



Call for evidence

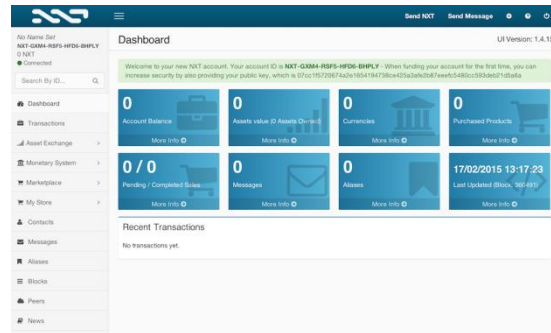
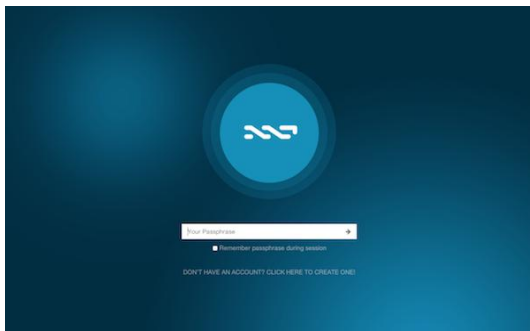
Investment using virtual currency or distributed ledger technology



Marcos José LOPEZ PORTO
marcos@lopezabogados.org
Neira de Mosquera 1ºA, 4ºA
Santiago de Compostela
15702 SPAIN

Q3: Do you have anything to add or suggest a change to the description of how virtual currency distributed ledgers work? Please clearly state to which virtual currency you are referring in your answer or whether your answer refers to virtual currencies in general.

This presentation is going to focus on **Nxt**, as the most advanced financial crypto-platform in the world. Nxt (Next) is an open source cryptocurrency and payment network launched in November 2013 by anonymous software developer BCNext, that uses a proof-of-stake technology to reach consensus for transactions. While Bitcoin uses hashing power as proof for verifying transactions, Nxt works with the stake-size the user owns. Block authors are selected in a practically random manner, with greater amounts of stake increasing the likelihood of adding a block to the chain. While in the former the investment in mining gear serves as incentive not to attack the network, an attacker in the latter would directly hurt the personal coin holdings. This method effectively removes the security issue of any miner gaining 51% of the hashing power and attacking the network.



History.

On 28 September 2013 Bitcointalk.org member BCNext created a forum thread announcing Nxt as second generation cryptocurrency, asking for small Bitcoin donations to determine how to distribute the initial stake. On 18 November 2013 fundraising for Nxt was closed, with 21 BTC raised. The genesis block was published on 24 November 2013. It revealed that 1,000,000,000 coins had been distributed to 73 stakeholders in proportion to their level of contribution. The source code was partially released on 3 January and the full source code was released on 1 March 2014 under MIT License.

Concept.

Just as with Bitcoin, the blockchain stands at the core of this currency. But Nxt is completely written from scratch and departed in several ways from existing cryptocurrencies. Most notably, in one of the founding statements BCNext asks the community not to consider the NXT coin as the important part, but rather create currencies on top of it - possibly devaluing the core currency. Nxt is coded in Java. The standard client works as brain-wallet: Instead of storing keys in a wallet file, security works via a secret passphrase. This means it can be accessed from any instance of the Nxt software. The standard client is running in web browsers. Nxt was the first currency to rely purely on proof-of-stake for consensus. Allowing a block creation rate of roughly one minute. Focused on being a developer friendly platform and fostering third party services.

Forging system.

Since Nxt has an unchanging coin supply, no new units are created for block rewards. Instead the transaction fees are passed on. After owning Nxt for about one day (1440 confirmations), the Nxt software will begin to contribute to the block generation process and can earn coins for as long as an account is "unlocked". This process is called forging (referring to the smith that takes existing iron and reshapes it).

At the moment Nxt is open to attacks if any account has 51% of the total coin supply that is forging. As outlined in the founding statements Nxt is aimed at implementing a process of "transparent forging", which allows the software to predict which accounts will forge upcoming blocks. This is basically done by iterating through all active accounts and seeing which one has the highest "hit". Transparent forging rapidly increases transaction processing, since the account that will forge the next block is known. Another benefit of this feature is that accounts that are due to forge, but do not, will be penalized by having their forging power temporarily reduced to zero. This raises the threshold for an attack to 90%.

Energy Efficiency.

The Proof-of-Stake algorithm is efficient enough to run on smartphones and small devices like the Raspberry Pi platform. As such there are no additional costs, no expensive mining hardware is needed and no additional energy burned. This makes Nxt use ca. 7000 times less energy than Bitcoin at the same network size. Nowadays Nxt platform can be securely maintained for just only 300 euros per day.

Q4.- Do you agree with the general investment process in VC based financial assets as described above? Please explain where this process could differ for different virtual currencies.

To explain how does the Nxt works, I would like to introduce the "*white paper*" as the fundamental document that summarizes the operation of this financial platform.

Abstract

Bitcoin has proven that a peer-to-peer electronic cash system can indeed work and fulfill payments processing without requiring trust or a central mint. However, for an entire *electronic economy* to be based on a fully decentralized, peer-to-peer solution, it must be able to do the following: process transactions securely, quickly and efficiently, at the rate of thousands per hour or more; provide incentives for people to participate in securing the network; scale globally with a minimal resource footprint; offer a range of basic transaction types that launch cryptocurrencies past the core feature of a payment system alone; provide an agile architecture that facilitates the addition of new core features, and allows for the creation and deployment of advanced applications; and be able to run on a broad range of devices, including mobile ones. Nxt (pronounced next) satisfies all these requirements.

Introduction and Overview

Nxt is a 100% proof-of-stake cryptocurrency, constructed from scratch in open-source Java. Nxts unique proof-of-stake algorithm does not depend on any implementation of the coin age concept used by other proof-of-stake cryptocurrencies, and is resistant to so-called nothing at stake attacks. A total quantity of 1 billion available tokens were distributed in the genesis block. Curve25519 cryptography is used to provide a balance of security and required processing power, along with more commonly-used SHA256 hashing algorithms.

Blocks are generated every 60 seconds, on average, by accounts that are *unlocked* on network nodes. Since the full token supply already exists, Nxt is redistributed through the inclusion of transaction fees which are awarded to an account when it successfully creates a block. This process is known as *forging*, and is akin to the mining concept employed by other cryptocurrencies. Transactions are deemed safe after 10 block confirmations, and Nxts current architecture and block size cap allows for the processing of up to 367,200 transactions per day.

