– RibbitRewards Whitepaper –

Welcome to RibbitRewards! **This Whitepaper is provided for general informational purposes only**. This is not a contract between You and Us nor is this Whitepaper to be considered terms and conditions for acceptance or Use of RibbitRewards. RibbitRewards and Ribbit Services are subject to change and this Whitepaper may not be contemporaneously updated and could become inaccurate. See the Terms and Conditions – First and Second Airdrops of RibbitRewards ("T&C") and Privacy Policy, at www.ribbit.me, for the terms and conditions which control Your Use of RibbitRewards and Ribbit Services. Some terms in this Whitepaper are capitalized and have special meanings which are defined in the T&C.

We are also excited about the Marketplace, www.marketplace.life, which is a planned commercial environment that we anticipate launching in late 2014 or early 2015 – as such, the descriptions in this Whitepaper of the Marketplace, and Ribbit Services related to the Marketplace, are conceptual only and subject to change. See www.marketplace.life for information about the Marketplace and the Terms and Conditions – Marketplace ("Marketplace T&C") which will explain the scope of services and controlling terms and conditions for Your Use of the Marketplace.

Thank you for Your interest in RibbitRewards!

RibbitRewards (RBT) are reward credits that will be tracked using a Bitcoin-derived blockchain. This gives RibbitRewards transaction abilities which typically are not possible with other rewards systems. Users will be able to exchange RibbitRewards into goods and services, as well as virtual or fiat currencies, without the involvement of Ribbit.me Furthermore, the value of RBT should “float” depending on the purchasing behavior of its holders.

The RBT blockchain is based off a clone of Bitcoin core, with minimal modifications. We intend to follow development of Bitcoin core and contribute back to it. In the event of security problems with or attacks on the Bitcoin core, We may be able to contribute solutions to Bitcoin as well as potentially import solutions that appear there.

Relative to Bitcoin, RibbitRewards tracks the existence of external events (specifically, purchases on market-places), and thus is not envisioned so much as a “currency”, though it can be used as such if its value is supported by the corresponding economic activity. Rather the RibbitRewards blockchain is a ledger of account for completed purchases.

The technology We propose may potentially be used to track non-financial events, among untrusted parties. We hope these ideas will be adopted in new and interesting ways. Our code is open and We welcome contributions. We emphasize that, due to the history of Bitcoin, We refer to units of account as “coins” however the long-term impact of these modifications maybe better referred to as “events” or “accounts”, divorcing the data stored in the blockchain from finance. One could just as easily use these ideas to track voters, logistic tracking of sensitive information or material, or accounting of any asset where that asset may be freely traded.

Since external events are not fixed in number in the way that currencies are, we require the ability to create coins or “events” out of thin air, depending on incoming information. Thus keeping a ledger of external events has two major modifications that will be discussed in detail in the following sections:

- Coin creation (minting)
- Multiple merged mining

1 Coin Minting

In Bitcoin, coins are distributed via the “coinbase” mechanism. Every 10 minutes (on average), a new group of transactions (a “block”) are incorporated into the ledger. In addition, the miner creating this new block is entitled to allocate coins to himself. In Bitcoin this serves to initially distribute the coins, as well as to incentivize miners to perform the Proof-of-Work (PoW) task which secures the blockchain and ensures consensus. The coinbase reward pays the miners via inflation of the coin supply.

A blockchain such as Bitcoin is simply a ledger. It keeps a series of addresses and balances but, unlike a paper ledger, individuals can exchange their balances with one another without the participation of any central authority. To do this they must pay a small fee to the “miner”. This system has only one value input: the electricity and hardware costs of miners.

Without an underlying source of value, a ledger is value-less. It is a tool which tracks external value. It is just a list. As a list, RibbitRewards is expected to track purchases of goods on the Marketplace (and potentially additional venues which may use the Plugin, discussed below) and it is expected to “create” coins (adds ledger entries) corresponding to Marketplace purchases that occur. This list of purchases may have monetary value and Ribbit.me may collect and selltransaction data. The advantage that RibbitRewards may provide is the potential to obtain cross-market, completed-purchase data and deliver a "reward" to the vendor and customer. The Marketplace may also receive fees from vendors for the use of the Marketplace and Ribbit Services. Again, all of the details will be finalized upon the launch of the Marketplace and the release of the Marketplace T&C.

