Technical Whitepaper

A Blockchain Safe Haven
for Investors and Like-minded Entrepreneurs

October 2022

Table of Contents

1 Introduction

1.1 What is a blockchain?

A blockchain is a public database that is constantly updated and shared across a network of computers. Blockchains are generally referred to as Distributed Ledger Technologies (DLTs). "Block" refers to the storage of data and state in clusters known as "blocks." Every transaction on the network is recorded on the blocks and denominated in NXT. "Chain" refers to the fact that each block references its parent block cryptographically. In other words, blocks are interconnected. The data in a block cannot be modified without modifying all subsequent blocks, which would need network-wide consensus.

Every computer in the network must concur on every new block in the chain. These machines are referred to as "nodes." Nodes ensure that all parties engaging with the blockchain share the same information. To achieve this decentralized consensus, blockchains require a consensus mechanism as will be explained in section 3.11.

A cryptocurrency is an exchange medium supported by a blockchain-based distributed ledger. A medium of exchange is anything that is universally recognized as payment for goods and services (i.e: the native token,) while a ledger is a data repository that records transactions. Users can conduct transactions on the ledger without relying on a trusted third party to maintain the record using blockchain technology.

1.2 What is NXT Technologies?

NXT Technologies Incorporated is a Layer1 permissioned blockchain company that is creating a global decentralized validator node ecosystem that will be directly used for enterprise solutions, small business, WEB 3 and other types of blockchain projects that require on and off-chain validation or blockchain services.

We believe deploying our blockchain with a robust decentralized network of internal & external nodes will give us the opportunity to have partnerships with innovative forward-thinking entities and operations.

NXT is the native coin for NXT Technologies and its designed to facilitate a market for computation and our ecosystem. Such a market offers members an early economic incentive to validate and execute transaction requests and contribute computational resources to the network. In section 3.2 of this whitepaper, it will be explained exactly why a native currency is essential for building contribution incentive for collaborators and thus ensuring participation on the network.

1.3 Why does NXT Technologies Exist?

To define why NXT Technologies is needed, we must first explain our mission and the necessity of blockchain technology. Firstly, blockchain is a transformative technology. A shared, immutable ledger is at the core of a blockchain. Once a transaction is entered, no one can modify

it, this makes the blockchain immutable and mitigates the risk. Furthermore, blockchain technology can also reduce costs and increase efficiency throughout many industries due to eliminating third parties, indecisiveness, and overhead costs.

However, the blockchain industry faces many significant issues, such as incoming regulations, slow network/transaction speeds, high fees, lack of trust, and weak security. NXT Technologies blockchain will create a permissioned network that will combat most of these issues while providing participants accountability, scalability, security, privacy, and financial incentives. Companies that aim to assist with enterprise-level blockchain solutions are typically large corporations with bloated infrastructures, which raise costs. Additionally, they generally neglect the importance of building a community organically and supporting the onboarding of projects, as we see with more recent blockchains such as Bitcoin or Ethereum.

To leverage software specific or businesses that have had technical obstacles in blockchain, NXT Technologies aims to provide the efficiency and transparency of DLT technology to the enterprise market. The primary goal is to enable solutions that more directly connect businesses, organizations, and even individuals. This will create a new way of sharing information between two entities. NXT Technologies is a lean, highly blockchain-specialized team of experienced experts with an emphasis in entrepreneurship and blockchain technology, which results in high efficiency and low overhead costs. Consequently, we can generate time and cost savings, which we can provide for our customers. Additionally, we understand the significance of a community to propel the NXT Technologies ecosystem and bootstrap new projects.

To maintain the community's health and transparency, NXT Technologies manages the development cycle, software licensing, security audits, node security, and provenance tracking for each line of code for any entity acting in our ecosystem.

1.4 What We Do

Our technologies primary focus is building a Layer1 solution and combining our blockchain technology with real-world enterprise—use cases that can achieve immutable record keeping, databasing, ledger atomization while utilizing our decentralized chain validated on our node network. We are aiming to implement our solutions in several types of industries from inventory management, human resources, medical records, and manufacturing processes to name a few. We feel that there are voids in industries that smart contracting and Web3 solutions will not only fit but enhance the process in which the companies conduct business.

1.5 Partners

NXT Technologies NXTChain utilizes Hyperledger’s collective intensive blockchain tools for an industry where government institutions are at a crossroads between protecting adoption and advancing in untapped territories. Hyperledger is a project hosted by the Linux foundation to help developers and companies work together to build collaborative blockchain projects. Similar to the Linux operating system, we are able to use Hyperledger’s resources to build and assist in

NXT Technologies from smart contracting to blockchain solutions. As a result, NXT Technologies has been foundationally built with software backed by the greatest technologies companies in the world. Some of these companies include IBM, Intel, and Samsung.

NXTChain is a permissioned open-source solution for enterprise—private or public, deployers, architects and engineers all around the globe can build and collaborate on our blockchain. As a result, NXT Technologies has been foundationally built with software backed by some of the greatest technological companies in the world. Currently, large business is not just working on the development of the software, they are creating and implementing use cases to create sustainability where they lack a trusted approach. NXT Technologies is choosing to work with software that is ready for global adoption regardless of what the individual government regulatory agencies bring to the table. We are prepared and ready to meet regulations head on.

1.6 NXT Community

We believe community is a staple in the journey in building a project of this caliber. Some of the largest projects in tech were built on bite-sized community adoption and took off from there. Our community is the backbone of our business and there is a shared interest in all things cryptocurrency, blockchain, enterprise and the technology. Our community is a place where we also provide an avenue to share our external roadmap, news and updates, exchange ideas and opinions from each and every voice. We believe in giving our community a place where they can ask questions and contact a developer or an individual at the executive level. This is beneficial in a market that is consistently moving.

2 Enterprise

2.1 Enterprise Pilot Testing

NXT Technologies Inc. is creating internal pilot tests with companies that are directly associated with the Board of Directors at NXT Technologies, Inc. We will continue to discuss the opportunities with our Board as we grow our network to combine our blockchain technology with their company or companies that they are directly associated with. This direct line of communication with large to mid-sized enterprise gives NXT Technologies an environment that we can test, deploy and excel in with minimal costs to NXT Technologies Inc.. After a successful pilot test which results in cost and/or time saving solutions, NXT Technologies will present the following enterprise with a proposal for our NXTChain or a tokenized internal system for there clients.

2.2 Enterprise Blockchain

NXT Technologies attracts a vast audience of investors and customers. Our primary objective is to work with businesses to develop enterprise blockchain value addition, ranging from commerce to gaming, and consists of:

1. Enterprise integration:

- *Integration with the current System of Record (SoR*): The solution must support current and established techniques, including reporting and analytics, business intelligence, and Customer Relationship Management (CRM). The fact that these systems are generally allocated significant investments and are integrated into many different operational aspects of a firm underscores the significance of this integration.

- The SoR may be maintained as a temporary strategy to implement blockchain. However, the transactions are not processed more than once.

- Design intent to include: Enterprise adoption is accelerated along the route of least disruption. Due to the associated costs and operational inconvenience, this is an essential factor.

2. *Auditing and logging*: Auditing and logging take into account corporate business procedures, reporting needs, and enterprise technology preferred practices, such as change management, support, and High-Availability Disaster Recovery (HADR) requirements. For nonrepudiation, technological root-cause analysis, fraud analysis, and other enterprise systems, you must abide by regulations about regulated systems.

3. *Monitoring*: monitoring the system is essential because any systemic impact—a business or technical anomaly—will affect the network and ecosystem participants. Additionally, you must adhere to laws and commonly accepted IT standards for high availability, capacity planning, pattern recognition, and fault identification.

4. *Reporting and Regulatory requirements*: Even for the temporary deployment of a blockchain as a transaction processing system, this is by far the most crucial stage. To offload the reporting and regulatory needs until the blockchain, or the business software, is blockchain aware, it is, therefore, advisable to build interfaces to existing SoR.

5. *Authentication, authorization, and accounting requirements*: In contrast to the *permissionless environment of the Bitcoin blockchain*, all participants in a permissioned enterprise network must be identified and tracked, with clearly defined roles. The digital identities of the many people and companies participating in a blockchain network are among the subjects that fall within this domain. To meet the numerous authentication and authorization requirements of a blockchain network, concepts such as a distributed or decentralized trust, digital identity, self-sovereign identification, consent management, and distributed access control (DACL) are developing.

2.3 Why Enterprise Blockchain?

Blockchain is important because no business exists alone. Several institutions can accomplish more than any one could on their own. Procedures can be made more cost-effective by implementing business processes that use the group's collective expertise. It is possible to design new systems that were not feasible before blockchain. These new possibilities give many businesses a competitive edge.

With the help of a blockchain, organizations may interact safely and securely while creating prospects for new business models, ecosystems, and economic situations. These prospects will help many organizations generate new revenue streams and outpace the competition by implementing modern vital technologies and possibly eliminate certain rivals from the value chain. A “Know Your Customer” (KYC) application can leverage blockchain to minimize friction and time to verify and onboard clients faster. For instance, a digital trade chain can simplify a trade finance platform and give access to more trading partners and companies.

As we noted previously, a blockchain can be identified as a shared, decentralized, cryptographically secured, and immutable digital ledger. An enterprise blockchain is similar but can be distinguished by the following characteristics:

***Accountability*:** Access permissions are assigned based on business role, and network members are known and identified by cryptographic membership keys. It would be challenging to comply with laws like the General Data Protection Regulation of 2018 (GDPR) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) without such responsibility.