Nxt transactions are based on a series of core *transaction types* that do not require any script processing or transaction input/output processing on the part of network nodes. These transaction primitives allow core support for:

- a fully-decentralized asset exchange
- alias creation, transfer and sale
- storage of small, optionally-encryptable strings of data on the blockchain
- a digital goods store
- account control features

By leveraging these primitive transaction types, Nxts core can be seen as an agile, base-layer protocol upon which a limitless range of services, applications, and other currencies can be built.

Ongoing Nxt development includes the implementation of a novel Transparent Forging feature which will allow a transaction processing capacity increase of two orders of magnitude using a deterministic block generation algorithm, coupled with additional network security mechanisms. The latest development roadmap also outlines the following short-term feature additions to the Nxt core:

- a voting system
- asset exchange dividend payments
- a monetary system for facilitating the creation of new cryptocurrencies and associated services that are secured by the Nxt blockchain
- atomic cross-chain trading, multi-signature transactions and escrow features
- additional mechanisms for securing the Nxt blockchain, including penalties for accounts that do not behave as expected on the network^[31]

This version of the whitepaper documents features and algorithms that are implemented in Nxt as of version 1.2.2. Future revisions will be made to reflect additional planned features and algorithm changes.

Core technologies

Proof of Stake

In the traditional Proof of Work model used by most cryptocurrencies, network security is provided by peers doing work. They deploy their resources (computation/processing time) to reconcile double-spending transactions, and to impose an extraordinary cost on those who would attempt to reverse transactions. Tokens are awarded to peers in exchange for work, with the frequency and amount varying with each cryptocurrency's operational parameters. This process is known as mining. The frequency of block generation, which determines each cryptocurrency's available mining reward, is generally intended to stay constant. As a result, the difficulty of the required work for earning a reward must increase as the work capacity of the network increases.

As a Proof of Work network becomes stronger, there is less incentive for an individual peer to support the network, because their potential reward is split among a greater number of peers. In search of profitability, miners keep adding resources in the form of specialized, proprietary hardware that requires significant capital investment and high ongoing energy demands. As time progresses, the network becomes more and more centralized as smaller peers (those who can do less work) drop out or combine their resources into pools.

Bitcoin's creator, Satoshi Nakamoto, intended for the Bitcoin network to be fully decentralized, but nobody could have predicted that the incentives provided by Proof of Work systems would result in the centralization of the mining process. This leads to possible vulnerabilities. The GHash.io Bitcoin pool has reached 51% of the Bitcoin mining power in the past, and the top five Bitcoin mining pools make up 70% of the Bitcoin network's hashing power^[5]. The concept of decentralization is at risk of being completely lost.

In the Proof of Stake model used by NXT, network security is governed by peers having a *stake* in the network. The incentives provided by this algorithm do not promote centralization in the same way that Proof of Work algorithms do, and data shows that the NXT network has remained highly decentralized since its inception: a large (and growing) number of unique accounts are contributing blocks to the network, and the top five accounts have generated 35% of the total number of blocks.

NXT's Proof of Stake Model

NXT uses a system where each coin in an account can be thought of as a tiny mining rig. The more tokens that are held in the account, the greater the chance that account will earn the right to generate a block. The total reward received as a result of block generation is the sum of the transaction fees located within the block. NXT does not generate any new tokens as a result of block creation. Redistribution of NXT takes place as a result of block generators receiving transaction fees, so the term forging (meaning in this context to create a relationship or new conditions) is used instead of mining.

Subsequent blocks are generated based on verifiable, unique, and almost-unpredictable information from the preceding block. Blocks are linked by virtue of these connections, creating a chain of blocks (and transactions) that can be traced all the way back to the genesis block.

Block generation time is targeted at 60 seconds, but variations in probabilities have resulted in an average block generation time of 80 seconds, with occasionally very long block intervals. An adjustment to the forging algorithm has been suggested by mthcl and modeled by Sebastien256 on NXTForum.org.

The security of the blockchain is always of concern in Proof of Stake systems. The following basic principles apply to NXT's Proof of Stake algorithm:

- A *cumulative difficulty* value is stored as a parameter in each block, and each subsequent block derives its new difficulty from the previous blocks value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty. This is covered in more detail in.
- To prevent account holders from moving their stake from one account to another as a means of manipulating their probability of block generation, tokens must be stationary within an account for 1,440 blocks before they can contribute to the block generation process. Tokens that meet this criterion contribute to an account's *effective balance*, and this balance is used to determine forging probability.
- To keep an attacker from generating a new chain all the way from the genesis block, the network only allows chain re-organization 720 blocks behind the current block height.

Any block submitted at a height lower than this threshold is rejected. This moving threshold may be viewed as Nxts only *fixed checkpoint*.

- Due to the extremely low probability of any account taking control of the blockchain by generating its own chain of blocks, transactions are deemed safe once they are encoded into a block that is 10 blocks behind the current block height.

Contrast with Peercoin Proof of Stake

Peercoin uses a *coin age* parameter as part of its mining probability algorithm. In that system, the longer your Peercoins have been stationary in your account (to a maximum of 90 days), the more power (coin age) they have to mint a block. The act of minting a block requires the consumption of coin age value, and the network determines consensus by selecting the chain with the largest total consumed coin age.

When Peercoin blocks are orphaned, the consumed coin age is released back to the blocks originating account. As a result, the cost to attack the Peercoin network is low, since attackers can keep attempting to generate blocks (referred to as *grinding stake*) until they succeed. Peercoin minimizes these and other risks by centrally broadcasting blockchain checkpoints several times a day, to freeze the blockchain and lock in transactions.

Nxt does not use coin age as part of its forging algorithm. An account's chance to forge a block depends only on its effective balance (which is a property of each account), the time since the last block (which is shared by all forging accounts) and the base target value (which is also shared by all accounts).

Tokens

The total supply of Nxt is 1 billion tokens, divisible to eight decimal places. All tokens were issued with the creation of the *genesis block* (the first block in the Nxt blockchain), leaving the *genesis account* with an initial negative balance of 1 billion Nxt.

The existence of anti-tokens in the genesis account has a couple of interesting side effects:

- the genesis account cannot issue transactions of any kind, since its balance is negative and it cannot pay transaction fees. As a result, the private passphrase for the genesis account is free for anyone to use.
- any tokens sent to the genesis account are effectively destroyed, since that accounts negative balance will cancel them out. Several thousand Nxt tokens have been *burned* in this manner.
- Nxt assets may also be burned by transferring them to the genesis account.

