DEXON Network

Empowering the Decentralized Future

DEXON Foundation

Last Modified 2018/7/19 v0.2.2

*This document describes the current plan and vision for DEXON network platform. While we intend to attempt to realize this vision, please recognize that it is dependent on a number of factors and subject to a wide range of risks. We do not guarantee, represent or warrant any of the statements in this document, because they are based on our current beliefs, expectations and assumptions, about which there can be no assurance due to various anticipated and unanticipated events that may occur. Please know that we seek to achieve the vision laid out in the white paper and website, but that you cannot rely on any of it coming true. Blockchain, cryptocurrencies and other aspects of our technology and these markets are in their infancy and will be subject to many challenges, competition and a changing environment.

Introduction

Blockchain technology[1] (or, DLT[2], decentralized ledger technology) is revolutionizing the Internet from a client-server/centralized architecture to a distributed/decentralized architecture. However, existing blockchain technology is unable to achieve the performance requirements of modern real-world practical mass-adopted applications because of limitations inherent to their architecture.

To solve this, the DEXON consensus algorithm has reinvented how blockchain technology works with its state-of-the-art **blocklattice** data structure. The DEXON consensus algorithm is **infinitely scalable**, **low-latency**, and **Byzantine fault tolerant**[3]. Furthermore, the DEXON inter-chain bridging protocol can support any kind of DLT to be bridged onto the DEXON network—making it **inter-operable** between different blockchain systems.

Vision and Mission

Our Vision

Reshape the future of the Internet with decentralized technology.

Our Mission

Accelerate the mass adoption of DLT by solving its fundamental performance bottlenecks and incubating DApp projects.

[1] "Blockchain - Wikipedia." https://en.wikipedia.org/wiki/Blockchain.
[2] "Distributed ledger - Wikipedia." https://en.wikipedia.org/wiki/Distributed_ledger.
[3] "Byzantine fault tolerance - Wikipedia." https://en.wikipedia.org/wiki/Byzantine_fault_tolerance.

Design Philosophy

DEXON is designed to solve the fundamental bottlenecks that hinder the mass adoption of blockchain technology. The following are the DEXON network's design goals:

Scalability:

- Support billions of users.
- Create an infinitely scalable, low-latency, and secure consensus layer.
- Create an infinitely scalable and limitlessly parallelizable smart contract[4] execution layer.
- Create an infinitely scalable decentralized storage layer, featuring a data persistent decentralized ledger, decentralized file storage, and decentralized key-value data store.

Advanced Smart Contract Programming Platform:

- Developer-friendly ledger API and smart contract programming language design.
- Upgradable smart contract capability.

Inter-Chain Protocol:

- Inter-chain assets and transactions bridging capability.
- Decentralized inter-chain digital asset exchange capability.

Developer-Friendly Software Stack:

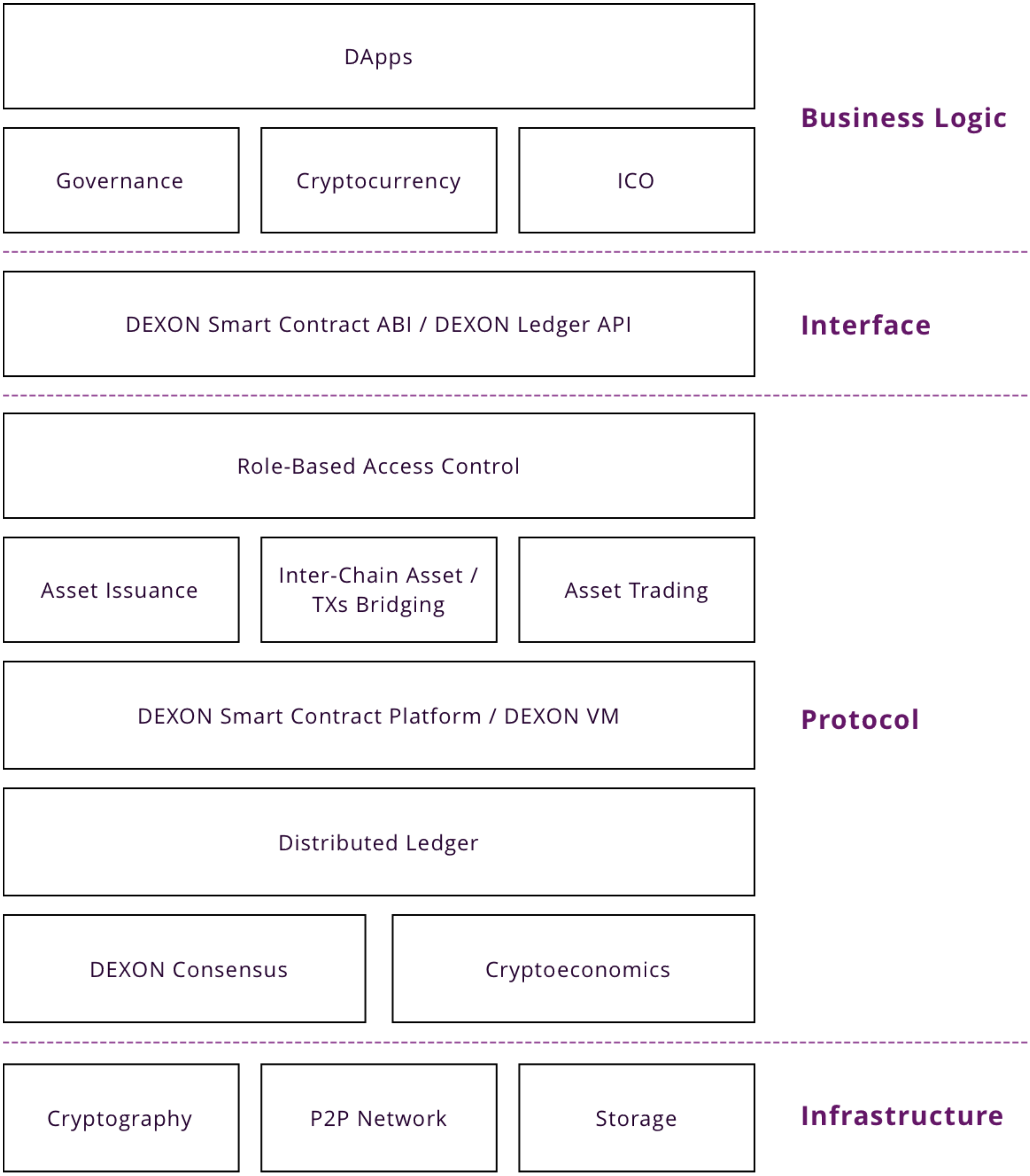
- Modular package designs for key software components.
- DevOps-friendly docker[5]-based software delivery.
- Lightweight node capability for mobile and IoT devices.

