

RNG Whitepaper

RangeCoin PLATFORM

Saving-Investment & Exchange

Abstract

Bitcoin has proven that a peer-to-peer electronic cash system can indeed work and fulfil 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. RANGE COIN PLATFORM (RNG) satisfies all these requirements.

1 Introduction

Financial saving has occurred since the beginning of modern civilization. With these characteristics people carry out economic activities only to meet their own needs or their organizations, while on the other side most can't plan their finances in the future, they don't know how to save what they have and create additional incomes. The growing number of people is the base reason that everyone needs a more organized, safe and planned financial system. The vision of RANGE COIN PLATFORM is to be a platform that can provide investment convenience for everyone, not limited to age, or amount of funds. To support this goal RANGE COIN PLATFORM will act as a bridge between the companies and investors or as proof of transactions, payments and, withdrawals of capital by companies from investors. RANGE COIN PLATFORM (RNG) cryptocurrency is the payment media of cooperation between those parts' through a dedicated platform, which can also be tradable in other cryptocurrency exchanges.

1.1 Root Cause

Investment can be interpreted as an action to grow your assets in the hope of giving additional income or returns of money in the future. So, if your assets do not grow, that's not an investment but only saving. However, investments are not easily done, and the following problems tend to appear when we want to invest:

Age: Not all ages can be involved to invest in a company, at least they must have a National ID.

Amount of funds: Many are interested to invest but their constraints are the very limited amount of their funds.

Company Access: Even when someone has enough funds to invest, they are confused thinking about how to connect with the correct company.

Fraud: Fraud is not a new thing that is often experienced by investors. They lose their funds which unclearly allocated.

The vision of RANGECOIN PLATFORM is to be a platform that can provide investment convenience for everyone, not limited to age, or amount of funds. To achieve that goal RANGECOIN PLATFORM becomes a trusted bridge between the company and investors.

RANGECOIN PLATFORM provides multi-sector investment combined with the power and broad possibilities of a cryptocurrency (RNG) running on its own blockchain, the RANGECOIN Blockchain Network, through NXT algorithm.

2 Core Technologies

2.1 Proof of Stake

RNG is a proof-of-stake cryptocurrency, constructed from open-source NXT¹. Its proof-of-stake algorithm does not depend on any implementation of the “coinage” concept used by other proof-of-stake cryptocurrencies and is resistant to so-called “nothing at stake” attacks. Curve25519 cryptography is used to provide a balance of security and required processing power, along with more commonly used SHA256 hashing algorithms.

RNG uses a system where each "coin" in an account can be thought of as a tiny mining rig. The more coins that are held in the account, the greater the chance that the 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. RNG does not generate any new coins as a result of block-creation. Redistribution of

RNG takes place as a result of block generators receiving transaction fees, so the term "forging" 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 these connections, creating a chain of blocks (and transactions) that can be traced back to the genesis block (the original block).

¹Source code for NXT is available at <https://bitbucket.org/JeanLucPicard/nxt/src>

Blocks are generated every 60 seconds, on average, by accounts that are unlocked on network nodes. Since the full supply already exists (23,333,333), RNG is redistributed through the inclusion of transaction fees that 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.

RNG 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, RNG's core can be seen as agile, base-layer protocol upon which a limitless range of services, applications, and other currencies can be built.

2.1.1 Some Security Principles

The security of the blockchain is always of concern in Proof of Stake systems. The following basic principles apply to RNG'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 block's value. In case of ambiguity, the network achieves consensus by selecting the block or chain fragment with the highest cumulative difficulty
- To prevent account holders from moving their stake from one account to another as a means of manipulating their probability of block generation, coins must be stationary within an account for several blocks before they can contribute to the block generation process. Coins that meet this criterion contribute to an account's effective balance, and this balance is used to determine to forge 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 RNG's 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.

2.1.2 Contrast with Proof of Work

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. Coins 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". This leads to possible vulnerabilities. The incentives provided by Proof of Work systems would result in the centralization of the mining process.

In RNG's Proof of Stake model, 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.

2.2 Network Nodes

A node on the RNG network is any device that is contributing transaction or block data to the network. Any device running the RNG 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 account's private key; this token can be decoded to reveal a specific RNG 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 to gain trustworthiness within the network and then use that trust for malicious purposes; the barrier to entry (cost of RNG required to build adequate trust) discourages such abuse.

Each node on the RNG network can process and broadcast both transactions and block information. Blocks are validated as they are received from other nodes², 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.

²All possible block parameters are verified, to prove that the generating account contains the effective balance (stake) that won the right to generate the block.

2.3 Blocks

As in other cryptocurrencies, the ledger of RNG 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 establishes the order in which transactions have occurred. A copy of the blockchain is kept on every node in the RNG network, and every account that is unlocked on a node (by supplying that account’s private key) can 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.

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 account's public key
- The ID and hash of the previous block
- The number of transactions stored in the block
- The total amount of RNG represented by transactions and fees in the block
- Transaction data for all transactions including 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

2.3.1 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 RNG 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 block's 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 block's 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:

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

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 account's 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 account's 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 to determine their hit value. This means it is possible to predict, with reasonable accuracy, which account will next win the right to forge a block. 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.