Tracking external events requires a new type of transaction: “minting”. While Bitcoin is commonly referred to as a “currency”, in our opinion it is useful to think of this “minting” as simply the mechanism by which new entries are recorded in our ledger. Our ledger tracks purchases. Thus traditional macroeconomic “money supply” arguments about currency may be difficult to apply. Rather, entries are added to the ledger with each transaction and each transaction adds value to the system in terms of advertising revenue, transaction fees, or vendor fees. Thus “coins” must be created out of thin air, when an external event occurs of value.

Ribbit.me envisions several entities receiving RBT upon completion of a purchase on the Marketplace or a correspondence venue which uses the Plugin described below: the vendor, the customer, Ribbit.me, and (to be defined) charities. Technically, this is implemented via a multi-signature coinbase-type (zero input) transaction. The transaction is a standard Pay-to-Script Hash (P2SH) transaction requiring at least three signatures:

Pubkey script: OP_HASH160 <Hash160(RedeemScript)> OP_EQUAL

Redeem script: OP_3 <client pubkey> <vendor pubkey> <mint pubkey> OP_3 OP_CHECKMULTISIG

Signature script: OP_0 <client sig> <vendor sig> <ribbit sig> <redeemScript>

A minting transaction has as its input (UTXO) all zeros, since it is a coinbase transaction. It has the outputs for each of the vendor, customer, Ribbit.me and charities.

1.1 Validation

To allow the maximum flexibility, We do not restrict the outputs or values of minting transactions. Initially We envision that minting outputs will go to the vendor, customer, Ribbit.me, the miner, and charities. The RibbitRewards validates this transaction by maintaining two lists of valid signing keys: “Minting” keys and “Vendor” keys. A valid minting transaction must be signed by all existing mint keys, one valid vendor key, and one one other key. The final signing key is the customer -- whose keys are created on demand and we do not track.

A minting transaction must be a multi-signature transaction of the P2SH type. The list of valid minting and vendor keys are updated with Minting Keypool transactions (Sec.1.3), so that nodes are autonomous from Ribbit.me.

1.2. Multiple Mint Keys

By using multi-sig transactions with multiple mint keys, we can force a would-be attacker to compromise multiple, isolated machines. As deployment expands, we will increase the required number of minting keys. The number of minting keys will begin with only one, hard-coded into the RibbitRewards daemon, but will increase over time via “Minting Keypool” transactions described in Sec.1.3 as resources are added.

1.2.1 Vendor Validation Authority

Upon the anticipated launch of the Marketplace, it is planned that Ribbit.me may validate vendors by creating and maintaining a database of vendors and their public keys.

1.3 Minting Keypool

The RibbitRewards daemon will start out with a set of minting keys hard-coded in but, if minting keys were compromised, that could potentially lead to serious consequences for the RBT blockchain. Therefore we propose a way to both add and remove valid minting keys:Add Mint Authority (AMA) and Remove Mint Authority Key (RMA). By starting from the initial mint authority keys and parsing the blockchain, RibbitRewards should arrive at the set of valid mint authority keys.

1.3.1 Vendor Keypool

Adding or removing Marketplace vendors should be signed by all currently-valid mint authority keys.

2 Airdrop

Between 12:01 a.m., November 8, 2014 – 12:01 a.m., December 14, 2014 EST ("Airdrop Period"), there will be two Airdrops wherein 200 million RibbitRewards will be given free to any User who registers for a Digital Wallet (Free Airdrop) and, concurrently, an additional 200 million RibbitRewards available for purchase (Paid Airdrop), for a total of 400 million RibbitRewards to be distributed after the Airdrop Period in December 2014.

2.1 Free Airdrop

In exchange for registering a Digital Wallet at www.airdrop.ribbit.me during the Airdrop Period, Users will receive free RibbitRewards "dropped" (distributed) into their Digital Wallet which will be available to them in December 2014. The Free Airdrop will consist of 200 million RibbitRewards which will be divided equally among all Users who register a Digital Wallet during the Airdrop Period. Hypothetically, if 200 people register a Digital Wallet, each person will receive 1 million RibbitRewards; likewise, if 2 million people register a digital wallet, each person will receive 100 RibbitRewards.