Other Desirable Features:

- Built-in native support for multi-signature[6] accounts and transactions.
- Built-in native support for comprehensive role-based access control[7].
- Full node software over-the-air upgradability.
- Sustainable governance mechanism.
- User privacy-centric design.

[4] "Smart contract - Wikipedia." https://en.wikipedia.org/wiki/Smart_contract.
[5] "Docker (software) - Wikipedia." https://en.wikipedia.org/wiki/Docker_(software).
[6] "Multisignature - Bitcoin Wiki." https://en.bitcoin.it/wiki/Multisignature.
[7] "Role-based access control - Wikipedia." https://en.wikipedia.org/wiki/Role-based_access_control.

System Architecture



DEXON Account System

Unlike Bitcoin's UTXO[8], DEXON is an *account-based* distributed ledger system. In DEXON, a deployed smart contract is also considered as an account. To enhance usability, DEXON implements the following features.

Multi-Signature Transaction Support

The multi-signature functionality is indispensable in any blockchain system. To support multi-signature[9] transactions, the DEXON network itself works as a multi-signature transaction signing pool that maintains the transaction signing states of multi-signature transactions.

Multi-Asset Account

In DEXON, each account natively supports multiple digital assets. DEXON's multi-asset account system works like a multi-currency bank account, making it easy to browse the balances of all digital assets.

Batch Token Transfer Transaction Support

To achieve banking level usability and flexibility, DEXON implements an innovative native batch token transfer transaction support, which works seamlessly with its multi-asset account system. For example, one can transfer 100 DEX, 10 ETH, and 1 BTC to another party with only a single token transfer transaction. One can also transfer 100 DEX to multiple transferees, like 50 DEX for Alice, 30 DEX for Bob, and 20 DEX for Carol using a single transaction.

Role-Based Access Control (RBAC)

DEXON's role-based access control is a comprehensive permission control system that works just like the Amazon Web Services (AWS) Identity and Access Management[10] (IAM), making DEXON's permission control for smart contract data fields and functions as easy as possible.

[8] "UTXO - Bitcoin Glossary." https://bitcoin.org/en/glossary/unspent-transaction-output.
[9] "Multisignature - Wikipedia." https://en.wikipedia.org/wiki/Multisignature.
[10] "Identity and Access Management (IAM)" https://aws.amazon.com/iam/.

DEXON Consensus Algorithm

Blocks are grown linearly in traditional blockchain systems, making them difficult to scale. On the DEXON network, blocks are grown by all nodes individually in parallel to each other and in a non-blocking fashion, creating a blocklattice structure. No node has to wait for any other node as it extends its own blockchain, enabling unprecedented scalability. In order to achieve consensus in a blocklattice, there must be a mechanism to identify the validity and order in which all of these blocks are being produced. This is accomplished by having each node broadcast the existence of the new blocks to all other nodes on the network once they have been produced. As other blocks receive the broadcast, they can perform an "*ack*[11]" or "*acknowledgement*" that serves as a validation and timestamping for the creation of the new block. Under this structure, all blocks are constantly *acking* each other, or in other words, cross-referencing the validity and timestamp of each block. In addition to confirming validity and timestamp, information such as the ID of the block producer, transactions contained in the block, acking history, block hash, block hash signature, block height, etc, is also shared between blocks through *acking*. Finally, in order to generate a globally-ordered chain which contains all the valid blocks that have been produced from all the nodes on the DEXON network, each node executes the *DEXON total ordering algorithm* and the *DEXON timestamping algorithm* individually. As a result, each node will maintain a copy of the globally-ordered data, called the *DEXON compaction chain*, so that it can be further compacted into *signed state milestone blocks* through the *Merkle tree*[12] technique. Note that all the procedures with the exception of broadcasting the blocks are performed by each individual node, thus, the network can achieve low-latency and infinite scalability.

In conclusion, the DEXON consensus algorithm determines a *total order*[13] of all blocks produced by each node with *Byzantine agreement*. Infinite scalability and low latency is achieved since the block proposing is non-blocking and does not have a theoretical rate limit.

The details of the DEXON consensus algorithm can be found in the paper attached in the appendix [14]. The advantages of the DEXON consensus algorithm are listed below:

[11] "Acknowledgement (data networks) - Wikipedia." https://en.wikipedia.org/wiki/Acknowledgement_(data_networks).

[12] "Merkle tree - Wikipedia." https://en.wikipedia.org/wiki/Merkle_tree.

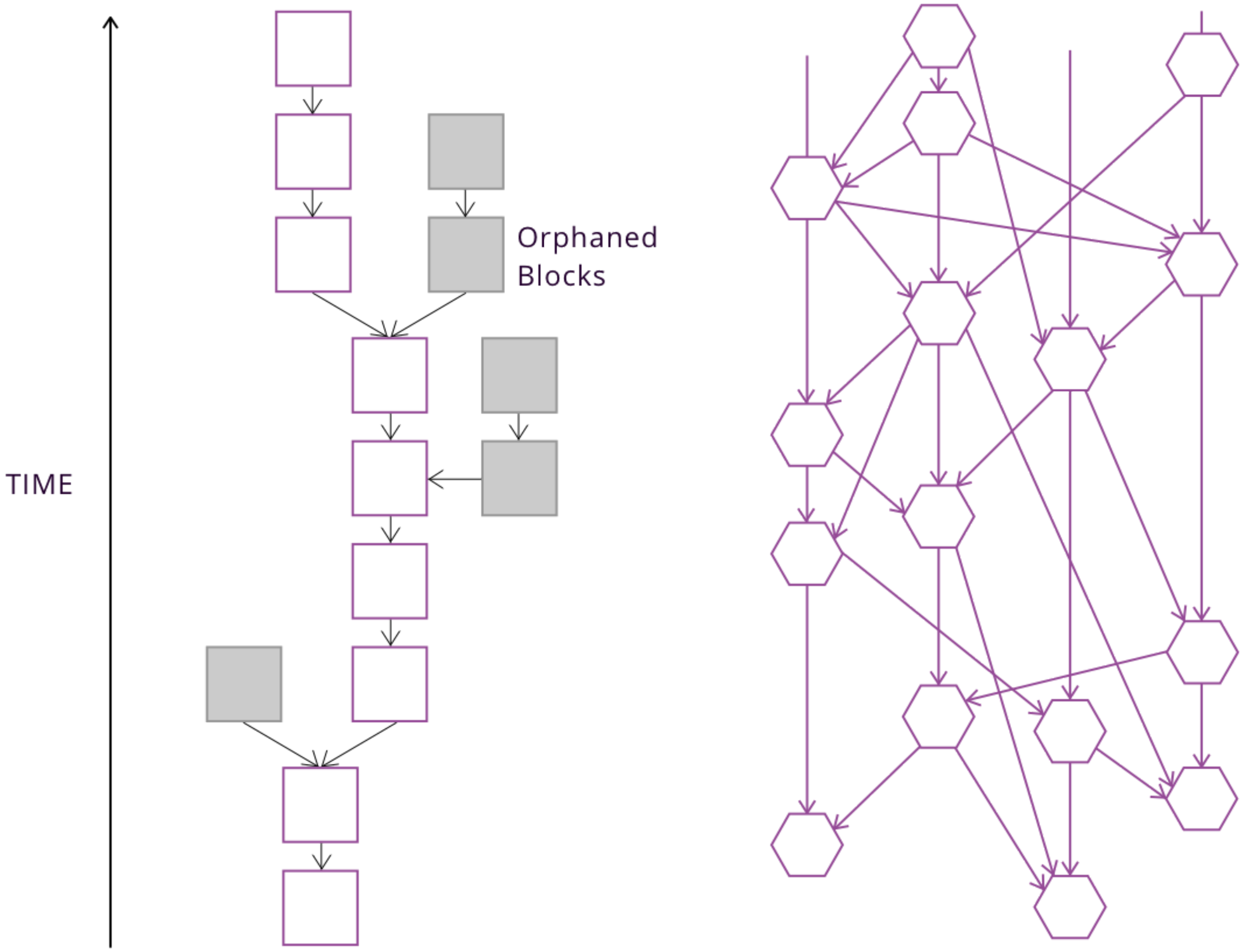
[13] "Total order - Wikipedia." https://en.wikipedia.org/wiki/Total_order.

