallet), a system may be secure only if it is usable. Once lost or stolen, identifier recovery mechanisms may be implemented to enable a subject to regain control of an identifier. In general, architectures that provide more privacy may reduce the risk of being targeted and having private keys stolen.
Data Withholding Attacks and Data Availability Issues:
When users manage their identifiers and credentials themselves, they benefit from a high-level of autonomy and can ensure the availability of their data. An alternate approach is for users to choose to rely on custodians to hold and manage their data for convenience. However, custodians can misbehave, compromising the ability of the user to access their identifiers and credentials. Although proper delegated control restrictions can help constrain such a rogue custodian, this does not prevent data withholding attacks.

Even a well-behaved custodian can experience temporary service disruptions (or even go out of business), thus making user data unavailable. Therefore, it may be important for a subject to implement data redundancy by storing multiple copies of identifier and credential data in locations that are either directly controlled by the user (such as identity wallets across different personal devices) or delegated to custodians with proper access and control permissions in place. This could involve identity hubs as mentioned in Section 3.3 on Emerging Standards. Note that these are issues with traditional IDMSs and that the use of blockchain can be seen as a potential improvement.

Quantum Computers:
Blockchain networks depend on cryptography for their security, in particular, on public-key cryptography. If a sufficiently powerful quantum computer is built in the future, the most widely used public key cryptographic algorithms in blockchain systems will become insecure. This represents a long term concern for identity data stored on a blockchain. Note that this concern applies to the entire Internet; it is not just a concern for blockchain technology.

Smart Contract Flaws:
The smart contracts implemented to support the blockchain-based IDMS may have security flaws. Such contracts are usually short and concise, but nonetheless there have been flaws discovered in published smart contracts that enabled them to be compromised. Audits, tests, and the use of well-audited libraries can help mitigate this risk. Furthermore, data integrity at the smart contract level may be achieved by establishing permissions to prevent unauthorized participants from accessing and modifying user identifiers and credentials.

Some blockchain identity management system architectures (e.g., top-down authority models) may incorporate logic that creates single points of failure. For example, they may provide a certain type of participant a high level of privilege that could be improperly used. This can be mitigated against by instituting appropriate separation of authorities between participants along with a security analysis of the system to identify single points of failure with respect to bad
actors in the system. Furthermore, governance architectures that rely on game theoretic incentives have their own risks

**Oracles and Second Layer Protocol Compromise:**
A blockchain IDMS may integrate off-chain data, logic, and processing in the form of oracles and second layer protocols. Should they get compromised, the on-chain part of the system may not be able to identify the threat adequately and cope with the compromised data, resulting in a “garbage in, garbage out” situation. It is therefore important to ensure that necessary checks and balances are in place.

**DNA Approach to 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.

**Oracles and Reliable Data.**

In order to implement real world application using public chain. It is necessary to provide reliable data source to avoid garbage in and garbage out problem. DNA leverages Avatars and Oracles for reliable data source.

Oracles are trusted entities that bring external information into the blockchain\(^1\). Blockchain as a distributed shared storage doesn’t have direct access to data that lives outside of its network. In order to guarantee the security of the blockchain network smart contracts are generally executed in closed environments, preventing them from accessing external data important for

---

their execution\textsuperscript{2}. Thus, smart contracts require services of an oracle. The role of oracles is not limited to simply querying the information from outside of the network, but also includes verifying the authenticity and validity of that data. Some authors define this as an “Oracles Problem”\textsuperscript{3} due to the challenges of bringing reliable data from real world into blockchain.

This aspect of oracles is crucial for the sustainability and fault tolerance of the blockchain, because oracles directly interact with smart contracts on the blockchain. Smart contract execution is triggered when a certain condition or data is provided by an oracle. Some contracts may initiate a financial transaction because of the trigger or settle disputes between parties. Therefore, it is important that oracles provide reliable and valid information to ensure consistency and validity of smart contract execution, making oracles an essential part of a successful blockchain implementation.