***Privacy*:** While network members are aware of one another, only the members who are required to have information about a specific transaction are informed of it. Enterprise blockchain uses various methods, such as peer-to-peer connections, privacy channels, and zero-knowledge proofs.

***Scalability*:** In business contexts, handling many transactions is essential. The number of peers and the complexity of the smart contract are only two of the numerous variables that will affect the transaction rates of any given firm. Transaction speeds measured in thousands of transactions per second are certainly attainable and provide the enterprise blockchain a significant advantage compared to conventional blockchains.

***Security*:** Enterprise blockchains are fault-tolerant, which enhances security. With fault-tolerant consensus methods, the network continues to operate even if specific nodes are not behaving correctly. RAFT is an illustration of a fault-tolerant consensus method.

***Motivating*:** A built-in incentive mechanism helps an enterprise blockchain's adoption curve grow faster. Consider this driver as a “loyalty point” or “token” that offers network providers and customers an economical and motivating incentive.

Enterprise blockchains are often wrongly labeled as private networks. In actuality, “the governors” determine the regulations surrounding how new members can join the network and manage access to an enterprise blockchain. How the network is regulated determines whether it is visible (public or private). Enterprise blockchains are permissioned, though not necessarily private.

3 Let’s Open A Block

3.1 What is a block?

Blocks are groups of transactions that include a hash of the preceding block in the chain. Because hashes are derived cryptographically from block data, this connects blocks together (in a chain). This avoids fraud because a single alteration to any block in the blockchain's history would invalidate all subsequent blocks, as all subsequent hashes would change, and therefore would not point to the right block. This results in a “fork” of the blockchain.

In order to maintain the transaction history, blocks are strictly ordered (each new block has a reference to its parent block) and transactions within blocks are also strictly ordered. All network participants are generally in agreement on the exact number and history of blocks at any one time, and are trying to group the current active transaction requests into the next block.

3.2 What is NXT?

A cryptocurrency is an exchange medium supported by a blockchain-based distributed ledger. A medium of exchange is anything that is universally recognized as payment for goods and services, while a ledger is a data repository that records transactions. Users can conduct transactions on the ledger without relying on a trusted third party to maintain the record using blockchain technology.

NXT is NXT Technologies native coin. NXT is designed to facilitate a market for computation and hence denominated in NXT. Such a market offers members with an economic incentive to validate and execute transaction requests and contribute computational resources to the network.

3.3 Allocation of NXT

Minting is the process of allocating NXT coin on NXTChain. 500M NXT is allocated to the validators as a reward incentive mechanism that is governed by the minting function that is initialized on the genesis block, and it is not possible for any more NXT (other then the initial 1B supply) to be minted. NXT is coined as a reward for each proposed block and at each epoch checkpoint for additional validator work related to consensus formation. The total quantity issued is dependent on the total amount of NXT staked by validators. In an ideal scenario when all validators are trustworthy and online, this total issuance is shared equally across validators, but in practice, it fluctuates based on validator performance.

3.4 Validator Rewards: Enabling Economy: Economic Allocation Reward Function

As mentioned previously, it is essential to reward active honest participation in NXTChain. Therefore, 500M NXT is allocated as liquidity and rewards for validators on our network. Each honest Validator will equally be rewarded a set APR. The APR will initially be set at 10% but

will dynamically adjust itself once the 500M tokens are fully allocated – due to gas fees. The reward function of NXT is inspired by the group at AVA Labs and is governed by equation [1].

In the "Gas fee" section, it was explained that any entity proposing a transaction to the network will have to pay a fee—Gas fee. This Gas fee is split. A portion of it will go towards the NXT Treasury and the rest will be used to aid in Validator rewards.

$$R_j = R_l + \sum_{\forall u} \left(\frac{c_j}{L} 0.002 * u.s_{time} + 0.896) * \frac{u.s_{amount}}{R_j} \right) * \frac{c_j}{L} * \sum_{i=0}^{j} \frac{1}{(\gamma + \frac{1}{1+i^{\lambda}})^i} \quad 3.1$$

Where

$$L = \sum_{i=0}^{\infty} \frac{1}{(\gamma + \frac{1}{1+i^{\lambda}})^i} \quad 3.1$$

Where

- R_j: Total number of tokens at year j
- R_l represents the last years value or R_{j-1}
- c_j is the un-rewarded supply of coins to reach 1B at year j
- u represents the staker
- $u.s_{amount}$ represents the total amount of stake for u
- $u.s_{time}$ is the time length for staker u
- γ and λ are governable

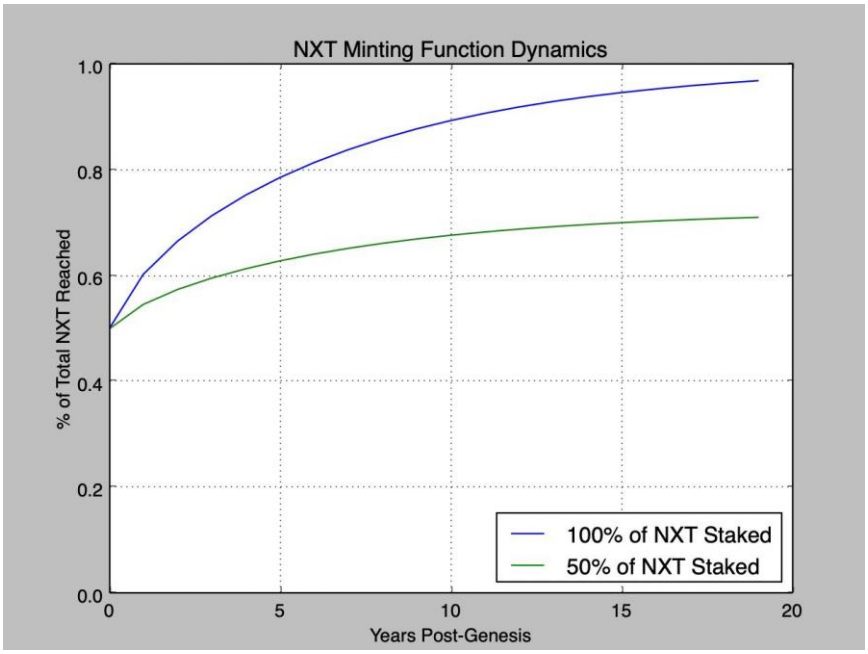


Figure 3.1. Represents the NXT token allocation 20 years post-genesis block. The curve labeled "100% NXT Staked" represents the case where every token is repeatedly staked for a maximum of one year. The curve labeled "50% NXT staked represents the case where only 50% of NXT are staked over the minimal staking period. For the purpose of this simulation the two governing variables, Gamma and Lambda are set to constant values of 1.15 and 1.1 respectively

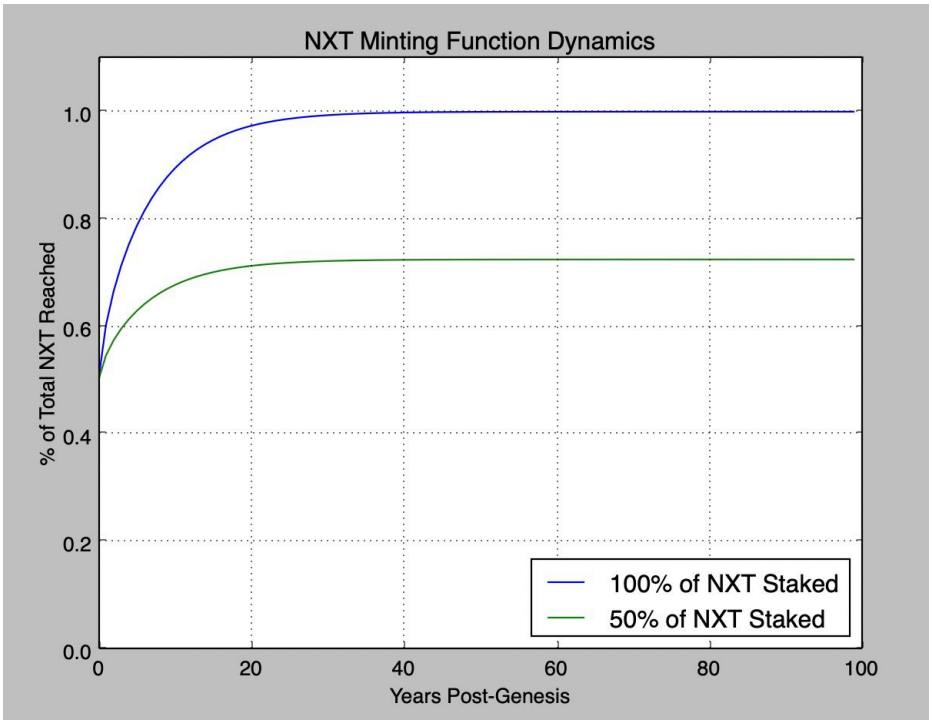


Figure 3.2. Represents the NXT token allocation 20 years post-genesis block. The curve labeled "100% NXT Staked" represents the case where every token is repeatedly staked for a maximum of one year. The curve labeled "50% NXT staked represents the case where only 50% of NXT is staked over the minimal staking period. For the purposes of this simulation the two governing variables, Gamma & Lambda are set to constant values of 1.15 and 1.1 respectively.

3.5 Bonding period

The bonding period refers to the governing mechanics behind staking and un-staking NXT. NXT can be staked for as long as the user pleases. However, once withdrawn, there is a 6-month vesting period until the user obtains their funds. During this period there will be no rewards.