2.2 Paid Airdrop

Users can also purchase additional RibbitRewards during the Paid Airdrop Period. Any User who registers a Digital Wallet will be able to submit a purchase order for a portion of the total 200 million RibbitRewards which will be available for purchase during the Airdrop Period. The RibbitRewards, which are available as part of the Paid Airdrop, are in addition to the RibbitRewards distributed as part of the Free Airdrop. Any RibbitRewards purchased as part of the Paid Airdrop will be distributed to Your Digital Wallet in December 2014.

3 Adjustment / Minting Schedule

It is conceivable that some fraction of customers on the Marketplace (and other sites which use the Plugin, described below) may not take steps beyond their transaction to register and open a Digital Wallet at www.ribbit.me/wallet. As described below, this may cause RBT to accrue in the customer's browser. After a number of purchases, the customer may become interested in the RibbitRewards which may be accruing and decide to register for a Digital Wallet in order to receive the RibbitRewards generated by their transactions.

However, some Users may never sign up for a Digital Wallet. As such, a fraction of the minted RBT may be "lost" to customers who do not to claim them.

In order to offset this, the RibbitRewards will make adjustments based on a "coin age" (*e.g.*, if a UTXO appeared n blocks ago, and the adjustment per block is $r \simeq 10^{-7}$ per block (about 5% per year with 60s blocks), a new transaction referencing that UTXO is eligible to spend $a(1+r)^n$ coins instead). Likewise queries to the RibbitRewards blockchain is expected to return age-adjusted, accrued balances, so that Users may see how much they have to spend.

The following is conceptual and is subject to change: In the first year, the RibbitRewards blockchain is anticipated to mint 500M total RibbitRewards. To achieve this, RibbitRewards will be set to have an internal daily *mint exchange rate* x_n =RBT/USD which is used to compute the number of RibbitRewards awarded. 500M RibbitRewards in the first year corresponds to 1.37M RibbitRewards per day. Each day, the remaining yearly RibbitRewards award is computed, and a prediction made for the expected number of RibbitRewards that would be minted tomorrow assuming the number of market transactions remains fixed. Thus, given the previous day's transaction volume v_n valued in USD, the previous day's number of minted RibbitRewards m_n, and the target yearly minting total $m = 500\times10^6$ RibbitRewards, the following day's mint exchange rate is:

$$x_{n+1} = \frac{v_n(365-n)}{t - \sum_{i=0}^{n} \quad m_i(1+r)^i}$$

Thus after 1 year approximately $t = 500$million RibbitRewards will have been minted. Here we have included an interest rate $r \simeq 5\%$, so that this target of 500M RibbitRewards includes both interest and newly minted RibbitRewards.

4 Plugin

At an undetermined time in the future, RibbitRewards are planned to be issued to customers on external markets via a Marketplace plugin. A vendor website would then have the Plugin available during the checkout process. Via a small badge it will:

- Show the User's balance in RibbitRewardss using RibbitRewards stored addresses.
- Show the User how many RibbitRewards would be earned from the pending transaction.
- Clicking on the badge will take the User to the Digital Wallet which will allow the User to Use those RibbitRewards.

In this scenario, at the end of the checkout process, the plugin will compose a special 'minting' transaction for the RibbitRewards blockchain which will create RibbitRewards for both the vendor and customer as described below. In order to store keys in the User's browser, there will be a public/private key pair in the browser. Javascript libraries such as BitcoinJS are capable of creating ECDSA key pairs and Bitcoin addresses from them.

1. Compute the corresponding RibbitRewards customer address C to the ECDSA public key.
2. Create an AES key K.
3. Create a RibbitRewards "minting" transaction, which is a 3-of-3 multisig involving (vendor V, customer C, Ribbit.me R).
4. Encrypt the AES key K using Ribbit.me's public key and send it to Ribbit.me.
5. Sign the "minting" transaction and send it to the vendor. From there, the transaction is in the hands of the vendor, who must sign it using the vendor's private key.

Continuing this scenario, the following will occur on the vendor's side of the plugin:

1. Receive partially signed "minting" transaction from the customer via https POST.
2. Sign this transaction using vendor's key.
3. Submit "minting" transaction, now signed by C and V to Ribbit.me.