The concept of a blockchain oracles was developed mostly by the industry and blockchain solution developers and did not exist in academia previously. It is important to note that the concept of oracles in blockchain should not be confused with random oracles in cryptography or oracles machines in complex theory. Majority of resources today that discuss blockchain oracles or provide implementation examples are mostly created within blogs, websites and written as whitepapers. In academic papers the notion of blockchain oracles has been inconsistent and while some authors use the term verifier and reverse-verifier\textsuperscript{4}, others use concepts like trusted data feeds\textsuperscript{5} and validation oracles\textsuperscript{6}.

Some blockchain implementations describe components that act like blockchain oracles without specifically calling them as such, while others have built solutions that make blockchain oracles a central part of their blockchain implementation. One of the first solutions to the oracles problem was Town Crier, which is an authenticated data feed for smart contracts. It aims to ensure that information injected into the network comes from a reliable source and hasn’t been tampered with. To achieve this it uses “trusted software” enclave on Intel processors.


\textsuperscript{3}D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain technology overview,” 2018


Few early implementations of blockchain oracles are centered around prediction markets. Project Augur, a prediction market where individuals can wager on the outcome of future events, utilizes a decentralized oracles consisting of profit-motivated reporters whose task is to simply report on the real-world outcome of an event. Decentralized oracles have been introduced and utilized by projects like Augur, ChainLink, Astraea and aim to overcome some of the shortcomings of a single oracle.

Primary challenge is the centralization since single oracles must be run by a third party as a service, making them vulnerable to tampering. Decentralized oracles aim to address this challenge by using a similar to blockchain consensus mechanism across multiple oracles. These projects are examples of attempts to develop solutions to the oracles problem by introducing new use cases, some of which are already profit generating businesses.

**Performance, Scalability and Interoperability.**

**Internet Design: Building a Platform Featuring Scalability and Interoperability**

DualChain utility can be compared with utility of Internet that was described as “packet switched communications facility in which a number of distinguishable networks are connected together using packet switched communications processors called gateways which implement a store and forward packet-forwarding algorithm” (see e.g. D. Clark, “The Design Philosophy of the DARPA Internet Protocols,” ACM Computer Communication Review – Proc SIGCOMM 88, vol. 18, no. 4, pp. 106–114, August 1988).

The packet from the Internet definition above is similar to transaction defined in DNA. The DNA child chains (similar to gateways) do not store any connection specific data to allow connection less transactions between end nodes. The DNA main chain acts as IP layer for generic communication. The DNA chain is similar to TCP layer.

---

Overall, there is considerable interest today in the use of blockchain technology to provide better visibility into shared information among a number of participants and systems arranged in a decentralized P2P topology. Several challenges in blockchain technology remain to be addressed, including the interoperability, survivability and manageability of blockchain systems.

Crucial to answering these challenges is the need to understand aspects of the Internet architecture that has made it scalable, resilient and a commercial success as a global connectivity infrastructure. DNA utilizes the design philosophy for interoperable blockchain systems, similar to the design philosophy and key design principles of the Internet architecture to create its interoperable blockchain architecture.

Interoperability is a crucial requirement for the survivability and manageability of blockchain systems. An interoperable blockchain architecture, in which common components of the blockchain architecture can begin to be standardized, leads to lowering of development costs, better reusability and higher degree of interoperability.

Sufficient attention needs to be placed on challenges around the aspects of the manageability of blockchain systems, the survivability of blockchain networks, and the cybersecurity of systems and infrastructures that participate in blockchain communities. Crucial to answering these challenges is the need to understand aspects of the Internet architecture that has made it scalable, resilient and a commercial success as a global connectivity infrastructure.

The goal DNA is to implement interoperability, survivability and manageability for blockchain systems. Our overall goal is to develop a design philosophy for an interoperable blockchain architecture, and to identify some design principles that promote interoperability using lessons learned from the three decades of the development of the Internet.

Currently there is considerable interest in blockchain systems as a promising technology for the future infrastructure of a global value-exchange network (what some refer to as the “Internet of value”). The original blockchain idea of Haber and Stornetta\(^8\) is now a fundamental construct

---

\(^8\) See S. Haber and W. Stornetta, \"How to Time-Stamp a Digital Document,\" in Advances in Cryptology - CRYPTO’90 (LNCS 537), 1991, pp. 437-455. And D. Bayer, S. Haber, and W. Stornetta, \"Improving the efficiency
within most blockchain systems, starting with the Bitcoin system which was first to adopt the idea and then deployed it in a digital currency context.

