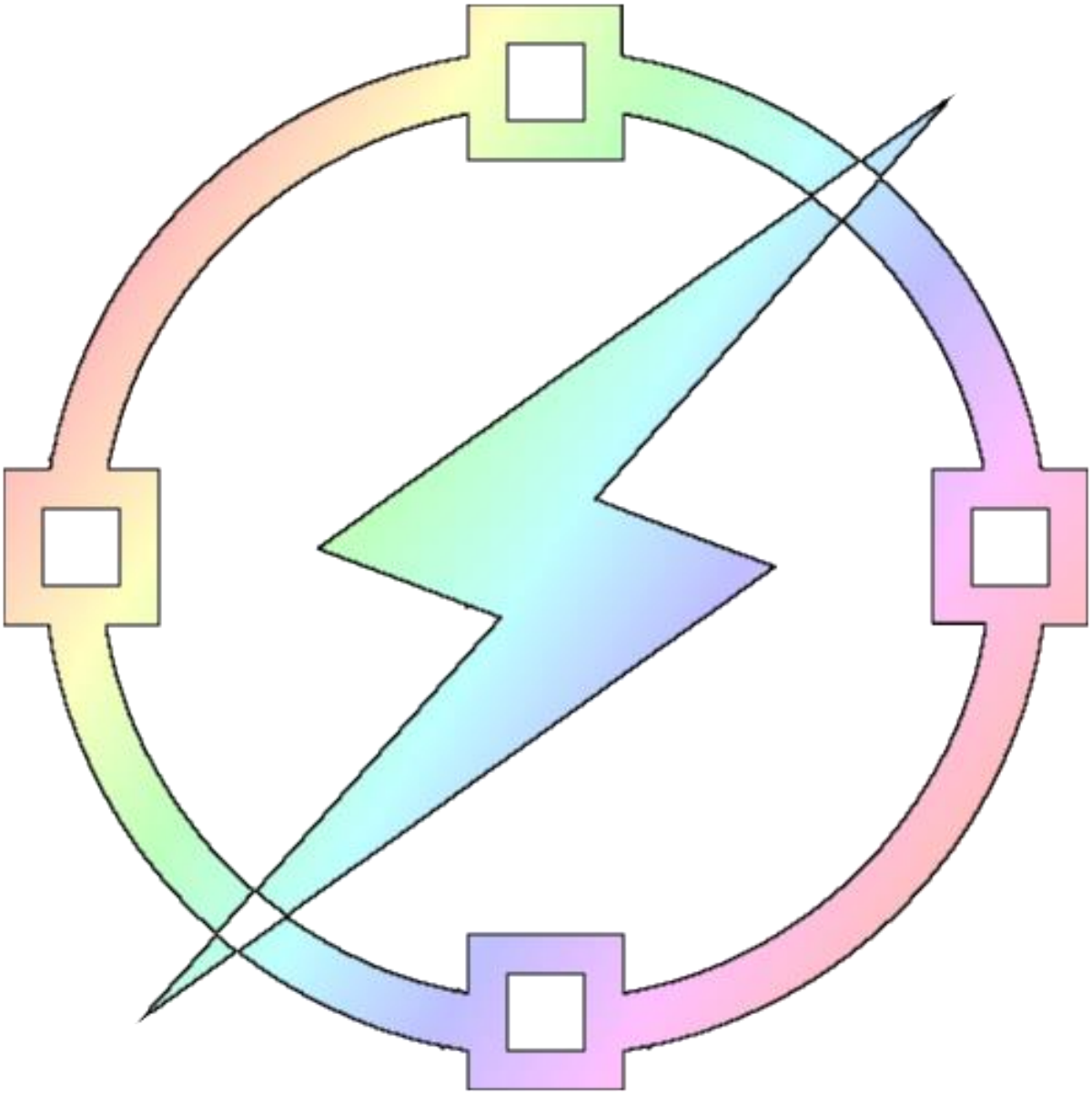

Cache – Privacy-Focused Decentralized Finance

The White Paper

December 2020
The Cache Core Team

TABLE OF CONTENTS

INTRODUCTION

The motivation behind the Cache project is simple: There are an estimated 2 billion people who currently lack access to financial services (Financial Team, 2019). Although existing infrastructure has been instrumental in generating wealth, truly little has ended up going to this excluded population. This will be an evolving document as Cache continues to address this disparity. **A special thanks to our contributors from the DigitalNote, Karbo, and Conceal Projects.**

SUMMARY

Decentralization means that there is not a single point of failure, as identical records are kept across computers located globally through a peer-to-peer network. Because Cache is a permissionless blockchain it is also open to anyone — irrespective of their wealth or where they live. And, whereas a bank or a payment processing company can close the account of a prejudiced customer, blockchains are censorship-resistant (Balut, 2020).

With Cache, the focus is on privacy and the opportunity to grow wealth universally. The consensus process is balanced out by a hybrid PoW/PoS algorithm, pairing the advantages of each process to create a secure platform. This makes the system less prone to double-spend attacks and improving overall security. The computational efficiency of the Cache network is powered by keycode design features like forward and backward compatibility, component-based modular structure, and asynchronous core architecture.

