ReCoal

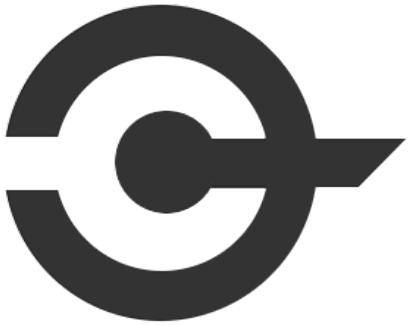
Untraceable PoW Digital Currency upgrade for BitCOAL

White Paper v1.0

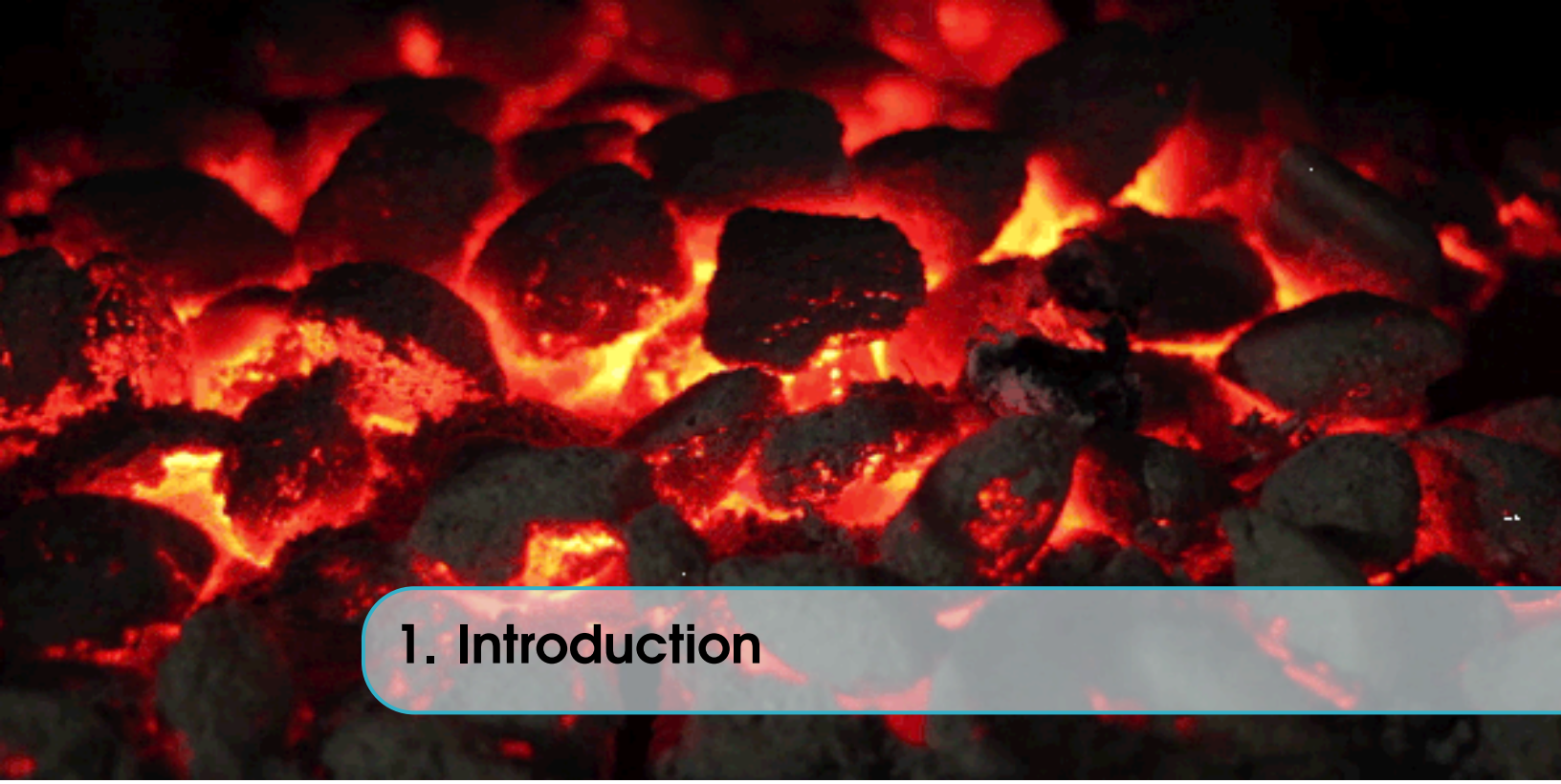
ReCoal is a private, secure, untraceable, decentralised digital currency upgrade for BitCoal which gives absolute control over funds to the user, with the option for complete privacy with traceless transactions thus allowing censorship resistant access to services and data across the world.

