R A M P A N T

SEEDSFORFUTURE

Blockchain technology, for all its merits, is not a new technology.

Rather, it is a combination of proven technologies applied in a new way. It was the particular orchestration of three technologies (the Internet, private key cryptography and a protocol governing incentivization) that made bitcoin creator Satoshi Nakamoto's idea so useful. The result is a system for digital interactions that does not need a trusted third party. The work of securing digital relationships is implicit -- supplied by the elegant, simple, yet robust network architecture of blockchain technology itself.

Blockchains are built from 3 technologies		
1. Private Key Crytography	2. P2P Network	3. Program (the blockchain's protocol)
Cash vs. Plastic	Tree falls in a forest	Tragedy of the commons
Identity	System of Record	Platform

WHAT IS BLOCKCHAIN?

Lets try to understand blockchain with simple wikipedia analogy. With a blockchain, many people can write entries into a record of information, and a community of users can control how the record of information is amended and updated. Likewise, Wikipedia entries are not the product of a single publisher. No one person controls the information.

Descending to ground level, however, the differences that make blockchain technology unique become more clear. While both run on distributed networks (the internet), Wikipedia is built into the World Wide Web (WWW) using a client-server network model.

A user (client) with permissions associated with its account is able to change Wikipedia entries stored on a centralized server. Whenever a user accesses the Wikipedia page, they will get the updated version of the 'master copy' of the Wikipedia entry. Control of the database remains with Wikipedia administrators allowing for access and permissions to be maintained by a central authority.

Wikipedia's digital backbone is similar to the highly protected and centralized databases that governments or banks or insurance companies keep today. Control of centralized databases rests with their owners, including the management of updates, access and protecting against cyber-threats.

The distributed database created by blockchain technology has a fundamentally different digital backbone. This is also the most distinct and important feature of blockchain technology.

Wikipedia's 'master copy' is edited on a server and all users see the new version. In the case of a blockchain, every node in the network is coming to the same conclusion, each updating the record independently, with the most popular record becoming the de-facto official record in lieu of there being a master copy.

WHAT IS RAMPANT COIN?

Forests cover 31% of the land area on our planet. They produce vital oxygen and provide homes for people and wildlife. Many of the world's most threatened and endangered animals live in forests, and 1.6 billion people rely on benefits forests offer, including food, fresh water, clothing, traditional medicine and shelter.

But forests around the world are under threat from deforestation, jeopardizing these benefits. Deforestation comes in many forms, including fires, clear-cutting for agriculture, ranching and development, unsustainable logging for timber, and degradation due to climate change. This impacts people's livelihoods and threatens a wide range of plant and animal species. We're losing 18.7 million acres of forests annually, equivalent to 27 soccer fields every minute.

Deforestation, primarily the conversion of forests to agricultural land, continues at an alarmingly high rate – about 13 million hectares per year. Forest planting, landscape restoration and natural expansion of forests have significantly reduced the net loss of forest area.

However, these newly replanted lands do not have the ecological value of older, more biologically diverse forests, and do not provide the same benefits and livelihoods for local communities. The net decrease in forest area is over the period. There are many causes of deforestation. The WWF reports that half of the trees illegally removed from forests are used as fuel. Some other common reasons are: To make more land available for housing and urbanization to harvest timber to create commercial items such as paper, furniture and homes to create ingredients that are highly prized consumer items, such as the oil from palm trees to create room for cattle ranching Common methods of deforestation are burning trees and clear cutting. These tactics leave the land completely barren and are controversial practices.

Clear cutting is when large swaths of land are cut down all at once. A forestry expert quoted by the Natural Resources Defense Council describes clear cutting as “an ecological trauma that has no precedent in nature except for a major volcanic eruption.” Burning can be done quickly, in vast swaths of land, or more slowly with the slash-and-burn technique. Slash and burn agriculture entails cutting down a patch of trees, burning them

and growing crops on the land. The ash from the burned trees provides some nourishment for the plants and the land is weed-free from the burning.

When the soil becomes less nourishing and weeds begin to reappear over years of use, the farmers move on to a new patch of land and begin the process again.