3.6 Locking NXT

In addition to being created through block rewards, NXT can also be withdrawn from the circulating supply through a process known as "locking." When NXT is locked, it is stored in a locked "vault" managed by the Treasury. NXT is used in every NXTChain transaction. When users pay for their transactions through gas, a network-determined, transaction-demand-based base gas cost is initiated. This, along with varying block sizes and a maximum gas fee, simplifies the estimation of NXTs transaction fees. When network demand is great, blocks may use more NXT than they mint, thus canceling out issuance.

3.7 Genesis Block

The Genesis Block, also known as Block 0, is the very first block in a blockchain that subsequent blocks are built upon. It is effectively the ancestor to which all other blocks can trace their lineage, as each block references the one that came before it. This initiated the process of validating bitcoin transactions and creating new bitcoins.

3.8 Block Time

Block time refers to the period of time between blocks. In NXTChain, time is split into increments known as “slots.” In each slot, an individual validator is chosen to propose a block. Assuming that all validators are online and fully operational, there will be a block in every available one. The set block time is set in the genesis block. However, validators may occasionally be unavailable when requested to submit a block, resulting in empty slots. This is in contrast to proof-of-work-based systems, where block timings are determined by the mining difficulty and are probabilistic.

3.9 Block Size

A final crucial point is that the size of individual blocks is limited. Each block has a goal size that is set in the genesis block; however, the size can increase or decrease based on network demand, up to a maximum specified in the genesis block. The total quantity of gas used by all transactions in a block must be less than the gas limit for the block. This is crucial because it prevents blocks from being arbitrarily huge. If blocks could be any size, less efficient full nodes would lose the ability to keep up with the network over time owing to space and speed

constraints. The higher the block size, the more computing power is necessary to process it before the next slot. This is a centralizing force that is resisted by limiting the size of blocks.

3.10 Transactions

A transaction on NXTChain is activity initiated by an externally owned account, i.e., a human-managed but not a controlled account and not a contract. If Bob sends 1 NXT to Alice, Bob's account must be debited and Alice's account must be credited. This state-changing action occurs inside the context of a transaction.

Transactions that modify the state of the EVM [2] must be transmitted to the entire network. After a node broadcasts a request for a transaction to be completed on the EVM, a validator executes the transaction and propagates the ensuing state change to the rest of the network.

Fees are required for transactions, which must be included in a validated block. To simplify this review, we will discuss gas prices and validation in the next section.

Included in a submitted transaction are the following details:

Recipient: The receiving address (if an externally-owned account, value will be transferred). If a contract account is associated with the transaction, the contract code (Smart Contract) will be executed.

Signature: Signature is the sender's identification. This is produced when the sender's private key signs the transaction and verifies that the sender has authorized the transaction.

Nonce: An incremental counter that indicates the transaction number based on the account

Value: Amount of NXT to be sent from sender to receiver.

Data: Optional field to include arbitrary data.

Gas Limit: The maximum quantity of gas units that may be consumed during a transaction. Units of gas signify computational operations.

Max Priority Fee Per Gas: the maximum quantity of gas to be added as a bonus to the validator.

Max Fee Per Gas: the maximum amount of gas for which a transaction participant is ready to pay (inclusive of base Fee Per Gas and Max Priority Fee Per Gas)

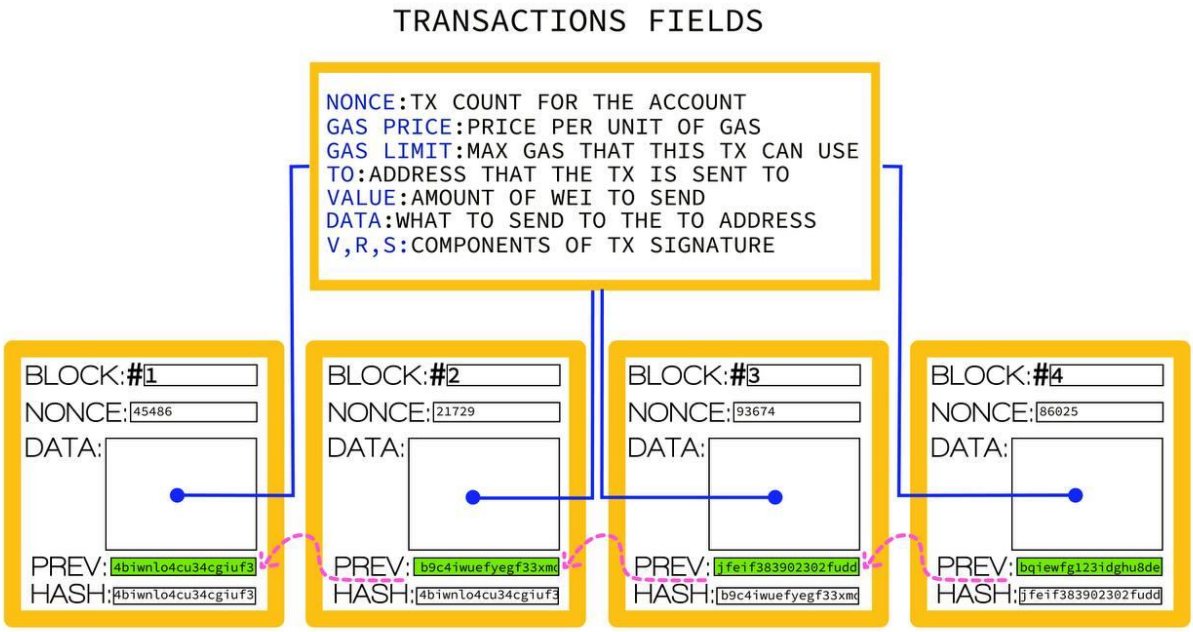


Figure 3.3. Depiction of a blockchain with the corresponding information in each block. The "transaction Fields" shows the components of transactions in the "data" field

3.11 What is Gas?

NXT facilitates a pricing system for NXTChains processing power. Gas is the unit used to quantify the computing effort necessary to conduct transactions on NXTChain. Since each network transaction requires computing resources to execute, a fee is required for each transaction. Gas is the fee necessary to successfully complete an NXTChain transaction. When users wish to conduct a transaction, they must pay NXTChain for the blockchain to recognize their transaction. These prices are referred to as gas fees, and they vary based on the amount of computing power necessary to perform the transaction and the current network-wide demand for computing power. Even if a malicious DAPP submitted an infinite loop, the transaction would ultimately run out of NXT coin and terminate, allowing the network to resume regular operations protecting the network from DDoS attacks. Furthermore, the gas fee complex is split in a set ratio between the NXTChain Reserve and the block-creating-Operator.

3.12 Block Generation (Consensus Mechanics)

Once a block is created by a validator on the network, it is propagated to the rest of the network; all nodes add it to the end of their blockchain, and a new validator is chosen to generate the next block. Proof of Work (PoW), which was originally proposed and used by the Bitcoin network, is the consensus protocol of the majority of the most prominent permissionless networks. This consensus protocol includes an incentive for block producers or validators, which is crucial for encouraging involvement in such networks. As a trade-off, PoW causes the consumption

of amounts of energy equivalent to the energy consumed by medium-sized countries and reduces the decentralization of block generation to a handful of individuals in charge of mining pools, which are responsible for determining which transactions are included in new blocks. Currently, NXTChains "Proof-of-Authority" protocol specifies the exact block-assembly and commitment/consensus procedures.

In general, permissioned blockchains, authorized validator nodes in permissioned networks take turns generating new blocks and are operated by known entities with a vested interest in the network's existence and functionality to enable blockchain-based government and enterprise to scale. This framework promotes a consensus protocol consisting of a practical fault-tolerant byzantine proof of authority with the following characteristics:

- To be valid, blocks must be signed by a majority of validator nodes.
- Instantaneous or near-instantaneous finality exists.
- Ledger is immutable
- Only validator-permitted nodes can propose and vote on new blocks.
- Validator nodes are allotted a window of time to propose a new block. When the time limit expires, the validator is replaced by an alternative validator.
- Validator nodes are required to accept valid transactions and flag invalid ones.
- Validator nodes must be robust.

Validators do not compete to make blocks, but instead take turns producing blocks. As a result, finality is instantaneous, and fresh blocks are always appended to the end of the chain; history is never rewritten. If a validator node attempted to rewrite history, any honest node in the network (validators and non-validators alike) might simply refuse to accept it if the preceding block's hash did not match the hash in the most recent version of the chain the honest nodes have.

3.13 Smart Contracts

Simply said, a "smart contract" is a software that executes on the blockchain. It is a collection of code (its functions) and data (its state) that exists at a specific blockchain address.

NXT accounts are a sort of smart contracts. This indicates that they have a balance and can participate in transactions. However, Smart Contracts are not user-controlled; rather, they are deployed to the network and run according to their programming. Then, user accounts can engage with a smart contract by submitting transactions that carry out a contract-defined purpose. As with conventional contracts, smart contracts can create and automatically enforce rules. By default, smart contracts cannot be deleted, and their interactions are irrevocable.

4 The Permissioned Blockchain

4.1 Permissioned vs Permissionless

Virtually anyone can participate in a permissionless blockchain, and each participant is anonymous. The only trust in this type of a network stems from the state of the blockchain itself.

Permissionless blockchains often employ a “mined” native coin or transaction fees to compensate for the exorbitant expenses of engaging in a sort of byzantine fault-tolerant consensus based on PoW.