The transactions on the Cache network are untraceable with ring signatures and stealth addresses. Transactional data is stored on the blockchain allowing access exclusively by private keys owners, and none of the private data is ever publicly published. The confidentiality of all Cache transactions is hardcoded into the core. As there is concealment and privacy enabled by the technology fungibility is ensured in the Cache network.

Extensive testing of the Cache system has addressed the issues frequently encountered in the early days of a blockchain project. This made the Cache network stable and release-ready from day one on November 20, 2020.

Banking functionality in Cache not only provides a financial service, it is implemented as a method of funding continued maintenance and development of the Cache vision.

ABOUT CACHE

Cache aims to study the best practices of the fiat world and work towards developing products to be user-friendly for people.

Cache acknowledges the projects and technology it builds upon. Cache has a vision to forward development of these great projects and facilitate sustainable adoption by the masses.

The Cache team is a worldwide-based entity of members dedicated to creating and assisting new means of use for digital economics in real-world situations.

The Cache Core Team provides guidance and initial investment of resources with a view to become redundant when effective community self-governance is achieved.

The Cache vision is of a sustainable jobs ecosystem where contributors are remunerated and incentivized to achieve Cache Core Values.

Cache Core Values

Universally Accessible

The fact we have different currencies depending on what geolocation we are in is absurd. With no geo-restrictions... Cache can be used everywhere, by anyone.

Mimic Everyday Cash & Becoming a Medium for Daily Transactions

This is a vital feature if we want the project to succeed. Everyday cash is fungible so therefore Bitcoin and Fiat are not the same. Privacy should not be an option.

Create stable jobs

Jobs are not safe in this modern age depending on who we work for and where we work. I want the project to give anyone a chance to earn a stable income by working for the project and get paid to do so.

Decentralized finance (aka DeFi)

The whole purpose of cryptographic currencies was to defeat the object of banks and what they represent. Cache has on-chain, private, legitimate financial features which mimics banks, which truly defeats the object of them.

The Cache Plan

Emission, Block Reward starts at 3 then + 0.25 every 3 months until 5. This has been ratified by the general consensus of the Cache Community. From block 525,600 the Block Reward will remain static at 5 ongoing, unless altered by Community Governance via consensus of the Cache Community.

Premine is 15,000, 000 $CXCHE, 5% of total possible supply.

The Premine will be regarded as split 60/40 between the Foundation Fund (a 3% Premine of 9 million $CXCHE) and the Community Governance Fund (a 2% Premine of 6 million $CXCHE).

The Foundation Fund will be managed by the Cache Core Team. The Core Team will respect the values of Cache and consensus within the Cache Community as they are part of the Cache Jobs ecosystem and therefore incentivized to act in the interest of Cache. Its function is to guide the development of Cache interim to effective Community Governance. The Core Team will be as transparent as possible and respond to any general consensus of Cache Community feedback or query.

The Foundation Fund will determine and pay all Cache wages, interim to transferring this function to Community Governance.

Foundation Fund will Bank half of its allocation (4.5 million) for 12 months repeated annually until Community Governance absorbs The Foundation. This will sustain a monthly budget delegation to fund Cache wages in the Cache Jobs Ecosystem, bounties etc.
Unspent funds in the monthly budget will remain with Foundation Fund.

The Foundation may transfer funds to the Community Governance Fund at any time. This allows for earlier start of Community Governance if in place and effective before 12 months.
The Foundation may use excess funds to pursue informal action consensus of the Cache Community.
When formal Community Governance is in place said governance may elect to absorb the Foundation and proceed Cache as entirely Community Governed if Cache Sustainable Jobs model is continued by design.

Community Governance Fund will Bank all 6 million $CXCHE allocation for 12 months to allow time for Community Governance to be established effectively.

Both funds will repeat banking each 12 months to sustain Cache and interest earned will be used to fund Cache vision.

With 10.5 M of 15 M Premine (70%) banked it is effectively not “dump-able” during exchange launches. This can be considered a Premine of only 1.5% (4.5 M). The 4.5 M allocation is liquid for the Foundation to develop Cache — marketing, exchange fees etc.

The Core Team will make available view keys for any addresses related to the Premine, the Foundation, and Community Governance.

The Core Team will commit to the above plan incentivized by their own roles in the Cache Sustainable Jobs Ecosystem.

SPECIFICATIONS

Attribute	*Value*	*Description*
Supply	300M	The total supply of the Blockchain should be a high figure to support longevity.
Premine	5%	The premine is divide into a Foundation Fund 3% and a Governance Fund 2%
Block Reward	3.00000 increasing to 5.00000 over ~ 2 years	The Block Reward should be low in amount to counteract the high total supply of the Blockchain. A Low Block Reward enhances intrinsic value
Block Time	120 seconds average	Average time taken for a block to be mined. This is controlled by Difficulty Algorithm.
Emission Rate	+0.25 every ~3 months (90days) until 5.00000 then static at 5.00000	A slowly increasing Block Reward overtime. This is a better option for new users who miss out on the initial FOMO of the project and encourages miners to mine as the block reward is not getting unfairly small such that the reward for smaller miners is miniscule.
Banking Term	1-month minimum 1-year maximum Minimum deposit 1 **$CXCHE**	To make things easy when it comes to banking, caps are in place to mimic real-life banking systems. Users can start gaining interest with as little as 1 full coin.
Interest Rate	0.408% - 8%	Tiered system mimics real-world banking
Fee	0.001 minimum - static	To save congestion on the Blockchain, there needs to be a reasonable fee. A dynamic fee may be implemented in the future.
Decimals	5	Large decimal places are usually harder for users to work with. Keeping decimals limited will help average users manage their funds better.

