Cash2: Cash Version 2

Porntawee Paul Aphivantrakul
cash2@protonmail.com
www.cash2.org

Abstract. We propose a new cryptocurrency called Cash2 that retains all the useful properties of cash but is also usable online, decentralized, borderless, and non-inflationary. This is an attempt to create the next evolution in cash.

1. Introduction

Cash has served as a useful method of payment for many centuries. Cash has many properties that make it an ideal form of money. It is hard to counterfeit, scarce, divisible, uniform, durable, fungible, easy to transport, easy to store, and is widely accepted. Also, payments with cash are private and irreversible. However, despite these useful properties, in today's society, the use of cash is declining, and the use of credit and debit cards is growing.

Credit and debit cards have many advantages and disadvantages compared to cash. The two biggest advantages over cash is the ability to be used online and the improved carrying convenience. Some of the disadvantages include the need for trusted financial third parties, reduced financial privacy, payment processing fees, payment reversibility, long-term payment processing contracts for merchants, and identity theft. The first step towards improving upon this system occurred with the invention of Bitcoin.

Bitcoin was introduced in 2008 and solved many of the problems with using credit and debit cards. The greatest contribution of Bitcoin is solving the double spend problem without the need for trusted financial third parties. Bitcoin is also an improvement over cash by being usable online, non-inflationary, and borderless. However, Bitcoin in its current state does not retain some of the useful properties of cash. In the next section, we discuss the properties missing in Bitcoin that have made cash a stable form of money.

2. Cash vs. Bitcoin

Cash has four properties that make it a better form of money than Bitcoin: low transaction fees, fungibility, privacy, and fast transaction speeds.

Low Transaction Fees: Cash cost no money to transact. If a customer pays a merchant using cash, the merchant receives 100% of the amount from the customer. Bitcoin originally had zero or near zero transaction fees. However, as more people started to use Bitcoin, the number of transactions quickly outpaced the processing capabilities of the network. Many attribute Bitcoin's 1 MB block size to the bottleneck in the network. The result has been that users have had to compete with each other through paying higher fees to have their transactions processed quicker. In 2017 Bitcoin fees were over 700 satoshis per byte, and average transaction fees were as high as $50.

Fungibility and Privacy: Fungibility is the property that every unit is equal to every other unit. Cash is fungible because the five dollar bill in your pocket is equal to the five dollar bill in my pocket. The amount of goods and services that can be purchased with your five dollar bill is equal to the amount possible with my five dollar bill. They are both equal in value and indistinguishable. Bitcoin is not fungible because not all Bitcoins are indistinguishable. What makes one Bitcoin different from another Bitcoin is its transaction history. Bitcoin uses an open public ledger to record the transaction history of every unit of Bitcoin to protect against double spends. Bitcoins that financed illicit activities are considered to be worth less due to the risk of the coins being blacklisted by exchanges. In addition, Bitcoin's public ledger also reveals the number of Bitcoins an individual owns, which causes a lack of financial privacy.

Fast Transactions: Cash transactions are nearly instantaneous. Bitcoin's average block time is 10 minutes. Many people recommend waiting for at least 6 block confirmations to ensure that funds are secure after being transferred. Therefore, the transaction time for Bitcoin could potentially be up to 1 hour on average. The block time of 10 minutes was chosen to allow enough time for information to propagate between nodes and also to reduce the number of orphaned blocks produced. However, many altcoins have shown that block times of less than 10 minutes is adequate for information propagation and maintaining integrity of the blockchain.

3. Cash2 vs. Bitcoin

The previous section discusses four beneficial properties of cash that are missing in Bitcoin. In this section, we discuss how Cash2 incorporates these properties.

Low Transaction Fees: Cash2 uses an adaptable block size to ensure that all valid transactions are able to be quickly processed. All Cash2 transactions are free.

Fungibility and Privacy: Cash2 is part of the CryptoNote family of cryptocurrencies. CryptoNote is a technology that obfuscates the public ledger by using ring signatures to hide the sender and stealth addresses to hide the receiver. These privacy features are present by default in every transaction. The result is that the entire Cash2 blockchain is obscured, and every unit of Cash2 is considered to be equal to every other unit, thus providing fungibility. Cash2 blockchain obscurity also ensures that the amount of Cash2 a user owns is not easily determined, allowing the user financial privacy.