Permissioned blockchains, on the other hand, operate a blockchain among a set of known, identifiable, and frequently vetted participants who operate under a governance framework that generates a certain level of trust. A permissioned blockchain provides a method for securing interactions between a set of entities that have a common objective but may not fully trust one another. By depending on the identities of the participants, a permissioned blockchain can use consensus methods that do not require costly mining, such as Crash Fault Tolerant (CFT) and Byzantine Fault Tolerant (BFT).

Moreover, in permissioned blockchains, the possibility of a player purposefully adding harmful code through a smart contract is reduced. First, the participants are known to one another, and all actions, including submitting application transactions, modifying the configuration of the network, and deploying a smart contract, are recorded on the blockchain in accordance with an endorsement policy established for the network and transaction type. Instead of being entirely anonymous, the guilty actor can be easily identified, and the incident can be managed in accordance with the governance model’s provisions.

Bitcoin was the first blockchain application using this decentralized architecture. Since then, blockchain technology and digital currencies have become synonymous in the public mind.

However, there is a distinction. Permissionless blockchains, like Bitcoin and Ethereum, make transactions possible across extensive public networks. Anyone can purchase, sell, trade, and deal across the ecosystem. Anyone can view the entire history of events as they have occurred, block by block. Users interact freely and frequently and remain anonymous.

Enterprise can combine technologies to balance privacy and performance and build permissioned, permissionless, or hybrid networks. NXT Technologies is primarily concerned with consortium networks that connect several stakeholders to speed up crucial, confidential business processes and transactions. These networks, or multiparty systems, are modular and adaptable enough to handle various sectors and use cases when constructed using this method. Thanks to the varied and expanding NXT Technologies ecosystem, they can interact with legacy systems or even access a cryptocurrency “mainnet.”

4.2 Permission Provider: Certificates of Authority

As NXTChain is a permissioned network, blockchain participants must demonstrate their identity to the rest of the network in order to transact on it. Certificate Authorities issue identities by generating a pair of public and private keys that can be used to verify an individual’s identity. In order for this identity to be recognized by the network, the MSP is required. A peer uses its private key, for instance, to digitally sign or endorse a transaction. The Membership Service Provider (MSP) is utilized to determine if the peer is authorized to endorse the transaction. The public key contained within the peer's certificate is then used to validate the signature associated to the transaction. Thus, the MSP is the mechanism that enables the rest of the network to identify and trust this identity.

While this requirement adds friction to on-boarding, it provides a host of anticipated long-term benefits and utility to the blockchain, leading to potential rapid adoption by institutional and regulated users. Identity service providers will need to ensure the claims of NXTChain users to remain active.

In particular, validating identities in the initial onboarding helps address a key challenge that most public blockchains ignore: Sybil resistance. Sybil resistance blocks users from freely creating multiple on-chain identities. With the addition of this feature to foundation of NXTChain, users can rely on the single identity and reputation of other users thus minimizing the risk that more sophisticated open finance protocols face with the traditional permissionless networks.

Other benefits of identity at the base layer of the chain include:

- ***NXT provenance*:** This allows regulated entities, including institutions, to use and acquire NXT tokens to access the network with the confidence that these tokens have a known provenance.
- ***Identity verification:*** Risk of users making payments to or transacting with applicable restricted or sanctioned nations, entities, or persons is mitigated
- ***Validated identity for regulated assets*:** Permits a tiered customer due diligence (CDD).

The governance structure of NXTChain is split up into 5 specialized overseeing committees to further retain a decentralized network. The set of sub-committees are as follows:

4.3 Governance

Governing Council:

- Oversees all committees
- Has the ability to create or dissolve committees
- Manage the distribution of resources in the network according to the resource distribution rules

Technical Committee:

- Oversees network upgrades
- Propose new architecture ideas
- Develop native developer tools
- Expose particular boot nodes that accept into the network in partnership with the community and other network members
- Maintain transaction explorer
- Keep complementing off-chain services accessible
- Provide data and dashboards that depict network performance
- Monitor the network to detect technical issues and identify areas for improvement
- Conduct regular stress tests
- Perform routine technological upkeep
- Provide backup nodes in the event that the primary nodes fail
- Offer technical assistance to organizations seeking to deploy nodes or apps

Economic Committee:

- Overseeing network economy including NXT emissions, policies and fees
- Propose changes to block reward amount and gas fee price to manage circulating supply
- Propose dedicated gas fee split ratio to relevant projects in the ecosystem
    - Incentivizes network growth
- Propose and plan Treasury allocation for ecosystem growth

Corporate Governance and Nominating Committee:

- *Corporate governance* refers to the committee of reference for each project
- *Nominating committee* refers to the individuals for syndicate purposes
    - The "voice" of the network
- Overseeing the operation of the Governing Council and Committees
- Overseeing the creation and implementation of NXTChain governance, code of conduct, and ethics policies
- Manage the relationship between "governance" and projects
- Ensures each project follows the standardized code of conduct and ethical policies
- Oversee validator work with the power to exclude malicious nodes

Advisory Committee:

- Overseeing special projects and activities not covered by the technical & economic committees
    - Individuals must have experience and industry background
- Aids in management and development of the blockchain

These committees will be comprised of NXTChain participants and will be responsible for fulfilling governing duties related to their specific council/committee. Any NXTChain entity with a proven identity can propose to any committee and will be given voting rights – very similar to a DAO. Furthermore, proposals are staked to prevent spamming.

4.4 Network Topology

NXTChain is primarily a permissioned public blockchain that is structurally built off our nodes — NXTreme. Intrinsically, the NXTreme has a license that gives the user the privilege of running a node on our network. Each adopted enterprise soltuion will have the option to choose whether they want their node to run on-site or in the cloud. As previously mentioned, we support networks that are as decentralized as possible in their management and governance. However, it is vital to set and enforce very explicit rights and obligations for each organization taking part in our network if we also intend to have well-established accountabilities and have risks minimized in accordance with a risk model.

The NXTchain network topology consists of a decentralized node network. The Technical team provides infrastructure and operation support for these nodes. NXTreme node functionality can easily be conceptualized as four individual nodes and are as follows:

- Validator node
- Boot node
- Writer node
- Observer node

NXTreme nodes are inherently only validator nodes. Due to the permissioned nature of NXTChain, specific node functions can be allotted to individual nodes. For example, a node consisting of just the validator node function or boot…etc. This makes NXTChain more efficient and robust when compared to typical permissionless blockchains. Furthermore, to meet a project's specific need, we are able to allocate a portion of our node network specifically to transactions pertaining to a certain project. Hence, projects with many transactions will not congest our network and thus ensuring our blockchain remains robust and efficient. For example, video game projects tend to generate many more transactions than enterprise projects. Therefore, we would isolate the transactions originating from the game to a pre-allotted network of our nodes. Hence, maintaining a stable and efficient network. At the core, NXTChain has an internal node structure based on AWS-Cloud and are as follows:

Example:

NXTreme is running *2,500* Nodes on our NXTChain Blockchain.

XYZ Metaverse project contacts NXT Technologies with a proposal to collaborate but XYZ Metaverse does not have the bandwidth to operate its WEB 3 application.

NXT Technologies will then allocate 50-Nodes to XYZ Metaverse so that they can accomplish their goal and receive a portion of the transaction fees.

With the utilization of our node network for enterprise solutions, NXT Technologies will generate revenue and therefore our holders will be compensated.

Internal Node System – 25 Allocated Nodes

22 were allocated as Validator nodes

1 were allocated as Boot nodes

1 were allocated as Writer nodes

1 were allocated as Observer nodes

With this 25 internal node structure, we ensure that our blockchain remains running even in the very unlikely instance that everyone contributing to the network decides to unplug their NXTreme. This is an extensive back-up system that is encrypted and backed up on AWS Cloud Services.

Validator responsibility (NXTreme nodes):

Figure 4.1. NXT Technologies flagship product -- NXTreme

A Validator node refers to the production of new blocks and participation in administering the consensus mechanism. Validator nodes only establish connections with each other and Boot nodes. If a transaction does not comply with the network's regulations, it is rejected. If a proposed block by another node contains invalid transactions, it must be reported. Below is a summary of the validator node's responsibilities and liabilities:

- Follow the routing rules.
- Do not connect with any node which is not in the permissioning smart contract.
- Vote for valid blocks.
- Do not vote for invalid blocks.
- Maintain the node resilient.
- Do not broadcast transactions.

The technical specifications of the NXTreme node are as follows:

- CPU: AMD R13305G
- RAM: 8GB DDR4
- SSD 1: 500GB NVME (blockchain)
- SSD 2: 1TB SATA (NXTsafe)
- Wifi & Bluetooth capabilities
- GPU: Radeon Vega Graphics
    - Display port: 2x HDMI 2.0

- Ethernet: 1GbE, RTL8111H, RJ-45
- WLAN: M2
- Audio: Realtek HD AL662
- Dimensions: 130mm x 128mm x 52mm
- Power: 12V DC

Boot nodes:

Boot nodes act as a communication governance between validator nodes and satellite nodes. They onboard new nodes by sharing the blockchain's history and current state with them. The state of the blockchain comprises information about the network's other nodes, routing rules, and whitelists and blacklists. Boot nodes actively listen to writer nodes and transmit the transaction to the validator node as long as the transaction itself is considered valid under the boot nodes governance rules. The support and function of the boot nodes are administered by the Technical Team. Furthermore, they inform satellite nodes about newly created blocks by validator nodes and have the following obligations and liabilities:

- Follow the Routing Rules.
- Replicate all transactions with their peers.
- Maintain the node resilient.
- Do not broadcast transactions.