Hashing Algorithm	Cryptonight/Cache_Hash	Cache Hash is a newly modified hashing algorithm to resist ASIC and FPGA.

TECHNICAL ISSUES AND SOLUTIONS

$CXCHE Fungibility

"Fungibility is the property of a good or a commodity whose individual units are essentially interchangeable" (Bartram, 2020). Bitcoins are not fully fungible. Any two bitcoins have the same exact value. But because all transactions are publicly available, it is common for bitcoin exchanges to discriminate between bitcoins based on the owner or their history. For example, some exchanges will attempt to block bitcoins, which have been confirmed as stolen or obtained illegally. This becomes an issue because when not every exchange accepts the so-called "dirty" bitcoins, the "dirty" bitcoins become less valuable.

The fungibility and privacy problem is solved in **$CXCHE** by CryptoNote protocol.

Transactions in **$CXCHE** are untraceable and un-linkable. **$CXCHE** provides anonymity and privacy using cryptographic technology of ring signatures. All transactions are signed on behalf of a group so that it is impossible to determine who exactly from the group signed the transaction and, accordingly, one cannot say with certainty who carried out the payment. "The more participants in the group, the more confidential the operation is". In addition, the transactions cannot be associated, – even if outgoing transactions are untraceable, everyone may still be able to see the transactions you have received. However, by using a variation of the Diffie-Hellman exchange protocol, a receiver has multiple unique one-time addresses derived from his single public key. After funds are sent to these addresses they can only be redeemed by the receiver and it would be impossible to cross-link these transactions.

Unique one-time addresses and ring signatures of transactions are providing resistance to blockchain analysis. Every transaction only increases entropy and creates additional obstacles for those who wish to dig into financial operations with **$CXCHE**. Resistance to the analysis, in turn, provides an especially important characteristic inherent in real **$CXCHE** money, – fungibility. Fungibility of money means that all units of one denomination have the same purchasing power.

Difficulty Algorithm

"The problem of hash rate instability has been well known for many years in the altcoin community. Multipool mining, where miners could quickly switch between mining coins with compatible Proof of Work algorithms, led to hash rate oscillation and instability. This rapidly switching hash power would often lead to unpredictable confirmation times, and long periods with slow blocks. There were also more serious problems when coins had widely divergent market values, which could leave the smaller coin vulnerable to miners gaming of the difficulty algorithm, and manipulating timestamps" (Mengerian, 2017).

In 2016 Karbo mitigated to some extent this problem by changing the default CryptoNote difficulty algorithm to the one proposed by Scott Roberts called “Zawy difficulty algorithm” (Karbo Project, 2018). The author of the difficulty algorithm developed a better version of his algorithm and it is proposed to update the difficulty algorithm to one of his newest versions: “LWMA (WHM)” or “The Simple DA” for better protection against hash rate attacks. The LWMA (WHM) algorithm was implemented after the attack in which vulnerabilities of the previous version were exploited. To mitigate part of other mentioned threats one solution that is considered is to change the POW algorithm. One of the possible solutions against hash rate attacks, which are mostly conducted by renting hashing power on the Nicehash and similar services, is to change the POW hashing algorithm to make it incompatible with Nicehash and thus remove from multipool hoppers the possibility to switch to **$CXCHE** when it is profitable for them. The second reason is the threat of ASICs developed for the CryptoNight algorithm. ASICs cause undesired centralization of mining and hashing power. On the other hand, ASICs provide a large hash rate that is the best protection against attacks on POW based coins. Cache considers accessibility of mining the priority and has a modified hashing algorithm to resist centralization to only those that can afford ASICs (Karbo Project, 2018).

Blockchain Monetary Deposits with Interest Rates

You can safely deposit your Cache with some interest rate. In general, it allows users to “lock” some of their **$CXCHE** for a while (from 1 month to 1 year) to earn interest and increase $CXCHE holding. If a user choses funds can be withdrawn after lock time and will become part of Cache liquid supply this extends Karbo Project, 2018. Longer periods give users a bigger interest rate. Deposits are implemented via new types of transaction output/outputs. It includes amount, destination key (or keys), and time (expressed in blocks) to lock. Transaction itself contains the field unlock time but output-specific parameters are much convenient, because users may want to send some money back as change (and surely do not want them to be locked). The transaction is included in the blockchain as usual and the counter starts. When the lock expires users can spend this output as usual, but the new transaction volume will be increased with the interest (XDN Project, 2016). For example, if a user deposits 1000 **$CXCHE** for 1 month an annual interest rate will be about 0.41%. This is broken up into 5 tiers: <5k, 5-10k, 10-15k, 15-20k, >20k (Maricopa Association of Government, 2003). It also means that deposits act as a source of emission. Cache multi-signature core feature enables a common ownership for any **$CXCHE** units and deposits. A family can store their **$CXCHE** savings in N-of-N deposits, which means that only all members together can withdraw the money. A company can keep its capital in M-of-N address, which is redeemable only by at least M members out of N. Interest rate depends on deposit time and varies from 1 month to 1 year. The latter case is the most profitable (gives users maximum possible profit — 8% of their deposit) (XDN Project, 2016).

