Raisin Technical Whitepaper

Background

The Raisin Blockchain is the key component which powers the Project Raisin platform and services. The base unit of this blockchain is termed as Raisin (RASN).

Purpose

Raisin blockchain is designed specifically to provide fast and secure transactions at scale. As such, the core philosophy is to keep on-chain data as lean as possible. The Raisin blockchain implements a straightforward, non-turing complete smart contract system, for token generation and self adaptive purposes. Another essential requirement of the blockchain is the ability to self-regulate and correct without user supervision.

The key objectives of the blockchain are to

- Provide high transaction capacity and fast confirmation times
- Be tamper-proof and fault-tolerant
- Minimal active participation (for node voting/mining etc)

Features

Due to its focus, the Raisin blockchain offers:

- High Transaction Throughput (up to 100,000tx/s)
- Fast Confirmation times (about 3s)
- Adaptive supply, tied to usage
- Automated election of nodes

Raisin Currency (RASN)

The utility token used in Project Raisin is known as Raisin (RASN).

Raisin is used as a medium of exchange on the GoRaisin platform and is also used to pay for the network fees incurred when making any on-chain transactions. Holders of Raisin also contribute an automated weighted vote for the Elected node based on the Raisin Consensus protocol (ADPOS).

Challenges with Existing Blockchains

Limitations of POW and POS Algorithms

In Proof of Work (POW) algorithms, consensus is achieved through miners and hash power. As the network and miners increase, the demand for hash power balloons. Proof of Stake (POS) attempts to address the issue with hashing demands but introduces network complexity in terms of staking nodes. Transaction times suffer as a result of a growing POS network.

Delegated Proof of Stake

Delegated Proof of Stake (popularly known as DPoS) is a consensus algorithm maintaining irrefutable agreement on the truth across the network, validating transactions and acting as a form of digital democracy.

Existing Delegated proof of stake networks uses real-time voting combined with a social system of reputation to achieve consensus. Every token holder can exercise a degree of influence about what happens on the network. Active Elected Nodes are voted into their roles by token holders. The voting power that the token holder has, otherwise known as voting weight, is determined by how many of the base tokens the account is holding.

Consensus is achieved by having a small group of elected nodes securing the network. These elected nodes are voted in by users whose votes are determined by the amount of currency or stake they hold. This process introduces an additional complexity for the average user as they

would not be able to reliably identify a good potential elected node without in depth understanding and research.

The selection of block producers allows for the transactions to be validated in a matter of seconds, rather than the 10 minutes it takes the proof of work system employed by Bitcoin. Raisin currently takes about 3 seconds to validate a block of transactions.

Adaptive Proof of Stake (ADPOS)

ADPOS is created based on the principle that the consensus algorithm should be secure and self regulating. Building on DPOS, the Raisin blockchain has an additional communication layer which enables wallets to automatically determine the node it should vote for based on real world hardware/network data.

Heartbeat Network

A key feature of the Raisin blockchain is its heartbeat network between elected nodes which allows the Elected Node voting process to have an automated default. The Raisin blockchain keeps an ongoing record of the connected nodes and wallets along with transaction throughput of each node. This is then used to model the health of the network and the effectiveness of the nodes. The blockchain is able to self assess the current and previous block data up to 1,000,000 cycles old.

Candidate Nodes

A Candidate Node is a type of account that has registered using a Candidate Node registration transaction as described in transactions. These accounts have a key role in the Raisin ecosystem as they generate blocks and validate transactions. Any account can become a Candidate Node, but only the 21 accounts with the most votes weighted by stake are allowed to generate blocks, thus being the “Elected Nodes”.

Block Cycle

A block cycle is exactly 21 blocks in length, identical to the total number of Elected Nodes. During each round, every Elected Node has one fixed time slot to produce a block. The time slot indicating the position of the Elected Node in the block generation process is assigned at the beginning of each round. If an elected Elected Node cannot produce during a round, its slot will be missed and the round will be extended by 10 seconds. In order to produce a block, the node associated with the Elected Node inserts up to 25 transactions into the block, signs it and broadcasts that block to the network. Once the block has reached the network, the next Elected Node will begin to produce in the next assigned slot.

Broadhash Consensus

Broadhash consensus serves a vital function in the Raisin network in preventing forks. The broadhash of a node is defined as an aggregated rolling hash of the past five blocks present in the node's database. Thus all peers with the same last blocks will produce the same broadhash and propagate that information via the system headers described in peer-to-peer communication. Broadhash consensus is established if 51 out of 100 randomly selected peers connected to a node maintain the same broadhash. Elected Nodes use the broadhash consensus as a guidance strategy to generate the block. Once broadhash consensus is established a Elected Node will generate a block in their assigned slot as described above.

Block Rewards

The Raisin network rewards the block producer a fixed amount of tokens for each block successfully generated and accepted by the system. All active Elected and Candidate Nodes that successfully participate are rewarded for securing the network. The amount of tokens rewarded is dependent on the Network Minting mechanism.