Writer nodes:

It is permitted for writer nodes to broadcast transactions to the network. These nodes create network traffic, which often originates from centralized applications, decentralized applications, end users, and other services. They act as a medium for transactions to pass to Boot nodes. Writer nodes are also able to establish private channels and side-chains between one another for private communication, which is necessary for specific enterprise needs such as healthcare. Furthermore, utilizing native decentralized storage within the network, they can exchange public documents and data. The nodes functionality is summarized as follows:

- Do not exceed the resource usage/consumption allowed per block.
- Do not send any transaction that violates network rules.
- Co-sign all transactions broadcasted to the blockchain.
- Be accountable for all transactions broadcasted.
- Do not attempt denial of service attacks.

Observer nodes:

Only able to read the blockchain. They can join the network by connecting to open boot nodes provided by the Technical Team for the purpose of reading the blockchain. In addition, these nodes are incapable of broadcasting transactions or generating blocks, therefore they cannot inflict harm.

As described in earlier sections, boot and validator nodes must adhere to the Permissioning Committees Routing Rules.

4.5 Connections between nodes (Routing Rules).

The Routing Rules as mentioned previously are outlined as follows:

- Each writer node can establish a connection with a chosen subset of boot nodes.
- Each observer node is able to connect to a particular group of boot nodes.
- Certain boot nodes must be accessible in order to connect with a particular set of writer nodes.
- Certain boot nodes must be accessible in order to connect with a particular set of observer nodes.
- Each boot node must be able to establish a connection with all active validator nodes.
- Each active validator node must be able to establish a connection with all boot nodes.
- Each active validator node must be able to communicate with all the other active validator nodes.
- Validator nodes are not permitted to communicate with writer nodes.

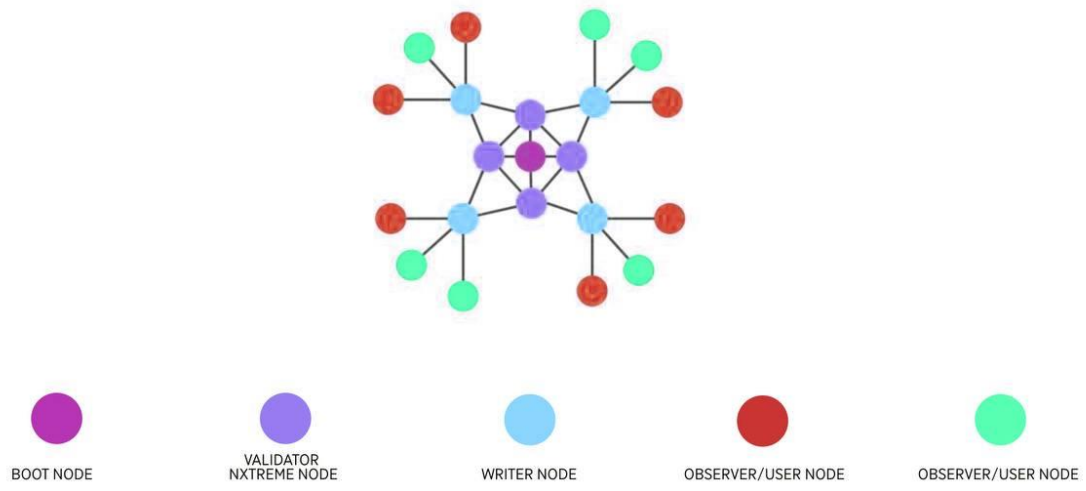


Figure 4.2. Graphical representation of the node network

4.6 Quantum Security

Quantum computing will usher in a new paradigm in which digital technology will face both obstacles and opportunities. There will be a range of security concerns in the digital environment, especially when powerful quantum computers are able to break several essential encryption techniques currently in use. As a technology that heavily relies on cryptography, blockchain is vulnerable to these dangers. In a 2019 article issued by the IDB, the combination of blockchain technology and quantum computing was presented in the four domains below [3].

Internet communication relies on protocols such as HTTP. HTTPS provides communication security via the SSL/TLS protocol stack. TLS allows one-time key generation (which is not quantum-safe) with AES for symmetric encryption as well as RSA, DH, ECDH, ECDSA, and DSA for exchange and authentication. This implies that all internet interactions, including transactions and messages transferred between apps and nodes in a blockchain, will no longer be quantum-safe when fully functional quantum computers are available.

Digital signatures are one of blockchain technology's most crucial components. Bitcoin and Ethereum utilize elliptic curve cryptography (ECC), specifically ECDSA signature techniques on curvesecp256k1. Others, such EOSIO, utilize the standard NIST secp256r1 curve. NIST recommends the replacement of ECDSA and RSA signature systems owing to the influence of Shor's algorithm [4].

Block mining is the foundation of PoW-based blockchain networks, as the consensus mechanism relies on the discovery of nonces. Using Grover’s technique, quantum computers will find these nonces (i.e., mine) quadratically faster [5]. However, this does not pose a significant threat to the security of blockchain networks, as the remedy is as simple as quadrupling the difficulty to counteract the quantum advantage. This threat does not present in networks with consensus procedures that do not encourage rivalry between nodes, such as the PoA proposed in this architecture.

Hash functions take an input from a set with an infinite amount of elements and return an output from a set with a finite number of elements, such as the SHA-256 function utilized by the majority of blockchain networks today. Therefore, it is statistically impossible to obtain the original element from a hash value stored on the blockchain. This trait, known as irreversibility or pre-image resistance, ensures the security of these operations even when quantum computers are present. Moreover, hash functions are always changing to improve security. For instance, if quantum computers evolve to the point where they pose a threat to SHA-2, the NIST standard FIPS202 [6] already specifies SHA-3 as an alternative that provides a better level of security.

Blockchain networks must account for the threat posed by quantum computers and implement cryptography and processes that are quantum-resistant. As data and assets are immutably stored and exposed to the public, blockchain networks will become an easy target for quantum computers if this is not prevented. When it is possible to deduce private keys from publicly disclosed public keys, assets and encrypted data will be compromised. The best method to achieve this is by incorporating post-quantum cryptography techniques into blockchain protocols.

Therefore, in a document released by the IDB, Cambridge Quantum Computing, and Tecnologico de Monterrey [https://publications.iadb.org/en/quantum-resistance-blockchain-networks], a method to withstand quantum computer assaults on blockchain networks is described. This technique does not need alteration of the algorithms employed by Internet or blockchain protocols, but instead adds a quantum security layer on top of them. This solution comprises of the two components shown below:

Establishing TLS tunnels by encapsulating communication between nodes using post-quantum X.509 certificates. Nodes receive a "post-quantum X.509 certificate" as part of the onboarding process. This certificate is an extension of an X.509 certificate using the v3 extension specification that permits the incorporation of new fields into the credential, such as complementary cryptographic algorithms; in this case, post-quantum. Using these certificates and a version of libSSL with the appropriate capabilities, nodes can establish secure post-quantum connections that encapsulate data sharing using the blockchain technology's default communication protocol.

In addition to the standard signature defined by the blockchain protocol, signing transactions with a post-quantum signature and establishing on-chain verification tools. This framework offers a second-layer cryptography method that permits writer nodes that broadcast transactions to sign them with a post-quantum signature that can be validated on-chain, in addition to the signature that comes by default with the blockchain protocol. If the default signature is corrupted by a quantum computer, the post-quantum signature safeguards the integrity. For this, post-quantum keys associated with post-quantum X.509 certificates may be used.

Guidelines set by NIST [7] should be closely followed when carrying out this standardization process.

4.7 Scalability

Three parameters limit the scalability of blockchain networks: block size, processing capacity, and storage. The network's genesis file specifies the block size, which is the first restriction on the amount of transactions that can fit in each block. The block size can be increased, but eventually the network's processing capability will become the second barrier. The consensus protocol requires validator nodes to execute new transactions and vote for new blocks. Blockchain networks are asynchronous, and transactions are replicated peer-to-peer between nodes. This suggests that the processing throughput of networks is restricted and dependent on the hardware of nodes. By updating the computers' hardware, the processing throughput of the network can be enhanced; however, at some point, the cost of maintaining a node no longer justifies the gain in throughput. Moreover, various blockchain applications impose inherent constraints on the throughput. Finally, storage is a third barrier. As nodes maintain a copy of the complete history, storage requirements become increasingly important over time.

This framework suggests the use of roll-ups and related techniques to facilitate scalability. Roll-up layers can be established either by the node operators directly or by the Entity that provides the underlying orchestration. In a multi-functional enterprise network, an exceptional Underlying

Orchestration Entity must offer mechanisms for writer node operators to meet the required throughput of the applications and services on the network's surface. These systems may involve layers that roll up for example ZK snark and optimistic rollups [8].

5 Monitoring

Monitoring is crucial for numerous reasons. It is useful for detecting failures, assessing performance, recognizing anomalies, and presenting data and dashboards. The responsibilities related with monitoring and evaluation should comprise at minimum the following:

- Analyze captured data using monitoring tools.
- Develop and maintain monitoring systems for infrastructure and performance metric capturing.
- Generate public reports on the network's statistics.
- Maintain a node status dashboard.
- Maintain a transaction explorer.
- Configure warnings for underperformance (such as a node being unavailable or not synchronizing) and misbehavior.