First release, June 2018

www.recoal.org



Contents



1. Introduction

1.1 Motivation

ReCoal // BitCOAL upgrade.

The aim of ReCoal is to provide a truly trustless token with absolute privacy, allowing the completely secure transaction of resources without fear of witness from undesirable parties or manipulation by bad actors. The result will bring access to services and data both to those under even the most oppressive regimes and those who may be otherwise blacklisted by vendors or exchanges due to their real-world associations.

As a fork of Monero, ReCoal is able to leverage Monero's technology for the obfuscation of origins, amounts, and destinations of all transactions. Transactions cannot be traced back to a user or real-world identity.

1.2 A Trustless Economy

With around 15% of all retail transactions now taking place online, not to mention personal transfers, digital payments and currency transfers form an ever-growing part of the world of commerce.

With an increasing demand, the weakness of the trust based model on which the implementation of a third party (ie a financial institution) is based becomes more prevalent.

1.3 References

Since I found so much good information about pretty much everything I wanted to know about, I will just create a remark and let you know where you can find more specific information about, just like below.

R For more information visit www.recoal.org

2. The ReCoal Model

2.1 Privacy

In a trust based system a third party, usually a financial institution, 'bears witness' to the transaction. This trusted party will be privy to the sum exchanged, the parties making the exchange, when and where the exchange was made and in many cases what the currency was being exchanged for. Further to witnessing a transation, the independent moderator for the transaction has complete control over the centralised record of the transaction. This means that his version of the transaction is the transaction as far as any investigative parties are concerned.

In a trusteless system there is no third party.

Forked from Monero, ReCoal takes advantage of Monero's ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of all transactions, providing all the benefits of a decentralized cryptocurrency, without any of the typical privacy concessions.

ReCoal uses a cryptographically sound system to allow you to send and receive funds without your transactions being easily revealed on the blockchain (the ledger of transactions that everyone has). This ensures that your purchases, receipts, and all transfers remain absolutely private by default.

2.2 Security

Using the power of a distributed peer-to-peer consensus network, every transaction on the network is cryptographically secured. Individual wallets have a 25 word mnemonic seed that is only displayed once, and can be written down to backup the wallet. Wallet files are encrypted with a passphrase to ensure they are useless if stolen.

2.3 Untraceability

By taking advantage of ring signatures, a special property of a certain type of cryptography, Recoal is able to ensure that transactions are not only untraceable, but have an optional measure of ambiguity that ensures that transactions cannot easily be tied back to an individual user or computer.

2.4 Untraceability

The Setting minimum transaction mixin to 7 would reduce chance of being attacked, traced or identified by (blockchain) statistical analysis.

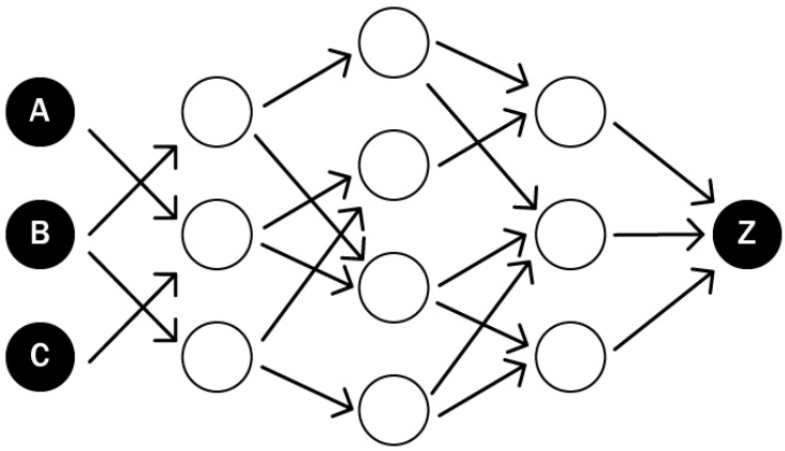
2.5 Ring Confidential Transactions (RingCT)