[14] "DEXON Consensus" https://gateway.ipfs.io/ipfs/QmbW8wFZbaUDP83vjwFr9JHLGAnphiAcNziVwrWaHDy1x6.

Infinite Scalability

Blocklattice

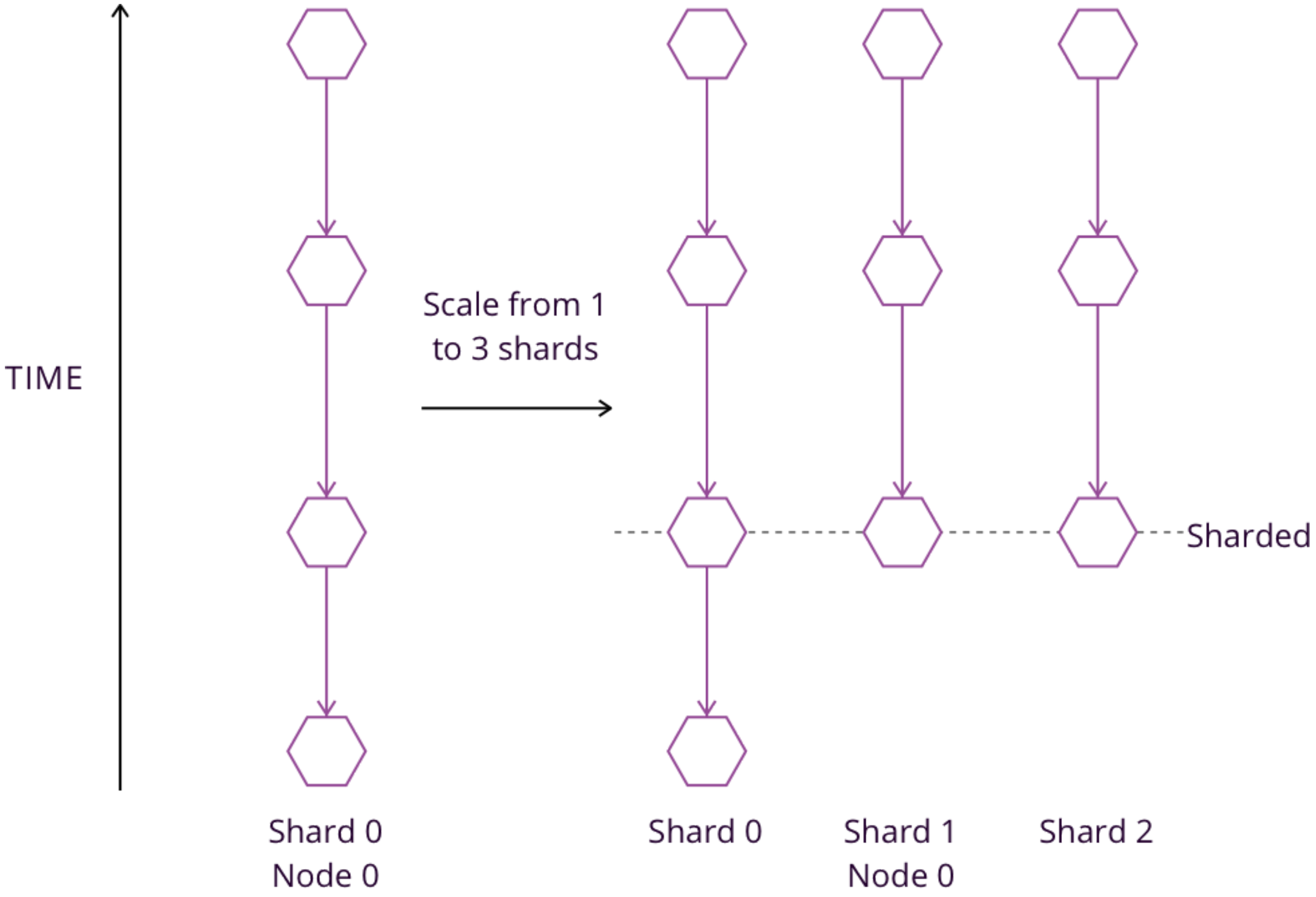
DEXON achieves infinite scalability through its blocklattice architecture. The transaction processing throughput scales linearly with the number of nodes participating in the DEXON consensus.



Blockchain vs. Blocklattice

Infinite Sharding Capability

Sharding[15] can be easily achieved on the blocklattice data structure. When a node has reached its maximum throughput, it can scale to an infinite number of shards to balance the transaction processing load—achieving infinitely scalable transaction processing throughput.



Sharding of a Validator

[15] "Shard (database architecture) - Wikipedia." https://en.wikipedia.org/wiki/Shard_(database_architecture).

Low Latency

Bitcoin transaction confirmations can take hours while Ethereum transactions can take minutes; in other so-called next generation proof-of-stake (PoS[16]) blockchains, confirmations can take seconds. The DEXON blocklattice achieves sub-second transaction confirmation latency because of its non-blocking blocklattice data structure. Moreover, the transaction latency remains the same no matter how large the transaction throughput scales.

