CloudCoin: A Theoretically Perfect Currency

Written by Sean Worthington and the CloudCoin Consortium SV

1. Introduction

Today's blockchain-based digital currencies cannot achieve both decentralization and high performance. The Redundant Array of Independent Detection Agents ("RAIDA"), which uses cutting-edge network architecture, has achieved both.

Highly decentralized digital currencies such as Bitcoin are extremely slow, non-scalable and expensive. Newer currencies, such as EOS, achieve much better performance but rely on a few nodes (21 in the case of EOS) which risk being taken-over and owned by a single entity or government.

Until relatively recently, all databases were owned by persons, companies or governments. Database owners have the ability to create, read, update and delete data. The owner can also turn off the system - or be forced to turn off the system - at any time.

Blockchain technology has removed the ownership of databases and has allowed us to achieve *Data Supremacy.* Data Supremacy is when a database cannot lose its confidentiality, integrity or availability to any threat including governments, tech giants, hackers, AI, quantum computers, System Administrators or even its creators.

2. The Problems with Existing Currencies

Throughout human history, until the creation of Bitcoin, governments have controlled currency and currency creation. This has proved to inevitably fail once governments begin to inflate the supply without controls. Cryptocurrencies were intended to be a solution to this problem, but there are other challenges with major cryptocurrencies in circulation today that cause cryptocurrency to be difficult to use for money.

2.1 The Threat of Centralization

A Centralized monetary system can create a big problem because it allows the owners of the monetary system (often governments) to dilute the money and rob the people of the goods and services that we the people earned.

When money appears in a monetary system by dilution, it disrupts the people's productive and efficient behaviors because it fools the people with inaccurate information. It is through the analysis of price information that we decide where to work and what to buy. Dilution corrupts monetary information and the only beneficiaries of the new currency are the creators of the new currency.

Consider the effects of Zimbabwe's centralized currency. "To ensure that the government funded its debts, the Reserve Bank of Zimbabwe increased its printing of currency causing a rise in inflation to triple digits as of 2001. By the end of 2008, consumer prices doubled every other day with joblessness being on the increase."[1] This crisis caused harm to all the people of Zimbabwe and this dilution would not have been possible without centralization.

E-Gold (launched in 1996), presents a concrete example of how centralization can destroy a digital currency. With E-Gold, people put their gold in a common vault and digital certificates were issued based on that gold. Then the State of California kicked in the doors and took the vault, effectively ending the currency.[2] Naturally, this was catastrophic for E-Gold users.

2.2 Bitcoin: The Decentralized Blockchain Solution

Bitcoin's underlying architecture is peer-to-peer. This means that all computers have the same authority. Bitcoin was the first digital monetary system to achieve Data Supremacy. However, it has problems including high energy usage, no true privacy, lack of speed, high fees, not being user-friendly, and most concerning: It is non-scalable. Scholars have noted that without scale, the blockchain cannot have many real-world applications. Therefore, this scalability vs. decentralization trade-off may impose a long-term limitation of blockchain-based technologies.[3]

With any information system, governance is required when decisions need to be made. With Bitcoin, there is no governance. Therefore, no decisions can be made. But what if there is a bug in the Bitcoin code? What if we want to update Bitcoin software to improve performance? Historically, to make improvements to the code, Bitcoin miners go to war with each other and the code is "forked." This means that some administrators (miners) run the old code while others run the new code.

We can see from Bitcoin that blockchain decentralization reduces performance and holds back the development of a coin.

2.3 The EOS Cryptocurrency: The more Centralized Blockchain Solution

EOS's underlying architecture is not peer-to-peer. Instead, there are 21 nodes that together decide who has what money. This architecture could be called client-multi-master because there are many master nodes and each master node is equal to the other master nodes. This model allows changes to occur at any master node, but it also introduces the possibility of conflicts when data is replicated to other nodes. These conflicts are settled with an algorithm. EOS was created to solve the shortcomings of the blockchain by reducing the number of nodes from thousands down to only 21. The efficiency, speed and scalability of EOS was a massive improvement over Bitcoin due to this centralization. But there are some problems. The system was designed to have a government and coin holders were given votes to decide who would be the node owners. The majority of these nodes ended up being either located in China or controlled by the Chinese. The Chinese were able to buy these nodes by a so-called vote.