The choice of the word *tokens* is intentional due to Nxts intention to be used as a base protocol that provides numerous other functions. Nxts most basic function is one of a traditional payment system, but it was designed to do far more.

Network Nodes

A *node* on the Nxt network is any device that is contributing transaction or block data to the network. Any device running the Nxt software is seen as a node.

Nodes can be subdivided into two types: *hallmarked* and *normal*. A hallmarked node is simply a node that is tagged with an encrypted token derived from an accounts private key; this token can be decoded to reveal a specific Nxt account address and balance that are associated with a node. The act of placing a hallmark on a node adds a level of accountability and trust, so hallmarked nodes are more trusted than non-hallmarked nodes on the network.

The larger the balance of an account tied to a hallmarked node, the more trust is given to that node. While an attacker might wish to hallmark a node in order to gain trustworthiness within the network and then use that trust for malicious purposes; the barrier to entry (cost of Nxt required to build adequate trust) discourages such abuse.

Each node on the Nxt network has the ability to process and broadcast both transactions and block information. Blocks are validated as they are received from other nodes, and in cases where block validation fails, nodes may be blacklisted temporarily to prevent the propagation of invalid block data.

Each node features built-in DDOS (Distributed Denial of Services) defence mechanisms which restrict the number of network requests from any peer to 30 per second.

Blocks

As in other cryptocurrencies, the ledger of Nxt transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred. A copy of the blockchain is kept on every node in the Nxt network, and every account that is *unlocked* on a node (by supplying that accounts private key) has the ability to generate blocks, as long as at least one incoming transaction to the account has been confirmed 1440 times. Any account that meets these criteria is referred to as an *active account*.

In Nxt, each block contains up to 255 transactions, all prefaced by a 192-byte header that contains identifying parameters. Each transaction in a block is represented by a maximum of 160 bytes, and the maximum block size is 32KB. All blocks contain the following parameters:

- A block version, block height value, and block identifier
- A block timestamp, expressed in seconds since the genesis block
- The ID of the account that generated the block, as well as that accounts public key
- The ID and hash of the previous block
- The number of transactions stored in the block
- The total amount of Nxt represented by transactions and fees in the block
- Transaction data for all transactions included in the block, including their transaction IDs
- The payload length of the block, and the hash value of the block payload
- The block's generation signature
- A signature for the entire block
- The base target value and cumulative difficulty for the block

Block Creation (Forging)[sub:Block-Creation-(Forging)]

Three values are key to determining which account is eligible to generate a block, which account earns the right to generate a block, and which block is taken to be the authoritative one in times of conflict: *base target value*, *target value* and *cumulative difficulty*.

Base Target Value

In order to win the right to forge (generate) a block, all active Nxt accounts compete by attempting to generate a hash value that is lower than a given *base target value*. This base target value varies from block to block, and is derived from the previous blocks base target value multiplied by the amount of time that was required to generate that block.

Target Value

Each account calculates its own target value, based on its current effective stake. This value is:

$$T = T_b \times S \times B_e$$

where:

T is the new target value

T_b is the base target value

S is the time since the last block, in seconds

B_e is the effective balance of the account

As can be seen from the formula, the target value grows with each second that passes since the timestamp of the previous block. The maximum target value is $1.53722867 \times 10^{17}$ and the minimum target value is one half of the previous blocks base target value.

This target value and the base target value are the same for all accounts attempting to forge on top of a specific block. The only account-specific parameter is the effective balance parameter.

Cumulative Difficulty

The cumulative difficulty value is derived from the base target value, using the formula:

$$D_{cb} = D_{pb} + \frac{2^{64}}{T_b}$$

where:

D_{cb} is the difficulty of the current block

D_{pb} is the difficulty of the previous block

T_b is the base target value for the current block

The Forging Algorithm

Each block on the chain has a *generation signature* parameter. To participate in the block forging process, an active account cryptographically signs the generation signature of the previous block with its own public key. This creates a 64-byte signature, which is then hashed using SHA256. The first 8 bytes of the resulting hash gives a number, referred to as the accounts *hit*.

The hit is compared to the current target value. If the computed hit is lower than the target, then the next block can be generated. As noted in the target value formula, the target value increases with each passing second. Even if there are only a few active accounts on the network, one of them will eventually generate a block because the target value will become very large. The corollary of this is that you can estimate the time that will be required for any account to forge a block by comparing that accounts hit value to the target value.

The last point is significant. Since any node can query the effective balance for any active account, it is possible to iterate through all active accounts in order to determine their individual hit value. This means it is possible to predict, with reasonable accuracy, which account will next win the right to forge a block. A *shuffling attack* could be mounted by moving stake to an account that will generate the next block, which is another reason why a Nxt stake must be stationary for 1440 blocks before it can contribute to forging (via the effective balance value). Interestingly, the new base target value for the next block cannot be reasonably predicted, so the nearly-deterministic process of determining who will forge the

next block becomes increasingly stochastic as attempts are made to predict future blocks. This feature of the Nxt forging algorithm helps form the basis for the development and implementation of the Transparent Forging algorithm. Since this algorithm has not yet completely been implemented, and because its implications on the Nxt network are significant, it will be outlined in a separate paper.

For an in-depth analysis of the mathematics and probabilities related to Nxt block forging, see mthcls paper, *The math of Nxt forging*, which is located at <http://www.docdroid.net/e29h/forging0-5-2.pdf.html>

When an active account wins the right to generate a block, it bundles up to 255 available, unconfirmed transactions into a new block, and populates the block with all of its required parameters. This block is then broadcast to the network as a candidate for the blockchain.

The payload value, generating account, and all of the signatures on each block can be verified by all network nodes who receive it. In a situation where multiple blocks are generated, nodes will select the block with the highest cumulative difficulty value as the authoritative block. As block data is shared between peers, forks (non-authoritative chain fragments) are detected and dismantled by examining the chains cumulative difficulty values stored in each fork.

Balance leasing

Since the ability for an account to forge is based on the effective balance parameter, it is possible to loan forging power from one account to another without giving up control of the tokens associated with the account. Using a transaction of the account control type, an account owner may temporarily reduce an accounts effective balance to zero, adding it to the effective balance of another account. The targeted accounts forging power is increased until the end of a time period specified by the original account owner, after which the effective balance is returned to the original account.

