Crave Financial Privacy

Crave Core Team

Crave Project
crave.cc

June 12, 2018

Abstract

The decentralized payment system of Bitcoin offers a mechanism for recording monetary transactions in an append-only ledger, called a blockchain. A major limitation of this is that it's possible to trace the history of any payment, since transactions are stored in a public ledger. This data could serve as a link to identify users and transaction patterns. Commercial and academic work has shown that this linking of transaction history is simple to perform. In this paper, we present Crave - a decentralized payment system which corrects the security and privacy issues of Bitcoin

To begin, we give a brief overview of the issues in the Bitcoin protocol. This covers problems with anonymity, scalability, and energy inefficiency of the Proof-of-Work system. We then detail Crave, beginning with an overview and description of the anonymity, untraceability, unlinkability, and unforgeability characteristics. The scalability of Crave is addressed, as well as some advantages of its Proof-of-Stake system. Next, we move on to many of Crave's technological features, including masternodes, LightX instant transactions, and the budget & governance system. There is also information on the implementation of the Zerocoin Protocol. This is a blockchain-based protocol which breaks the link between an address that receives non-anonymous funds and the subsequent transaction that spends those funds. Finally, we end with the future work of Crave, along with developments on the 2018 calendar year roadmap.

I. Introduction

Contrary to some belief, Bitcoin transactions are not completely anonymous. Transaction history is public information, meaning that anyone can follow the addresses of users transacting on the blockchain.

Even though Bitcoin makes some tangible efforts to keep its transaction processing chains anonymous by using new public keys or hashes from time to time, a breach of its anonymity may still occur if a Bitcoin user participates in multi-input transactions. The user's activities can be traced through their addresses. Bitcoin has suffered some privacy breaches in the past - compromised through Bitcoin address reuse, web-spidering, IP address monitoring nodes, tainted Bitcoin payment and analysis methods, and through other processes.

This makes Bitcoin unappealing to users who desire strong and enduring privacy and anonymity.

i. Scalability

Bitcoin has a scalability issue that has remained unresolved, leading to forks and division among the community. This is because the current Bitcoin code base is very similar to the one that was created over nine years ago. The old Bitcoin ecosystem was constructed to handle a small block size, even as increasing number of transactions were conducted on the blockchain. This has resulted in a slow hash rate and high transaction fees. Technologies such as SegWit and the Lightning Network are being implemented in attempt to solve this issue. However, many people believe that this will not be a complete solution, or that there will be tradeoffs in decentralization. It is the

expensive transaction fees that makes Bitcoin unappealing (in terms of day-to-day transactions) for many users.

ii. Energy Use with Proof-of-Work

Bitcoin utilizes Proof-of-Work (PoW) protocols to restrict the number of blocks miners can create to roughly one in every 10 minutes. To accomplish this, a miner has to undertake computational programming by providing solutions to cryptographic puzzles. This costly and time-consuming action serves as a way to verify that a miner has performed work before being compensated with rewards and generation of a new block. These new blocks are then built on the preceding ones to form a 'chain'.

To stay competitive, there is the need for mining rigs which serve little purpose once they become obsolete. Many people argue that this is a waste of resources. Another downside of using a Proof of Work model is that it consumes a lot of energy. Processing a Bitcoin transaction requires an estimated 5000 times more energy than using a Visa Card. This makes the sustainability of Bitcoin somewhat unrealistic in the long term. Furthermore, the huge cost of energy is passed over to the users as transaction fees. Due to the increase in network load and energy consumption, transaction processing time on the Bitcoin blockchain also increases. The confirmation time for mining a block with Bitcoin ranges between 30 minutes and 1 hour. Other blockchains can do this in minutes or seconds.

II. Introducing Crave

Crave is a Proof-of-Stake cryptocurrency which uses cutting-edge technology to provide completely secure and anonymous transactions. This is all done while maintaining minimal transaction costs and lightning fast speeds. Crave launched on 20 March 2015 as the first coin to implement masternodes on a Proof-of-Stake code base. Many changes have been made since then, including a new team, updated specs, and modern advancements. With the core code based on Bitcoin, DASH, and PIVX, technology includes Zerocoin Protocol, masternodes, LightX zero confirmation instant send, once-only transaction broadcasting, and an advanced and user friendly interface.