Many parallels have been made between blockchain systems and the Internet. However, many comparisons often fail to understand the fundamental goals of the Internet architecture as promoted and led by the Defense Advanced Research Projects Agency (DARPA), and thus fail to fully appreciate how these goals have shaped the Internet to achieve its success as we see it today. There was a pressing need in the Cold War period of the 1960s and 1970s to develop a new communications network architecture that did not previously exist, one that would allow communications to survive in the face of attacks.

If blockchain technology seeks to be a fundamental component of the future global distributed network of commerce and value, then its architecture must also satisfy the same fundamental goals of the Internet architecture, and DNA aims to utilize this approach.

The Design Philosophy of the Internet

In considering the future direction for blockchain systems generally, it is useful to recall and understand goals of the Internet architecture as defined in the early 1970s as a project funded by DARPA. The definition of the Internet as view in the late 1980s is the following: it is “a packet switched communications facility in which a number of distinguishable networks are connected together using packet switched communications processors called gateways which implement a store and forward packet-forwarding algorithm”

Fundamental Goals

It is important to remember that the design of the ARPANET and the Internet favored military values (e.g. survivability, flexibility, and high performance) over commercial goals (e.g. low cost, simplicity, or consumer appeal), which in turn has affected how the Internet has evolved and has been used. This emphasis was understandable given the Cold War backdrop to the packet-switching discourse throughout the 1960s and 1970s. The Advanced Research Projects Agency

Network (ARPANET) was an early packet-switching network. It was the 1st network to implement the TCP/IP protocol suite.

The DARPA view at the time was that there are seven (7) goals of the Internet architecture, with the 1st three being fundamental to the design, and the remaining four being second level goals. The following are the fundamental goals of the Internet in the order of importance:

**Survivability:**
Internet communications must continue despite loss of networks or gateways.

This is the most important goal of the Internet, especially if it was to be the blueprint for military packet switched communications facilities. This meant that if two entities are communicating over the Internet, and some failure causes the Internet to be temporarily disrupted and reconfigured to reconstitute the service, then the entities communicating should be able to continue without having to reestablish or reset the high level state of their conversation.

Therefore to achieve this goal, the state information which describes the on-going conversation must be protected. But more importantly, in practice this explicitly meant that it is acceptable to lose the state information associated with an entity if, at the same time, the entity itself is lost. This notion of state of conversation is related to the end-to-end principle discussed below.

**Variety of service types:**
The Internet must support multiple types of communications service.

What was meant by "multiple types" is that at the transport level the Internet architecture should support different types of services distinguished by differing requirements for speed, latency and reliability. Indeed it was this goal that resulted in the separation into two layers of the TCP layer and IP layer, and the use of bytes (not packets) at the TCP layer for ow control and acknowledgement.

---

Variety of networks:
The Internet must accommodate a variety of networks.

The Internet architecture must be able to incorporate and utilize a wide variety of network technologies, including military and commercial facilities.

The remaining four goals of the Internet architecture are:

- distributed management of resources,
- cost effectiveness,
- ease of attaching hosts, and
- accountability in resource usage.

Over the ensuing three decades these second level goals have been addressed in different ways. For example, accountability in resource usage evolved from the use of rudimentary management information bases (MIB) into the current sophisticated traffic management protocols and tools. Cost effectiveness was always an important aspect of the business model for consumer ISPs and corporate networks.

The End-to-End Principle

One of the critical debates throughout the development of the Internet architecture in the 1980s was in regards to the placement of functions that dealt with reliability of message delivery (e.g. duplicate message detection, message sequencing, guaranteed message delivery, encryption). In essence the argument revolved around the amount of effort put into reliability measures within the data communication system, and was seen as an engineering trade-off based on performance. That is, how much low-level function (for reliability) needed to be implemented by the networks versus implementation by the applications at the endpoints.