Banking Level	***Tier 1***	***Tier 2***	***Tier 3***	***Tier 4***	***Tier 5***
Principal	Under 5,000	5,000 - 9,999	10,000 - 14,999	15,000 - 19,999	Over 20,000

Minimum Interest	0.41%	0.45%	0.49%	0.53%	0.57%
Maximum Interest	6.00%	6.50%	7.00%	7.50%	8.00%

Crypto Assets Intrinsic Value

"Everyone can create money; the problem is to get it accepted"

Hyman Minsky, an American economist the target of stable coin design requires that this crypto asset has a certain intrinsic value. Without this value, it is possible to build a stable coin only with exogenous factors involved. In other words, manually managing its value by market interventions. There is not the only opinion regarding whether crypto assets have their own intrinsic value or not. Some authors claim that crypto assets do not have any intrinsic value. Some authors on the other hand speak about this value represented by mining infrastructure. Proof of Work (PoW) algorithm is usually criticized for excessive waste of energy on the one hand and it is postulated that crypto assets based on PoW consensus do not have intrinsic value on the other. "The criticism stems from the belief that Bitcoin violates Mise's regression theorem of money because it is not backed by a commodity." However, mining infrastructure consuming megawatts of electricity which is a commodity and if we accept the fact that it represents the intrinsic value of a particular crypto asset then we admit that mining infrastructure actually represents this commodity backing, and energy spent on mining represents the real value of such an asset. The more real-world resources we attract for mining the higher is crypto asset capitalization. One can say that cryptocurrency is backed by the energy spent on its mining.

"Bitcoin production seems to resemble a competitive market, so in theory, miners will produce until their marginal costs equal their marginal product. Break-even points are modeled for market price, energy cost, efficiency, and difficulty to produce. The cost of production price may represent a theoretical value around which market prices tend to gravitate. It seems to be the case that the marginal cost of bitcoin production matters in value formation. Instead of approaching bitcoin as a digital money or currency, it is perhaps more appropriate to consider it a virtual commodity with a competitive market of producers."

Any mineable crypto asset has a so-called positive feedback loop, which means that when the price of a crypto asset decreases or block reward is decreasing, "mining" becomes less profitable and some "miners'' will be forced out of business. When there are less miners, the network automatically adjusts to decrease the difficulty of the cryptographic problems and therefore makes "mining" profitable again. In other words, proof of work mineable crypto assets are designed to make "mining" barely profitable on average. The main idea of those who believe in crypto-asset intrinsic value is based on production or mining being a competitive process that represents the value that we are looking for. In that sense, we can call **$CXCHE** and any other mineable crypto asset a commodity money backed by electricity and hardware expenditure consumed for network support. This approach will let us find endogenous factors or data from the blockchain to first estimate and then keep crypto asset value stable over time without relying on any third party or exogenous impact. This is the key

point in building such a system because any third party involved in a process could be compromised and/or hacked over time. Previous works like Ferdinando M. Ametrano's proposal relied on some exogenous commodity indexes consisting of crude oil and wheat, but we think that it makes sense to peg a crypto asset to electric energy as a commodity stable in its value. Difficulty represents this energy spent on mining and therefore, from our point of view, the difficulty is an endogenous factor which in the best way reflects crypto-asset intrinsic value. Difficulty gives us a real estimate of mining efforts expressed in electric energy and hardware commodity costs spent in the real world on our crypto asset network support and emission. Scott Roberts in his blog proposes a solution to how to use blockchain data to determine the coin price being outside, real-world parameter: "Difficulty is exactly proportional to network hash rate, and network hash rate is closely proportional to coin price". Our solution is based on his work, which finds confirmation by the research of Vitalik Buterin, published in his blog post, where he describes methods of the decentralized measurement problem. According to Buterin, there are two known major classes of solutions: exogenous solutions, mechanisms that try to measure the price concerning some precise index from the outside, and endogenous solutions, mechanisms that try to use internal variables of the network to measure price. We chose a second method which was independently discovered and described by Scott Roberts.

The research of Vitalik Buterin confirms Scott Robert's idea: to measure the price of a currency endogenously, what we essentially need is to find some service inside the network that is known to have a roughly stable real value price and measure the price of that service inside the network, as measured in the network's own token.