III. Fair Distribution

The initial distribution method was a Proof-of-Work period that took place over the first 10000 blocks, which was then followed by a complete shift to Proof-of-Stake. Crave was launched without an ICO or premine. On 26 February 2018, a coin swap concluded to update to a new blockchain and code base. After the conclusion of the swap, all remaining coins set aside for the swap were burned.

IV. Advanced Anonymity, Untraceability, Unlinkability, and Unforgeability

Crave has taken into consideration the major concerns that users have about keeping their privacy and anonymity intact from unauthorized external violators. Blockchains can involve a large number of transactions within minutes. To safeguard these activities, maximum security of the blockchain is required by protecting the privacy and confidentiality of the information shared on this decentralized system.

i. Anonymity

Blockchains can involve serious financial transactions. It would be a mistake to let anyone know a user's transactions, as that serves as a vulnerability for attack. For example, say someone buys a rare painting. If their information is released to the public, it puts them at a greater risk, as other people now know that they own this item. There also exists the implied financial status that comes along with the purchase. By using Crave to complete the transaction, they would be able to keep these details private.

Crave serves to protect its users' privacy and anonymity by using advanced cryptography techniques, SHA-256 hashing of public keys, and the implementation of the Zerocoin Protocol, which uses the RSA-2048 accumulator encryption.

ii. Untraceability & Unlinkability

Using blockchain parlance, blocks are built upon one another to form a blockchain. Since blocks are linked together on the blockchain, it is possible for external attackers to trace the source of a block to target a user's cryptocurrency assets. Crave incorporates a system that prevents this traceability, allowing the user to clear the transaction history of their coins. In doing this, any attacker would run into a dead-end when trying to link the transaction to its origin, particularly if the receiving address is used only once. This is detailed more clearly in a later section on the Zerocoin Protocol.

iii. Unforgeability

Public-key cryptography allows for the generation of a pair of keys that are mathematically linked to each other. The public key is used for encryption, while the private key is used for decryption. Public-key cryptography is also used to create a digital signature, which is critical for authentication and data integrity. This works by using a mathematical algorithm to combine the user's private key with the data wished to be signed. One feature of a digital signature is that the signed data is an integral part of the signature. If the data is altered in even the slightest way, the signature will show as invalid when checked. This feature allows for the secure transfer of data, ensuring that nobody can attempt to forge a signature by attaching it to another file.

When a transaction is created, it is signed with the user's private key, and then broadcast to the network. The network checks the digital signature to verify that it matches the public key of the address in which coins are being sent from. If verified, the transaction is considered valid, relayed to other peers, and placed on the blockchain. Only the user in possession of the matching private key could have produced a valid signature. If someone were to try to create a non-genuine transaction by sending funds from an address they do not own, the signature will show as invalid and the transaction will be rejected.

V. Scalability and Fees

One of the largest issues Bitcoin faces relates to its scalability. The limited block size and slow transaction rate increases the transaction fees for users.

Crave attempts to resolve this knotty issue by providing each user with ample block size for transactions and keeping fees at a minimum. Crave has a maximum block size of 40MB, which is in sharp contrast to Bitcoin's 1MB block size. The increased block size allows for continued growth into the future, due to the higher number of transactions that can be included in each block. This also provides a faster transaction verification time, since at higher block capacity percentages, there exists a lower probability that a transaction will be included in the block.

There are also drawbacks to a larger block size. Due to the increase in amount of data that could be sent with larger filled blocks, it could become slower to broadcast new blocks. This could result in more orphaned blocks. Also, the large block size could lead to database sizes that reach a high level. Nodes that do not have the capacity to increase their storage would drop off the network, decreasing decentralization of the network.

In 2018, Crave is rolling out its Adaptive Blocks plan, which makes it possible to adjust the block size to current network requirements. This will allow faster transactions and increase scalability, without any observable limitations.

Standard transaction costs are around 0.0001 Crave/kb, although this adapts according to network load. Due to the linear coin supply growth, this cost will stay minimal, even in the case of mass adoption. Crave transactions can also be processed as zero-fee, in which up to

6 inputs can be sent without any transaction cost.

i. Proof-of-Stake System and Energy Efficiency

Rather than using the Proof-of-Work protocols to validate its users' mining activities, Crave adopts a more timely and less expensive technique. Proof-of-Stake requires the prover to show ownership of coins (the "stake") to verify blocks and transactions. Verifiers within the network do not need to solve intense computational puzzles. This approach is practical for mass-market applications of blockchain systems, showing an advantage in promoting scalability

Staking on a Raspberry Pi is also supported if desired, drawing less power and increasing energy efficiency. A Raspberry Pi is (generally speaking) a very small, cheap computer that uses almost no electricity. This is attractive for those who do not want to waste electricity by leaving their computer on, or run their wallet on a Virtual Private Server.