We categorize information as infrastructure, nodes, smart contracts, transactions, and blockchain accounts. The infrastructure information enables us to determine the resources (e.g., gas, RAM, CPU, NET) utilized by each node. The knowledge about the nodes enables us to comprehend the ledger’s performance. The information regarding smart contracts, transactions, and blockchain accounts enables us to realize the ledger usage by applications. It is essential to examine at least the following KPIs:

- Details regarding the routing and connectivity between nodes.
- Performance and latency of validator and boot nodes.
- A list of nodes, node types, node locations, and the entities behind each node.
- Quantity of transactions produced by every writer node.
- Reason for a node's rejection of a given number of transactions.
- The number of transactions refused by a node and the reason for their rejection.
- The performance-based rating of the validator nodes.
- Versions of software utilized by each node.

For Smart Contracts, Transactions, and Blockchain Accounts KPIs:

- Individual oversight of significant smart contracts (e.g., DID registries, on-chain DNS, resource distribution, permissioning smart contract, and stable-coins, among others).
- List of the most active recipients.
- List of the most prolific senders.
- List of the most frequently called smart contracts.
- List of transaction averages per block, hour, and day.
- Number of intelligent contracts.
- Number of unique senders.

- Number of unique recipients.
- Percentage of resource use for each block, hour, and day, as well as averages.

5.1 Network Upgrades

In traditional permissionless blockchain systems, network upgrades present a possibility of forks that cause duplication of block instances across the node network. This is detrimental to the finality of the blockchain in certain industries such as financial. NXTChain upgrade process is featured through a on-chain governance process and therefore does not require any hard-forks. The WASM runtime of NXTChain is directly stored on the blockchain through the governance process. Consequently, the propagation of a network upgrade will automatically enable the nodes to pull the latest version of the governance rules. Furthermore, since the WASM runtime is stored on the blockchain itself, all the nodes are guaranteed to have access to the same version. Additionally, this on-chain governance protocol also gives all observers a transparent view of the official version of the chain and thus removing uncertainty.

5.2 Finality

Proof-of-Authority offers deterministic finality that can be instantly trusted. Validators vote on the blocks generated, and once more then two thirds of the validators have voted in favor of a block, it is finalized. Since every block stores a cryptographic hash of the previous hash, once a block is finalized, all preceding blocks are therefore finalized. This allows finalizing a batch of blocks in one round/vote rather than traditional permissionless chains that must vote on every block. Batching allows the chain to remain live and scalable with guaranteed finality within seconds as opposed to minutes.

5.3 Compliance

On NXTChain, automated compliance of assets is both transparent and real-time to help simplify regulatory reporting for asset transfers, remove the need for complex systems to track and authorize digital asset transfers, reduce operational costs, and lower barriers to liquidity. Managing asset distribution and token ownership on NXTChain gives issuers the authority to enforce compliance in real time using Digital Asset Extensions (DAE) that represent various compliance rules. DAEs are provisioned by third-party developers and made available to all NXTChain issuers. They are used to validate asset transfers and provide flexibility when managing compliance for a mixture of asset types, jurisdictions, and offering types. Issuers are responsible for selecting, configuring, and implementing the appropriate suite of smart extensions for their digital assets. This includes specific regulatory, contractual, or other justified requirements. Issuers can also govern the rules bounding certain assets. For example, issuers can restrict ownership of their asset to investors that have completed specific know-your-client and anti-money-laundering (KYC/AML) processes or can manage transfer restrictions that apply to their employees/affiliates.

6 NXT Safe

Due to its immutability, blockchain networks should not be utilized to store sensitive data, especially if they are public. Blockchain networks should also not be utilized to store documents, files, or huge amounts of data because to the impracticality of the storage requirements. Generally speaking, blockchain networks should be utilized to store cryptographic proofs of off-chain data and carefully chosen public information.

In certain instances, however, blockchain-based solutions involve the exchange of documents and would therefore benefit from decentralized storage. This decentralized storage would enable end users to communicate off-chain with information linked to blockchain transactions either without or with authorization. Therefore, NXT Technologies has added 1 TB of storage integrated within the NXTreme that we call the NXTSafe. The chosen framework for decentralized storage is IPFS. IPFS allows users to store and transfer verifiable, content-addressed data in a peer-to-peer network. IPFS users usually persist the data they want on their own IPFS node. However, in the event the user runs out of space on their NXTSafe, there will be a open market where users can either rent-out or rent storage on other users NXTremes storage and generate revenue.

When a file or document is stored in the decentralized storage, a hash of the file or document is returned. This hash is used to associate a transaction on the blockchain with it. In this method, information can be retrieved by viewing the hash recorded in the smart contract and utilizing the hash to gain access to the decentralized storage and retrieve the file's content. In IPFS decentralized storages, the content is addressable, so the document's hash guarantees both its immutability and its location within the storage network.

7 Private channels

Privacy is the capacity to keep transactions between a group of participants private, such that other participants cannot access the transaction content or the list of members in the private channel. Numerous blockchain-based applications necessitate the sharing of sensitive information. In certain circumstances, despite the possibility of decentralized storage in a permissioned mode, it is preferable to enable a private side-channel in which some entities can set access rules and add or remove members, with each entity having its own centralized storage for the information exchanged. The Technical Team must allow simple techniques for the development of private side channels by groups of writer nodes in an enterprise blockchain architecture with multiple uses.

8 Use cases

It must be noted that blockchain has a vast amount of enterprise solutions and below are some standard examples of use cases for NXTChain – but not limited to. This section is intended to give the reader an understanding of different avenues in which blockchain as a technology can aid enterprise solutions.

8.1 Applying for a Loan

A banks primary goal is to lend, however in order to make a precautionary decision it is necessary to gather personal information (PII) such as birth certificate, annual income, ID...etc. Regulations may stipulate that specific PII be disclosed to law enforcement, for instance to stop money laundering. However, the retention of so much PII makes any bank an attractive target for hackers. Utilizing NXTChain, we can produce zero-knowledge proofs that applicants are over 21, that their income on last year's taxes exceeded a certain threshold, that they have a valid government ID number, and that their credit score recently met a certain threshold in place of disclosing any personally identifiable information (PII). Only the information necessary for the banks to make a judgment may be disclosed by applicants, and will be done in a matter that ensures objectivity, fosters trust in the lender, and satisfies regulatory requirements. As a result, the market will function more efficiently and effectively: Banks will confidently offer loans, while applicants can successfully protect their PII.

8.2 Financial Services: Post-Trade-Processing

Today's financial services can be driven by blockchain because it promotes privacy, secrecy, and accountability. Banks and service providers are required to be able to confirm a customer's legal identification and grant them approval to conduct transactions in accordance with compliance regulations like "Anti-Money Laundering" and "Know Your Customer." Due to the possibility of participants' privacy and confidentiality being violated on public blockchains, these criteria encourage the adoption of permissioned and private blockchains. Currently, all of these stages are often carried out through a disjointed workflow that crosses several departments across various entities, including brokers, central security depositories, clearing houses, exchanges, settlement agents, and so forth. There are numerous different interfaces, procedures, and settlement attempts involved in every trade. By utilizing a blockchain's peer-to-peer capabilities, one party can insert transaction information for the other party to confirm. Since the network itself can operate as a trusted third party due to the immutable and irrefutable nature of transactions on the blockchain, doing both operations on the same system can greatly simplify the process. While all data from all steps and all actors may be stored on the blockchain and be accessible to those who need to know it, the complexity can be further reduced. Any additional verification is no longer required. Additionally, the blockchain system can provide an effective foundation for transaction reporting and regulatory reporting. In summary, validation, clearing, settlement, and reporting can all be streamlined when using blockchain—in particular a permissioned blockchain.

8.3 IT: Managing Portable Identities

Self-sovereign identification, or the idea that an individual owns their own "identity" and controls the data surrounding it, is one of the most interesting uses of blockchain. The implications for enterprise IT are significant. A distributed ledger with a primary focus on self-sovereign identity can be created using NXTChain. It will have several characteristics in common with conventional enterprise identity systems, including industrial-strength cryptography, rich metadata about identities, and sophisticated access control and policy. However, there is a significant distinction: NXTChain identities are shared rather than federated and segregated. Anywhere that accepts the distributed ledger, you can travel with your NXTChain identity. This means that John Q. doesn't have 10 different identities created by the 10 systems that permit the IDs. Instead, John's pre-existing identity on the blockchain is accessed by all 10 systems. Just show up and use John's identification. John's access can be terminated by an organization, but he will never lose control of his identity because he owns it. And John controls access to his data, not the locations that recognize John's identity.

8.4 Supply-Chain Management: Tracking Fish from Ocean to Table:

It is estimated that 20 percent of the fish caught are either caught illegally or mislabelled—yet only a small fraction are ever inspected. Fish are delivered from the ocean to the table via a very intricate and opaque supply chain. There are numerous participants from various businesses, and there are international regulatory regulations involved in the processing process. Due to this, blockchain technology presents an ideal potential for this supply chain. We can utilize NXTChain to develop a traceability prototype to track telemetry parameters during capture, processing, and transmission using a distributed ledger, IoT sensors, and sophisticated communications. Furthermore, the ledger can also offer analytics for the scientific study of fish harvesting and consumption as well as regulatory enforcement.

9 Tokenomics

The token distribution details can be seen below. There will be a maximum supply of 1 billion NXT and 500 million tokens will be alloted at launch. The remaining 50% of the token supply will be used as staking rewards governed by the minting function as shown in equation [3.1] and voted on by the board of directors.