The best thing we can do for our environment is itself an enormous subject. The most obvious one is **PLANTING MORE TREES**, so that's where our initial focus is placed. As further research into sustaining our habitat is released this will be subject to review. Supporting nature is the mandate. Rampant will fund the planting of millions of trees worldwide just by people buying, supporting and using it.

Our project aims to bring a new solution to this case. Rampant Coin will be used for buying and selling seedlings and saplings around the world. We will be working together with tree nurseries globally to encourage people to help forests. At the same time we will be reaching out to major ecologic foundations for coordination, working together for a green future. The goal of Rampant is to achieve a decentralized sustainable crypto currency with near instant full-time private transactions, fair governance and community intelligence.

Ecologic Governing! We are going to implement a governance system where our Masternode owners can donate part of their earnings to ecologic foundations, decide if they want to grow their own forests anywhere in the world or to help mending the wounds of forest fires.

YOUR ROLE AS A SUPPORTER

When you buy, use or hold RCO, you will be helping us to support tree nurseries and foundations. This is the easiest way for you to donate to foundations that aim to make the world greener. You won't have to donate each of them separately, you won't have to give your credit card & personal information just because you want to support their cause. You will be donating and supporting such foundations with just clicks and without having to share your personal information.

RAMPANT SPECS

COIN NAME	Rampant
TICKER	RCO
COIN TYPE	POS-POW-MN
BLOCK TIME	90 seconds
MAX SUPPLY	28.000.000
PREMINE COIN	2%
MINIMUM STAKE	6 Hours
ALGO	C11
DIFFICULTY RETARGETING	Dark Gravity Wave

INSTANTX	4500
LAST POW BLOCK	250000th Block
FIRST POS BLOCK	1001th Block
BLOCK REWARD	50 Coins
BLOCK SIZE	3 MB
COIN MATURITY	90 Blocks
MN COLLATERAL	5000 coins

PREMINE

Premine will be used for helping Rampant Coin's needs such as maintenance, listings on exchanges, to develop web wallet, Android/IOS wallets and much more which is listed on the roadmap. For that we think %2 will be enough.

CONSENSUS

Rampant is a cryptocurrency, like Bitcoin—In fact we have made it as similar to Bitcoin as possible. Because, from consensus view, Bitcoin totally nailed it.

Currently with the craze of Ethereum's ERC20 ICO tokens for example, along with a whole host of other crypto projects, they are unable to do anything like Bitcoin in perspective of mass adaption.

SO WHAT DOES IT MEAN TO BE LIKE BITCOIN?

Proof of Work—the basis of the network—or more specifically, the cryptographic creation of tokens derived from real time activity on a network, shared out automatically by an integral algorithm to all participants of that network proportionately to their contribution to its operation (breathe) is a process so unique and complex that it rewrote the rulebook of international finance.

The distributed ledger that is the Bitcoin blockchain was designed to be unstoppable by any entity—government, corporation or even groups of both.

WHAT IS MASTERNODE

Masternodes, once unique to the Dash network, are full nodes. A masternode is a server connected to the network which guarantees a certain minimum level of performance and functionality to perform certain tasks. Using a concept known as Proof of Service, Masternodes in addition to the Proof of Work done by miners build up the two-tier network. Since the masternodes provide crucial services to the network. In fact, the entire network is overseen by the masternodes, which have the power to reject improperly formed blocks from miners. If a miner tried to take the entire block reward for themselves or tried to run an old version of the Dash software, the masternode network would orphan that block, and it would not be added to the blockchain. Running a Masternode helps the network throughout, as there will always be a stable node, with multiple connections around the world, running. As a reward for hosting one of these Masternodes, RCO will be paid to your wallet on a recurrent basis.

Masternodes helps in stabilizing and increasing the value of a currency if the governance system is introduced. In Masternodes, the proposals can be made by any person unlike other coins who charge a proposal fee and this makes Masternode a favorite among investors.