The Setting minimum transaction mixin to 7 would reduce chance of being attacked, traced or identified by (blockchain) statistical analysis.

2.6 Blockchain Analysis Resistance

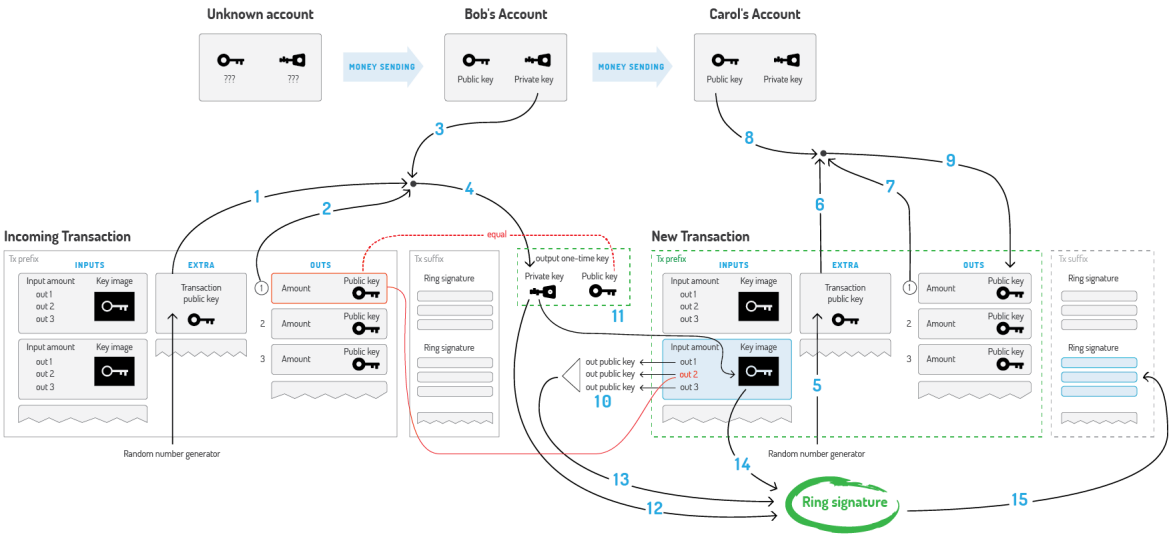
There are many academic papers dedicated to the analysis of the Bitcoin's blockchain. Their authors trace the money flow, identify the owners of coins, determine wallet balances and so on. The ability to make such analysis is due to the fact that all the transfers between addresses are transparent: every input in a transaction refers to a unique output. Moreover, users often re-use their old addresses, receiving and sending coins from them many times, which simplifies the analyst's work. It happens unintentionally: if you have a public address (for example, for donations), you are sure to use this address in many inputs and transactions.

ReCoal's CryptoNote is designed to mitigate the risks associated with key re-usage and one-input-to-one-output tracing. Every address for a payment is a unique one-time key, derived from both the sender's and the recipient's data. It can appear twice with a probability of a 256-bit hash collision. As soon as you use a ring signature in your input, it entails the uncertainty: which output has just been spent? Trying to draw a graph with addresses in the vertices and transactions on the edges, one will get a tree: a graph without any cycles (because no key/address was used twice). Moreover, there are billions of possible graphs, since every ring signature produces ambiguity. Thus, you can't be certain from which possible sender the transaction edge comes to the address-vertice. Depending on the size of the ring you will guess from "one out of two" to "one out of a thousand". Every next transaction increases the entropy and creates additional obstacles for an analyst.