Low Transaction Fees

Bitcoin transactions cost an average of 30–50 USD per transaction around January 2018 and transaction fees are continuously rising[17]. This can be attributed to the increase in mining costs and reduction in block rewards as the overall hash power in the network increases. Ethereum works the same way since they are both based on proof-of-work (PoW[18]) consensus algorithms. The next generation PoS blockchains can reduce the costs of a transaction, but fees start to skyrocket when the network is congested. Due to the network's low scalability, fees will eventually be substantially high when the network throughput is depleted.

The DEXON consensus algorithm has the lowest communication overhead compared to all other consensus algorithms and it does not require its network to waste energy on solving PoW puzzles. The transaction fees will thus be negligible. In practice, we estimate the actual transaction fee for a typical token transfer on the DEXON network to be less than 10^{-10} USD.

Safe and Secure

Double-Spend Attack Resilience

The security of blockchain technology has been criticized recently due to double-spend attacks[19] that occured on BTG, MONA, and XVG. These blockchain systems are vulnerable to such attacks because their consensus algorithm is based on PoW, and the overall mining power in the network is not large enough to withstand a malicious party to launch a 51% attack.

[16] "Proof-of-stake - Wikipedia." https://en.wikipedia.org/wiki/Proof-of-stake.
[17] "Bitcoin Avg. Transaction Fee chart." https://bitinfocharts.com/comparison/bitcoin-transactionfees.html.
[18] "Proof-of-work system - Wikipedia." https://en.wikipedia.org/wiki/Proof-of-work_system.
[19] "Double-spending - Bitcoin Wiki." https://en.bitcoin.it/wiki/Irreversible_Transactions.

For example, in the BTG attack[20], an attacker borrowed huge hashing power from a mining pool at very low cost for a short timespan and launched a double-spend attack on its deposit transaction of BTG cryptocurrency on an exchange.This caused the exchange to lose about 20 million USD worth of BTG. The root cause of this kind of attack event is that in any PoW blockchain system, the transactions will never be guaranteed to be finalized. This is called probabilistic finality[21]. A malicious miner who has control of a significant portion of hashing power can launch a selfish mining attack[22] to rewrite the transaction history.

On the DEXON network, double-spend attacks will never happen. The DEXON consensus algorithm itself guarantees explicit transaction confirmation with probability 1 through provably secure Byzantine agreement.

Fairness

Front-Run Attack Resilience

A block miner in typical blockchain systems can independently determine the transaction ordering within a block, launching a *front-run attack*[23]. In some applications like decentralized digital asset exchanges, the front-run attack problem is serious because a malicious miner always has the option to perform arbitrage[24] based on the transaction information it receives as a miner. This gives him a perpetually unfair advantage over other traders.

On the other hand, no single mining node in DEXON can determine the transaction ordering in the DEXON consensus algorithm because the final consensus ordering of a transaction is determined by all mining nodes in the blocklattice data structure. DEXON determines a transaction's consensus timestamp by calculating the median time that the majority of all nodes in the network witnessed the creation of a given block, which is considered "truly fair."

[20] "Bitcoin Gold Hit by Double Spend Attack" https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions/.

[21] "Blockchain Finality- Proof of Work and Proof of Stake" https://medium.com/coinmonks/blockchain-finality-pow-and-pos-35915a37c682.

[22] "Selfish Mining: A 25% Attack Against the Bitcoin Network" https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/.

[23] "Front-Running - Investopedia." https://www.investopedia.com/terms/f/frontrunning.asp.

[24] "Arbitrage - Investopedia." https://www.investopedia.com/terms/a/arbitrage.asp.

Biased Randomness Attack Resilience

A malicious block miner can manipulate the randomness in smart contract executions, launching a *biased randomness attack*[25]*.* Taking a jackpot machine smart contract deployed on Ethereum as an example, a malicious miner can win the jackpot at anytime the miner wants by manipulating the random function in the EVM[26] (Ethereum Virtual Machine).

DEXON is resilient to biased randomness attacks since its blocklattice data structure generates unbiased randomness for smart contract executions.

Decentralization

PoW Blockchains

In regards to the decentralization of blockchain systems, many people who believe in blockchain technology may argue that a decentralized network is better than a centralized one. This is a contentious topic in current mainstream blockchain systems. In PoW systems like Bitcoin and Ethereum, massive portions of the total network mining power are controlled by mining pools[27]. These mining pools can easily collude and launch a 51% attack.

DPoS Blockchains

In some newly proposed DPoS[28] (Delegated Proof-of-Stake) systems like EOS[29], transaction message complexity increases at a quadratic rate[30] with the increase in the number of nodes. This can be deduced from its underlying consensus algorithm complexity: $O(N^2)$, where N is the number of nodes. Since the number of nodes cannot easily scale, something called *supernodes*[31] must exist — this forces the network to relinquish its decentralized nature as the decision making power will once again be centralized on supernodes.

[25] "What is randomness bias? - Quora." https://www.quora.com/What-is-randomness-bias.
[26] "What is the Ethereum Virtual Machine?" https://nulltx.com/what-is-the-ethereum-virtual-machine/.
[27] "Chinese Mining Pools Take Up 90% Of The Global Hashpower" http://news.8btc.com/chinese-mining-pools-take-up-90-of-the-global-hashpower.
[28] "Delegated Proof of Stake - BitShares." http://docs.bitshares.org/bitshares/dpos.html.
[29] "EOS.IO - Wikipedia." https://en.wikipedia.org/wiki/EOS.IO.
[30] "Quadratic growth - Wikipedia." https://en.wikipedia.org/wiki/Quadratic_growth.
[31] "Prof. Cao: Why EOS Super Node Election Becoming a Farce? - Medium." https://medium.com/usechain/huining-cao-the-founder-of-usechain-why-is-the-eos-super-node-election-becoming-a-farce-cdbcca53c760.

DEXON Symmetric PoP Blocklattice

In traditional PoS blockchain systems, nodes can mine or validate block transactions according to how many tokens the node holds. In DPoS, nodes have *asymmetric* voting power[32] proportional to their delegated stakes. It's easy to comprehend that this empowers the potential for centralization. DEXON, on the other hand, adopts a *symmetric* design implemented in its PoP (Proof-of-Participation) block mining, in which every node has equal voting power, fostering full network decentralization.

Furthermore, since DEXON's blocklattice maintains a constant network communication overhead regardless of how large the transaction throughput grows, it can easily scale to thousands of nodes.

DEXON Symmetric Randomized PoP Blocklattice

As the capacity and number of nodes on the DEXON network grows, DEXON will migrate from PoP to *Randomized PoP*. Under the randomized PoP setting, DEXON will be able to operate with millions of nodes while still maintaining low communication overhead. The randomization is achieved through an unbiased random oracle[33] generated from the DEXON blocklattice data structure, allowing the communication overhead to drop from $O(N^2)$ to $O(NLogN)$ without compromising security.