After proposals are submitted, a vote is made by master node holders and proposal is voted in. The Masternode system utilizes people's competitiveness and creativity to get ideas of improving the coin. The best ideas are generated from proposals submitted by coin holders. These ideas improve the currency value which in turn increases the block reward. Investing in Masternode coins gives you the ability of not only being an investor, but part of the decision makers in shaping the coin advancement. Owning own gives a voice to an investor and makes it more than just money.

This is done through submitting proposals. The foundation of Masternodes is stable and has long term values at the core of the infrastructure.

REWARD TABLE

BLOCK	POW	POS	POS%	MN REWARD	MN(%)
1 to 10	560000	0	0	0	0
11 to 200	5	0	0	0	0
201 to 400	15	0	0	0	0
401 to 700	20	0	0	0	0
701 to 1000	25	0	0	0	0
1001 to 250000	10	10	25%	30	75%
250001 to 500000	0	10	20%	40	80%
>500000	0	5	25%	15	75%

We are trying to give everyone a fair start by keeping POW rewards high till block 1000. After block 1000 Masternode payments will start. We are going to stop POW Consensus after block 250.000 and we will lower rewards after block 500.000.

ROADMAP

Q2 2018

Listing on CryptoBridge Exchange and masternodes.online ranking website. Start developing Ecologic Governance. Release Android and Ios Wallets.

Q3 2018

Contacting various tree nurseries around the world for inviting them to use Rampant Coin as payment method. Listing on Coinexchange.

Q4 2018

Contacting ecologic foundations for coordination, cooperation. Release Ecologic Governance model for Masternodes.

Q1 2019

Team expansion and reveal. Growing first Rampant Coin forest on location decided by Ecologic Governance. Listing on Cryptopia.

TECHNICAL DETAILS

DARKSEND / PRIVATESEND

PrivateSend is a novel, decentralized mixer for creating an on-demand system of removing the history from coins on the network. This is mainly for fungiblity, which is the attribute of money that allows any token to be exchanged with any other token, without having a difference in price in the form of a premium for tokens with less or no history. Without PrivateSend, tokens with less history would become increasingly valuable as the network grows, because of their lack of association with prior transactions. Without fungibility, there is a risk that certain tokens could be “red listed” and lose some or all of their value if at any point in the past they had been found to be used in illegal or questionable activities. Nobody wants to hold money that was involved in illegal activity, yet after the activities take place, tokens re-enter the supply and pass to new users who had no connection with the prior illegal acts. We remove this issue with the implementation of PrivateSend, which is included as part of the core protocol of the Dash network.

PRIVATESEND STATUS CODES

The system has various modes which allow servers to keep track of the current state of their mixing pool. These mixingpools are single use, allowing three people to use them at a time. Statuses

are idle, queued, accepting_entries, finalizing_transaction, signing_transaction and transmitting transaction.

Users begin by connecting to a node, which is in the idle state. The masternode then moves the status to “queued” and issues a message to the network, telling other users that’s it’s currently available for mixing. Users can utilize multiple servers at a time to mix, what is called multi-session mixing. This greatly speeds up the mixing process at the cost of creating more addresses and thus requiring more frequent wallet backups.

PRIVACY THROUGH AMBIGUITY

Mixing is the process of joining multiple transactions together, from multiple users, where all unique information about the users is removed from the transaction. Users send tokens to themselves through the system, and at no time do these tokens ever leave the users’ wallet. Masternode operators are therefore completely separate from the process of mixing.

Masternodes simply serve as a transit method for the storing and signing of transactions, allowing users a safe place to initiate the process in an anonymous way.

Privacy is achieved by using denominated amounts of 10, 1, 0.1 or 0.01. Each session initiated on a masternode only carries a single denomination, such as having 10x 10D inputs and 10x

10D outputs. Users then individually sign their inputs to the collective outputs, allowing the transaction to be valid once complete and broadcastable.

FEE MODEL ANONYMITY

In other implementations of mixing software, fees can be used to break the transactions apart and identify users on the networks. On the Dash Network this is avoided by allowing masternodes a special type of message which allows them to broadcast fee-less transactions. We use this technology to decouple the fees from the transactions, so that for every 10 transactions using the PrivateSend technology, there is only one fee transaction. This prevents a timing attack on the PrivateSend implementation.