VI. Technological Features

The following section offers information about Crave's technological features, along with the characteristics that set the cryptocurrency apart from the others.

VII. Proof-of-Stake v3.0

PoS v3.0 has solved some of the problems with earlier versions of the consensus protocol. Listed are some of these advantages:

- **Energy Efficiency**: PoS v3.0 reduces the cost of energy during the forging or mining operations, since it does not rely on solving intense cryptographic puzzles.
- **No Coin-Age**: PoS v3.0 does not factor in coin-age as a criteria to award block rewards for staking. This protects against consecutive double spend attacks, and helps keep as many nodes connected as possible, which is imperative to security.
- **No Blockchain Precomputation**: In previous versions, it was possible to fork a block by changing its previous timestamps. In that situation, a stake modifier would not completely obfuscate the hash to prevent revealing the future proofs. PoS v3.0 makes it mandatory to change the stake modifier at every modifier interval. Doing this obfuscates any calculations that may reveal the next proof-of-stake.
- **Block Reward**: A block reward of up to 11 Crave serves to incentivize nodes to stay connected to the network. In a decentralized environment, a higher number of nodes connected to the network leads to increased security. This occurs through the shifting of trust from a single user to several users.

i. Block Reward Distribution

The 11 Crave block reward gets split up for three different purposes:

- 6 to masternodes
- 4 to staking
- Up to 1 for budgeting, infrastructure development, and governance

ii. Budgeting Block Reward

Technically there is only 10 Crave minted per block, with 1 Crave per block temporarily 'set aside' for budgeting. Since the block spacing is 60 seconds (one block is added to the blockchain every minute), there are 1440 blocks per day, and 43200 blocks per month. This means that every 30 days, 43200 Crave are set aside for governance.

Anyone is able to submit proposals to further the growth and development of Crave. If the community likes the idea behind a proposal, masternode holders can vote to have it passed. On the contrary, they can also reject the proposal. One part of the proposal is a one-time or monthly payment amount. This introduces a bit of competition among those submitting proposals - since everyone is fighting for a portion of the 43200 monthly reserved Crave.

Every 30 days (43200 blocks) a superblock occurs. The point of the superblock is to reward the addresses that are associated with accepted proposals. It is not until this superblock in which the reserved funds are actually minted and added to the circulating supply. For example, say that during a certain month, 6 proposals are accepted, and will take 40000 of the 43200 possible budget funds. The extra 3200 Crave do not go to any Crave wallet or developer address - they are simply never created.

To summarize - if the accepted proposals were to take 100% of the reserved funds, it would be the equivalent to having a constant 11 Crave block reward in terms of supply emission. However, if no proposals were accepted and 0% of this reserve was allocated, it would likewise be the equivalent of having a 10 Crave block reward.

iii. Staking Reward System

The simplest model of this system is called the 'simulated mining rig', in which every account has a certain chance per second of generating a valid block, much like a piece of mining hardware. This chance is proportional to the account's balance. A general equation for this can be shown as...

$$SHA256(prevhash + address + timestamp) \Rightarrow \frac{2^{256} * balance}{diff} \quad (1)$$

...where 'prevhash' is the hash of the previous block, 'address' is the address of the stake-miner, 'timestamp' is the current Unix time in seconds, 'balance' is the account balance of the stack-miner and 'diff' is an adjustable global difficulty parameter. If a given account satisfies this equation at any particular second, it may produce a valid block, giving that account a block reward for staking.

Receiving rewards from staking depends on the amount staked. In other words, the more coins a user stakes, the higher probability of receiving a reward. However, it is still a random process, meaning that a user could go a week without receiving a reward, then proceed to get three in a row. A staking calculator can be found on the Crave website which estimates the time for rewards.

VIII. Masternodes

A masternode is a cryptocurrency full node or computer wallet which possesses the entire copy of the associated blockchain in real-time. Masternodes are always up and running so that transactions can be processed without hitches at any time.

i. Purpose of Masternodes

The functions of masternodes are different from that of normal nodes, and some of these functions are highlighted below:

- ◇ Facilitate instant transactions.
- ◇ Instrumental in the governance and management of the blockchain through active participation of users in the voting process(es).
- ◇ Make it possible to undertake budgeting and treasury accountability.

ii. How Crave Incorporates Masternodes

Crave masternodes can run on any port, and multiple masternodes can use the same IP address. Monitoring is available in the Crave wallet to check on the status of masternodes and transactions. Along with this, multiple cold wallet addresses are allowed for maximum transactional security.