Fast Transactions: Cash2 has an average block time of 9 seconds. Usability studies have shown that 10 seconds is the limit for keeping a user's attention on a particular task before the user moves on to another task. We chose 9 seconds to maximize the time for information to propagate while still being under the attention time limit.

4. Cash2 Retains the Useful Characteristics of Cash

There are seven characteristics of cash that make it an ideal form of money: hard to counterfeit, scarce, divisible, fungible, durable, easy to store, and easy to transport. In this section we discuss how Cash2 retains these seven properties of cash.

1. *Hard to Counterfeit*: Cash2 uses cryptography, mathematics, and computational proof-of-work to secure the network similar to Bitcoin and other CryptoNote cryptocurrencies. These tools are used to create a blockchain that ensure the security of one's funds and to prevent arbitrary minting.
2. *Scarce*: Cash2 has a maximum supply limit of 15 million units.
3. *Divisible*: Every unit of Cash2 can be divided into 100 million subunits
4. *Fungible*: Obfuscation of Cash2 transaction histories ensure that all units are equal in value and indistinguishable.
5. *Durable*: Record of one's funds are permanently stored on the blockchain. The integrity of the Cash2 blockchain is dependent on the miners securing the network and their degree of decentralization.
6. *Easy to Store*: User's only need to keep a record of where their funds are located on the blockchain (the public address) and the key required to access those funds (private key).
7. *Convenient to Transport*: Cash2 transactions can be made using a smartphone. This eliminates the need to carry paper notes, metal coins, and plastic credit cards.

5. Technical Specifications

Maximum Supply	15,000,000
Transaction Fee	0
Smallest Unit	0.00000001
Block Time	9 seconds
Code Family	CryptoNote

6. Cash2 Limitations

Blockchain Size: Low fees, dynamic block size, and ring signatures could cause a rapid growth in the size of the Cash2 blockchain. Assuming Cash2 handles the same amount of traffic as Bitcoin, the Cash2 blockchain size would be 10 to 100 times larger than that of Bitcoin's. Some argue that a large blockchain will require expensive, specialized hardware to run a node and will reduce the number people able to run nodes, thus causing network centralization and decreased network security. Although this is possible, we believe that the advancements in computing and networking technology will keep up and even outpace the requirements of the Cash2 blockchain.

Privacy: Cash2 strives to provide the highest level of financial privacy and anonymity possible while still maintaining its other cash-like properties. We have adopted the best privacy enhancing technology that we believe exists today. However, there are limits to the level of privacy possible with Cash2 compared to other cryptocurrencies that are solely focused on privacy. If privacy is of utmost importance to a user, we recommend using those other cryptocurrencies. Cash2 aims towards fungibility and uses blockchain obfuscation technologies to help achieve it, but Cash2 should not be considered a "privacy coin".

Maximum Supply Limit: Many CryptoNote based cryptocurrencies have a small tail emission of coins. This results in an infinite supply of those cryptocurrencies. The reason for having a tail emission is to ensure that miners have adequate financial incentive to secure the network. Bitcoin does not have a tail emission and has a maximum supply limit of 21 million coins. The reward for mining a Bitcoin block will eventually drop to zero, but miners will still be able to collect fees from the transactions included in the block. Like Bitcoin, Cash2 believes that transaction fees will be enough to incentivize miners to continue securing the network and that a tail emission is unnecessary.

7. Fair Launch

The genesis block of Cash2 will be created on December 5, 2018 at 9:00 am EST. Every effort will be made to announce Cash2 to the public both before and after the launch date. Users will be given ample opportunity to view the source code and download the compiled Cash2 software for Linux, Windows, MacOS, and ARM platforms prior the the genesis block being created. There will be no premine, founder's reward, development taxes, or mining taxes. Funding for Cash2 development and marketing will be done solely through donations from the community.

8. Conclusion

We have proposed a new cryptocurrency called Cash2 that retains all of the properties of cash that make it an ideal form of money, but unlike cash, Cash2 is also usable online, decentralized, non-inflationary, and borderless. Cash2 builds upon the Bitcoin ideals of a trustless electronic payment system while also adding back some of the beneficial properties of cash such as low fees, fast transactions, privacy, anonymity, and fungibility.