Energy Efficiency

PoW blockchain systems require massive computation power for solving cryptographic puzzles, producing significant energy waste and potentially irreversible environmental implications. DEXON, on the other hand, achieves the highest level of energy efficiency since it has the lowest overhead in achieving consensus.

[32] "An easy to understand guide to PoW, PoS, DPoS, consensus ...." https://medium.com/@TronDotLive/an-easy-to-understand-guide-to-pow-pos-dpos-consensus-mechanism-and-super-representative-eb1f5504a8e.

[33] "Random oracle - Wikipedia." https://en.wikipedia.org/wiki/Random_oracle.

DEXON Smart Contract Platform

The DEXON smart contract platform is feature-rich and easy to use. To maximize scalability, usability, and flexibility, the DEXON smart contract platform implements the following features:

DEXLang

DEXLang is DEXON's native programming language, which is functional and Turing-complete[34], allowing formal verifications essential to mission-critical smart contracts. DEXLang supports many advanced features including digital signature validation, merkle proof [35]validation, and various hash functions.

DEXLang Compiler

DEXLang compiler compiles DEXLang programs to byte-codes[36]. The DEXLang compiler is designed with the following features.

- EVM byte-code compatibility.
- Multiple popular programming languages support (Java, JavaScript, ...)
- LLVM-IR[37] to eWASM[38] under the hood.

DEXON Virtual Machine

DEXON virtual machine (DEXON VM) executes the byte-codes of compiled DEXON smart contracts.

Actor Model Parallelization

DEXON is built with an infinitely scalable consensus layer. The aforementioned layer needs to work with an infinitely scalable smart contract execution layer to achieve the goal of an infinitely scalable transaction processing engine. To this end, the actor model[39] parallelization computation paradigm is adopted. The actor model works like an *event-driven*[40] programming model where

[34] "Turing completeness - Wikipedia." https://en.wikipedia.org/wiki/Turing_completeness.
[35] "Merkle tree - Wikipedia." https://en.wikipedia.org/wiki/Merkle_tree.
[36] "Bytecode - Wikipedia." https://en.wikipedia.org/wiki/Bytecode.
[37] "LLVM Language Reference Manual — LLVM 7 documentation." https://llvm.org/docs/LangRef.html.
[38] "GitHub - ewasm/design: eWASM Design Overview and Specification." https://github.com/ewasm/design.
[39] "Actor model - Wikipedia." https://en.wikipedia.org/wiki/Actor_model.
[40] "Event-driven - Wikipedia." https://en.wikipedia.org/wiki/Event-driven.

each smart contract receives transactions as events, and when a contract receives an event, it *activates* the contract for execution.

The actor model design achieves maximum concurrency and performance for DApps executions. The atomicity[41] of smart contract executions are guaranteed within an actor. Inter-actor communications can also be conducted efficiently without congesting the network, and the smart contract execution layer is thus infinitely scalable for the DEXON network.

Unbiased Random Oracle in Smart Contract

The DEXON consensus algorithm generates unbiased randomness on its blocklattice data structure on the fly and does not require running additional algorithms for randomness seed generation, which is often very costly. The randomness seed generated by the DEXON consensus algorithm is then accessible in the DEXON smart contract and can provide unbiased randomness in smart contract executions when needed.

Upgradable Contract

DEXON smart contracts are versioned. The contract owner can upgrade an existing contract by deploying new business logics, while also writing a *data migration*[42] *script* to transform the original data storage variables to new ones in the upgraded contract. The contract upgrade process is completely atomic and traceable.

Asset Issuance Contract

A limitless number of digital assets can be registered and issued on the DEXON network through a special kind of *asset issuance contract*. This contract contains business logics to increase or decrease the issued digital assets supply[43] and defines its *symbol*[44]. Once the assets are transferred from an asset issuance contract to a user's account, the asset balance will be recorded on the user's account, instead of on the asset issuance contract. The asset issuance contract is perfectly suitable for launching ICOs (initial coin offering), government-backed digital currencies, and inter-chain digital asset bridging from other blockchain systems. For example, one party may act as a *bank* of Bitcoin, issuing 1:1 backed Bitcoin assets on the DEXON network.

[41] "Atomicity (database systems) - Wikipedia." https://en.wikipedia.org/wiki/Atomicity_(database_systems).
[42] "Data migration - Wikipedia." https://en.wikipedia.org/wiki/Data_migration.
[43] "Money supply - Wikipedia." https://en.wikipedia.org/wiki/Money_supply.
[44] "ERC20 Token Standard" https://theethereum.wiki/w/index.php/ERC20_Token_Standard.

Inter-Chain Bridging Contract

To enable the fully decentralized transfer of value, a bridging protocol that works among different blockchain systems is indispensable. Polkadot[45] is the most famous among various inter-chain bridging protocols that have been proposed. The way Polkadot bridges transactions is by a *collator* [46] which is nominated by *nominators*[47]. A nominator's voting right to elect a collator is bonded to Polkadot's native token, making the collators among different blockchain systems stake-coupled.

We argue that the stake-coupled model will not work in the practical world. Taking one case as an example, if Polkadot's market cap is 1B USD and the bridged total amount of Bitcoin amounts to 10B, then theoretically, any malicious party's best strategy is to purchase enough Polkadot tokens to break the Bitcoin collator system and steal all funds stored in the collator-managed multi-signature Bitcoin wallet. In reality, the value of bridged assets tends to exceed the bridging network's total assets value, thus we conclude that for a practically feasible blockchain bridging protocol to work, the bridging protocol collator must be stake-decoupled from the bridging network's token value.

