Kema Coin 2.0

By William W. Corless Jr.
wmcorless@gmail.com

The purpose of this paper is to propose the features for a new cryptocurrency that answers many of the defects of cryptocurrencies that exist today.

When Bitcoin was first proposed it was based on the concept of decentralization, and lack of trust. The network of wallets would connect and verify all transactions in a public ledger, known as the Blockchain. Bitcoin's philosophy is that centralization is bad and decentralization is good. I would argue the opposite is true. Fear of centralization is similar to class envy a staple of marxist ideology. In this paper I will show that centralization is good, and that it is used in cryptocurrency today. I will demonstrate the flaws of Bitcoin and other cryptocurrencies and to offer a better solution.

Proof of Work

Proof of Work is the method that Bitcoin uses to drive forward the blockchain. Bitcoin would pay a block reward, the same reward would be paid to the person receiving the reward with no concern for the amount of effort or resources used to obtain that reward. Only one miner would receive the reward, and it favored the one with the higher hash rate. Sort of like a lottery where the winner is the one who buys the most lottery tickets. Each wallet uses consensus to determine and or verify transactions.

- Cryptocurrencies pay the same reward for each block irrespective of the cost to obtain it.
- Because of rising difficulty, mining equipment usually become obsolete before they pay for themselves.
- Businesses are not rewarded by investing in mining equipment.
- Mining with Bitcoin is not a sustainable business strategy.

Free Enterprise

Free markets create wealth better than any other form of economic system tried by people throughout history. Because people are encouraged to work for unlimited rewards, as opposed to rewards that paid equally to people regardless of how hard they work. Social Justice strives for equality. That is the basic flaw with all cryptocurrencies. The reward is the same regardless on how much money you paid on electricity to get it.

Another concept I want to touch on is that centralization is beneficial to man, not decentralization. In history man went from agrarian societies to small cities. In the cities men were able to specialize and become artisans. Whether they made shoes or leather products, blacksmiths made armor, horse shoes. Others made wagons, etc. People made things for others and were paid for their products. As certain individuals were recognized by their skill their products were more prized and they were paid more for them. Merchants brought products from far away, farmers had a market to sell to, etc. Therefore centralization improves people's lives. The economy of cities gave people the opportunity to raise their standard of living, that hard work was rewarded by higher pay.

If you work for an employer this is not the case. The job has a set paycheck, and therefore your ability to earn more is stifled. As a result your incentive to work harder is negated. Employers prefer the employment model, as the employee is under the authority of the employer. This gives the employer a certain amount of control over their employees lives.

One benefit employment provides is a sense of security and predictable income that can provide a stability not found in self employment. However independent business people enjoy the benefits of setting their own hours and working as hard as they want and experience more freedom. America’s greatest benefit in my opinion is the ability for anyone to start their own business and become wealthy. So it is better to be an entrepreneur, than an employee.

When bitcoin first started anyone could mine their own wallet with their own computer. As the difficulty increased, it required investment in ever more powerful computers to get the same reward. Then the move to Video Cards and their faster processors were used, then the use of specialized equipment based on ASICs, etc. I call it the arms race to mine bitcoin.

Even those who support decentralized cryptocurrency discovered the benefits of centralization. As the difficulty rose, the need for centralization rose to counter it. Here are some examples of how centralization is key to obtaining benefits that cryptocurrencies lack.

- Pools
- Exchanges
- Masternode Services

Pools create a form of centralization to combat ever higher difficulties that cryptocurrencies naturally produce due to competition. Pools give individuals access to shares of block rewards otherwise not given to them. This is an example of how benefits are created through centralization.

Exchanges came about due to the need to convert coins to fiat. After all not everyone accepts crypto currencies for payment, so a need to convert to fiat produced another form of centralization called exchanges. Exchanges created the concept of purchasing crypto currencies as and investment, as the coins go up or down based on market pressures.

Masternode services allow people to invest in masternodes hosted by a third party and pay a fee for that service. This is a third example of how centralization provides benefits to users.

In free markets competition creates new opportunities, in cryptocurrencies they create higher difficulties and less opportunities. However some may argue the higher difficulty leads to less coins, which leads to higher values due to scarcity. This of course speaks to the free market concept of supply and demand.

Proof of Stake

Proof of Stake was another method introduced by Sunny King in Peercoin to move the blockchain forward. It paid a reward to those who had coins in their wallet, the idea being that those who owned coins had a bigger stake in the security of those coins than those who had none. In many other coins Proof of stake pays the same reward similar to the bitcoin method.

Masternodes

Coins based on Dash use masternodes to provide a Masternode Reward. Again this is a fixed reward that is paid on a round robin method. As the number of masternodes increases the time to get paid gets longer and longer. This is another flaw in the system.