4.1 Plugin data storage

Again, the Plugin is a planned service to be available at an undetermined time in the future. The Plugin remains in the conceptual stage and is subject to change.

The plugin must send the following data along with the plugin code

- Public key for Ribbit.me (we can compute the Ribbit.me receiving address R)
- Public key for vendor (we can compute the vendor's receiving address V)
- RibbitRewards receiving address for vendor (if not be the same as above)
- RibbitRewards receiving address for Ribbit.me (if not be the same as above)

Ribbit.me then stores the following keypair information information, which can be later associated with a user account:

- Customer UUID: encrypted AES key

The plugin must then store the following information in the User's browser, in a way that is retrievable on a vendor's website as well as on www.ribit.me.

- UUID user identifier
- AES encrypted private key for each transaction (multiple of these)
- RibbitRewards address(es) (for balance inquiry via blockchain.info type query – balance is inflating)

4.2 Vulnerabilities and Attack Vectors

- Javascript injection to send the user's private keys somewhere else (must occur during the checkout process, before the keys are AES encrypted and stored).

- Obtaining the Ribbit.me “minting” key.
- Compromising the user’s computer and/or browser to retrieve AES encrypted private keys.
- Fraudulent request of user’s AES key from Ribbit.me.
- DDoS the MSA.
- DDoS the VVA.

5 Digital Wallets

The Digital Wallet allows Users to both store and transfer RibbitRewards. Digital Wallets will only be created when a User registers on www.ribbit.me/wallet. During the initial Airdrops, a User will have to register for a Digital Wallet to receive RibbitRewards during the initial Airdrops. However, after the blockchain is launched, it is planned that Users will be able to obtain and Use RibbitRewards without registering for a Digital Wallet however a User will have to have a Digital Wallet in order to collect RibbitRewards as a "reward" for completing a Marketplace purchase and/or a transaction on a site which uses the Plugin described above.

6 Blockchain parameters

These modifications of the Bitcoin blockchain parameters are chosen for convenience and are largely inconsequential. More important changes are detailed in the previous sections. While these are the most common modifications made for alt-coins, they are largely inconsequential to the operation of the coin, and we reserve the right to change them before launch.

- Block time: 60s
- Consensus mechanism: PoW
- Hash function: sha256d (merge mined) and scrypt (merge mined)

One of the most dangerous threats to RibbitRewards is a fast variation in hash rate. To mitigate this, we implement merged mining as describedin the following section.

6.1 Merged Mining

As of this writing, the two most advanced hashing functions are sha256d and scrypt. Hash functions are entirely useless computations, and in the long run we desire a non-PoW solution to securing the blockchain. But until such a thing appears, we need to achieve a stable hash rate. By tying ourselves to the two largest hash rate solutions available, it is unlikely that any entity can quickly dump a large hash rate onto our network to disrupt it.

Bitcoin re-adjusts its target difficulty every 2016 blocks. Any alt-coin will see variations in hash rate far quicker than this, so adopting Bitcoin’s paradigm is simplistic and treacherous. By implementing multiple merged mining, the fast appearance (or disappearance) of one kind of hash power leaves the others to pick up the slack and publish a block in a timely manner. Secondly by tying ourselves to the two largest hash rate providers available, it is prohibitively difficult for large increases in hash rate to occur.

Finally, we implement an adjustable difficulty that adjusts with every block. We use the actual hash value used to create a block, which is a better measure of the network's hash rate but is subject to more significant variation (once out of every 100 blocks, the hash value will be 100 times smaller than the target).

Hash values form a uniform distribution, such that any value less than the target difficulty is accepted as the PoW for the current block.

7. Conclusion

Thank you again for Your interest in RibbitRewards. To confirm, this Whitepaper is conceptual and for general information purposes only and not intended for You to rely upon before making any purchase of or decision about RibbitRewards. Please review the specific information in our Terms and Conditions – First and Second Airdrops of RibbitRewards and our Privacy Policy at www.ribbit.me. The Marketplace and other services are conceptual and subject to change – please visit www.marketplace.life for the most current information, including our forthcoming Terms and Conditions – Marketplace.