Block Production

Raisin's blocks are produced in cycles. In each cycle, a pre-defined number of elected nodes are selected to create and sign blocks of transactions. 1 elected node is selected from the pool of eligible nodes to ensure distributed participation. Any elected node who has missed and not

produced a block for 20,000 cycles will be dropped and another elected node selected from the pool of eligible nodes.

Voting and Regulation

Elected nodes, Voting and Self Regulation

Raisin employs a merit based node voting mechanism. All wallets will have 2 voting modes with automatic mode as the default. In automatic mode, wallets vote for the best nodes which are serving them in terms of connectivity and speed, while in manual mode, wallets can vote for any specific node which they prefer.

Full nodes on the Raisin Blockchain help to verify transactions and act as alternatives to the main elected nodes should they fail to produce blocks or requalify. Elected nodes are chosen based on the following:

- Manually voted in by staking wallets
- Latency and uptime to the network
- Historical transaction verification accuracy
- Amount of nominated wallets transactions processed

(Nominated wallets are geo-distributed, randomised wallets with at least 2 transactions during the evaluation to prevent elected nodes from creating transactions without purpose, even with fees.)

An initial 20 pre-selected elected nodes will form the base of the network. 1 additional elected node is always rotated around within the pool of eligible nodes. Subsequently, any full node is eligible to become an elected node with the following criteria:

- Indicate agreement to participate in elected node selection
- Pass the minimum latency, uptime and verification accuracy threshold for at least 1,000,000 cycles.

The number of elected nodes will also increase by 2 for every time Raisin supply increases by a multiple of 4. The first milestone this will occur at is 4 billion Raisins.

Network Determined Minting Mechanism

To ensure sufficient token circulation and to ensure future price stability, the Raisin blockchain will have an in-built mechanism that will trigger the release of new Raisins to the system. To cater for the initial growth of Raisin, this mechanism will not be active until the minimum transaction rate is sustained.

The rate is set as 30 transactions per block

Once the Raisin network has enough transactions to sustain the minimum rate, the blockchain will assess the network every 1 million cycles. If the averaged transaction rate of the 1 million cycles is higher than the previous average, the blockchain will get "grow" flag. After every 9 million cycles, if there are more than 4 grow flags, the network will mint 0.4% of the total Raisin supply for every "grow" flag above 4. The new Raisins will be released to all nodes and voting wallets over the next 9 million cycles.

Peer to Peer Communication

Block Propagation

Block propagation serves a vital function on the Raisin network. Blocks are made in a decentralized fashion and must be sent to all nodes on the network in order to establish consensus. When a block is generated, it is broadcast to 25 randomly selected peers. These forward the validated block to 25 randomly selected peers and so on. In order to prevent over-broadcasting of data, every block is given a relay limit of 3 and blocks that have already been received are not broadcast again.

Transaction Propagation

Transactions must move from one node to all other nodes in order to be included in blocks. The broadcast queue for transactions works by drawing up to 25 transactions from the transactions pool and performing a validation process on those transactions. These transactions are then broadcast to other nodes in a bundled JSON object. This can be represented as an array of objects, depending on the transaction type. The bundle is then broadcast to the network at regular intervals, currently specified as every 5 seconds. The time delay allows the bundle to accumulate additional transactions from the network (up to 25). In addition to broadcasting the object, the bundle is given a relay limit to prevent spamming the network. In the current implementation the relay limit is set as 3, which means that every bundle will be broadcast for at most 3 hops by the peers on the network.

Transaction Pool

The transaction pool provides the Raisin network a robust solution for preserving unconfirmed transactions that have overflowed into the next block. As described in blocks, each block can only include 25 transactions and the transaction pool allows up to 1.000 multi-signature transactions and other 1.000 for the remaining transaction types to remain queued for the next block(s). The transaction pool could be thought of as a memory pool, keeping transactions ready until they are signed into a block. The second usage of the transaction pool is to provide a mechanism for propagating transactions. When a node prepares a transaction bundle, it draws up to 25 transactions from the pool and broadcast them to the network. In order to keep the

transaction pool tidy, all transactions are given a time to live. This time to live is defined as 10800 seconds, or 1080 blocks. The final use for the transaction pool is to house transactions with pending signatures. Like unconfirmed transactions, these transactions will expire out of the pool based on the lifetime specified when the transaction is first received.

Transaction Fees

A small fee is required for each transaction to ensure transactions are not frivolous, as well as being a way to "pay" elected nodes for their efforts in maintaining the network. The preset rate initially is 0.01 Raisins. This will be paid to elected nodes and eligible nodes in accordance to their contribution priority. Alongside the network minting mechanism, if the average transaction value of the bottom 20% is within a single decimal place, the minimum fee will be readjusted and reduced by a factor of 10. Consequently, this will also be adjusted back up if average transaction values rises, to a cap of 0.01 Raisins. The dynamic reduction and increase of the fee can be overturned by manual participation of the elected nodes.

Fee Payment

To simplify transactions, network fees are deducted from the transaction amount rather than being paid separately by the sender by default. This allows users who wish to fully transfer a wallet's value to do so without additional calculations. For merchants, the Raisin price feed automatically accounts for the network fee as well as other conversion costs.