The required collateral to set up a masternode is 5000 Crave. A masternode can be stopped at any time, and the coins then become unlocked to the operator to use as they wish.

iii. Masternode Reward System

Crave's masternode reward system follows the payment logic described below.

- ◇ **Global List**: Every masternode running for over 8000 seconds is available on a decentralized global list. Its position on this list depends on the time since the last payment was made according to the network. Eligible new masternodes joining the network, restarted masternodes, and the masternodes last receiving payment are placed at the end of the global list. Over time, masternodes migrate toward the top of the list until they enter the selection pool.
- ◇ **Selection Pool**: The selection pool is estimated as the top 10% of the global list. If there are 1000 total masternodes waiting in the global list queue, the first 100 masternodes will be available for the block reward. The selection pool has no order, so the chance of a masternode receiving a reward is determined by probabilities.
- ◇ **Probabilities**: Once in the selection pool, masternode reward selection is based upon probabilities determined by block hash entropy and randomness. Each masternode in the pool should have a chance of receiving a payment at each block, according to:

$$\frac{1}{\#\ of\ Masternodes\ in\ Selection\ Pool} \quad (2)$$

The exception to this payment logic lies in brand new masternodes, which have a longer period of time before receiving an inital reward. The blockchain transaction that placed the 5000 Crave collateral must have as many confirmations as the total number of current masternodes on the network. Only then will the masternode be able to receive a reward. This is contained in the following code:

$$if(mn.GetMasternodeInputAge() < nMnCount)\ continue; \quad (3)$$

There is also an additional overriding check for the first masternode payment:

$$if(fFilterSigTime\ \&\&\ mn.sigTime + (nMnCount * 2.6 * 60) > GetAdjustedTime())\ continue; \quad (4)$$

In other words, if a user were to start their masternode with 1100 total masternodes running on the network, it will be eligible to receive its first reward after 1100 * 2.6 * 60 seconds = 47.67 hours.

iv. Tor Masternode Support

Tor uses a technique called onion routing to conceal information about user activity. This means that it protects the user by bouncing communications around a distributed network of relays run around the world. Using Tor encrypts all network traffic so that both the user's IP address and data cannot be accessed. Rather than being associated with an IP address, it allows for the use of .onion suffix addresses, which are not actual DNS names.

IX. Zerocoin Protocol and zCrave

The main function of the Zerocoin Protocol is to use zero-knowledge proofs to break the link between an address that receives non-anonymous funds and the subsequent transaction that spends those funds. In other words, it acts as a security-shield for transactions.

zCrave is the name of the unit used in Crave's version of this coin mixing service.

Using zCrave allows for complete untraceability and anonymity of transactions. This protects against potentials thieves who could otherwise attempt to follow the transaction history back to the original address.

i. How the Zerocoin Protocol Works

To simplify how it works, read this short analogy by Matthew Green:

"People throw dollars in a hat. Each time they throw a dollar, they get a token in return,