PHASES OF PRIVATESEND

The process begins when a user denominates some funds to be used as a "cash account," then they simply tell a random masternode they would like to mix a specific denomination such as 100D. The masternode has no information about the transaction at this point, since the denomination carries no information about which inputs the user would ultimately like to mix.

The masternode receives the request and issues a message to the network saying that it is ready to mix that denomination and that there is a user waiting.

At this point if other users are wishing to mix inputs of that denomination, they can connect to the masternode that is hosting the other user's transaction. When three users queue themselves on the same masternode, the next stage, "accepting_ entries," is initiated.

In this stage, all users send their inputs and outputs to the masternode, where they are collected and put into memory until all users have identified the full list of inputs/outputs they would like to mix. Once this is complete, the process moves onto the next stage, "finalize."

At this point, the masternode sends a message back to the users, showing the merged transaction they all jointly created.
All inputs are from the user's wallet and all outputs are sent back directly to the user's wallet. The funds involved in this process never leave the user's wallet at any time, allowing the masternode to be completely segregated from users' funds.
This is how the process of PrivateSend remains trustless and secure, without risking user's funds or exposing masternodes to excessive legal risk. Once the finalized transaction is approved, the process moves onto the next phase, "signing."

Users sign only the inputs for which they have keys, and the funds are then released to all outputs simultaneously. It's worth noting that inputs and outputs are not directly tied to each other in this process, since inputs are in a separated list and only tied

to each other. Outputs are also in a separated list, only tied to each other. This means, literally, that all users are paying all users in this process. The users are not only paying themselves, but everyone else. This means you can't say input #4 went to output #14 (e.g. you can't trace the input to the output, they are processed in concert). When all inputs are signed to all outputs, the transaction suddenly becomes valid, and the masternode broadcasts using a special message called DSTX. The network keeps track of these messages, allowing masternodes to submit one PrivateSend transaction every N hours without paying fees.

C11 ALGORITHM AND DIFFERENCES BETWEEN C11 AND X11

X11

Algorithm X11 is a widely used hashing algorithm created by Dash core developer Evan Duffield. X11's chained hashing algorithm utilizes a sequence of eleven scientific hashing algorithms for the proof-ofwork. This is so that the processing distribution is fair and coins will be distributed in much the same way Bitcoin's were originally. X11 was intended to make ASICs much more difficult to create, thus giving the currency plenty of time to develop before mining centralization became a threat. This approach was largely successful; as of early 2016, ASICs for X11 now exist and comprise a significant portion of the network hashrate, but have not resulted in the level of centralization present in Bitcoin. X11 is the name of the chained proof-of-work (PoW) algorithm that was introduced in Dash

(launched January 2014 as “Xcoin”). It was partially inspired by the chained-hashing approach of Quark, adding further “depth” and complexity by increasing the number of hashes, yet it differs from Quark in that the rounds of hashes are determined a priori instead of having some hashes being randomly picked.

The X11 algorithm uses multiple rounds of 11 different hashes (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo), thus making it one of the safest and more sophisticated cryptographic hashes in use by modern cryptocurrencies. The name X11 is not related to the open source GUI server that provides a graphical interface to unix/ linux users.

C11

C11 uses an algorithm similar to X11 with 11 hashes, but in a different order. Often overlooked and used rarely C11 is an alternative solution against mining rentals. By thus making it possible for everyone to mine fairly. That is why we have chosen C11 algorithm for Rampant Coin. We hope that it will provide a fair mining experience for those who are interested in Rampant Coin.

CONCLUSION

Rampant coin aims to be a successful ecologic sanctuary for those who share the same dream with us; Greener future. Teaming up and acting together with ecologic foundations will allow us to cooperate against deforestation. With Ecologic Governance Rampant Masternode owners will be able to take action by theirselves and grow their own trees. Project Rampant will work hard on sowing the “seeds for future”!