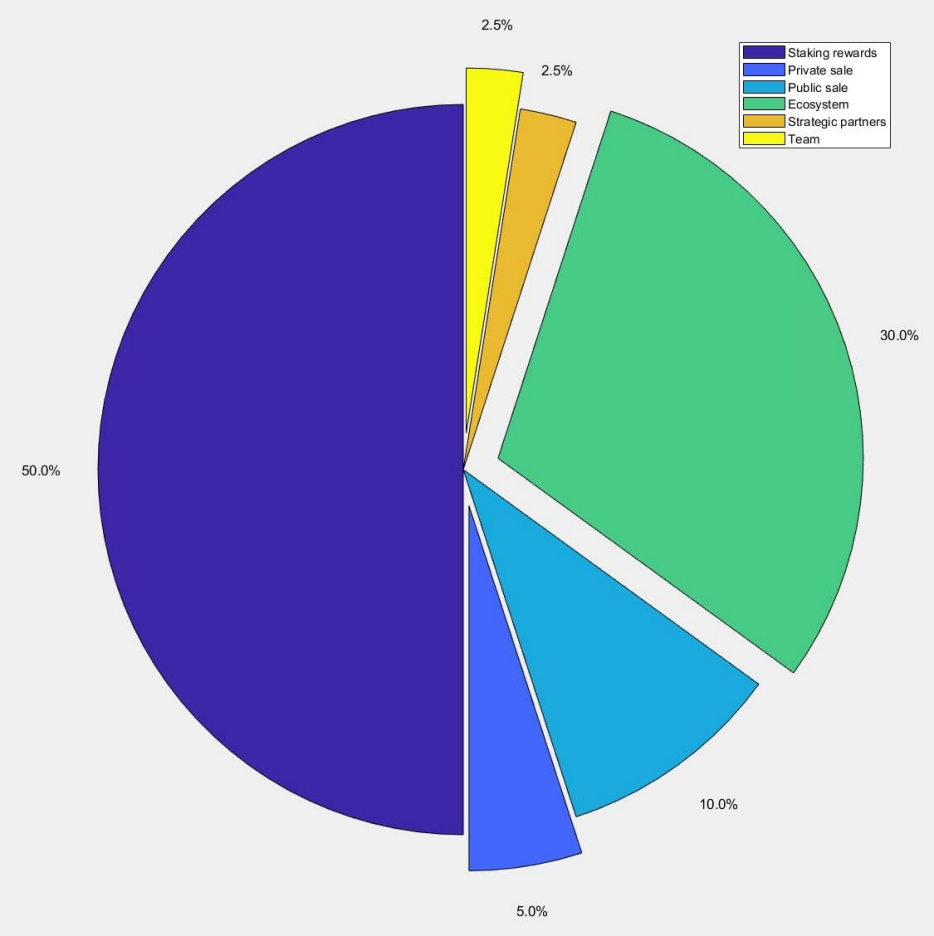


Figure 9.1. Pie chart representing the NXT token allocation

9.1 Staking Rewards (50% or 500,000,000 NXT)

500 million NXT is used as staking rewards to validators and the rewards will be governed by equation 3.1.

9.2 Private Sale (0.25%) 2,500,000 NXT

0.25% of the tokens are set aside to vetted investors. If tokens remain after they will be set aside for the public sale. Each investor will have their tokens allocated through a vesting period as described below:

- Private sale tokens will be the same as launch price
  - $0.50 USD
- Private sale tokens will have no vesting period

9.3 Public Sale (14.75%) 147,500,000 NXT

These tokens will be used for exchange liquidity. There will be no vesting period for this allocation.

9.4 Ecosystem (30%) 300,000,000 NXT

These tokens will be used for building the NXT Technologies Inc. ecosystem. This includes marketing, incentive programs, airdrops, community, and development endowment…etc. These tokens will have the following vesting period:

- 5% will be distributed at launch
- 45% will be released 24 months post launch
- The remaining 50% will be released 2% a month for 25 months
    - This will begin 24 months post genesis block

9.5 Strategic Partners (2.5%) 25,000,000 NXT

These tokens are allocated with the specific mandate of being distributed to groups, organizations, enterprises that are building their business on the NXT Technologies Inc. ecosystem. For example, someone that wants to invest or partner offchain, this is where the allocation will live managed by the board. These tokens will follow the vesting period shown below:

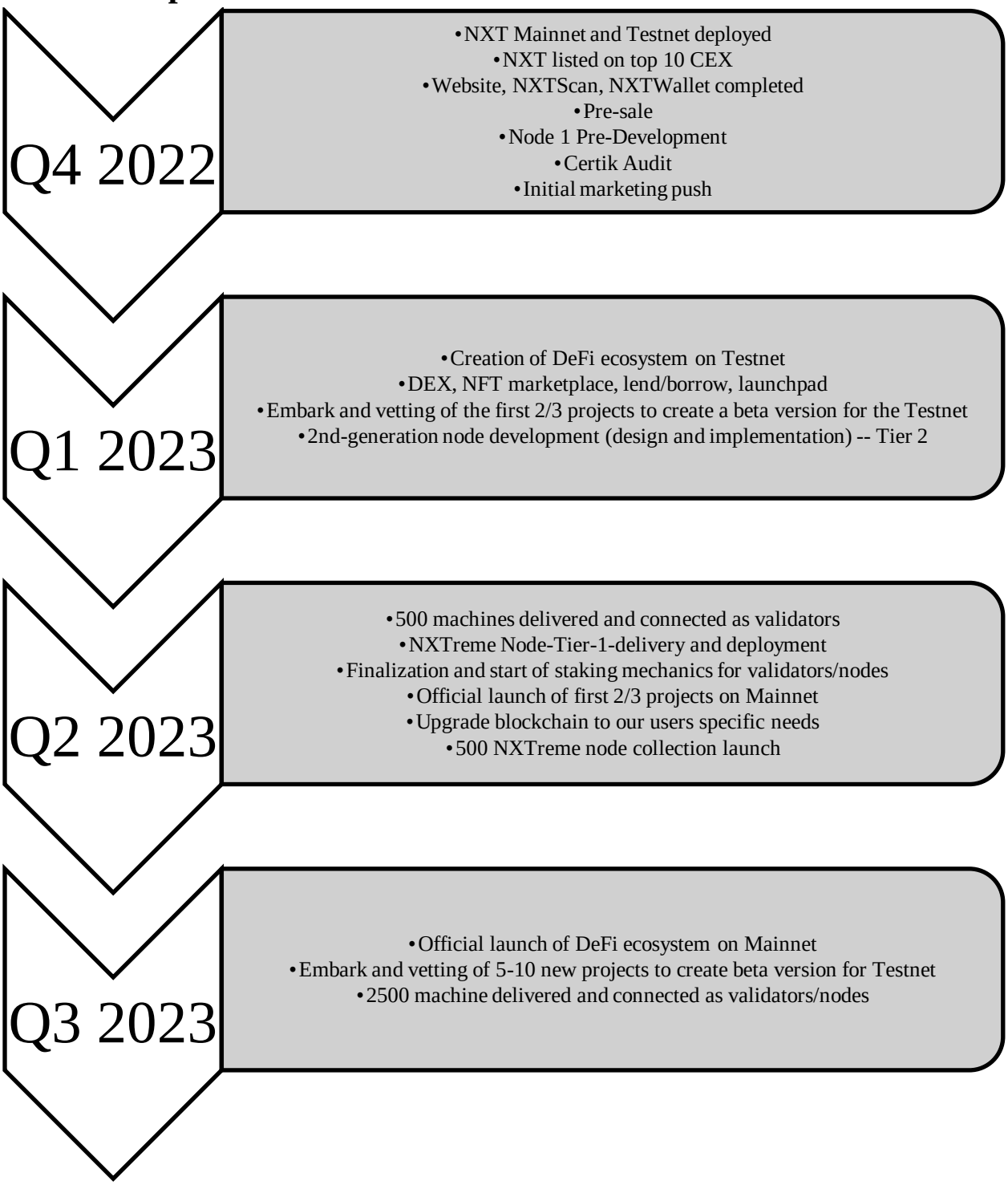
- 100% pNXT will be distributed via board of directors approval and multi-sig wallet will be completely transparent to the community
    - pNXT is a 1:1 migration token to NXTchain → NXT is our native token

9.6 Team (2.5%) 25,000,000 NXT

These tokens are allocated to the core team of NXT Technologies Inc. and will have the vesting period shown below:

- 100% of their tokens in pNXT will be distributed at launch
- The NXT will be migrated pNXT:NXT 1 to 1 after Mainnet launch
- Locking Period will be as follows:
- 20% of the tokens will be allocated at launch and locked for 24 months
- The remaining 80% will be unlocked 10% annually

10 Roadmap



11 Team

Rondell Fletcher -- CEO: Rondell is an executive producer / television engineer with a strong emphasis in entrepreneurship and investing. He has been in business for 20+ years and in blockchain and cryptocurrency since early 2012. While being in the crypto space as an early

adopter and investor, he noticed a void in the market and has concentrated on integrating enterprise with the fast-moving cryptocurrency space.

Bradley Kitzul -- COO: Brad is an Electrical Engineer who aims to bridge the gap between technology and business as we develop new business ventures using blockchain technology. He has completed his masters in electrical engineering and has been involved in the blockchain industry since early 2015. Furthermore, he has developed and launched multi-million-dollar blockchain businesses prior to working on NXT Technologies. Brad also has extensive experience in Solidity and Python.