Imagine working for a company and instead of getting paid at the end of the week, each employee gets paid every day, one after the other. As the number of employees grows, the time it takes to get paid takes longer and longer. If the company had 7 employees each employee would get paid once a week, but if the company had

30 employees then they would get paid once a month. If the company had 365 employees, you'd only get paid once a year. If you have to wait for a year to receive the same pay you received once a week, you'd be in big trouble. Obviously this method is no good.

Kema Coin works on the proof of stake model with masternodes. However as I have shown above this system is not good. That is the reason for this paper to propose a new set of rules in Kema Coin 2.0.

A Better Way

A better cryptocurrency in my opinion would be one that offered greater rewards to those who worked harder to get those rewards.

An example would be to mine the coin with faster hash power would result in a higher reward. The reward would be based on hash power, the higher the hash the higher the reward. There would be no need for a difficulty setting. This would negate the need for pools because anyone could mine with a simple computer or a warehouse full of specialized ASIC equipment. Also Instead of one person receiving a block reward, everyone working would get paid as a transaction, not as a block reward. So everyone is paid for their work, not the lottery winner as is done Bitcoin.

To explain the concept more clearly, with Bitcoin a block reward is paid every 10 minutes. The winner is the one who solves the problem first, it could be the same person every time if they have the higher hash power. I call this winning the bitcoin lottery. My proposal would be to pay everyone submitting hash power, if the block time were 10 minutes and one person solves the problem a hundred times and another solves it a thousand times within that ten minutes both would receive rewards, the first would receive a hundred rewards, the other would receive a thousand rewards. Therefore everyone submitting hash power gets paid based on their contribution not just one person per block. At some point the cost would exceed the benefit. See chart below.

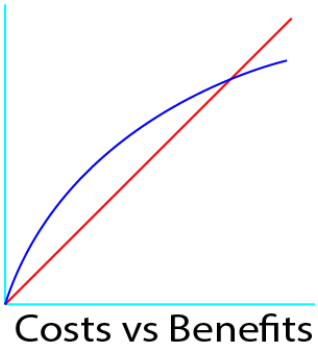

Figure 1. Cost of Mining vs the reward would scale and eventually reach the point where it is no longer viable, as the costs would exceed the reward. However as more innovative mining lowers costs, efficiencies would allow higher rewards at less cost.

In Free Markets competition creates new opportunities for individuals, where a person strives for efficiency to produce more at less cost. An example of this were the use of assembly lines to produce more products in the same period of time.

I think a better method instead of Proof of Stake and Masternodes is to have a node that acts like a bank. You deposit your coins in your “banknode” and it pays Interest on the coins you have on deposit, so that if you have more coins, you receive a bigger reward. This encourages savings which is another free market concept. It is more noble to put off an immediate desire and save the funds to obtain interest and therefore receive a greater reward later.

In the current situation of masternodes, if you want to receive more rewards you have to have more masternodes. Usually this results in having to pay for additional servers or use persons that are centralizing masternodes on masternode services.

Blockchain Balloon

Another problem the current cryptocurrencies have is what I call Blockchain Balloon. Because every wallet keeps every record from the genesis block to the current day the size of block continues to grow exponentially. Other wallets include extra information in the blockchain such as smart contracts, or storing other information. This is counter productive to the point of cryptocurrencies. The only information stored in the blockchain should be the financial transaction only. The transaction id, the amount, the date/time, the sender and the receiver.

Banknodes

My solution is that Banknodes will operate like masternodes. Their job is to verify transactions and to pay interest. This interest is then compounded. Banknodes can backup previous years blockchain to separate files to be stored offsite to reduce storage size. That way old years can be archived and not needed to be kept with the current wallet.

Wallets are used for mining. They mine on your computer, your cellphone, etc. Once you have a balance in your wallet, you can move it to your Banknode to earn interest. Individual wallets will start their database when they are installed on your computer. No need to synchronize the entire network each time you start your computer. They connect to the network, once connected they start mining. The only transactions recorded on your computer are your own transactions.

Mined Rewards as Transactions

This is a new concept as Mined Rewards have always been associated with a block reward. Kema Coin 2.0 will use blocks differently. Instead of a block being associated with a mined reward, it is associated with time. Blocks are created every 10 minutes, and transactions that occur between those block times and are added to blockchain. Mined transactions are verified by the banknodes, and are added to your wallet accordingly. Any transactions not verified during the block are simply rolled into the next one. No limit to the number of transactions allows the network to scale to any size.

In order for a wallet to be able to mine it must connect to the network of banknodes. A wallet will need at least 3 connections before mined transactions can be verified. The banknodes verify the hash power used to mine, create the reward transactions and credit your wallet. Instead of rewards orphaning out, they are simply rolled over into the next block.

Closed Source

Kema Coin will not be open source. The reason for this is open source code can be manipulated, and hackers can find ways to cheat the system. Kema coin will therefore use a proprietary method of encryption to secure the network. Another reason is we don’t want thousands of copycats where someone uses our code and simply changes the logo and makes a new coin, as what happens in cryptocurrency now.