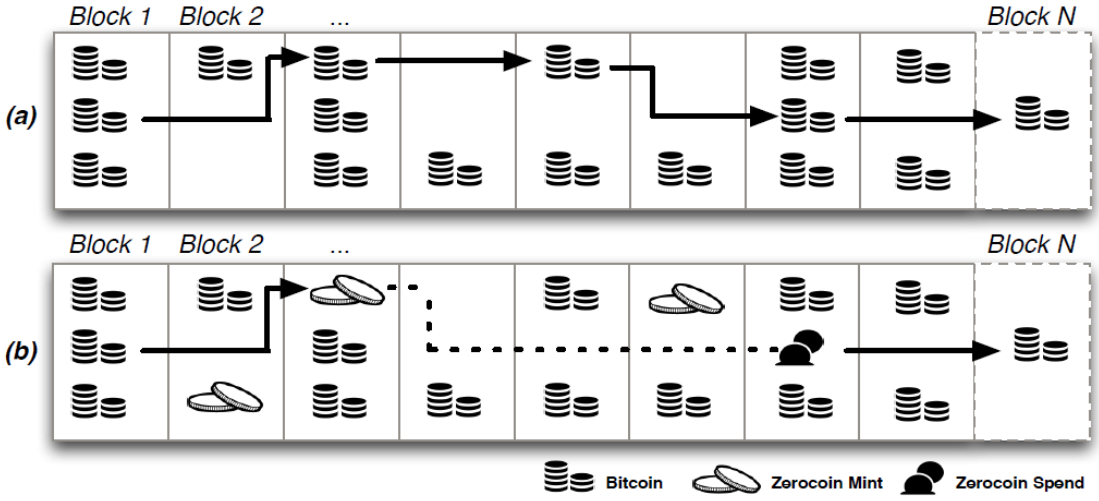

Figure 1: *Example blockchains showing Bitcoin transaction histories. In (a), it can be seen that each transaction can be linked to a previous transaction. The use of the Zerocoin Protocol can be seen in (b), in which the link between minting and spending (the dotted line) cannot be determined from the blockchain.*

and all tokens look exactly the same. Bob receives a token and walks away. Bob comes back an hour later with a mask on. Bob exchanges his token, and he takes out a totally different dollar."

Zerocoin works by allowing direct anonymous payments between parties. There are two steps that must be taken

1. Minting
2. Spending

Let's look at an example.

1. Minting
   (a) Bob wants to send 1250 Crave to Amy using an anonymous transaction.
   (b) Bob first converts the 1250 Crave to 1250 zCrave, which is automatically broken down into denominations. In this case, Bob's zCrave would be contained in the following denominations ...
      ◇ 1 x 1000 zCrave
      ◇ 2 x 100 zCrave
      ◇ 1 x 50 zCrave
   (c) Bob's balance now reflects that he owns 1250 less Crave and 1250 more zCrave than he began with.
   (d) There now exists a "secret knowledge key" associated with Bob, used to verify ownership of his specific denominations of zCrave.
2. Spending
   (a) After the zCrave denominations mature, Bob now sends the 1250 zCrave to Amy's Crave address.
   (b) The "secret knowledge key" is verified by the Zerocoin Protocol.
   (c) Amy's account is credited with 1250 Crave from an anonymous sender, while Bob's zCrave balance shows a decrease of 1250.
   (d) Amy now has 1250 Crave which shows no prior transaction history, making it impossible to track its origins back to Bob's Crave address.
   (e) The "secret knowledge key" used now becomes invalid, preventing the minted balance from being re-spent.

ii. Denominations

Supported denominations of zCrave are 1, 5, 10, 50, 100, 500, 1000, and 5000.

These values were chosen to promote untraceability and reduce transaction size, while still allowing the user some flexiblity in the amount that can be spent. Due to these zCrave denominations, only whole numbers of coins can be sent from one address to another using the Zerocoin Protocol.

iii. Advantages of Using zCrave

- ◇ Wipes the transaction history of the sent coins, as completely new coins are being minted, while the old coins with history are burned.
- ◇ Anonymous transactions only take 1-2 seconds to complete.
- ◇ Allows for direct spending of zCrave straight to another Crave address.
- ◇ Reduces transaction sizes.

X. LightX

The traditional banking system has developed the means by which people can send money to another party within minutes, including Western Union or Moneygram. With the advent of cryptocurrency, there now exists a much faster method of sending a payment - transactions which are sent nearly instantly. LightX is Crave's model of the instant-send payment system.

i. Purpose of LightX

The main purpose of Crave LightX is to facilitate the process of sending payments from one party to another in little to no time at all. It will be possible for people using LightX to pay for their shopping activities or other necessary payments as quickly as possible. For example, when a credit card is used for payment, it is not possible to confirm the payment to the sellers immediately, taking days or weeks to do so. With LightX, the verification of payments will be done in a near instant, meaning that coins will be spendable within seconds of being sent.

ii. How LightX Works

Masternodes play a significant role in the Crave instant-send process. Using LightX, secure payments could be sent to store owners and any other parties that someone may need to settle payments with.

LightX payments use the masternode network to immediately lock the exact amount of remitted funds in the user's account. This prevents the funds from being double spent. A notification will be sent once the funds have been locked. Since a transaction has just been carried out, the Crave blockchain records this in the public ledger where all other users can see it. The locked funds are then released to the designated party, and a notification for the completed payment is received within seconds.