In the past, the owners of these 21 nodes have worked together to freeze accounts that had been shown to hold stolen tokens. "The decision to freeze those accounts shows the controversy the blockchain is

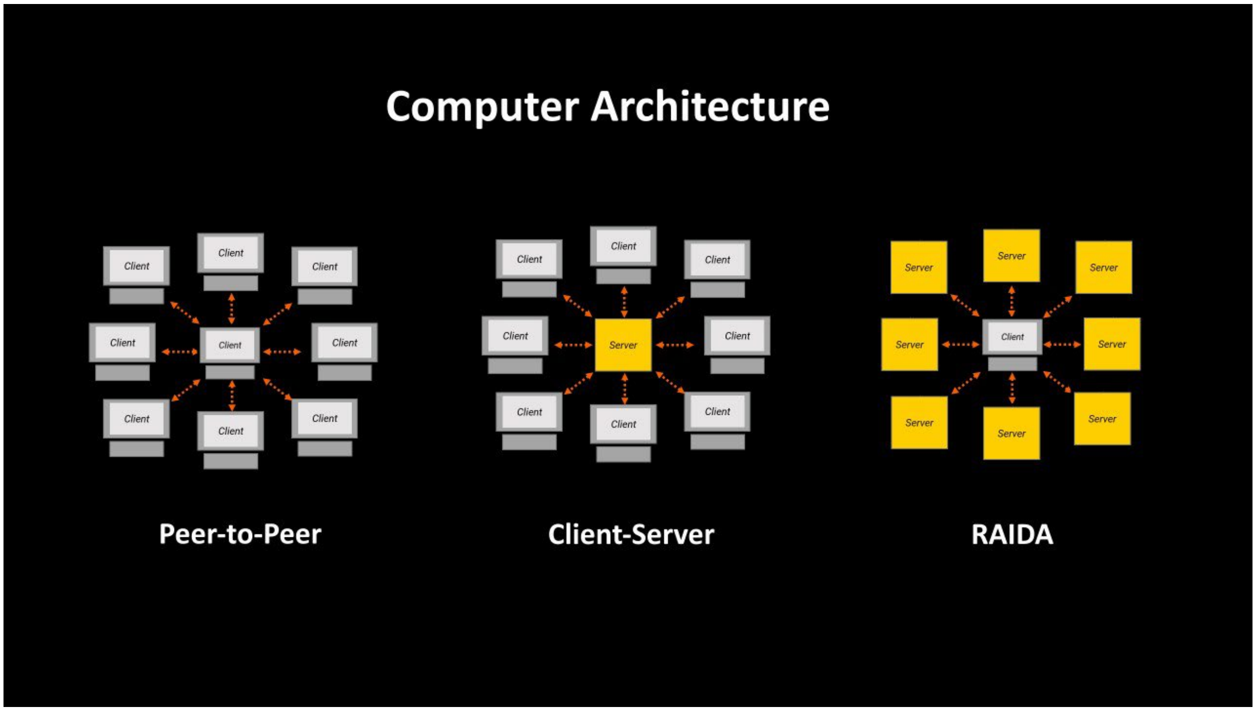
[1] https://studentshare.org/history/1457991-inflation-in-zimbabwe

[2] https://www.investopedia.com/terms/d/digital-gold-currency-dgc.asp

[3] [The Limits to Blockchain? Scaling vs. Decentralization.] Social Science Research Network. Cybersecurity, Privacy & Networks eJournal. Accessed 21 April 2019.

facing now, because the top (nodes) did so without any kind of agreed-upon governance process. A "constitution" had been drafted, but it had not passed a referendum of EOS users." .[4]

EOS shows that while centralization increases blockchain performance, it can reduce the integrity of a currency.


Computer Architecture

3. The RAIDA and CloudCoin as an Alternative Solution

The RAIDA uses an architecture that can be called *Client-Redundant Array of Servers.* Instead of a client talking to a peer or a server, the client talks to many servers in parallel. Using the RAIDA can be compared to asking dozens of different coin dealers if a coin is authentic whereby it is the user who needs to decide if the coin is authentic based on the user's own opinions. This architecture provides the speed of client-server with the decentralization of peer-to-peer.