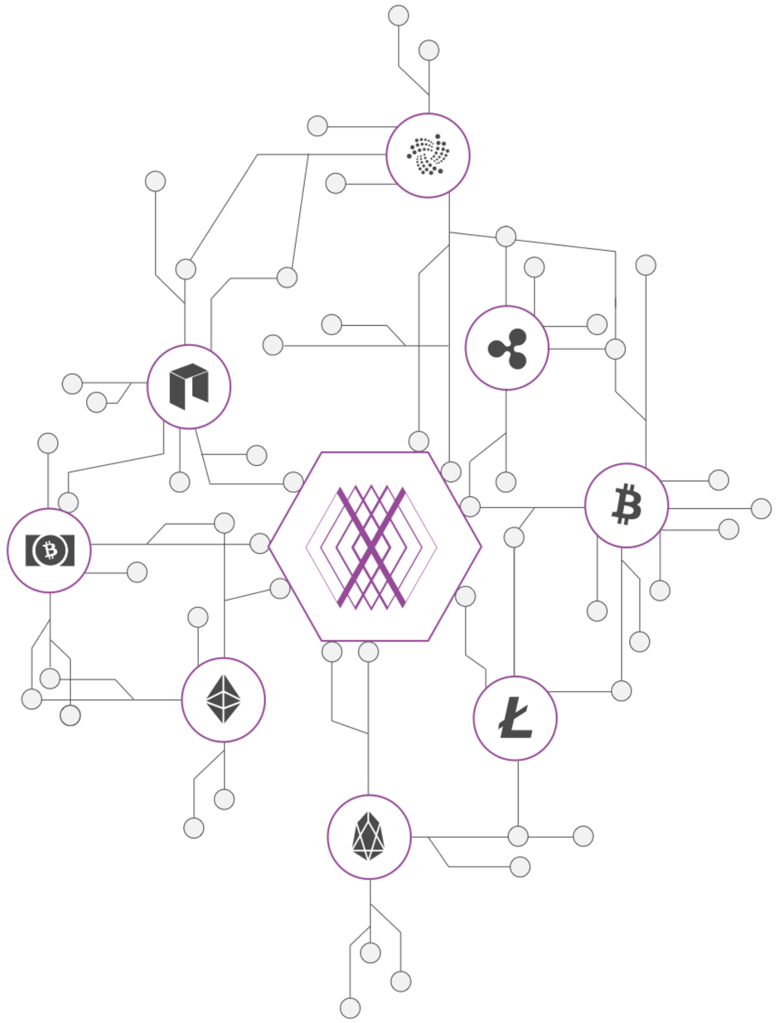
Another issue that arises from using a unified collator on a bridging network is that the bridged blockchain system may fork[48] due to 51% attacks. In that case, the history of the bridged blockchain system may be overwritten and a unified collator has no contingency when faced with a network fork situation.

The PoA Model

In DEXON, the inter-chain bridging mechanism is operated in a PoA (proof-of-authority) model to solve all the issues mentioned above. The goal of the PoA model is to achieve stake-decoupled and fully decentralized bridging operations. To this end, there is a special type of contract called *inter-chain bridging contract*, which can be used to bridge transactions between different blockchain systems. The inter-chain bridging contract is operated by an inter-chain *bridging committee* which acts as an *authority* to *two-way peg*[49] the transactions in other blockchain systems. We call the members of the bridging committee *bridging operators*.

[45] "Polkadot." https://polkadot.network/.
[46] "polkadot/polkadot/collator at master · paritytech/polkadot · GitHub." https://github.com/paritytech/polkadot/tree/master/polkadot/collator.
[47] "Polkadot & the Internet of Blockchains explained in simple words." https://medium.com/@thibauts/polkadot-the-internet-of-blockchains-explained-in-simple-words-9981ded05bc9.
[48] "Fork (blockchain) - Wikipedia." https://en.wikipedia.org/wiki/Fork_(blockchain).
[49] "What is the 2-Way Peg? - FAQ." https://faq.rsk.co/hrf_faq/what-is-the-2-way-peg/.

The inter-chain bridging contract has predefined interface functions to feed in generic transaction payloads from other blockchain systems. The bridged transaction signature, block hash, and merkle proof can be easily validated with handy built-in functions. It is the bridging committee's responsibility to facilitate the bridged transactions from the pegged blockchain system and to vote on the validity of an input transaction. This is called *break-in transaction bridging*. The business logic can also be programmed in the inter-chain bridging contract to send transactions from the inter-chain bridging contract to pegged blockchain systems. This is called *break-out transaction bridging*. On the DEXON network, the bridging system is completely decentralized and the bridging contract can be deployed by any party. For example, we may have multiple parties to help bridge transactions from Ethereum to DEXON, and each may consist of different bridging operators.



Asset Trading Protocol

DEXON is best suited for serving as a high-frequency digital asset trading settlement layer across different blockchain systems due to its sub-second transaction confirmation latency, front-run attacks resilience and inter-chain bridging capability. To facilitate digital asset trading, the DEXON network is built with an atomic swap[50] digital asset trading protocol.

Order Matching Model

On the DEXON network, each user can place a *limit order*[51] to trade digital assets. The limit orders are recorded under the user's account. The user needs to specify a percentage of traded assets as trading fees that he/she is willing to pay to an *order matcher*. In DEXON, any user can become an order matcher, and the fastest order matcher that successfully matches the orders will earn the trading fees. Moreover, DEXON's order matching system natively supports *partially filled* orders[52].

Liquidity Sharing Among Different Markets

To maximize liquidity among different digital asset exchange markets, DEXON is built with a novel liquidity sharing mechanism. In DEXON, if one user has 1 ETH, he can place an order to either buy 10 EOS for 1 ETH or 0.1 BTC for 1 ETH concurrently, without having to divide his account balances to different digital asset exchange markets. Using this mechanism, all digital asset exchange markets now share liquidity together, and thus, traders can enjoy the lowest spread[53] throughout different markets.

Cryptoeconomics

Native Token

The DEXON network's native token is called "*DEX*" and the minimum unit of DEX is called "*Dei*".

$$1 \text{ DEX} = 10^{18} \text{ Dei}, 1 \text{ DEX} = 10^{9} \text{ GDei}$$

[50] "Atomic swap - Wikipedia." https://en.wikipedia.org/wiki/Atomic_swap.
[51] "Limit price - Wikipedia." https://en.wikipedia.org/wiki/Limit_price.
[52] "Partially ordered set - Wikipedia." https://en.wikipedia.org/wiki/Partially_ordered_set.
[53] "Bid-Ask Spread - Investopedia." https://www.investopedia.com/terms/b/bid-askspread.asp.

Validator Node

A validator node, or block producer, is responsible for participating in the DEXON consensus algorithm to validate transactions and to produce blocks. To become a validator, a predefined minimum DEX tokens must be deposited and all other users can also deposit their DEX tokens to support a validator. The DEXON network has a predefined number of validator nodes, and only top-ranking validator nodes with highest DEX token deposits will be granted the permission to become a validator node.

Governance

On the DEXON network, there is a special smart contract called the *DEXON governance contract.* The governance contract serves as the *constitution* for the DEXON network. The governance contract defines the DEXON network's configuration parameters such as the maximum number of validator nodes and the transaction fees. Moreover, the DEXON governance contract works with the DEXON OTA (over-the-air) upgrade mechanism to complete the software upgrades of the DEXON network in a fully decentralized and automated way, avoiding any possibility of network *hard forks*[54]. As the DEXON network evolves, updates to the governance contract parameters can be proposed, and all members in the *DEXON governance council* will jointly decide on whether or not to accept the proposed changes.