The line of reasoning against low-level function implementation in the network became known as the end-to-end argument or principle. The basic argument is as follows: a lower level subsystem that supports a distributed application may be wasting its effort in providing a function that must be implemented at the application level anyway. Thus, for example, for duplicate
message suppression the task must be accomplished by the application itself seeing that the application is most knowledgeable as to how to detect its own duplicate messages.

Another case in point relates to data encryption. If encryption/decryption was to be performed by the network, then the network and its data transmission systems must be trusted to securely manage the required encryption keys. Also, when data enters the network (to be encrypted there) the data will be in plaintext and therefore susceptible to theft and attacks. Finally, the recipient application of the encrypted message will still need to verify the source-authenticity of the message.

The application will still need to perform key management. As such, the best place to perform data encryption/decryption is the application endpoints (there is no need for the communication subsystem to provide for automatic encryption of all traffic). That is, encryption is an end-to-end function.

The end-to-end principle was a fundamental design principle of the security architecture of the Internet. Among others, it influenced the direction of the subsequent security features of the Internet, including the development of the IP-security sublayer and its attendant key management function.

Today the entire Virtual Private Network (VPN) subsequent of the networking industry started based on this end-to-end principle. (The global VPN market alone is forecasted to reach 70 billion dollars in the next few years). The current day-to-day usage of the Secure Sockets Layer (TLS) to protect HTTP web-traffic (i.e. browsers) is also built on the premise that client-server data encryption is an end-to-end function performed by the browser (client) and by the HTTP server.

The Autonomous Systems Paradigm

Another key concept in the development of the Internet is that of autonomous systems (AS) (or routing domains) as a connectivity unit that provide scale-up capabilities. More specifically, the classic definition of an AS is a connected group of one or more networks (distinguishable via IP
prefixes) run by one or more network-operators which has a single and clearly defined routing policy.

The notion of autonomous systems provides a way to hierarchically aggregate routing information, such that the distribution of routing information itself becomes a manageable task. This division into domains provides independence for each domain owner/operator to employ the routing mechanisms of its choice. IP packet routing inside an autonomous system is therefore referred to as intra-domain routing, while routing between (across) autonomous systems is referred to as inter-domain routing. The common goal of many providers of routing services (consumer ISPs, backbone ISPs and participating corporations) is that of supporting different types of services (in the sense of speed, latency and reliability).

In the case of intra-domain routing the aim is to share best-route information among routers using an intra-domain routing protocol (e.g. distance vector such as RIP, or link-state such as OSPF ). The routing protocol of choice must address numerous issues, including possible loops and imbalances in traffic distribution.

Today routers are typically owned and operated by the legal owner of the autonomous system (e.g. ISP or corporation). These owners then enter into peering agreements with each other in order to achieve end-to-end reachability of destinations across multiple hops or domains. The primary revenue model in the ISP industry revolves around different tiers of services appropriate to different groups of customers.

There are several important points regarding autonomous systems paradigm and the positive impact this paradigm has had on the development of the Internet for the past four decades:

**Autonomous systems paradigm leads to scale:**

The autonomous system paradigm, the connectionless routing model and the distributed network topology of the Internet allows each unit (the AS) to solve performance issues locally. This in turn promotes service scale in the sense of throughput (end-to-end) and reach (the large numbers of connected endpoints). As such, it is important to see the global Internet today a
connected set of “islands” of autonomous system, stitched together through peering agreements.

Domain-level control with distributed topology:

Each autonomous system typically possesses multiple routers operating the same intra domain routing protocol. The availability of multiple routers implies availability of multiple routing paths through the domain. Despite this distributed network topology, these routers are centrally controlled (e.g. by the network administrator of the domain). The autonomous system as a control-unit provides manageability, visibility and peering capabilities centrally administered by the owner of the domain.

Each entity is uniquely identifiable in its domain:

All routers (and other devices, such as bridges and switches) in an autonomous system are uniquely identifiable and visible to the network operator. This is a precondition of routing. The identifiability and visibility of devices in a domain is usually limited to that domain. Entities outside the domain may not even be aware of the existence individual routers in the domain.