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 its required parameters. This block is then broadcast to the network as a candidate for the blockchain.

The payload value, generating account, and all 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 coins associated with the account. Using a transaction of the “account control” type, an account owner may temporarily reduce an account’s effective balance to zero, adding it to the effective balance of another account. The targeted account’s forging power is increased until the end of a 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 pay-outs to participants.

2.3.2 Accounts

RNG 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 account’s 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-Solomon³ error-correcting notation that allows for detection of up to four errors in an account address, or correction of up to two errors. 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 account’s private key.
2. The private key is encrypted with Curve25519 to derive the account’s public key.
3. The public key is hashed with SHA256 to derive the account ID.
4. The first 64 bits of the account ID is the visible account number.

5. Reed-Solomon encoding of the visible account number, prefixed with “RNG-”, 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 (2256) is larger than the address space for account numbers (264), 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.

³For more information: http://en.wikipedia.org/wiki/Reed-Solomon_error_correction

Account Balance Properties

For each RNG 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 account’s forging calculations⁴. An account’s effective balance consists of all coins that have been stationary in that account for 1440 blocks. Also, the Account Leasing feature allows an account’s effective balance to be assigned to another account for a temporary period.
- The guaranteed balance of an account consists of all coins that has 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 RNG that has been earned as a result of successfully forging blocks.

- The unconfirmed balance of an account is the one that is displayed in RNG clients. It represents the current balance of an account, minus the coins involved in unconfirmed sent transactions.
- Guaranteed asset balances list the guaranteed balances of all the assets associated with a specific account.
- Unconfirmed asset balances list the unconfirmed balances of all the assets associated with a specific account.

⁴See 2.3.1 Block Creation (Forging)

2.3.3 Transactions

Transactions are the only means RNG accounts have of altering their state of 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. When an RNG 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 enough 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.

Confirmations

All 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.

Deadlines

Every transaction contains a deadline parameter, set to several 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.

3 Core Features

3.1 Technological

As derived from NXT the following features are also applicable to RNG:

Agile architecture

First-generation cryptocurrencies were primarily designed as payment systems. RNG 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, RNG strips away unnecessary complexity in its core, leaving only the most successful components of its predecessors intact. As a result, RNG 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 RNG make simple adjustments to account balances instead of tracing sets of “input” or “output” credits. Also, 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 how those transaction types can be used and do not create significant overhead for using them. This flexibility is further amplified by RNG’s 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 RNG’s most fundamental transaction type, and it allows for basic payment functionality.

Arbitrary Messages

Arbitrary strings of data up to 1000 bytes in length can be stored on the RNG blockchain using the Arbitrary Messages feature, and these strings may optionally be AES-encrypted. At the basic level, the system can be used to transmit human-readable messages between accounts. Device Portability Due to its cross-platform, Java-based roots, and its Proof of Stake hashing, RNG is extremely well suited for use on small, low-power, low-resource devices. The low cost and resource consumption of these devices significantly reduce network costs in comparison with traditional Proof of Work cryptocurrencies.

3.2 Applications

The RANGECOIN PLATFORM (RNG) offers several features that can be applied to various sectors, such as:

Contract Payment

Anyone in the world can submit their company proposal to be listed on RANGE COIN PLATFORM and explain more about their company or their company's funding needs. The team behind RANGE COIN PLATFORM will collaborate with experienced and highly qualified legal and economic experts, we will analyse the prospects of the submitted proposals. If the future of the company and has a good track record, the team will take part to connect companies and investors, and investors who have interested only need deposited of RNG with the specified amount according to their ability.

Main Payment Instrument

The RNG will be the main payment instrument for all transactions on RANGE COIN PLATFORM. Funds withdrawn by the company after the contract agreement or profit given by the company to the investor will be RNG with the conversion of the real price of RNG on the market at that time.

Affiliate Program

All affiliate programs for RANGE COIN PLATFORM promotions will be paid in RNG so users of RANGE COIN PLATFORM and RNG holder community are widespread.

Investments

Low-risk investment services through staking, that can be accessed by everyone without age restrictions. Medium to long-term investment services in companies.

Saving Asset Management Saving services through RANGE COIN WALLET with portfolio assistance.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System. (n.d.). Retrieved July 06, 2014, from <https://bitcoin.org/bitcoin.pdf>

[2] Eyal, I., & Gun Sirer, E. (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. Unpublished manuscript. Retrieved July 06, 2014, from <http://arxiv.org/pdf/1311.0243v5.pdf>

[3] The Well-Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. (n.d.). Retrieved July 06, 2014, from <http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortuneofsatoshi-nakamoto/>

[4] Learn Cryptography — 51% Attack. (n.d.). Retrieved July 06, 2014, from <http://learncryptography.com/51-attack/>

[5] Crypto Review of Curve25519.java & Crypto.java. (n.d.). Retrieved July 06, 2014, from <https://gist.github.com/doctorevil/9521116>

[6] Yung, M., Dodis, Y., Kiayias, A., Malkin, T., & Bernstein, D. J. (2006). Curve25519: New Diffie-Hellman Speed Records. Public Key Cryptography, 2006, 207-228. doi: 10.1007/11745853_14