DEXON Governance Council

Initially, DEXON Foundation and several highly-reputable enterprises and organizations in the world will form the DEXON governance council. It is the DEXON governance council member's duty to determine how the DEXON network will evolve and ensure the fulfillment of DEXON's vision. As time passes, more governance council seats will be added to reflect participation across multiple industries and perspectives.

Proof-of-Participation (PoP)

On the DEXON network, validator nodes must participate in transaction validations in the DEXON consensus algorithm to earn *mining rewards*.

[54] "Hardfork - Bitcoin Wiki." 30 Nov. 2017, https://en.bitcoin.it/wiki/Hardfork. Accessed 9 Jul. 2018.

In most DPoS blockchain systems like EOS or Cardano[55], the blockchain consensus validation power of each node is asymmetric. DEXON's PoP consensus enforces symmetric blocklattice consensus validation power among all nodes, making the whole system truly decentralized and fair.

Validator nodes that violate the DEXON consensus algorithm rules may be punished by triggering a *slash condition*[56], causing a percentage of the deposited DEX tokens of the violating node to vaporize. A *fisherman*[57] mechanism is also employed on the DEXON network to reward those who expose faulty or malicious behaviour throughout the network.

Mining Rewards

The mining rewards will be distributed according the to total time span that a node actively participates in the transaction validation of the DEXON network. The mining validator node can decide whether or not to distribute a certain percentage of the mining rewards to its DEX deposit supporters.

Transaction Fees

In DEXON, every transaction sender needs to pay a flat predefined transaction fee to validator nodes for transactions to be processed. The transaction fee will then be distributed among active validator nodes.

Storage Fees

While most blockchain systems don't charge fees for storage space on smart contracts, in DEXON, the contract owner will have to pay for the storage fees of data to avoid storage space depletion attacks from malicious clients. The storage fee is calculated based on the amount of space used over a period of time, and all collected storage fees will be remitted to validator nodes.

[55] "Cardano (platform) - Wikipedia." https://en.wikipedia.org/wiki/Cardano_(platform).
[56] "Proof of Stake FAQs · ethereum/wiki Wiki · GitHub." https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs.
[57] "polkadot-white-paper/references.bib at master · polkadot-io ... - GitHub." https://github.com/polkadot-io/polkadot-white-paper/blob/master/references.bib.

Gas Fees

Gas is required to execute smart contracts on the DEXON network. Gas consumption of each operation code[58] in the DEXON VM is predefined in the governance contract. Gas fee is paid in the DEXON's native token DEX. The gas fees will be remitted to validator nodes who actively participate in transaction validations.

DEXON Application Scenarios

Digital Asset Issuance

The combination of DEXON's multi-asset account system and its digital asset issuance contract makes DEXON the ideal platform to issue digital assets such as government-backed digital cash, and to host ICOs (Initial Coin Offering).

Digital Asset Exchange

DEXON's multi-asset account system and its high-frequency digital asset trading protocol can work with DEXON's inter-chain asset bridging protocol to establish a fully decentralized inter-chain high-frequency digital asset trading platform with negligible transaction fees. For example, one can trade Ether for Bitcoin on the DEXON network. Moreover, since liquidity is shared throughout all trading markets on the DEXON network, all traders can enjoy the highest liquidity and the lowest spread being offered.

Micropayment Networks

DEXON's negligible transaction processing fees, infinite scalability, and sub-second transaction confirmation latency makes it best suited for digital cash micropayments. Moreover, existing digital assets that have high transaction latency and high transaction fees such as Bitcoin and Ethereum can be bridged onto the DEXON network, making them micropayment-capable.

[58] "Opcode - Wikipedia." https://en.wikipedia.org/wiki/Opcode.

Online Gambling

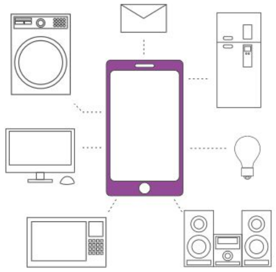
DEXON provides unbiased randomness and low transaction latency in its smart contract platform, making it ideally suitable for online gambling applications.

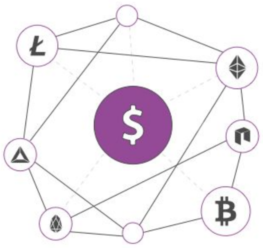
Internet-of-Things (IoT) or Machine-to-Machine (M2M) Data Exchange Network

DEXON will be upgraded with stored data privacy and privacy preserving computation on its smart contract platform, making it ideal for IoT and M2M data exchange application.

Other Kinds of DApps

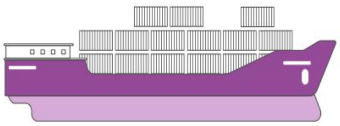
DEXON will keep upgrading its functionality to include a decentralized instant messaging system, decentralized database, and decentralized storage network. All together, any centralized applications such as supply-chain finance, ads exchange, social networks, or MMO (Massively Multiplayer Online) games, etc, can all be built on DEXON network.


IoT


Payment Network

FinTech

Identity Verification


Supply Chain

Digital Assets Exchange

Prediction Market

DEXON DApps Ecosystem Partners

COBINHOOD

COBINHOOD is the ICO services partner of DEXON Foundation. COBINHOOD provides expertise in the ICO space to help DApp projects backed by DEXON Labs with marketing, PR, and funding efforts. COBINHOOD will also work with DEXON Foundation to launch a decentralized digital asset exchange operating through the DEXON network. This decentralized exchange will provide the ultimate trading experience with its world-class web and mobile apps cryptocurrency exchange.

IDG Capital

IDG Capital, one of the top VCs in the world, backed DEXON along with many other top global VCs. IDG Capital is DEXON's official DApps integration partner. Companies in IDG's investment portfolio already have daily active users ranging from millions to billions, and their integration into the DEXON network will help achieve the mass-adoption of DEXON DApps in no time.

Future Works

DEXON Blocklattice Explorer - DEXScan

DEXScan is a web-interface tool to easily examine the status of transactions and the operating status of the DEXON network.

DEXON Smart Contract IDE[59]

DEXON will offer a fully functional smart contract compiler and deployment tool on web and desktop environments, supporting Windows, Mac OS, and Linux.

[59] IDE - "Integrated development environment - Wikipedia." https://en.wikipedia.org/wiki/Integrated_development_environment.

DEXON Wallets

Web, mobile, desktop-based wallet apps, and DEXON wallet SDK libraries will be released as an open-source resource on GitHub in multiple popular programming languages. The multi-signature wallet functionality will also be supported by a user-friendly interface.

DEXON Name System (DNS)

DEXON will build a human-readable, and globally-unified addressing system built on the DEXON network, which is similar to the domain name system on the Internet. The DNS will maintain a mapping for human-readable names to account addresses and any identifiers. With the DNS, users can transfer digital assets and interact with smart contracts much easier.