Davide Cotti – CTO: Davide is a serial entrepreneur and blockchain architect who aims to bring blockchain technology to the masses. He has been coding since his teenage years. In 2017, he shifted his focus towards Solidity and the blockchain. His goal is to develop relationships with government officials, leaders of the industry, and business professionals, while revolutionizing the way data is managed and shared.

Octocode – Development firm: Code Development: Octocode is an innovative boutique agency with a wide scope of development capabilities, including web, apps, and blockchain. Located in Mexico City CDMX, the team, led by Javier Villegas, has extensive experience, and consistently exceeds client demands with out-of-the-box solutions.

Brian Jaramillo – Creative Director: Brian is a designer/entrepreneur who has developed a variety of innovative apparel brands and shipped ~1.5 million T-shirts to retail. As a designer, he has done work for Nike, Nickelodeon, and Lids, and most recently, he did the personal logos for Jrue Holiday, Julius Randle, and Tyrese Haliburton. In crypto since 2015, and now involved in multiple crypto projects.

Nikita Brown – Consulting Engineer: Nikita Brown is a Senior Engineering Project Manager for The Boeing Company, managing modifications for all Boeing production aircraft. He has a Mechanical Engineering degree and a Master in Business Administration. Nikita developed a passion for blockchain and cryptocurrency in 2019. He advises the team and is helping to grow and guide the community.

Cedera Solutions -- Accounting firm: Cedera Solutions is a small accounting firm that has been serving residents of Southern Nevada for almost ten years now. Cedera Solutions specializes in personal income tax, corporate tax, bookkeeping, payroll, cost accounting, financial reporting, as well as many other areas of accounting. Working with the IRS is another one of Cedera

Solutions specialties. Their expert team handles all IRS notices and letters and represents clients on both the state and federal levels—up to appeals and/or litigation.

Larenz Hamilton - Graphic Design: Larenz is a full-time graphic designer and has a passion to design product packaging with 100% unique design, high quality, and amazing service. He is an experienced designer and has worked as a graphic designer for more than 5 years.

Devin Cooke – In house Accountant: Devin is currently working as a managerial and tax accountant for Cedera Solutions. He obtained his bachelor's degree in business administration from Utah Tech University and his master's in accountancy from UNLV. Devin plans on furthering his education by obtaining both his CMA and CPA license in the near future. Being from St. George, UT, Devin has a passion for the outdoors as well as spending quality time with his family. He currently lives in Las Vegas with his wife and their puppy, Remy.

Infocus Media –Infocus media aims to bring all your media and productions to life. They are well versed in a multitude of live and taped mainstream programs, such as live sports, multi-media, post- preproduction, animation, and graphic design. Having a knowledgeable team and the combined experience of over 30-years in the industry, we have collaborated and produced content for clients such as ABC, NBC Universal, MTV and Latin American networks to name a few.

Lunar Strategies: Lunar Strategy is a leading marketing firm and specializes in web 3 marketing and covers a wide range of services and techniques. The specific company market strategy is based on their business needs and goals. They contribute the following: Blockchain PR, Web3 Communities, Crypto Influencer Marketing, Crypto Paid Ads, Web 3 Social Media.

12 References

[1] A. M. K. S. a. E. G. S. Stephen Buttolph, "Avalanche Native Token ($AVAX) Dynamics," AvalancheLabs, 2020.

[2] @wackerow, "ETHEREUM VIRTUAL MACHINE," 26 09 2022. [Online]. Available: https://ethereum.org/en/developers/docs/evm/) . [Accessed 20 10 2022].

[3] M. Allende López, D. López León, S. Cerón, A. Leal Batista, A. Pareja, M. Da Silva, A. Pardo, D. Jones, D. Worrall, B. Merriman, J. Gilmore, N. Kitchener and S. E. Venegas-Andraca, "Quantum-Resistance in Blockchain Networks," IADB, 2021.

[4] S. J. (. Y.-K. L. (. D. M. (. R. P. (. R. P. (. D. S.-T. Lily Chen (NIST), "Report on Post-Quantum Cryptography," NISTIR, 2016.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Semantic Scholar*, 1996.

[6] M. J. Dworkin, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," NIST, 2015.

[7] J. A.-S. (. D. A. (. D. C. (. Q. D. (. J. K. (. Y.-K. L. (. C. M. (. D. M. (. R. P. (. R. P. (. A. R. (. Gorjan Alagic (NIST), "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," NIST, 2020.

[8] @corwintines, "ZERO-KNOWLEDGE ROLLUPS," ETHER, 2 10 2022. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/zk-rollups/. [Accessed 20 10 2022].

NXT TECHNOLOGIES CORPORATION LEGAL DISCLAIMER

PLEASE READ THIS STATEMENT CAREFULLY BEFORE JOINING OR ADOPTING NXT TECHNOLOGIES CORPORATIONS PRODUCTS OR SERVICES. ISSUES REGARDING YOUR USE OF THE WEBSITE AND ALL MATERIALS ON THE SITE HAVE BEEN REGARDED WITHIN THE SCOPE OF THE NOTICE.

The user's responsibility is to regularly check our website and social media channels for such notices and updates. When we make such changes, we will update the Whitepaper and post a notice on our social media channels. It is your responsibility to regularly check our website for updates. This article is for informational purposes only and is subject to change. We cannot guarantee the › All representations and warranties (whether express or implied by law), including but not limited to: Any representations or warranties of merchantability, fitness for a particular purpose, fitness, price, title, or non-infringement. The contents of this document are correct, error-free; and That such content does not violate third-party rights. We will not be liable for any damage resulting from the use, reference to, or reliance on any of the content of this Whitepaper, even if we have been informed of the possibility of harm. This Whitepaper may contain references to third-party data and industry publications. To the best of our knowledge, the information provided on behalf of NXT Technologies Incorporated is correct, and the estimates and assumptions contained herein are reasonable. However, we make no warranty as to the accuracy or completeness of this data. While the information and data reproduced in these documents are believed to be from reliable sources, we have not independently verified any of the information or data from third-party sources referenced in this technical information or identified the underlying assumptions on which such sources are based. As of the date of publication of this Whitepaper in August 2022, NXT Technologies Incorporated has no known or previous NXT Tokens. No promises of performance or value will be made concerning NXT Tokens, including no promises of inherent value, promises of ongoing payments, and no guarantees that NXT Tokens will have any value. Potential participants should not participate in the NXT Token Sale unless they fully understand and accept the nature of NXT Technologies Incorporated's business and the potential risks involved in acquiring, storing, and transferring NXT Tokens. NXT Technologies Incorporated NXT Tokens are not structured or sold as securities. NXT Tokens have no rights or interest in NXT Technologies Incorporated equity. NXT Tokens are sold or issued by ownership allowance, private sale, CEX or DEX exchanges. (*See Tokenomics for further details*) NXT Technologies Incorporated applications with intended future functionalities and partnerships onchain. All proceeds generated during the Token Sale or Sales (referred to as the Initial Token Offering in the Technical documentation) are provided by NXT Technologies Incorporated for the development of its business and the underlying technological infrastructure. This Whitepaper does not constitute a prospectus or disclosure document and is not an offer to sell or a solicitation to purchase any investment or financial instrument in any jurisdiction. NXT Technologies Incorporated / NXT Tokens should not be purchased speculatively or for investment purposes with the expectation of a return on investment. No regulatory agency has reviewed or approved any of the information contained in this Whitepaper. No such action has been or will be taken under the law, regulatory requirements, or the rules of any jurisdiction. The publication, distribution, or distribution of this Whitepaper does not imply compliance with applicable laws or regulatory requirements in the United States or WorldWide. Participating in NXT Technologies Incorporated Token Sale carries significant risk and may involve unique risks that may result in the loss of all or a substantial portion of the user's contribution.

Please make sure to read, understand, and be prepared to accept the risks of participating in any NXT or NXT Technologies Incorporated Token Sale before sending us a contribution. The Token Sale or NXT Tokens may be affected by regulatory action, including possible restrictions on the ownership, use, or

possession of such tokens. Regulators or other authorities may require us to review the Token Sale mechanism and/or the functionality of NXT Technologies Incorporated Tokens to comply with legal requirements or other governmental or business obligations. However, we believe we have taken commercially reasonable steps to ensure that the Token Sale mechanics and the issuance of NXT Tokens does not violate applicable laws and regulations. ABOUT FORWARD-LOOKING STATEMENT This whitepaper contains forward-looking statements or information regarding our current expectations of future events. In some cases, these forward-looking statements are "may", "will", "expect", "anticipate", "intend", "predict", "plan" It can be defined by words or expressions such as "to arrange", "to prepare". "seek", "believe", "potential", "continue", "likely to happen" or other similar expressions to describe negative terms or forward-looking statements. We have based these forward-looking statements on current estimates of future events and financial trends that we believe may affect our financial condition, results of operations, business strategy, financial needs, or the Token Sale and allocation results. Although the forward-looking statements contained in this Whitepaper are based on what we believe are reasonable assumptions; there are risks, uncertainties, assumptions, and other factors that could cause NXT Technologies Incorporated actual results, performance, success, and/or experience to differ materially. Expectations expressed, implied, or perceived in forward-looking statements. Given such risks, prospective participants in the Token Sale should not unduly rely on these forward-looking statements.

Permissioned Public Blockchain Network
by NXT Technologies, Inc.

The NXT Generation Blockchain

NXTChain