Examples of such services include:

- Computation (measured via mining difficulty)
- Transaction fees
- Data storage
- Bandwidth provision

A slightly different, but related, strategy is to measure some statistic that correlates indirectly with price, usually a metric of the level of usage; one example of this is transaction volume. Statistical methods, however, are prone to be manipulated therefore we will not use them. Aside from manipulations, "...the problem with all of these metrics is, however, that none of them are very robust against rapid changes due to technological innovation" he adds. Therefore, we must include Moore's Law compensation. As Buterin states, "difficulty is a function of both price and Moore's law, and so it gives results that depart from any accurate measure of the price exponentially over time." "The first immediate strategy to fix this problem is to try to compensate for Moore's law, using the difficulty but artificially reducing the price by some constant per day to counteract the expected speed of technological progress; we'll call this the compensated naive estimator". Having determined the leading factor influencing crypto assets, we can proceed with an attempt to estimate the crypto assets fair value, for which we take as a basis the suggestions of Scott Roberts. The basis for his approach is the assumption of a relationship between the crypto asset price and the mining cost, ideally energy costs. The equation is valid for the PoW (Proof of Work) mining algorithm:

P1 * R1 / D1 * L1 = P2 * R2 / (D2 / M) * L2 (1)

where, 1 and 2= moments in time 1 (now) and 2 (future); P = USD price per crypto-asset unit; R = reward, crypto-assets units per block; D = PoW mining difficulty; M = Moore's Law adjustment which represents the reflective change over time in the mining equipment productivity (H/s), is calculated as 2^n, where n is the number of doubling productivity periods; L = loss factor, equal to the estimated volume of lost crypto assets units due to private keys loss. Coefficient 1 means that 100% of crypto-asset units are available, a coefficient of 0.75 means that every fourth unit of crypto assets is unavailable due to the private keys lost. If hash power is not able to keep up with coin price (which is a temporary effect), the value would be larger than expected. Otherwise, the real-world value slowly decreases as hashing efficiency increases, which may be a desired effect if it is for dev fees because software gets outdated. But Moore's Law has become slow for computers. Hashing should get closer to being a constant hardware cost per hash. Also, electricity is more than half the current cost of hashing and could soon be 3/4 or more of the cost. Worldwide electricity cost is very stable and possibly the best single-commodity measure of constant value. The same equation can be rewritten simpler:

P1 * R1 / E1 * L1 = P2 * R2 / E2 * L2 (2)

where E = mining electricity consumption in kWh. Now we rewrite the equation having in mind that P1 = P2 to define R2 (next reward for the block): R2 = R1 * (D2 / M) / D1 * L1 / L2 (3) The logic that determines the next block reward is as follows: R1 = previous block reward; (D2 / M) / D1 = increase in complexity, that is, an increase in the mining capacity leads to an increase in the crypto asset price, taking into account the Moore's Law adjustment; L1 / L2 = over time, an increasing number of crypto assets units are lost due to the loss of the private keys, a reduction in the issuance of crypto assets in this way increases its price. We must mention that this equation gives crypto-asset fair price estimates and does not consider the speculative component, the so-called "pumps and dumps".

Encrypted Messages

Imagine, an encrypted untraceable messaging platform where even the fact of message sending is unknown, only the recipient can decrypt his message and the message can be stored in blockchain forever. Cryptocurrency is about digital money and how the money flows between parties. However bare transfers are sometimes just inconvenient, the payee needs to get some additional information from the payer, like secret text messages. For example, an online store supports a "money-back feature", and its customer should be able to attach a refund address to their transaction. Alternatively, if a user makes donations they may want to specify how their funds should be distributed between all possible charities (just like Humble Bundle allows you to divide your purchase between games' developers). The urgency of this feature is supported by the fact that some cryptocurrencies have already implemented it: Bitcoin, Florin, Cosmos coin etc. But their developers did not attend to the convenience of private communication. Whilst there is no problem with attaching a plain-text message, it is tricky to provide an easy-to-use way of handling secret data. Both parties can share some symmetric private key and use it for encrypting and decrypting messages. But this method is only suitable for a long-time communication and/or repeated transactions. Another way: they

can use a public-key encryption scheme, but such algorithms are less effective in the case of arbitrary-length messages (when compared with symmetric crypto). We propose a protocol for transferring encrypted messages within transactions, which does not require any preliminary data exchange. Also, it is based on the modern symmetric stream cipher — ChaCha20 — and results in excellent performance.

The Protocol

We now describe step-by-step the protocol for encrypting and decrypting a message. The message is being sent from Alice to Bob.

Scheme
Alice generates common secret via Diffie-Hellman key exchange protocol in the same CryptoNote one-time keys are generated.
She encrypts her message under this key and sends the transaction.
Bob re-generates the common secret, just like he recovers CryptoNote outputs private keys.
He tries to decrypt all available messages in the transaction and determines (via a checksum) those which were sent to him.

Encryption
Let (A, B) be Bob's Cache address and H() to be the cryptographic hash function Keccak. Alice generates a random value r and computes the common secret $x = H(r \cdot B)$. Additionally, she stores $R = r \cdot G$. Then Alice takes the plain-text message M and adds four zero bytes at the end. The motivation of this step will be shown later. After that, she uses x as a key for stream cipher ChaCha20 and gets a pseudo-random bit sequence S. The resulting encrypted message is $E = M \oplus S$. It is stored in the transaction along with R.