2.7 Standard Cryptonote Transactions

A standard ReCoal CryptoNote transaction is generated by the following sequence covered in the white paper. Bob decides to spend an output, which was sent to the one-time public key. He needs Extra (1), TxOutNumber (2), and his Account private key (3) to recover his one-time private key (4). When sending a transaction to Carol, Bob generates its Extra value by random (5). He uses Extra (6), TxOutNumber (7) and Carol's Account public key (8) to get her Output public key (9). In the input Bob hides the link to his output among the foreign keys (10). To prevent double-spending he also packs the Key image, derived from his One-time private key (11). Finally, Bob signs the transaction, using his One-time private key (12), all the public keys (13) and Key Image (14). He appends the resulting Ring Signature to the end of the transaction (15).



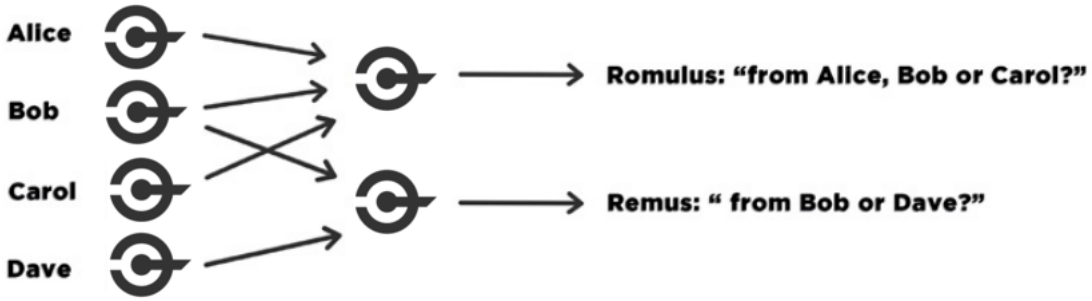
2.8 Untraceable Payments

The ordinary digital signature (e.g. (EC)DSA, Schnorr, etc...) verification process involves the public key of the signer. It is a necessary condition, because the signature actually proves that the author possesses the corresponding secret key. But it is not always a sufficient condition.

Ring signature is a more sophisticated scheme, which in fact may demand several different public keys for verification. In the case of ring signature, we have a group of individuals, each with

their own secret and public key. The statement proved by ring signatures is that the signer of a given message is a member of the group. The main distinction with the ordinary digital signature schemes is that the signer needs a single secret key, but a verifier cannot establish the exact identity of the signer. Therefore, if you encounter a ring signature with the public keys of Alice, Bob and Carol, you can only claim that one of these individuals was the signer but you will not be able to pinpoint him or her.

This concept can be used to make digital transactions sent to the network untraceable by using the public keys of other members in the ring signature one will apply to the transaction. This approach proves that the creator of the transaction is eligible to spend the amount specified in the transaction but his identity will be indistinguishable from the users whose public keys he used in his ring signatures.



It should be noted that foreign transactions do not restrict you from spending your own money. Your public key may appear in dozens of others' ring signatures but only as a muddling factor (even if you already used the corresponding secret key for signing your own transaction). Moreover, if two users create ring signatures with the same set of public keys, the signatures will be different (unless they use the same private key).