The RAIDA allows for true digital cash. True digital cash does not use a ledger to track who owns it. Digital cash is more akin to physical money. Instead of printing ink on paper (as with dollars), data is written on hard drives in the form of files. Ink on paper and magnetic fluxes on hard drives are both 'symbols with meaning' (data). There exists the obvious question: What is to stop people from making copies of the files, thereby creating an infinite supply of cash that dilutes the system and creates mass inflation? This is where the genius of the RAIDA comes in. The RAIDA stops people from spending their money twice.

[4] https://www.coindesk.com/markets/2019/09/19/everyones-worst-fears-about-eos-are-proving-true/

3.1 How the RAIDA Works

Suppose there is a file called a CloudCoin. Inside this file there is a unique serial number and 25 extremely strong passwords, called “authenticity numbers”. The owner of the file owns the money because only the owner has the true authenticity numbers. If the owner wants to buy something from a seller, the owner will pay with this file. Now, both the owner and the seller have possession of the file. Anyone with the numbers can change them. That person simply makes a request to the RAIDA telling it which serial number to authenticate, what the password is and what the password should be changed to. If the coin is authentic, then the person who reauthenticates will immediately be the new owner because that person is now the only person with the authenticity numbers. In the case of CloudCoin, the new authenticity numbers are automatically generated when a request to authenticate the CloudCoin is made. The process of reauthenticating a CloudCoin is called “POWNing,” which stands for “Password Owning,” and will be used further in this whitepaper to describe reauthentication of CloudCoins.

3.2 The RAIDA Achieves the Highest Performance

The RAIDA is much faster and more scalable than the Blockchain. The RAIDA has been shown to handle requests in just 2 millionths of a second, fast enough to support the entire global transaction network like the Root DNS does. Like the DNS, RAIDA is able to use UDP instead of TCP. Note that all network protocols must choose UDP or TCP because there are no alternatives. UDP is much faster but will lose packets. RAIDA is so redundant that packet loss is acceptable. RAIDA does not use SSL encryption but instead uses AES encryption. SSL is much slower than AES because SSL requires a "handshake" that adds latency to the network data transmission.

The RAIDA may be the most efficient payment system in the world. It uses less electricity than an average American household, making it the first truly energy-efficient monetary network in existence. RAIDA uses less bandwidth as it is able to transmit requests using as little as 1.5 KB. AES encryption uses less electricity than SSL encryption. This efficiency is achieved because the RAIDA uses a simple "update" process rather than verifying encryption hashes that require major processing power.

3.3 The RAIDA is Privacy-Friendly

The RAIDA is possibly the most privacy-friendly network for currency ever created. It does not track every transaction. It does not require users to have accounts or provide any identifying information. CloudCoin, built on the RAIDA, is also immune to the attacks of quantum computers. It would be impossible for the RAIDA to freeze CloudCoin accounts because there are no accounts.

The RAIDA is also easy to integrate into software packages and therefore CloudCoin is a "crossover currency". This means it can be taken into the virtual world and video games, traded and then taken back out.

3.4 The RAIDA Achieves the Highest Decentralization of Data

Client-server models such as PayPal have one central database that can be a single point of failure. Peer-to-peer models like the Blockchain have one central database that is mirrored on thousands of servers. The RAIDA has many independent databases that are all unique and do not share data with each other.

PayPal does not have Data Supremacy. Blockchains do have Data Supremacy but are not quantum safe or private. RAIDA achieves both: It is quantum safe and private. RAIDA has no whole-database that can be unencrypted, read by the public or even read by the RAIDA's own administrators.

A decentralized database must store its data so that its data cannot be tampered with, spied on or made unavailable by anyone including the system admins and the creator. The RAIDA achieves this by using redundant authentication systems. Each authentication system has its own database, primary server, mirrored server, backup server and administrators. RAIDAs are located in different legal jurisdictions. Blockchains allow anyone, including governments, to see what money each person has. If a user's address is known by a person, that person can see every transaction that the user has used that account for and how much money the user has. With RAIDA, there is no public data. How is it possible to tell that there is no inflation? Each CloudCoin has a three-byte serial number that limits the number of coins to 16,777,216. Any serial number outside of this is a fake.

The RAIDA does not use "consensus." Consensus is not the truth. The RAIDA uses trust. The Root DNS also uses trust and it has been shown to work. Should a RAIDA be taken over by a hostile organization, users can simply remove that RAIDA from their trusted RAIDA list which is located in their desktop software. Users can also add RAIDAs that they trust. RAIDA Admins can additionally control any other RAIDA that they trust.