Decryption
Bob receives the transaction and re-generates the common secret as $x = H(b \cdot R)$. With x he recovers the same sequence S. Then for every encrypted message Ei he computes $Mi = Ei \oplus S$. Mi which has the last four bytes zeroed indicated they were sent to him: i.e., decrypted correctly. The others may belong to other recipients of the transaction or even be Alice's comments for herself.

Separate Messages

Our solution does not rely on any output properties: payee, amount, any other content. That means that transaction comments may be used separately with money transfer: i.e., like just private messages (without payments). Alice can send many messages to different addresses in a single transaction which sends some funds to each). Due to CryptoNote's un-linkable one-time keys no one can prove that there was or was not money transfer at all: i.e., private message via transaction is indistinguishable from ordinary transactions. Cache can serve as a service of private encrypted communication, as well as secure money transfers.

CONCLUSION

- **Cache** is unique in the contemporary blockchain sphere in having not only addressed significant technical issues but also attended to project sustainability including infrastructure and ongoing development resources.

- **Cache** has provided a solution to project sustainability by incentivizing from the blockchain itself continued input from developers and contributors. This is achieved by banking the prime within Cache banking functionality itself providing interest earnings ongoing to sustain the Cache Jobs Ecosystem with remuneration to contributors. Developers and contributors have a vested interest in Cache, its development, future support, maintenance, and evolution. This makes Cache resilient.

- **Cache** provides Defi privacy whilst at the same time enabling a support community oriented to self-governance. Its “un-owned” nature enacts the very principle of decentralized.

- **Cache** self-funding infrastructure provides stability to its blockchain. This also provides scalability.

- **Cache** builds upon proven and accepted technologies and provides a sustainable way to forward development. Many other good blockchain projects technologies have development thwarted because of a lack of focus on a sustainable funding model. Cache by design provides a sustainable solution.

- **Cache** by providing a sustainable jobs ecosystem enables contributors to apply skills and be adequately remunerated ongoing. A well skilled international team has been established to develop Cache.

- **Cache** allows anyone anywhere to participate without the disadvantage of not being an early adopter. No FOMO, no developer “dumps”, simply engage in Cache and its benefits.

- **Cache** is an alternative to cash and exhibits the same qualities of being a means of exchange and a storage of wealth. Fungibility of Cache is provided without a particular sovereign government authority, currency manipulation or ability to print money.

- **Cache** transactions cannot be censored by any participant or a government bureaucracy, or by Cache’s own community governance. This enables all users to participate in the benefits of Cache with immunity from nefarious acts. Cache is a financial system for a worldwide community governed by a worldwide community. It is not discriminatory, political or location based.

Most projects fail because they lack sufficient financial resources to run, at scale, and the needed technological resources for the project. Cache has been planned to create and utilize a modest Premine to fund essential ongoing work and base resources for several years. Locking the Premine in the interest-earning Cache banking facility supports the concept of a

stable income for Cache core developers and project contributors. Some funds will also be used to market the project to potential new users. The Premine is documented and available public information to allow users to login to a view-only version of the Premine wallet.

Disclaimer

This *White Paper* is for informational purposes only, and not a binding commitment Cache by nature is developing dynamically. Do not rely on this information when interacting with **$CXCHE** coins as ultimately the development and timing remains at the discretion of the Cache Team, the Cache Community, and ultimately Cache Community Governance. We, the Cache Team, intend in no way harm of any kind to anyone in any shape or form. There has never been a crowd sale of coins, presale, or any other crowdfunding method used for the Cache project or its developers. The Premine itself is committed to locking and tasks beyond the access of the Cache Team. Please understand the risks involved with cryptographic blockchain technology and their respective coins. The Cache Team cannot be held responsible for any lost, stolen, or otherwise missing funds of any kind. If you are unsure or have any doubt about this project, we urge you to NOT invest or become involved as this is a developing technology and only engage at your own risk after your own research.

REFERENCES

Admin. (2020, August 10). What is Blockchain example? Retrieved December 30, 2020, from https://www2.ict.ufvjm.edu.br/index.php/2020/08/10/how-where-to-buy-dragonchain/

Balut, S. (2020, February 07). Decentralized Finance (DeFi) as a monetary system. Retrieved December 30, 2020, from https://medium.com/zoidcoin-network/decentralized-finance-defi-as-a-monetary-system-3055c920c5d7

Bartram, S. M. (2020, December 03). Fungibility. Retrieved December 30, 2020, from https://en.wikipedia.org/wiki/Fungibility

Conway, L. (2020, November 18). Blockchain Explained. Retrieved December 30, 2020, from https://www.investopedia.com/terms/b/blockchain.asp

Fairweather, L. (2020, October 26). The Problems That Ethereum 2.0 Proof-of-Stake Aims to Solve. Retrieved December 30, 2020, from https://medium.com/better-programming/the-problems-that-ethereum-2-0-proof-of-stake-aims-to-solve-5361c155461a

Frankenfield, J. (2020, September 16). Proof of Stake (PoS). Retrieved December 30, 2020, from https://www.investopedia.com/terms/p/proof-stake-pos.asp

Hertig, A. (2020, December 17). What Is DeFi? Retrieved December 30, 2020, from https://www.coindesk.com/what-is-defi