Accounts with leased forging power generate blocks more often and earn more transaction fees, but those fees are not automatically returned to lease accounts. With a bit of coding, however, this system allows for the creation of nearly-trustless *forging pools* that can make payouts to participants. The most notable current implementation of this idea can be found at <http://pool.nxtcrypto.org/>

Accounts

Nxt implements a *brain wallet* as part of its design: all accounts are stored on the network, with *private keys* for each possible account address directly derived from each accounts *passphrase* using a combination of SHA256 and Curve25519 operations.

Each account is represented by a 64-bit number, and this number is expressed as an *account address* using a Reed-Solomon error-correcting notation that allows for *detection* of up to four errors in an account address, or *correction* of up to two errors. This format was implemented in response to concerns that a mistyped account address could result in tokens, aliases, or assets being irreversibly transferred to erroneous destination accounts. Account addresses are always prefaced by NXT-, making Nxt account addresses easily recognizable and distinguishable from address formats used by other cryptocurrencies.

The Reed-Solomon-encoded account address associated with a secret passphrase is generated as follows:

1. The secret passphrase is hashed with SHA256 to derive the accounts *private key*.
2. The private key is encrypted with Curve25519 to derive the accounts *public key*.
3. The public key is hashed with SHA256 to derive the *account ID*.

4. The first 64 bits of the account ID are the *visible account number*.
5. Reed-Solomon encoding of the visible account number, prefixed with NXT-, generates the *account address*.

When an account is accessed by a secret passphrase for the very first time, it is not secured by a public key. When the first outgoing transaction from an account is made, the 256-bit public key derived from the passphrase is stored on the blockchain, and this secures the account. The address space for public keys (2^{256}) is larger than the address space for account numbers (2^{64}), so there is no one-to-one mapping of passphrases to account numbers and collisions are possible. These collisions are detected and prevented in the following way: once a specific passphrase is used to access an account, and that account is secured by a 256-bit public key, no other public-private key pair is permitted to access that account number.

Account Balance Properties

For each Nxt account, several different types of balances are available. Each type serves a different purpose, and many of these values are checked as part of transaction validation and processing.

- The *effective balance* of an account is used as the basis for an accounts forging calculations^[15]. An accounts effective balance consists of all tokens that have been stationary in that account for 1440 blocks. In addition, the Account Leasing feature allows an accounts effective balance to be assigned to another account for a temporary period.
- The guaranteed balance of an account consists of all tokens that have been stationary in an account for 1440 blocks. Unlike the effective balance, this balance cannot be assigned to any other account.
- The *basic balance* of an account accounts for all transactions that have had at least one confirmation.
- The *forged balance* of an account shows the total quantity of Nxt that have been earned as a result of successfully forging blocks.
- The *unconfirmed balance* of an account is the one that is displayed in Nxt clients. It represents the current balance of an account, minus the tokens involved in unconfirmed, sent transactions.
- *Guaranteed asset balances* lists the guaranteed balances of all the assets associated with a specific account.
- *Unconfirmed asset balances* lists the unconfirmed balances of all the assets associated with a specific account.

Wallet.dat

Bitcoin and related currencies often use an encrypted file, called a *wallet*, to store generated addresses for receiving tokens. The core design of Nxt does not mimic this functionality, but also does not preclude it. As has been demonstrated by the Offspring client and the online wallet service provided by nxtblocks.info, it is possible for client developers to implement a system where a group of private keys for Nxt accounts are stored in an encrypted, offline file.

Transactions

Transactions are the only means Nxt accounts have of altering their state or balance. Each transaction performs only one function, the record of which is permanently stored on the network once that transaction has been included in a block.

Transaction Fees

Transaction fees are the primary mechanism through which Nxt are recirculated back into the network. Every transaction requires a minimum fee of 1 Nxt; currently, the only exception is the fee for issuing an asset on the Nxt Asset Exchange, which is 1000 Nxt. When a Nxt account forges a block, all of the transaction fees included in that block are awarded to the forging account as a reward.

Until the size of all the transactions in a block exceeds the current 32 kilobyte block size limit, the minimum fee will be sufficient for all transactions to be included in blocks. In situations where the number of unconfirmed transactions exceeds the number that can be placed in a block, forging accounts will likely select transactions with the highest fees. This suggests that transaction processing may be prioritized by including a fee that is higher than the minimum.

Transaction Confirmations

All Nxt transactions are considered *unconfirmed* until they are included in a valid network block. Newly-created blocks are distributed to the network by the node (and associated account) that creates them, and a transaction that is included in a block is considered as having received one confirmation. As subsequent blocks are added to the existing blockchain, each additional block adds one more confirmation to the number of confirmations for a transaction.

If a transaction is not included in a block before its deadline, it expires and is removed from the transaction pool.

Transaction Deadlines

Every transaction contains a deadline parameter, set to a number of minutes from the time the transaction is submitted to the network. The default deadline is 1440 minutes (24 hours). A transaction that has been broadcast to the network but has not been included in a block is referred to as an *unconfirmed transaction*.

If a transaction has not been included in a block before the transaction deadline expires, the transaction is removed from the network.

Transactions may be left unconfirmed because they are invalid or malformed, or because blocks are being filled with transactions that have offered to pay higher transaction fees. In the future, features such as multi-signature transactions may be able to take advantage of deadlines as a means of enforcing an expiry date.

Transaction Types

Categorizing Nxt transactions into types and subtypes allows for modular growth and development of the Nxt protocol without creating dependencies on other base functions. As features are added to the Nxt core, new transaction types and subtypes can be added to support them.

The following five transaction types and associated subtypes are supported by Nxt. Each type dictates a given transactions required and optional parameters, as well as its processing method.