The cost of completing an instant LightX transaction is a constant 0.01 Crave, slightly more than the default transaction cost of 0.0001 Crave/kb. This is an optional feature which can be toggled on and off as desired.

XI. Budget System & Governance

Crave is a community-dependent project, meaning that it relies on the active participation of its users to help carry out and develop its services and usability.

Each new block is created by Crave users, who are in turn rewarded for their activity in keeping the network strong and secured. During this process, up to 1 Crave from each block reward is set aside for use in the budgeting system - more information on this was described earlier in the Budgeting Block Reward section. This amount is then awarded to any accepted proposals in the form of monthly superblocks. Specific instructions for submitting a proposal and voting can be found in both the Crave setup guide, or on the official website.

i. Vote on Community Created Proposals

Crave is completely decentralized, and masternode holders from all over the world will be able to take part in the voting processes. Each masternode receives 1 vote. Voting is held to decide on any proposal put forth by community members, which can include (but are not limited to):

- ◇ Expanded marketing efforts.
- ◇ Hiring new members to the team.
- ◇ Adding features to the current architecture.
- ◇ Any other proposal that aims to improve the operations of the Crave network.

ii. Community Guided

As summarized above, Crave depends on its members to regularly carry out the following functions to stay active and usable for anyone across the world.

- ◇ **Staking & Masternodes**: Those who run masternodes or stake coins help secure the network, and are rewarded for doing so.
- ◇ **Governance**: Crave is decentralized, which means that there is no central management system for the cryptocurrency. Crave users have the ability to propose ideas and vote to help determine the direction of the project.
- ◇ **Improvement**: While many of Crave's improvements are due to a skilled development team, community members can contribute however they see fit to improve the ecosystem.
- ◇ **Stewardship**: Community members are entrusted to help explain features of Crave to new and prospective users. This helps expand the network and grow the community.

XII. Future Work

There is still much to be done, and we are always in a constant state of development. The roadmap contains major feature releases to look out for in 2018, including a unique new wallet, zCrave staking, adaptive block sizes, and the integration of an anonymous network layer.

XIII. Roadmap

The planned work for the rest of the 2018 calendar year has been spelled out in the Crave Roadmap. There may be slight adjustments, additions, or removal of items if deemed appropriate.

i. Quarter 1

- ◇ **Release of Roadmap**: Guidance for future developments.
- ◇ **Ending of Coin Swap**: Crave held a coin swap to implement a new code base, blockchain, features, and wallet. The supply was also increased to better fit zCrave denominations. Any remaining coins were burned, staying true to the 'No Premine' aspect of Crave.
- ◇ **Listing on Cryptopia**: Application and payment fee for listing Crave on the exchange, Cryptopia.
- ◇ **Coinomi Integration**: Coinomi is a secure, multi-asset HD wallet for Bitcoin, altcoins, and tokens. It is mobile-device friendly, serving as a mobile wallet.
- ◇ **Website Updates**: Addition of auto-updating statistics, roadmap, and additional language support to the official Crave website.

ii. Quarter 2

- ◇ **Crave Redesign**: Crave will receive a fresh new design to adopt a more widespread audience, changing the logo and website design.
- ◇ **Governance & Budget System Activation**: Community members can propose ideas and projects, which masternode holders will then be able to vote for or against. This method allocates funds set

aside from the Crave block reward to fund projects that support the network.
- ◇ **Brainwallet Integration**: Storage of the user's zCrave will be available with a mnemonic, one-seed recovery phrase.
- ◇ **Crave Knowledge Base**: Crave's own medium to answer common questions that users have, ranging from beginner to advanced levels.
- ◇ **Website Upgrades**: Improvements will be made to add all important information in a single, user-friendly location.
- ◇ **Paper Wallet Generator**: Support for an offline mechanism of storing public & private keys on paper.

iii. Quarter 3

- ◇ **zCrave Staking**: The network mixing security will be increased by allowing the staking of zCrave.
- ◇ **New QT Wallet Design**: Complete reworking of the wallet's UI for increased usability.
- ◇ **In-Wallet Voting**: Support for performing all budget voting from the internal QT wallet's GUI.
- ◇ **In-Wallet Proposals**: Support for performing all governance functions from the internal QT wallet's GUI.

iv. Quarter 4

- ◇ **Adaptive Blocks**: Block sizes will automatically adjust to the current network requirements, allowing for faster transactions and increased scalability.
- ◇ **I2P Network Integration**: Invisible Internet Project (I2P) is an anonymous network layer that allows for censorship-resistant, peer to peer communication. When implemented with Crave, this will also serve to encrypt network traffic so that the user's IP address cannot be accessed.