Hong Kong Crypto Exchange Launches Hardware Wallet With Fingerprint Recognition WALLETS | Oct 14, & $25, B. (2020, April 08). How to Use Multisig to Keep Your Coins Ultra-Safe: Wallets Bitcoin News. Retrieved December 30, 2020, from https://news.bitcoin.com/how-to-use-multisig-to-keep-your-coins-ultra-safe/

Karbo Project. (2018, May 30). Karbo Whitepaper. Retrieved from https://karbovanets.org/whitepaper.pdf

Kenton, W. (2020, October 01). Bitcoin Mining Definition. Retrieved December 30, 2020, from https://www.investopedia.com/terms/b/bitcoin-mining.asp

Maricopa Association of Government. (2003, May 22). Regional Transportation Plan. Retrieved from http://azmag.gov/Portals/0/Documents/pdf/cms.resource/RTP-modeling-scenarios.pdf?ver=2003-05-16-110100-000

Mengerian. (2017, September 30). Bringing Stability to Bitcoin Cash Difficulty Adjustments. Retrieved December 30, 2020, from https://medium.com/@Mengerian/bringing-stability-to-bitcoin-cash-difficulty-adjustments-eae8def0efa4

Rasiklal, R. (2014, October 16). Explain Network Model. Retrieved December 30, 2020, from http://kalpeshrakholiya.blogspot.com/2014/10/explain-network-model.html

Team, M. (2019, June 20). 2 Billion People Don't Have Access to Formal Financial Services. Retrieved December 30, 2020, from https://gomedici.com/2-billion-people-dont-have-an-access-to-formal-financial-services

XDN Project. (2016, June 6). DigitalNote Whitepaper.

APPENDIX

Cache Resources

Cache Official Website: https://cxche.org

Cache Official Wallets: https://github.com/Cache-core/Cache/releases
https://github.com/Cache-core/Cache-Desktop/releases

Cache Official Blockchain Explorer: https://explorer.cxche.org

Cache Official GitHub Repository: https://github.com/Cache-core

Pool List: https://miningpoolstats.stream/cache (informal, official tba)

Guides: https://github.com/Cache-core/Guides/blob/master/README.md

API: https://github.com/Cache-core/Cache-api-js

Point of Sale Plugin: https://github.com/Cache-core/Cache-POS

Mobile wallet (WIP): https://github.com/Cache-core/Cache-Mobile

Cache Social Media

Discord: https://discord.gg/2eu4DqbyQX
Bitcointalk: https://bitcointalk.org/index.php?topic=5292068
Telegram: https://t.me/cxche
Chinese telegram: https://t.me/cxche_cn
Twitter: https://twitter.com/Cachecore
Medium: https://cxche.medium.com
Reddit: https://reddit.com/r/CXCHE

Timeline and Milestones

- **Cache Hash** Aug 20

To make sure there are no ASIC or FPGA machines mining Cache, we have taken the steps to modify a pre-existing algorithm to create what is essentially a new algorithm. There is also Mining & Pool software for this algorithm but not from its official base yet. The modified software is completely open-source, and it can be found on GitHub.

- **Testnet** Sep 20 - Nov 20

It is standard for any new network to undergo a test net stage before they initially launch a new Blockchain. This is to potentially fix any problems that may arise during the early blocks of the Blockchain. All the coins from the Testnet are worthless and in no way represent any sort of value, nor can they be swapped for the real, Mainnet asset.

- **Mainnet** Nov 20

After 22,000 blocks had been mined on the Testnet network, the Cache team and community felt confident about launching Cache's Mainnet asset. Cache was launched fairly on the 15th November 2020

- **Cache Mobile.** TBA

Giving you the ability to interact with the Cache Blockchain via mobile device.

- **Cache Web.** TBA

Giving you the ability to interact with the Cache Blockchain within a browser for quick access.

- **Multi-Sig Wallets.**TBA

Multi-signature, or multi-sig, is a wallet configuration that requires at least two keys to authorize a transaction. Commonly used by cryptocurrency exchanges to ensure funds cannot be moved by a rogue employee, multisig also has applications for end-users. A multisig wallet is a wallet shared by two or more users called copayers. Depending on the kind of wallet, the number of signatures required to sign a transaction will be lower or equal to the number of copayers of the wallet (Hong Kong Crypto Exchange Launches Hardware Wallet With Fingerprint Recognition WALLETS | Oct 14 & $25, 2020).

- **Hardware Wallet Support.** TBA

Hardware wallets are special types of wallets that make use of a secure hardware device to store a user's private keys. ... Users simply plug in their devices to any internet enabled device. They enter a pin, initiate a transaction, and then confirm to send the cryptocurrency.

- **Community Governance.** TBA

Community governance focuses on the power that communities exercise to achieve policy outcomes that suit their needs. To fund this, we will set aside part of the foundation fund each year. We then would deposit the funds set aside onto the Cache blockchain for a maximum of 1 year. Once the deposit has matured over 12 months, and the interest has been gained, then the reward would be split into the 2 funds equally. 50% back to the Foundation fund and 50% into the Governance fund.

- **Cache Social Platform.** TBA

The Cache developers have an idea to create a decentralized community social platform that can be accessed from any online machine. This platform may or may not be on-chain with Cache's blockchain but that's because decentralization is not solely blockchain-based.