1. *Payment*: used for sending Nxt tokens from one account to another
 - Ordinary payment

2. *Messaging*: used by messaging, alias, voting, and account info features
 - Arbitrary message
 - Alias assignment
 - Poll creation
 - Vote casting
 - Account info

3. *Colored coins*: an implementation of the colored coins concept, which enables the Nxt Asset Exchange
 - Asset issuance
 - Asset transfer
 - Ask order placement
 - Bid order placement
 - Ask order cancellation
 - Bid order cancellation

4. *Digital Goods*: transactions that enable the Nxt Digital Goods store
 - Listing
 - Delisting
 - Price change
 - Quantity change
 - Purchase
 - Delivery
 - Feedback
 - Refund

5. *Account control*: transactions that place limits on how accounts may or may not be used.
 - Effective balance leasing

Transaction Creation and Processing

The details of creating and processing a Nxt transaction are as follows:

1. The sender specifies parameters for the transaction. Types of transactions vary, and the desired type is specified at transaction creation, but several parameters must be specified for all transactions:
 - the private key for the sending account
 - a specified fee for the transaction
 - a deadline for the transaction
 - an optional referenced transaction

2. All values for the transaction inputs are checked. For example, mandatory parameters must be specified; fees cannot be less than or equal to zero; a transaction deadline cannot be less than one minute into the future; if a referenced transaction is specified, then the current transaction cannot be processed until the referenced transaction has been processed.

3. If no exceptions are thrown as a result of parameter checking:
 1. The public key for the generating account is computed using the supplied secret passphrase
 2. Account information for the generating account is retrieved, and transaction parameters are further validated:
 - The sending account's balance cannot be zero
 - The sending account's *unconfirmed balance* must not be lower than the transaction amount plus the transaction fee

If the sending account has sufficient funds for the transaction:

0. A new transaction is created, with a type and subtype value set to match the kind of transaction being made. All specified parameters are included. A unique transaction ID is generated with the creation of the object
1. The transaction is signed using the sending account's private key
2. The encrypted transaction data is placed within a message instructing network peers to process the transaction
3. The transaction is broadcast to all peers on the network
4. The server responds with a result code:
 - the transaction ID, if the transaction creation was successful
 - an error code and error message if any of the parameter checks fail.

Key exchange in Nxt is based on the Curve25519 algorithm, which generates a shared secret key using a fast, efficient, high-security elliptic-curve Diffie-Hellman function. The algorithm was first demonstrated by Daniel J. Bernstein in 2006. Nxt's Java-based implementations were reviewed by DoctorEvil in March, 2014.

Message signing in Nxt is implemented using the Elliptic-Curve Korean Certificate-based Digital Signature Algorithm (EC-KCDSA), specified as part of IEEE P1363a by the KCDSA Task Force team in 1998.

Both algorithms were chosen for their balance of speed and security for a key size of only 32 bytes.

Encryption Algorithm

When Alice sends an encrypted plaintext to Bob, she:

1. Calculates a shared secret:
 - $\text{shared_secret} = \text{Curve25519}(\text{Alice_private_key}, \text{Bob_public_key})$
2. Calculates N seeds:
 - $\text{seed}_n = \text{SHA256}(\text{seed}_{n-1})$, where $\text{seed}_0 = \text{SHA256}(\text{shared_secret})$
3. Calculates N keys:
 - $\text{key}_n = \text{SHA256}(\text{Inv}(\text{seed}_n))$, where $\text{Inv}(X)$ is the inversion of all bits of X
4. Encrypts the plaintext:
 - $\text{ciphertext}[n] = \text{plaintext}[n] \text{ XOR } \text{key}_n$

Upon receipt Bob decrypts the ciphertext:

1. Calculates a shared secret:
 - $\text{shared_secret} = \text{Curve25519}(\text{Bob_private_key}, \text{Alice_public_key})$
2. Calculates N seeds (this is identical to Alice's step):
 - $\text{seed}_n = \text{SHA256}(\text{seed}_{n-1})$, where $\text{seed}_0 = \text{SHA256}(\text{shared_secret})$
3. Calculates N keys (this is identical to Alice's step):
 - $\text{key}_n = \text{SHA256}(\text{Inv}(\text{seed}_n))$, where $\text{Inv}(X)$ is the inversion of all bits of X
4. Decrypts the ciphertext:
 - $\text{plaintext}[n] = \text{ciphertext}[n] \text{ XOR } \text{key}_n$

Note: If someone guesses part of the plaintext, he can decode some part of subsequent messages between Alice and Bob if they use the same key pairs. As a result, it's advised to generate a new pair of private/public keys for each communication.

Core Features

Advanced JavaScript client

A second-generation, user-friendly client application is built into the Nxt core software distribution, and can be accessed through a local web browser. The client provides full support for all core Nxt features, implemented such that users private keys are never exposed to the network. It also includes an advanced administrative interface and built-in javadoc documentation for Nxts low-level Applications Programming Interface.

Agile architecture

First-generation cryptocurrencies were primarily designed as payment systems. Nxt recognizes that decentralized blockchains can enable a broad range of applications and services, but is not prescriptive about what those services should be or how they should be built. By design, Nxt strips away unnecessary complexity in its core, leaving only the most successful components of its predecessors intact. As a result, Nxt functions like a low-level, foundational protocol: it defines the interfaces and operations required to operate a lightweight blockchain, a decentralized communication system, and a rapid transaction processing framework, allowing higher-order components to build on those features.

Transactions in Nxt make simple adjustments to account balances instead of tracing sets of input or output credits. In addition, the core software does not support any form of scripting language. By providing a set of basic, flexible transaction types that can quickly and easily be processed, Nxt creates a foundation that does not limit the ways in which those transaction types can be used, and does not create significant overhead for using them. This flexibility is further amplified by Nxts low resource and energy requirements, and its highly readable, highly organized object-oriented source code.

Basic Payments

The most fundamental feature of any cryptocurrency is the ability to transmit tokens from one account to another. This is Nxts most fundamental transaction type, and it allows for basic payment functionality.

Alias System

The Nxt Alias System allows any string of text to be permanently associated with a specific Nxt account. Since its inception, a convention for the format of these strings, using JSON notation, has been formalized. As a result, an alias can currently be human-friendly text alias for an account address or a Uniform Resource Identifier (URI)

The ability to store any URI on the Nxt blockchain enables the creation of any number of decentralized services that rely on small, persistent strings of text, such as a distributed Domain Name Server (DNS) system. One example of a simple implementation of this concept is the browser extensions developed by wesleyh of <http://nxt.org/>

Arbitrary Messages

Arbitrary strings of data up to 1000 bytes in length can be stored on the Nxt blockchain using the Arbitrary Messages feature, and these strings may optionally be AES-encrypted. These messages are intended to be removable, in the future, when blockchain size needs to be reduced; nonetheless, they form a critical building block for a number of next-generation features.