XIV. Acknowledgments

Special thanks to the community members that aided in the writing, editing, and feedback of this white paper.

- ◇ Asif Rahman
- ◇ HP3480
- ◇ MichaelJackson
- ◇ CryptoADavid
- ◇ Wonkee
- ◇ Wayne

The original v1.00 Crave white paper was released on 9 May 2018. This white paper is a living document, and the date noted in the header indicates the most recent revision.

References

[1] M. Conti, S. K. E, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," Jun. 2017.

[2] F. Saleh, "Blockchain Without Waste: Proof-of-Stake," p. 39

[3] G. Zyskind, O. Nathan, and A. ' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184.

[4] H. Vranken, "Sustainability of bitcoin and blockchains," Current Opinion in Environmental Sustainability, vol. 28, pp. 1-9, Oct. 2017.

[5] 'The Blockchain Is Only as Strong as Its Weakest Link," Security Intelligence, 27-Oct-2017.

[6] R. Yap, "Understanding how Zerocoin in Zcoin works and how it compares to other anonymity solutions Part 1," Zcoin, 10-Mar-2017.

[7] 'Bitcoin Explained Like You're Five: Part 3 - Cryptography," Escape Velocity, 07-Sep-2013. [Online]. Available: https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-

digital-signatures-explained/. [Accessed: 02-Apr-2018].

[8] wiki: The Ethereum Wiki -. ethereum, 2018. [Online]. Available: https://github.com/ethereum/wiki. [Accessed: 20-Mar-2018].

[9] dash: Dash - Reinventing Cryptocurrency. Dash, 2018. [Online]. Available: https://github.com/dashpay/dash/blob/master/src/masternodeman.cpp. [Accessed: 09-Apr-2018].

[10] 'Understanding Masternodes - Dash latest documentation." [Online]. Available: https://docs.dash.org/en/latest/masternodes/understanding.html. [Accessed: 09-Apr-2018].

[11] 'On Stake," Ethereum Blog, 05-Jul-2014. [Online]. Available: https://blog.ethereum.org/2014/07/05/stake/. [Accessed: 02-Apr-2018].

[12] 'Bitcoin Energy Consumption Index," Digiconomist. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed: 28-Feb-2018].

[13] 'Bitcoin Scaling Problem, Explained," Cointelegraph. [Online]. Available: https://cointelegraph.com/explained/bitcoin-scaling-problem-explained. [Accessed: 27-Feb-2018].

[14] 'Dash: Solving the Challenges of Instant, Private Payments," CoinCentral, 11-Jan-2018. [Online]. Available: https://coincentral.com/what-is-dash/. [Accessed: 10-Mar-2018].

[15] 'How zerocash works | Zerocash." [Online]. Available: http://zerocash-project.org/how_zerocash_works.html. [Accessed: 10-Mar-2018].

[16] 'Proof of work - Bitcoin Wiki." [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_work. [Accessed: 27-Feb-2018].

[17] 'Zerocoin Project." [Online]. Available: http://zerocoin.org/index. [Accessed: 10-Mar-2018].

[18] 'Staking Sidechains? New Paper Proposes Twist on Bitcoin Tech," CoinDesk, 27-Sep-2017. [Online]. Available: https://www.coindesk.com/staking-sidechains-new-paper-proposes-twist-bitcoin-tech/. [Accessed: 09-Mar-2018].

[19] A. Nordrum, "Wall Street Firms to Move Trillions to Blockchains in 2018," IEEE Spectrum: Technology, Engineering, and Science News, 29-Sep-2017. [Online]. Available: https://spectrum.ieee.org/telecom/internet/wall-street-firms-to-move-trillions-to-blockchains-in-2018. [Accessed: 03-Mar-2018].

[20] 'What Is A Masternode And How Is It Useful For Cryptocoin Investors," CoinSutra - Bitcoin Community, 04-Jan-2018. [Online]. Available: https://coinsutra.com/masternodes/. [Accessed: 09-Mar-2018].

[21] 'Security Analysis of Proof-of-Stake Protocol v3.0," BlackCoin, 17-Oct-2016. [Online]. Available: https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf. [Accessed: 10-Mar-2018].