- **Cache Card.** TBA

A bank card is typically a plastic card issued by a bank to its clients that performs one or more of several services that relate to giving the client access to the bank account. In our instance, we would be able to replace the usage of banks and any form of centralized entity. Your wallet, and only you, would have control of the assets on the card.

- **Cache ID.** TBA

Wallet addresses for Cache are formed using a random string of 99 letters and numbers, starting with **cxche**, and this can be hard to memorize. Cache ID would allow you to send a transfer to bob.cache.id instead of cxcheABC123..., making it even easier for normal users to send transactions.

Glossary

Addresses — A cryptographic location or account where units are stored in a blockchain. It comprises a public and a private key. A user with the private key has ownership and control of units stored at the address and may send them to another address.

Algorithm — It is a process or set of rules to be followed in calculations or other operations in a blockchain.

API — An Application Programming Interface exposes information in an application so that it is available or interaction with other applications.

ASIC— Application-Specific Integrated Circuit designed to do a specific task efficiently.

Asynchronous — It mathematically guarantees that consensus is eventually achieved even if an attacker controls almost a third of the network. Asynchronous in this context means that no assumptions are made about timing.

Blockchain — is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain (Admin, 2020).

Block — Blocks are data pertaining to the Cache network added to the blockchain and permanently recorded. A block is like a page of a ledger or record book. Each time a block is 'completed', it gives way to the next block in the blockchain. A block is thus a permanent store of records which, once written, cannot be altered or removed.

Block Reward — refers to the amount of **$CXCHE** produced with each new block accepted by blockchain consensus.

Block time — in the context of cryptocurrency, is a measure of the average time it takes to produce a new block (Kenton, 2020)**.**

Cipher —A mathematical function used in the encryption and decryption process.

Confirmations — A count of how many blocks have passed since a transaction was added to the blockchain. The more confirmations, the more secure the transaction.

Decryption— The process of retrieving information that has been encrypted.

DeFi — an abbreviation of "decentralized finance," This is an umbrella term for a variety of financial applications in cryptocurrency or blockchain geared toward disrupting financial intermediaries (Hertig, 2020).

Emission— A set of rules determining when coins are created and released as the blockchain lengthens over time.

Encryption — converting data into code that is only accessible with matching public and private keys.

Fiat— Currency that a government has declared to be legal tender (Like USD, EURO, PKR etc).

FOMO — a social anxiety phenomenon known as Fear Of Missing Out (McGinnis, 204)

FPGA — Field-Programmable Gate Array, an integrated circuit designed to be reconfigured to a task after manufacture.

Fungibility— all units are of the same value and interchangeable with each other without difference or prejudice.

Hash Rate — A hash rate in blockchain operations is defined as the number of hash operations done in each amount of time attempting to solve the mathematical challenge or the speed of a miner's performance.

Hybrid PoW/PoS — It is a hybrid algorithm in which both PoW and PoS algorithms are combined for more stability.

Mainnet — Mainnet is simply the main network of the blockchain, where actual transactions take place on a distributed ledger.

Mining — is a process of solving a mathematical challenge by computer to confirm or validate transactions over a blockchain network and produce blocks by consensus of the P2P network.

Mining Pools — are groups of miners who share their computational resources. Mining pools utilize these combined resources to strengthen the probability of finding a block.

Moore's Law— is the observation that the number of transistors in a dense integrated circuit (IC) doubles about every two years (Mead, 1975).

Peer to peer — a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. Simply a user-to-user network (Rasiklal, 2014).

Permissionless blockchain—A blockchain where anyone can participate in the network, also known as a public blockchain.

PoS — Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more coins owned by a miner, the more mining power he or she has (Frankenfield, 2020).

PoW — Proof-of-Work, or PoW, is the original consensus algorithm in a Blockchain network. In Blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded (Fairweather, 2020).

Premine — is the creation of an initial amount of cryptocurrency determined by the core code on block one. It is used to provide initial funding for the project but can be used nefariously (dumping) by unscrupulous project creators targeting quick profit. Cache treats the Premine in a different manner by locking the Premine within its banking system.

Private Key — A cryptographic key that allows a user ownership of the funds at a given address by facilitating decryption.

Protocol — The rules that govern a blockchain network are referred to as a protocol. It is essentially the common communication rules that the network plays by.

Public key— A public key is a cryptographic code that that represents an address on the blockchain. The possession of the matching private key allows decryption and ownership of funds sent to that address.

Ring signatures—a type of cryptographic signature in which it cannot be determined which key was used to produce the signature.

Signature — A cryptographic code used to prove ownership of a public key without exposing its private key.

Stealth addresses—a mechanism that uses a combination of various public and private keys that are dynamic and for one-time use only for the purpose of obscuring the public address of a transaction recipient (Todd, 2014).

Testnet — The testnet is an alternative blockchain used for testing. Testnet coins are distinct from actual coins, and testnet coins do not have any monetary value.

Wallet — A blockchain wallet is software that allows users to store and manage their **$CXCHE** securely and do other tasks on blockchain. It holds the private keys to addresses (Conway, 2020).