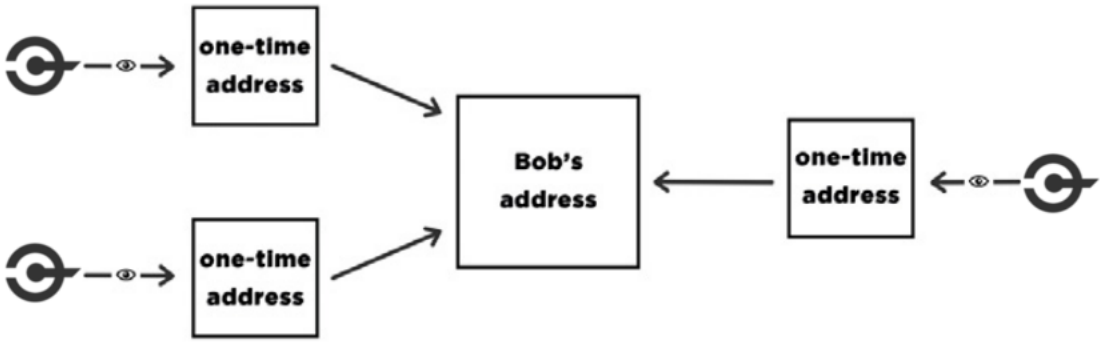
2.9 Unlinkable Transactions

Normally, when you post your public address, anyone can check all your incoming transactions even if they are hidden behind a ring signature. To avoid linking you can create hundreds of keys and send them to your payers privately, but that deprives you of the convenience of having a single public address.

ReCoal's CryptoNote solves this dilemma by an automatic creation of multiple unique one-time keys, derived from the single public key, for each p2p payment. The solution lies in a clever modification of the Diffie-Hellman exchange protocol. Originally it allows two parties to produce a common secret key derived from their public keys. In our version the sender uses the receiver's public address and his own random data to compute a one-time key for the payment.

The sender can produce only the public part of the key, whereas only the receiver can compute the private part; hence the receiver is the only one who can release the funds after the transaction is committed. He only needs to perform a single-formula check on each transactions to establish if it belongs to him. This process involves his private key, therefore no third party can perform this check and discover the link between the one-time key generated by the sender and the receiver's unique public address.

An important part of our protocol is usage of random data by the sender. It always results in a different one-time key even if the sender and the receiver both remain the same for all transactions (that is why the key is called "onetime"). Moreover, even if they are both the same person, all the one-time keys will also be absolutely unique.



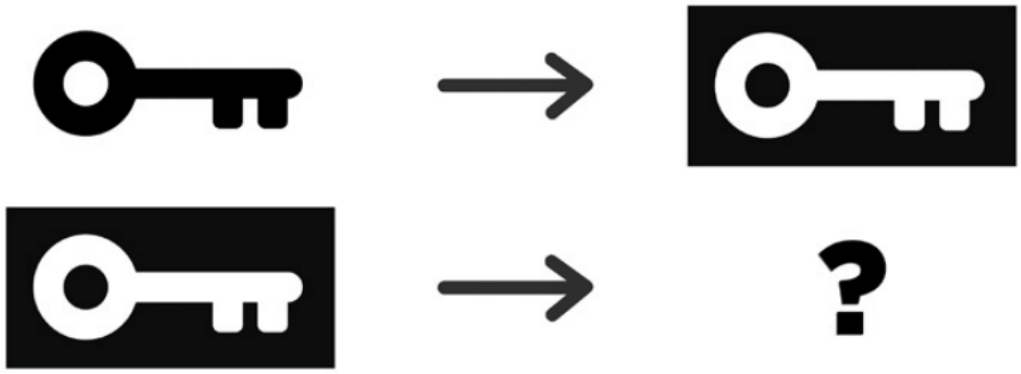
2.10 Double-spending proof

Fully anonymous signatures would allow spending the same funds many times which, of course, is incompatible with any payment system's principles. The problem can be fixed as follows.

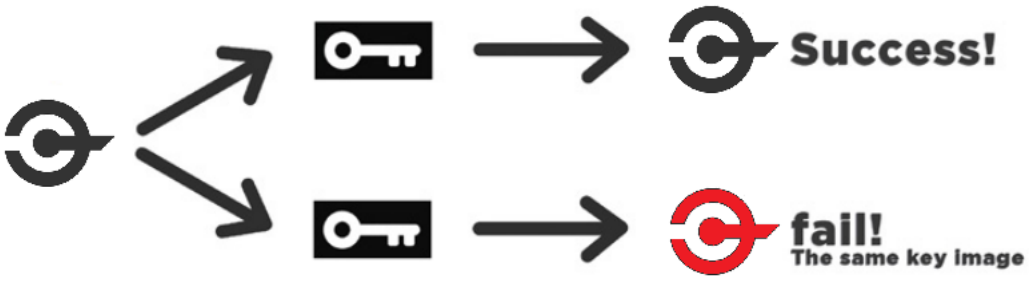
A ring signature is actually a class of crypto-algorithms with different features. The one ReCoal's CryptoNote uses is the modified version of the "Traceable ring signature". In fact we transformed traceability into linkability. This property restricts a signer's anonymity as follows: if he creates more than one ring signature using the same private key (the set of foreign public keys is irrelevant),