DEXON Messaging Network (DMN)

The DMN is a low-latency, highly-available, and infinitely scalable messaging service built on top of the DEXON network. The messaging system works like a globally distributed Pub/Sub[60] service. Messaging channels can be registered and administered easily with fine-grained permission control. The messaging content privacy will be fully protected by a novel and efficient DEXON distributed key generator (DKG[61]) service provided on the DEXON network for multi-party secure communication channels.

DEXON Storage Network (DSN)

The DSN works in the same way as proposed in the FileCoin[62] whitepaper. The DSN provides file storage replicas for high availability and guarantees data privacy through cryptography. While the FileCoin whitepaper did address the method to achieve decentralized file retrieval (proof-of-retrieval) and decentralized file storage (proof-of-space-time and proof-of-replication), as well as a bid/ask free market mechanism for DSN usage, it did not, address how to solve the file allocation table[63] scalability issue on its backbone blockchain system. We argue that only DEXON's infinitely scalable blocklattice can work with the FileCoin protocol to build an infinitely scalable

[60] "Publish–subscribe pattern - Wikipedia." https://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern.
[61] "Distributed key generation - Wikipedia." https://en.wikipedia.org/wiki/Distributed_key_generation.
[62] "Filecoin: A Decentralized Storage Network." https://filecoin.io/filecoin.pdf.
[63] "File Allocation Table - Wikipedia." https://en.wikipedia.org/wiki/File_Allocation_Table.

decentralized storage network. The DSN will operate as a decentralized Amazon S3[64] (storage network) and a decentralized CDN[65] (content delivery network).

DEXON Database Service (DDS)

The DDS is a key-value database service built on the DEXON network. The DDS will have rich features such as ACID[66] operations, batch operations, range query operations[67], and others. One can think of DDS as a decentralized version of Cassandra or MongoDB. The DDS provides high availability and infinite scalability and works with the DEXON smart contract platform with an intuitive database query interface.

DEXON Network Anonymizer

Although DEXON transactions cannot be censored by any validator node, it is possible that all validators' IPs or transaction packets are monitored or censored by ISP[68]-level entities or governments. In our future work, we will implement DEXON Network Anonymizer, which works pretty much like TOR[69]. It will encrypt packet content, hide source and destination IP address, and mix up packets to avoid network IP censorships.

DEXON Anonymous Transactions

Transaction privacy is always a concern in DLTs. Techniques such as zk-STARK[70] of Zcash[71] and RingCT[72] of Monero[73] achieves this functionality, but still suffers from high-latency of transaction or censorship vulnerabilities of validator nodes. The ideal solution to this issue is yet to be solved, thus, we leave this as a future work.

DEXON Private Smart Contracts

Some enterprise blockchain applications desire data privacy on smart contracts. By using

[64] "Amazon S3 - Wikipedia." https://en.wikipedia.org/wiki/Amazon_S3.
[65] "Content delivery network - Wikipedia." https://en.wikipedia.org/wiki/Content_delivery_network.
[66] "ACID - Wikipedia." https://en.wikipedia.org/wiki/ACID.
[67] "Range query (data structures) - Wikipedia." https://en.wikipedia.org/wiki/Range_query_(data_structures).
[68] "Internet service provider - Wikipedia." https://en.wikipedia.org/wiki/Internet_service_provider.
[69] "Tor (anonymity network) - Wikipedia." https://en.wikipedia.org/wiki/Tor_(anonymity_network).
[70] "Non-interactive zero-knowledge." https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof.
[71] "Zcash - Wikipedia." https://en.wikipedia.org/wiki/Zcash.
[72] "Ring signature - Wikipedia." https://en.wikipedia.org/wiki/Ring_signature.
[73] "Monero (cryptocurrency) - Wikipedia." https://en.wikipedia.org/wiki/Monero_(cryptocurrency).

homomorphic encryption[74] schemes, computations can be done directly on encrypted data. Leveraging this technique, DEXON Foundation aims to build a private smart contract system on the DEXON network that would facilitate privacy of data and computation on privacy-preserved data. However, homomorphic encryption is still in its early stage, and the computational cost involved is huge and thus, not very practical. We leave this as a future work for DEXON.

DEXON Post-Quantum Resistance Consideration

At the time of publishing this whitepaper, Google has released a 72-qubit[75] quantum chip. As the number of qubits of quantum computer[76] keeps increasing, it threatens the security of asymmetric encryption[77] and digital signature algorithms based on discrete logarithm problem[78] intractability. At the time of DEXON's development, PQC[79] (post-quantum cryptography) standard algorithms have not been decided by NIST[80] yet. Therefore, initially, DEXON will still use ECDSA[81] for its digital signature. Once the PQC standard is confirmed, PQC-based digital signature and account systems will be added to DEXON.

Conclusion

The DEXON network serves as an infinitely scalable, low latency transaction processing engine with the lowest transaction fees in the decentralized Internet era, making it extremely well-suited for DApps development and deployment. DEXON's inter-chain bridging protocol serves as a decentralized hub for all blockchain systems, bridging assets and transactions across different blockchain networks, and providing the infrastructure for instant decentralized micropayments and high-frequency digital asset exchange. All together, DEXON unleashes the true power of decentralized technology. Through DEXON, the future of the decentralized Internet can finally be realized.

[74] "Homomorphic encryption - Wikipedia." https://en.wikipedia.org/wiki/Homomorphic_encryption.
[75] "Qubit - Wikipedia." https://en.wikipedia.org/wiki/Qubit.
[76] "Quantum computing - Wikipedia." https://en.wikipedia.org/wiki/Quantum_computing.
[77] "Public-key cryptography - Wikipedia." https://en.wikipedia.org/wiki/Public-key_cryptography.
[78] "Discrete logarithm - Wikipedia." https://en.wikipedia.org/wiki/Discrete_logarithm.
[79] "Post-quantum cryptography - Wikipedia." https://en.wikipedia.org/wiki/Post-quantum_cryptography.
[80] "NIST: National Institute of Standards and ...." https://www.nist.gov/.
[81] "ECDSA." https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

DISCLAIMER

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. CONSULT LEGAL AND FINANCIAL EXPERTS FOR FURTHER GUIDANCE.

The following information may be incomplete and in no way implies a contractual relationship. While we make every effort to ensure that all information in this Whitepaper is accurate and up to date, such material in no way constitutes professional advice. DEXON Foundation neither guarantees nor accepts responsibility for the accuracy, reliability, or completeness of this content. The content may be subject to change at any time without prior notice. Individuals intending to invest in the platform should seek independent professional advice prior to acting on any of the information contained in this paper.