Autonomous system reachability: Autonomous systems interact with each other through special kinds of routers called “Gateways” that are designed and configured for cross domain packet routing. These operate specific kinds of protocols (such as an exterior Border Gateway Protocol), which provides transfer of packets across domains. For various reasons (including privacy and security) these exterior-facing gateway protocols typically advertise only reachability status information regarding routers and hosts in the domain, but do not publish internal routing conditions.

Autonomous systems are owned and operated by legal entities:

All routing autonomous systems (routing domains) today are owned, operated and controlled by known entities. Internet Service Providers (ISPs) provide their Autonomous System Numbers (ASNs) and routing prefixes to Internet Routing Registries (IRRs). IRRs can be used by ISPs to develop routing plans. An example of an IRR is the American Registry for Internet Numbers (ARIN), which is one of several IRRs around the world.
In the next section we re-map the fundamental goals of the Internet architecture in the context blockchain systems, with the goal of identifying some fundamental requirements for blockchain interoperability.

DNA Dual Chain Design Inspired by Internet Design Approach
We believe that scalability and interoperability are complementary but separate concerns, and best addressed through different sub-protocol layers. As such, the DNA Chain is further divided into two layers - The Performance Layer and the Interoperability Layer.

For simplicity's sake we refer to the Performance Layer as DNA-PL and Interoperability Layer as DNA-IL. The following section provides the rationale behind such division of the chain. The key idea is the "abstraction" of the same simple concern into one layer, to make the whole technology "stack" more sustainable.

The internet is the best example of a layered protocol architecture, and this design was a key factor in the internet's growth and usefulness. Different pieces of functionality are split into separate protocols that build on one another, rather than being bundled together in one monolithic system.

Layered protocol architectures provide a number of important benefits:

- **Interoperability** - The current internet is built upon Internet Protocol (IP) which works across many different networking technologies by abstracting away their differences. As long as a link can send data, IP can communicate over it. This means we can connect seamlessly no matter what type of underlying network we are using.

- **Scalability** - Abstractions enable different layers to evolve separately. While the internet was built in the 1970s, the fact that IP abstracts away the different networking technologies has enabled us to upgrade from dial-up to fiber optic and 4G links. The higher level protocols did not need to change, but our connections keep getting faster as newer networking technologies are developed.

- **Common Infrastructure for Multiple Use Cases** - IP is also independent of any particular use case, which enables the same infrastructure to be used for applications ranging from the Web to email and Voice over IP (VoIP). If the internet had been built specifically for file transfers, we might have needed whole separate networks for each different use
case. Instead, we have a single internet that can be used for many types of communication.

The DNA protocol stack draws inspiration from the internet protocol suite, largely because we found that splitting functionality into analogous layers helped solve issues at each level.
Team

Metaverse has assembled a dynamic and professional international team with a management layer that pursues excellence and experienced developers. Eric Gu will be the strategic architect of DNA. Chen Hao will be delivering technical expertise such as consensus algorithm and network communication. Ken Huang is responsibility for the security, digital identity and token economy design of DNA.

Eric Gu
Founder & CEO
Early crypto adopter, famous investor and advisor for blockchain projects

Eric Gu is a Chinese FinTech investor and industrial guru. Eric Gu is known for founding Metaverse and leading Metaverse Foundation as its chairman and chief executive officer. Eric is an experienced blockchain leader, mainly an expert in digital identity and smart assets. As a lifetime member of the Bitcoin Foundation, Eric was one of the earliest entrepreneurs who introduced blockchain technology to China and published the translation of the book "Blockchain: New Economic Blueprint and Guide" in Chinese. Eric is a firm believer of blockchain technology who has predicted and indicated publicly that the value of bitcoin will exceed $360,000 by the end of 2021.
Ken Huang

Ken Huang is the co-founder of Metaverse DNA, and a member of the Blockchain Branch of The Chinese Institute of Electronics (CIE). He was a blockchain expert at Huawei, and CISSP certified by IS2. Ken has published the book called “Blockchain Security Technical Guide”. Ken was also the member of Blockchain and Al Committee of 2018 Association for Computing Machinery. Ken is an active speaker at many blockchain conferences. He indicated that the mission of Metaverse DNA’s Identity System is to implement the storage of encrypted sensitive data, registration of digital assets, self-control of identity data, and the reputation-based identity.