these signatures will be linked together which indicates a double-spending attempt.

To support linkability, ReCoal's CryptoNote introduced a special marker being created by a user while signing, which we called a key image. It is the value of a cryptographic one-way function of the secret key, so in math terms it is actually an image of this key. One-wayness means that given only the key image it is impossible to recover the private key. On the other hand, it is computationally impossible to find a collision (two different private keys, which have the same image). Using any formula, except for the specified one, will result in an unverifiable signature. All things considered, the key image is unavoidable, unambiguous and yet an anonymous marker of the private key.



All users keep the list of the used key images (compared with the history of all valid transactions it requires an insignificant amount of storage) and immediately reject any new ring signature with a duplicate key image. It will not identify the misbehaving user, but it does prevent any double-spending attempts, caused by malicious intentions or software errors.



3. Coin Specification

Whilst BitCOAL was built upon forknote code, ReCoal is built on the Monero code, utilising Cryptonote V7 algorithms.

ReCoal values the support of its miners and we believe that true decentralisation comes from a wide dispersal and fair distribution of tokens. In order to reduce the possibility of centralised mining and to put mining capabilities in the hands of our community, we have chosen to develop an ASIC resistant currency.

Total Supply	18.4 Million ReCoal Coins. + 0.3 RECL/minute
Premine	About 10.8% (2m) to reserve for future development of ReCoal and Charity Purposes.
Community Mine	16.4 Million coins available
Coin Symbol	RECL
Hash Algorithm	CryptoNight V7 (Proof-Of-Work with Asic Resistance)
Emission Scheme	ReCoal's Block reward changes every block .This is to ensure the stability of supply. However, the emission path of ReCoal is generally not far apart.

3.1 Adaptive Limits

A decentralized payment system must not depend on a single person's decisions, even if this person is a core developer. Hard constants and magic numbers in the code deter the system's evolution and therefore should be eliminated (or at least be cut down to the minimum). Every crucial limit (like max block size or min fee amount) should be re-calculated based on the system's previous state. Therefore, it always changes adaptively and independently, allowing the network to develop on it's own. ReCoal's CryptoNote has the following parameters which adjust automatically for each new block.

3.2 Difficulty

The general idea of our algorithm is to sum all the work that nodes have performed during the last 720 blocks and divide it by the time they have spent to accomplish it. The measure of the work is the corresponding difficulty value for each of the blocks. The time is calculated as follows: sort all the 720 timestamps and cut-off 20% of the outliers. The range of the rest 600 values is the time which was spent for 80% of the corresponding blocks.

3.3 Max block size

Let MN be the median value of the last N blocks sizes. Then the "hard-limit" for the size of accepting blocks is 2*MN. It averts blockchain bloating but still allows the limit to slowly grow with the time if necessary. Transaction size does not need to be limited explicitly. It is bounded by the size of the block.