Appendices

A. Crave Core Team

- **CooleRRSA**: Core Development
- **Slothman**: Communications
- **tkon**: Support
- **zrero**: Front-End Development
- **DruMn**: Front-End Development
- **Green_crypto_and_ham**: Marketing
- **SoundDrGenie**: Video and Film Outreach

More information: https://crave.cc/team

B. Useful Links

Listed here are important links, social media channels, and exchanges that support Crave. Please check our website for a full list.

i. Main

- **Website**: https://crave.cc/
- **GitHub**: https://github.com/Crave-Project/Crave-NG/
- **Emails**: https://crave.cc/team
- **Wallets**: https://crave.cc/wallets/
- **Mobile Wallet**: https://coinomi.com/
- **Block Explorer**: http://explorer.crave.cc/

ii. Masternodes

- **Masternode Setup Guide [PDF]**: https://crave.cc/pdf/Complete_Masternode_Guide_for_Crave_NextGen.pdf
- **Masternode Setup Guide [Video]**: https://www.youtube.com/watch?v=GUDvUz7gkBA
- **Masternode Compilation Script [Linux]**: https://cdn.discordapp.com/attachments/373145814643638282/420218710826156032/crave-install.sh
- **Masternode Hosting**: http://nodeshare.in/coins/crave/order/

iii. Statistics

- **CoinMarketCap**: https://coinmarketcap.com/currencies/crave
- **Masternodes.online**: https://masternodes.online/currencies/CRAVE/
- **Masternodes.pro**: https://masternodes.pro/stats/crave
- **Staking Calculator**: https://crave.cc/staking

iv. Community

- **Crave Forum**: https://forum.crave.cc
- **Twitter**: https://twitter.com/craveproject
- **Discord**: https://crave.cc/discord
- **Telegram**: https://t.me/craveproject
- **Medium**: https://medium.com/@CraveProject
- **Facebook**: https://www.facebook.com/craveproject/
- **BitcoinTalk**: https://bitcointalk.org/index.php?topic=2547950
- **Reddit**: https://www.reddit.com/r/craveproject/

v. Exchanges & Trading Pairs

CRAVE/BTC

- **Cryptopia**: https://www.cryptopia.co.nz/Exchange?market=CRAVE_BTC
- **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/BTC
- **CryptoBridge**: https://wallet.crypto-bridge.org/market/BRIDGE.CRAVE_BRIDGE.BTC
- **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_BTC
- **BiteBTC**: https://bitebtc.com/trade/crave_btc
- **altilly**: https://www.altilly.com/market/CRAVE_BTC

CRAVE/USD

- **BiteBTC**: https://bitebtc.com/trade/crave_usd

CRAVE/LTC

- ◇ **Cryptopia**: https://www.cryptopia.co.nz/Exchange?market=CRAVE_LTC
- ◇ **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/LTC
- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_LTC
- ◇ **BiteBTC**: https://bitebtc.com/trade/crave_ltc
- ◇ **altilly**: https://www.altilly.com/market/CRAVE_LTC

CRAVE/ETH

- ◇ **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/ETH
- ◇ **BiteBTC**: https://bitebtc.com/trade/crave_eth
- ◇ **altilly**: https://www.altilly.com/market/CRAVE_ETH

CRAVE/DOGE

- ◇ **CoinExchange.io**: https://www.coinexchange.io/market/CRAVE/DOGE
- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_DOGE

CRAVE/BCH

- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_BCH

CRAVE/USDT

- ◇ **TradeSatoshi**: https://tradesatoshi.com/Exchange?market=CRAVE_USDT
- ◇ **altilly**: https://www.altilly.com/market/CRAVE_USDT

C. Specifications

Specification	Description
Ticker	CRAVE
Block Spacing	60 seconds
Max Block Size	40 MB
Total Block Reward	Up to 11 Crave
Masternode Reward	6 Crave per block
Staking Reward	4 Crave per block
Budgeting Reward	Up to 1 Crave per block
Maturity	88 blocks
Stake Minimum Age	8 hours
Masternode Collateral	5000 Crave
Default Masternode Port	48882
Default RPC Port	48883
Maximum Supply Cap	Infinite
Hashing Algorithm	SHA-256
Premine	0 Crave
Min Transaction Cost	0.0001 Crave/kb
LightX Transaction Cost	0.01 Crave
Zero-Fee Transactions	Yes
Protocol Support	IPV4, IPV6, Tor
Consensus Algorithm	Blackcoin v3.0 PoS