Chen Hao

CTO & Co-founder. Strong C++/Python and architecture experience in Fech-tech, architect of crypto exchange, famous blockchain writer in China.
William Jiang
Global Marketing Manager. Extremely strong and solid background in both finance and sales

Magnus Dettmar
Business Development
Account Manager with international finance background and deep fintech and blockchain understanding.

Sven
Senior Blockchain Fullstack Engineer. Analyst and full-stack developer with strong experience in blockchain, major in Javascript/Typescript and smart-contracts.
Kesalin Luo
Senior Blockchain C++ Engineer
Tencent Senior C++ engineer(Former), Over 10 years of experience in C++ and Python.

Michael Jiang
Head of R&D & Co-founder. Solid experience in big data analysis and application development

Stephanie Ma
Marketing Operations Specialist. Experience in global marketing operation and event planning
Jowen Show
Senior Blockchain C++ Engineer. More than 10 years' developing experience in open source projects (LibreOffice etc.)

Patrick Tsoi
Business Analytics Manager. Vast experience (5 years) in Fin-tech and PM

Laurent Salou
Senior Blockchain Fullstack Engineer
Analyst and developer with strong experience in Financial banking
Advisors

Mike Costache

Born in Romania in 1977, Mike migrated to Israel in 1988 and in 1992 to the US. Mike was featured in USA Today, Wall Street Journal, Inc., Entrepreneur, CCTV, Business Week, Top Gear and numerous other media outlets.

Mike serves on the Advisory Board of Token-as-a-Service (TaaS), the first ever tokenized closed-end fund dedicated to investments in blockchain assets. TaaS raised $7.6 million through its ICO in early 2017 and produced a 780% ROI within the first year. TaaS invested $10 million in 35 ICOs and is active with daily crypto trading.

During 2017 and 2018, Mike served the Managing Partner of KrowdMentor, a strategic investment and advisory firm and as CEO of d10e, a leading conference on decentralization with 23 global editions all over the world.

From 2011 to 2018, Mike was a member of Tech Coast Angels (TCA), a network of 330 angel investors in Southern California who invested $200 million in 400 deals and raised over $2 billion from VCs.

From 2006 to 2011, Mike was the founder & President of Leo & Leo, which represented brands such as Maserati, Segway, NetJets, PrivatSea, Sunseeker Yachts, NetSuite, Marsh, Orgil Greenhouses, Miss Universe, and Rockstar Energy Drink. Total sales amounted to €60 million.

From 2000 to 2006, Mike was the founder & CEO of Pioneer TeleCare, an e-commerce firm with revenues of $4 million. From 1998 to 2003, Mike was an Associate at WestPark Capital, The Interlink Group, Millennium Capital Partners.

Mike holds a degree in Economics from Pepperdine University, a Graduate Certificate in Dispute Resolution from Pepperdine’s School of Law and has completed the Program on Negotiations for Senior Executives at Harvard.
Alex is an expert in digital thought and transformation. He has joined the Metaverse DNA team as Global Strategy Advisor. Alex has over 30 years of experience in deploying new and novel hardware, software, communications, and Internet products, platforms, and protocols.

Alex Lightman is an award winning writer, entrepreneur, educator and government policy advisor in technology and trade. He has organized and chaired over 300 international events. He graduated from MIT In Civil and Environmental Engineering and attended graduate school at Harvard’s Kennedy School of Government and MIT’s Sloan School of Management.

Lightman has worked for, contracted for or been an advisor or invited speaker to over 40 national governments and dozens of US federal agencies including the US Senate, the White House, Department of Transportation, Department of Defense, Defense Information Systems Agency, and the Institute for Defense Analyses, NATO, as well as the United Nations.

Lightman teaches Kingsland University’s 16 hour two day Blockchain Executive Education program that he authored which has received 100% 5 out of 5 star ratings from participants. His goal is to take the body of knowledge around the Blockchain and make

He has served as an advisor to 20+ Blockchain companies and speaks around the world on “solving big problems with Blockchain, AI and IoT”, “CryptoHistory 2009-2050”, and “Visionary Blockchain Projects”. He also speaks widely on renewable energy and his TEDx talk on “How to Get Rid of Fossil Fuels” by 2030 has thousands of views.