At the basic level, the system can be used to transmit human-readable messages between accounts, creating a decentralized chat system. However, advanced applications can use this feature to store structured data, such as JSON objects, that can be used to trigger or facilitate services built on top of Nxt. The most notable current implementation is the Nxt

Multigateway (MGW), part of the NXTServices layer, which employs the Arbitrary Messaging system to drive a nearly-trustless method for automatically transforming Bitcoin, Litecoin, and other cryptocurrencies into Nxt assets (based on the colored coins concept) that can be traded, bought, and sold on the fully-decentralized asset exchange.

Asset Exchange

An entire class of Nxt transactions is used to implement a fully-decentralized and automated asset exchange that operates on the Nxt blockchain. Using the colored coins concept, Nxt assets may be issued and tracked on the Nxt ecosystem, supported by transactions and processing that allow for asset transfer, bid and ask order placement, and automatic order matching.

Since its inception, the Nxt Asset Exchange has been used for fundraising & IPO offerings, tipping tokens, and the development of advanced services such as the Multigateway (MGW) system.

By combining the features of the Nxt Asset Exchange with other features such as the Arbitrary Messaging System, value-added services can be created. Most notably, another feature of the NXTServices layer is a system for the automated calculation and disbursement of dividends based on the performance of existing Nxt assets.

Digital Goods Store

The Nxt Digital Goods store gives account owners the ability to list assets for sale in an open, decentralized market place. Goods can be purchased, discounted, delivered, refunded, and transferred, using a dedicated class of transaction types that manage and secure store listings on the decentralized blockchain.

Device Portability

Due to its cross-platform, Java-based roots, its Proof of Stake hashing and its future ability to reduce the size of the block chain, Nxt is extremely well suited for use on small, low-power, low-resource devices. Android and iPhone applications are currently in development, and the Nxt software has been ported to low-powered ARM devices such as the RaspberryPi^[32] and CubieTruck platforms.

The ability to implement Nxt on low-powered, always-connected devices such as smartphones allows us to envision a scenario where the majority of the Nxt network is supported on mobile devices. The low cost and resource consumption of these devices significantly reduce network costs in comparison with traditional Proof of Work cryptocurrencies.

Concerns

Proof of Stake Attacks

Nothing at Stake

In a nothing at stake attack, forgers attempt to build blocks on top of every fork they see because doing so costs them almost nothing, and because ignoring any fork may mean losing out on the block rewards that would be earned if that fork were to become the chain with the largest cumulative difficulty.

While this attack is theoretically possible, it is currently not practical. The Nxt network does not experience long blockchain forks, and the low block reward does not provide a strong profit incentive; further, compromising network security and trust for the sake of such small gains would make any victory pyrrhic.

As part of Nxts development roadmap, a feature called Economic Clustering will provide further protection against attacks of this nature by forcing transactions to include hashes of previous blocks, and by grouping nodes into clusters that can detect unusual behavior on the network and impose penalties (in the form of temporary loss of the ability to forge).

History Attack

In a history attack, someone acquires a large number of tokens, sells them, and then attempts to create a successful fork from just before the time when their tokens were sold or traded. If the attack fails, the attempt costs nothing because the tokens have already been sold or traded; if the attack succeeds, the attacker gets their tokens back. Extreme forms of this attack involve obtaining the private keys from old accounts and using them to build a successful chain right from the genesis block.

In Nxt, the basic history attack generally fails because all stake must be stationary for 1440 blocks before it can be used for forging; moreover, the effective balance of the account that generates each block is verified as part of block validation. The extreme form of this attack generally fails because the Nxt blockchain cannot be re-organized more than 720 blocks behind the current block height. This limits the time frame in which a bad actor could mount this form of attack.

Distribution

Because blocks may only be generated based on existing stake, at least some of the token supply must be available when a Proof of Stake network is bootstrapped. As a result, Nxt issued and distributed its full supply of tokens with the creation of the genesis block.

The initial supply of Nxt was distributed to 73 original stakeholders, most of whom have been incentivized to further disperse their stake through the use of giveaways, contests, and bounties. Eight months after its creation, Nxts largest single account contains 5% of Nxts total supply. By contrast, Satoshi Nakamoto is thought to hold almost 9% of Bitcoins total supply after more than five years of that networks existence.

It will never be possible for Nxts proponents to dispel the distribution concerns raised by the wider community. Relative to the levels of profit achieved by early investors in IBM, Apple, Google, Facebook, and Bitcoin, the amount of inequality present in the Nxt blockchain is not out of line.

When asked: How would you solve the problem with scam accusations leveled against the unfair distribution of Nxt to 73 big stakeholders? BCNext (Nxts creator) answered: This problem can not be solved. Even if we had a million stakeholders the [other] seven billion people would call this unfair. A world with the [sic] money can not be perfect.

Transaction Fees

As the value of Nxt increases, the cost of minimum transactions fees, expressed in fiat terms, also increases. Plans are underway to reduce the minimum fee, scaled according to transaction byte-size, in order for micro-transactions to be practical. This will be implemented after changes to Nxts internal database are made, and that development is planned for version 1.3.0 of the Nxt software.

Whitepaper Timing

Most cryptocurrency creators issue a whitepaper before their currency is bootstrapped. Nxts first formal whitepaper was created for version 1.2.2 of the Nxt software, almost eight months after the creation of the genesis block.

The core development team has always been of the opinion that Nxts source code is its whitepaper: since Java is human-readable and the full source is available, anyone is welcome to gain an understanding of Nxts mechanics by examining the source. This whitepaper can be seen as a translation of key components of the Java source code into English, and it was created in order to make the design and function of Nxt more accessible to people who do not possess programming skills.

Q5.- Which VC based financial assets exist other than the broad categories mentioned?

At present, the most common use of the AE is to create and trade dividend-paying assets, effectively shares of revenue-generating companies. Issuing an asset is a popular way of raising money for a new project. For example, mining enterprises can raise capital to buy ASICs by issuing and selling assets. The mining rigs using the ASICs then generate income in the form of Bitcoin or other PoW coins, which is exchanged for NXT and paid out to asset holders as dividends every week.

However there are different VC based financial assets:

USD-pegged asset

Coinomat's USD asset is tied to the US dollar. The idea is that this can provide a degree of stability within a crypto-portfolio, without necessarily having to cash out by selling the assets and transferring the money to a bank account (with the costs, time and inconvenience which that would entail). It also means that you can send USD over national borders for just a 1 NXT fee. Using Coinomat's service you can withdraw your USD assets to any VISA / Mastercard. Of course, the CoinoUSD asset's utility/value depends on Coinomat honouring its promise to redeem it, and would be worthless if the company failed to do so; the concept therefore requires centralization to achieve its aims. You can read more in this article or on the NXT forum.