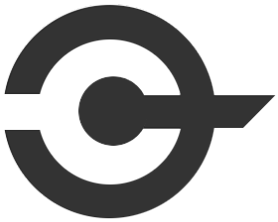
3.4 Egalitarian Proof-of-work

The proof of work mechanism is actually a voting system. Users vote for the right order of the transactions, for enabling new features in the protocol and for the honest money supply distribution. Therefore, it is important that during the voting process all participant have equal voting rights. ReCoal's CryptoNote brings the equality with an egalitarian proof-of-work pricing function, which is perfectly suitable for ordinary PCs. It utilizes built-in CPU instructions, which are very hard and too expensive to implement in special purpose devices or fast memory on-chip devices with low latency. We propose a new memory-bound algorithm for the proof-of-work pricing function. It relies on random access to a slow memory and emphasizes latency dependence. As opposed to scrypt, every new block (64 bytes in length) depends on all the previous blocks. As a result a hypothetical "memory-saver" should increase his calculation speed exponentially. Our algorithm requires about 2 Mb per instance for the following reasons:

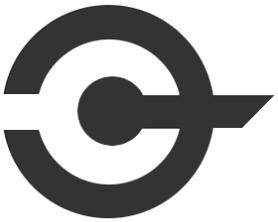
- It fits in the L3 cache (per core) of modern processors, which should become mainstream in a few years;
- A megabyte of internal memory is an almost unacceptable size for a modern ASIC pipeline;
- GPUs may run hundreds of concurrent instances, but they are limited in other ways: GDDR5 memory is slower than the CPU L3 cache and remarkable for its bandwidth, not random access speed.
- Significant expansion of the scratchpad would require an increase in iterations, which in turn implies an overall time increase. "Heavy" calls in a trust-less p2p network may lead to serious vulnerabilities, because nodes are obliged to check every new block's proof-of-work. If a node spends a considerable amount of time on each hash evaluation, it can be easily DDoSed by a flood of fake objects with arbitrary work data (nonce values).

One of the proof-of-work algorithms that is in line with our propositions is CryptoNight. It is designed to make CPU and GPU mining roughly equally efficient and restrict ASIC mining.

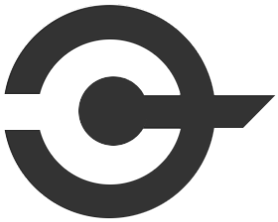
3.5 Our Team



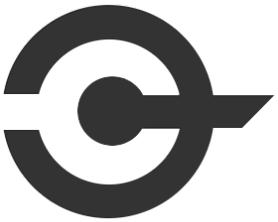
Pranav M S
Lead Developer and Founder



Elektryon Mihai
Developer



Deep Raj
Wallet and Paper Wallet Developer



Romy Toklio
Mobile Wallet Developer

3.6 Community Powered

In the true spirit of decentralisation, ReCoal is a wholly community-sponsored endeavour.

This is the core implementation of Monero. It is open source and completely free to use without restrictions, except for those specified in our license agreement. There are no restrictions on anyone creating an alternative implementation of ReCoal that uses the protocol and network in a compatible manner. As with many development projects, the repository on Github is considered to be the "staging" area for the latest changes. Before changes are merged into that branch on the main repository, they are tested by individual developers in their own branches, submitted as a pull request, and then subsequently tested by contributors who focus on testing and code reviews. That having been said, the repository should be carefully considered before using it in a production environment, unless there is a patch in the repository for a particular show-stopping issue you are experiencing. It is generally a better idea to use a tagged release for stability. Anyone is welcome to contribute to ReCoal's codebase. If you have a fix or code change, feel free to submit it as a pull request directly to the "master" branch. In cases where the change is relatively small or does not affect other parts of the codebase it may be merged in immediately by any one of the collaborators. On the other hand, if the change is particularly large or complex, it is expected that it will be discussed at length either well in advance of the pull request being submitted, or even directly on the pull request.

3.7 Charity

Around 20% of the premine has been reserved for charitable donations to support the provision of resources, education and shelter for communities local to our Lead Developer.

3.8 Advantages Over BitCoal

	ReCoal	BitCoal
Total Supply	18.4 Million ReCoal + 0.3 RECL/minute	12.5 Million COAL
Privacy	Untraceable	Yes
Code Base	Monero V7	Forknote
Mining	CPUs, GPUs	CPUs, GPUs, ASICs, etc.
Block Time	120s	90s
Release Date	6th June 2018	7th Nov 2017
Mining Algorithm	Cryptonight V7	Cryptonight
Bullet Proofing	Yes. Reduces Transaction size by 80%	No