His awards include the first Economist magazine Readers’ Award in behalf of 4G Wireless, vs. Elon Musk and five other innovators in a global vote, after 4,000 innovations were submitted. The only other recipient was Steve Jobs. He has also won SGI’s Internet VR competition out of
over 800 entries, a global Avatars competition, and the Johnson Foundation’s recognition as one of “America’s ten most innovative educators”.

He is a co-founder and one of the seven steering committee members of the Digital Asset Trade Association (DATA) and is one of the most prolific creators of crypto content in 2018. He is the first columnist for ICO Crowd magazine, with 35 articles, an Amazon.com best-selling author in seven categories, and keynote speaker at 30+ Blockchain conferences in 20+ countries during 2018. He has authored 15 crypto white papers, possibly the most of any individual.

Lightman is the author of Brave New Unwired World (the first book on 4G) and Reconciliation: 78 Reasons to End The US Embargo of Cuba, and the coauthor (with Brett King, the #1 Fintech influencer) of Augmented: Life In The Smart Lane. His next books will be published in 2020, How To Be Good At Crypto, and Food Security via Clean Energy and Blockchain Technology.
DNA Roadmap, Long Term Goals, Milestones, and Relevant FAQ

Roadmap overview
The Dualchain testnet is slated to launch in December of this year, while the decentralized exchange will launch in May of 2020, with BTC/ETH/EOS/TRON/etc. crypto assets cross-chain swaps coming in September of 2020.

Selected Long-term goals:
High performance, interoperable and secure public infrastructure for blockchain and fintech which remains decentralized and censorship resistant.

Milestones:

So far DNA has continuously met and exceeded all of its timeline objectives

- June 2016 - Metaverse Whitepaper version draft
- Feb 11 2017 - Metaverse ETP main net, ability to create digital assets
- June 2018 - Metaverse version code Supernova, ability to create digital identity
- March 2019 - Metaverse version code Pillars of Creation, hybrid consensus algorithm
- May 2019 - Dualchain network architecture announced
- Dec 2019 - DNA test net
- March 2020 - DNA main net
- June 2020 - Decentralized exchange
- Oct 2020 - Virtual machine for smart contract

Marketing, Outreach and Development Strategy and Tactics
DNA has currently established offices in Shanghai and Toronto. We are currently actively recruiting developers, analysts and researchers. We also have a global presence and understanding, with a specific focus on presence in selected Asian countries, including

- China
- Korea
- Vietnam
- Japan
We believe the DNA project should be a community based project. We have set up bounty and ambassador programs to motivate community participation. Meanwhile we are actively speaking to large enterprises for cooperation and support.

DNA is involved in local community partnerships and major corporation partnerships; government partnerships might be initiated as well.

Selected ongoing marketing and outreach activities include

- Roadshows across major cities in China, North America(San Fran Blockchain Week & ETH Waterloo) and Europe
- First bounty program via both organic and paid channels to increase market exposure and gathering DNA community volunteers into DNA telegram group. Currently, having more than 300 members joined first bounty program.
  *Details: [https://medium.com/metaverse-blockchain/were-launching-the-dna-community-bounty-614d6affc2b9](https://medium.com/metaverse-blockchain/were-launching-the-dna-community-bounty-614d6affc2b9)
- Content marketing: Educating oversea market about Metaverse, Metaverse Dualchain:
  - What’s Metaverse dualchain
  - How dualchain will solve current industrial issues
- *Content marketing breaks down to the DNA interoperability, scalability, security, governance, digital identity and egaming...
- Influencer marketing: KOL youtuber to talk about DNA token review
- Press Release on big announcement, such as strategic partnership, advisor, and new exchange listing
- Second bounty program(Ambassador program) will be announced by the end of November 2019, ambassador will be responsible for hosting meetup, creating content, etc.

Examples of relevant long term activities include:

- Overseas strategic partnership with Finwise Conference.
- Decentralized technical bounty program will be announced when testnet taking progress
- Endorse dApps
FAQ on Selected Details of Roadmap and Token Sale

How would you handle and motivate independent communities of different blockchain systems and ensure a win-win for those communities going forward?