Reward points

Nxterpoints (NXTP) are reward points given to people who contribute to nxter.org. Every month, Nxter.org dividends out its net profit (generated by advertising, store sales and services fees) to all NXTP holders: writers, translators, editors, graphic designers, site developers etc. This means that any person who is having an influence on nxter.org's net worth, gets monthly rewards in NXT through the asset exchange according to their contribution to the income. The dividends are transferred to their Nxt account for as long as they own the Nxterpoints, which can of course also be traded on the AE.

Company shares

Coin IPOs are commonplace in the crypto world, and after doing just a little research in the field you should realize that some of them are scams. It can't be overstated that you must ALWAYS do your due diligence before investing in anything.

On the AE, it's important to distinguish between revenue sharing assets and assets representing ownership (including voting rights) in companies. Here are some examples of each type:

Revenue sharing assets include BGCaffe, a South African café (with plans to expand), Lyth; an upcoming MMORPG based on Nxt features; FinHive (AI on the Nxt blockchain); Pangea, a decentralized poker game; Coinomat, an exchange accepting Nxt, Tradebots (NxtCoinsco) and a lot of revenue sharing mining assets.

Company stocks (shares of the entire company) include examples like Jinn Labs (which is developing a general purpose processor based on ternary logic); SuperNET; Nxt Mobile Applications Company (the company behind the Nxtty mobile messaging app), and more.

Crypto backed assets

mgwBTC, for example, is a crypto backed Nxt asset representing Bitcoin. mgwBTC is used by Multigateway, the distributed cryptocurrency exchange developed on top of Nxt by j1777. You simply transfer your Bitcoins (or LTC, BTC, and what other coins are supported) to an address generated by the multigateway, and these are automatically made tradeable in the MGW exchange and on Nxt AE.

Software licensing

toknormal describes an example from the software development industry.

I am an independent software developer and I plan to use the NXT asset exchange to issue software licenses as follows:

[1] – a licensing component in the software makes a call to the NXT network and creates an account (instantaneous).

[2] – it writes the private key to disk and informs the user of the account number.

[3] – the user purchases one license unit from the NXT asset exchange.

[4] – on a subsequent launch (or periodically) the software detects the presence of the appropriate asset in the account it created for itself and considers the installation licensed.

InstantDEX: addition to the Asset Exchange

Nxt is among the fastest cryptos with 1 minute block times, compared to Bitcoin's 60 mins. To some though, even this may not be fast enough. Step forward InstantDEX: A Nxt 3rd party service, and now also a core service of the innovative SuperNET project, which aims to provide its users with nearly instant transactions. It's also an asset which will dividend out a percentage of the commissions generated by the service; currently, it's paying asset dividends to its investors from its holding of NXTventure.

"With the NXT AE, people are able to trade things, but there will be the blocktime to wait. 1 minute usually, but sometimes could be more. Also 1 minute will feel like a really long time if the market is changing dramatically. The goal of InstantDEX is to offer realtime trading of NXT, NXT assets and other cryptos. there won't be any centralized servers, there won't even be an actual website as the GUI will be running locally. Just direct peer to peer trading in realtime. The monetization model is very clear and simple. InstantDEX will not have any fees for withdrawals [or for changing a bid or ask] and the commissions will be set to 0.1% at first."

Multigateway.

Multigateway (MGW) is a third party service developed on top of the NXT network that allows you to move cryptocurrencies in and out of the NXT Asset Exchange, the peer-to-peer exchange that offers decentralized trading with no trading fees. To see the coins currently supported by MGW, jump to their website. (<http://multigateway.org/>)

MGW creates a unique deposit address for your account, for each of the supported coins. When you send coins to that deposit address, MGW will deliver to your Nxt account the same quantity of coin assets to your NXT account. Coin assets can be traded in the NXT Asset Exchange like any other asset: you can buy them with NXT, sell them for NXT and send them to any other NXT user with the fast speed of the NXT network.

Similarly, MGW allows you to easily withdraw your coin assets back into your corresponding coin wallet, with the lowest withdrawal fee in the market – equivalent to the minimum transaction fee for the coin.

Every coin asset is equivalent to one coin. The coin assets are backed up by the coins deposited in MGW, stored by the three MGW servers in multiple multisignature accounts for every supported coin. In a multisignature account, the same address has several associated private keys or signatures. This means the servers have to agree, each of them providing their signature, in order to process the coin transactions – similar way to a joint bank account. The use of multisignature accounts and independent servers is what makes MGW more secure than any traditional centralized exchange account.

Secure Asset Exchange.

Secure Asset Exchange, Inc. (SAE) does NOT OPERATE an EXCHANGE. It is a web application that allows you to access the NXT blockchain and interact with the information presented there.

Q6.- Do you agree with the analogies to traditional regulated entities as outlined?

Unlike usual marketplaces, Nxt Asset Exchange is not "run" by anybody. It is totally decentralized, based on Nxt's blockchain, and fees are kept at a minimum (1 NXT per transaction, 1000 NXT to create an asset). The Nxt Asset Exchange, started May 11th, 2014, rapidly saw many assets being offered and exchanged, like mutual funds, commodities (silver, other crypto currencies), startups IPOs, etc. It is a place where business ideas can be easily funded. It works much like a regular marketplace, minus the heavy fees and the regulation. Indeed, the AE being decentralized, there is no way to impose any regulation on it. This may be a drawback if seen from the point of view of institutional investors, but it is quality assurance for capital risk and early adopters.

The NXT community has organized a grant for start-up businesses planning to develop NXT activity. This ensures there will be funding for helping NXT to grow. Also, mutual funds are being created for investing in the crypto currencies world. This being a very technical domain, specialists, just like in the classical world of finance, invest the shareholders' money based on their knowledge of the crypto economy, so that the funds can pay dividends to investors proportionally to the funds' earnings.

Q7.- Do you have more evidence on how widespread ownership of VC based financial assets/securities is? Please mention your sources.

Nowadays there are plenty of VC based financial assets/securities and all of them are listed in the site, <http://coinmarketcap.com>, however the most advanced and used VC is Nxt.

- The Nxt blockchain has these statistics:
 1. **Number of transactions: 1,440,647**
 2. **Number of accounts: 116,897**
 3. **Number of assets: 573**
 4. **Number of asset transfers: 135,646**
 5. **Number of asset trades: 110,336**
 6. **Number of open ask/bid orders: 4,921**
 7. **Lists 272 full nodes, estimates currently consuming around \$300 a day in electricity**








- This information can be contrasted in:

1. <https://nxtportal.org/monitor/>
2. <http://nxtreporting.com/stats.php>
3. <http://www.peerexplorer.com/>
4. <https://www.mynxt.info/assets>
5. <https://trade.secureae.com/>
6. <http://nxt.org/>

- This picture shows the main assets listed in the Nxt blockchain:

#	Name	Platform	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
2	SuperNET	Nxt	\$ 2,067,556	\$ 2.53	816,061	\$ 10,288	-3.51 %	
4	InstantDEX	Nxt	\$ 1,596,170	\$ 1.60	1,000,000	\$ 243	-2.19 %	
7	SolarFarm	Nxt	\$ 843,406	\$ 0.009514	88,646,150	\$ 49	-1.50 %	
9	MMNXT	Nxt	\$ 710,105	\$ 0.014202	50,000,000	\$ 28	-2.51 %	
10	NXTventure	Nxt	\$ 506,720	\$ 0.506720	1,000,000	\$ 152	?	
11	SkyNET	Nxt	\$ 498,093	\$ 0.557012	894,223	\$ 11	13.51 %	
13	sharkfund0	Nxt	\$ 399,196	\$ 304.05	1,313	\$ 27	-4.08 %	
15	Jinn	Nxt	\$ 367,372	\$ 3.67	100,000	\$ 5,018	-0.61 %	
16	LIQUID	Nxt	\$ 365,516	\$ 3.79	96,500	\$ 38	-5.66 %	
17	Nxttycoin	Nxt	\$ 202,544	\$ 0.000203	1,000,000,000	\$ 54	21.01 %	
18	Jay	Nxt	\$ 200,613	\$ 0.202549	990,440	\$ 190	-0.61 %	
21	Privatebet	Nxt	\$ 120,599	\$ 0.301498	400,000	\$ 60	?	
23	CoinoIndex	Nxt	\$ 94,159	\$ 254.77	370	\$ 202	-0.59 %	
24	DeBuNe	Nxt	\$ 55,123	\$ 0.239425	230,231	\$ 36	6.60 %	
25	BTCOR	Nxt	\$ 46,910	\$ 0.192680	243,463	\$ 190	?	
27	MMBTCD	Nxt	\$ 38,004	\$ 0.095010	400,000	\$ 19	14.68 %	
28	NXTinspect	Nxt	\$ 32,627	\$ 0.048265	675,996	\$ 18	-0.61 %	

- Features of the most developed virtual currencies:

							
	NXT	Bitshares	Bitcoin	Ripple	Counterparty	Mastercoin	NEM
Operational	✓	✓	✓	✓	✓	✓	✗
Consensus Mechanism	PoS	Delegated PoS	PoW	Consensus	Timestamp Auth. Bitcoin	Timestamp Auth. Bitcoin	Pol
Block Production Time	1 Minute	5 Minutes	10 Minutes	10 Seconds	10 Minutes	10 Minutes	1 Minute
Recommended Confirmation Time	10 Blocks	1 Block	6 Blocks	1 Block	6 Blocks	6 Blocks	10 Blocks
Worst Case for Confirmation Time	720 Blocks	51 Block	120 Blocks	N/A	120 Blocks	120 Blocks	360 Blocks
Transaction Load	3 TPS	10 TPS	7 TPS	-	2 TPS	2 TPS	2 TPS
Anonymous Transactions	⚠	⚠	✗	✗	✗	✗	⚠
Transaction Fee Costs	1 NXT	Variable	0.0001 BTC	0.00001 XRP	0.0001 BTC	0.0001 BTC	Progressive
Network Security Costs	Tx. Fees	Fraction of Tx. Fee	10% mining inflation	Zero	10% mining inflation	10% mining inflation	Tx. Fees
Share Supply	1 Billion	2.5 Billion	14 Million	100 Billion	2.6 Million	563 Thousand	8.99 Billion
Profit sharing/dividends	✓	⚠	✗	✗	✓	✗	✗
Market Pegged Assets	✓	⚠	✗	✗	✗	✗	⚠
Inflation	0 %	Delegate Positions	10 %	Deflationary	Deflationary	Deflationary	0 %
User Issued Assets	✓	✓	✗	✗	✓	✓	⚠
User Registered Accounts	✓	✓	✗	✗	✗	✗	⚠
Encrypted Messaging	✓	⚠	✗	✗	✗	✗	✓
Monetary System	✓	✗	✗	✗	✗	✗	✗
Alias: Decentralized DNS	✓	✗	✗	✗	✗	✗	⚠
Asset Exchange	✓	✓	✗	✗	✗	✗	⚠
Decentralization	✓	✗	✓	✗	✓	✓	✓
Marketplace	✓	✗	✗	✗	✗	✗	✗
Transparent Forging	⚠	✗	✗	✗	✗	✗	✗
Cross Chain Trading Support	✗	✓	✗	✗	✗	✗	✗
Smart Leasing	✗	✗	✗	✗	✗	✗	✗
Multisig	⚠	✗	✓	✗	✗	✗	✓
Account Control	⚠	✗	✗	✗	✗	✗	⚠
Voting System (Stake/token/share based)	⚠	✗	✗	✗	✗	✗	✗
Automated Transactions	⚠	✗	✗	✗	✗	✗	✗
DAC (Dec. autonomous corporative support)	⚠	✗	✗	✗	✗	✗	✗
Smart Contracts	⚠	✗	✗	✗	✗	✗	✗
Blockchain Pruning / Trimming	✗	✗	✗	✗	✗	✗	✗

Related links:

1. <http://nxt.org/>
2. <http://nxter.org/>
3. <https://en.wikipedia.org/wiki/Nxt>
4. https://wiki.nxtcrypto.org/wiki/Main_Page
5. <https://nxtforum.org/>
6. <https://nxtportal.org/>
7. <http://www.secureae.com/>
8. <http://multigateway.org/>
9. <http://coinmarketcap.com/>
10. <http://coinmarketcap.com/assets/>
11. <https://bitcointalk.org/>
12. <http://www.supernet.org/index.php>
13. <http://www.instantdex.org/>
14. <https://melodius.me/>
15. <http://debune.org/>
16. <http://nxtlegal.org/>