Bounty programs would be initiated in the short term with individual volunteers paid by DNA token, midterm with capable teams paid by community partner funding (USD$1-2k), long term project collaboration.

What is the total required funding to execute on the roadmap?

20 million USD over 3 years.

What is the projected use of funds, and what are your measures to ensure transparency of processes and results?

25% for marketing, 25% for compensation of the technical team,

35% for market stabilization, 15% for bounty programs and community building. We are committed to releasing spending reports for community review/audit.

What would be the high level financial governance structure making sure that funds are spent on existing/updated roadmap?

Quarterly report to ensure transparency and proper spending of funds.

What is the brief overview of the planned token generation event?

The token will be distributed to pre-selected, proper KYCed qualified investors through a mobile investment tool.

Would DNA tokens be security or utility ones?

It will be utility tokens. It will be used as gas for transactions and smart contracts.
What would be the setup of transactions involving tokens?

Currently DNA is listed on RightBTC.com

What would be the incentive structure, including vesting and lock up periods for team, advisors, backers and partners?

Team advisors and partners should be compensated by fiat currency, ETH or BTC but never DNA.

What would be your current and future focus regarding target audience?

Current target audience for our tokens include backers from all over the world. Ideally have experience in Fintech or blockchain investment. In terms of the DNA project itself, we’d like to market to medium and large corporations or financial institutions.

Do you consider launching an IEO (Initial Exchange Offering) and if yes, which exchanges would you consider for that?

No, we are not considering launching an IEO but DNA is a public chain so there will be a lot of DAPP running on top of DNA and we are considering using RightBTC exchange to IEO these DAPPs.

What is the total percentage of token are you selling? What is the total cap?

We intend to sell 90% of the tokens. The cap is 100B tokens.

When will revenue stream start?

May 2020 when decentralized exchange is online.

Have you raised equity earlier?
Is there geography restriction for usage of DNA tokens once these tokens are purchased? 
No

What’s your treasury management strategy - will you keep your funds in ETH, BTC, EOS, USD, CNY, HKD? 
We will keep funds in ETH, BTC and PAX.

Which Currencies would be accepted (BTC, ETH, EOS anything else?)? 
Currently ETH only. We might also accept ETP later on.

Do you have or plan to introduce “Know your Customer” (KYC) process? 
We don’t have KYC at this moment and we raise funds through bit reserve foundation and KYC process will rely on their technology.

What is the minimal and maximum investment size in DNA tokens? 
Minimum is 1000 USD and there is no maximum.

Will you be using a SAFT or an alternative? 
Yes we will have a SAFT.

What is your legal setup & structure? 
Swiss Foundation.
Where and how are you incorporated?

Zurich, Switzerland, not-for-profit organization.

Are you setting up a foundation to be a steward of the DNA token related processes, governance, etc?

Yes, Metaverse Foundation.
Conclusion

Issues that blockchains face include performance, scalability, security and interoperability. Are we aiming for decentralization or speed? Based on current technology, you may enhance one at the expense of the other.

A common misunderstanding is trying to solve the dilemma of decentralization or speed through one single chain, like what Quarkchain is trying to do. How do public chains interoperate with private chains and alliance chains? We have a couple of examples in Cosmos and Polkadot who are trying to solve this issue, and although they are technically sound, they are an intermediary and somewhat centralized as gatekeepers.

The solution to the problems and challenges mentioned above comes in the form of Dualchain Network Architecture (DNA), which consists of a fast parallel chain with a DPoS consensus, a three-layered node incentive model, a lightning network protocol, and eventually, a decentralized exchange.

A token called DNA will be the utility token for the parallel chain. Specifically, it will act as the token incentive for the lightning network between nodes. Along with the DPoS consensus, DNA will instill a three-layered governance system.

A decentralized exchange will eventually be established, bound to DNA, to provide a TPS of up to 600,000 with low fees, allow token issuing and transfers, and incentivize the 23 super nodes to share in the partner dividends.

Therefore DNA will be able to deploy the so far impossible trinity of security, decentralization, and scalability with the Dual Network Architecture.
Dualchain Network Architecture

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.

**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.
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