Attackers would have to be able to rule all of the RAIDA databases before the RAIDA Administrators and users would be affected by the attack. As of the time of writing in August 2022, CloudCoin has 25 nodes. This is nearly twice the number of nodes that the Root DNS has. Like the Root DNS nodes, the likelihood of all nodes being compromised is astronomically low.

3.5 The RAIDA is Quantum-Safe

The redundancy of the RAIDA is so extreme that no technology that exists at the time of writing, or is even popularly theorized to be possible, can crack a CloudCoin. If one of the RAIDA servers were captured by an attacker, the attacker would only have 1/25th of the authentication data. So, if the attacker was able to decrypt the server, it would not give the attacker ownership of any CloudCoins. In order to crack a CloudCoin, the attacker would need to guess the Authenticity Numbers of a majority of the RAIDA. Each Authenticity Number uses a 16-byte password that is 100% random, and each byte consists of 8 bits, which causes the total possible number of permutations for each Authenticity Number to be 2^{128}, or 3.4028×10^{38} possibilities. The RAIDA has a bottleneck of how many guesses can be done each second. Only 8 million guesses per second are allowed per RAIDA. This means that it would take more guesses than there is the time in the universe to crack the RAIDA, making the RAIDA quantum-safe.

3.6 The RAIDA is Scalable

Strong money requires scalability and simplicity. A non-inflationary currency should require that as adoption increases, counting the money does not become increasingly difficult. As the adoption of other cryptocurrencies has gone up, calculating the cost of transactions has become increasingly difficult. When the cost of a small everyday transaction requires fractions to the hundred millionths, as it does with Bitcoin, it is difficult to calculate without a calculator, and mistakes can easily be made by missing a '0' in the fraction of the currency being exchanged.

The RAIDA allows for the splitting of CloudCoins. In the event that CloudCoin becomes too expensive for simple transactions, the RAIDA Administrators have the authority to ‘split’ the CloudCoins by multiplying the network, infrastructure and fault tolerance of the coins. This multiplies the number of CloudCoins, but causes distribution to remain unchanged, so any owner of CloudCoins now just owns more at a divided portion of the value.

In addition to splitting, CloudCoins can be fractionalized. At the time of writing, the RAIDA Administrators have not caused CloudCoins to be fractionalized, but the RAIDA could be easily upgraded to allow for this to be done. This could be done by creating a second tier of databases, similar to how the .com, .net, and .edu are a second tier to the root DNS servers.

3.7 CloudCoins are Recoverable if Lost

One of the primary challenges facing cryptocurrency is the possibility of permanent loss. While the total supply of bitcoins is recorded and public, the actual amount of bitcoins accessible to the public is unknown. This is because the private key for a Bitcoin wallet can be lost, thereby permanently preventing the bitcoins in the lost wallet from ever being recycled through the economy. There is no way of truly knowing how many bitcoins are in circulation, and the number can only be speculated upon, because bitcoins never re-enter circulation. If the owner of a Bitcoin wallet dies or the hardware that the wallet is stored on is lost, damaged or corrupted, and the private keys are not written down and stored somewhere, the bitcoins are permanently lost. This is a problem that is indicative of nearly every blockchain in existence at the time of writing.

The RAIDA presents a solution to this problem. Just as bank accounts that are inactive for years can be recovered by a governing entity, the RAIDA Administrators are incentivized to continue operating the RAIDA without imposing transaction fees because RAIDA Administrators have the ability to recover CloudCoins that have not been POWNed within the most recent five years. This is great for the ecosystem of CloudCoin because the existing supply in circulation is constant—there is no permanent loss to circulation—and because CloudCoin is the first currency that allows for no transaction fees whatsoever in electronic transfer.

As of writing, the current CloudCoin Manager as released by the CloudCoin Consortium allows for the POWNing of CloudCoins with the simple press of a button in the CloudCoin Manager. The risk of permanent loss is zero, so long as this button is pressed within a five-year period. And, in the event that a wallet is lost, CloudCoins are recoverable through the RAIDATech help desk. All serial numbers are required for recovery, and coins may only be recovered at the end of the five-year period if they have not been re-POWNed (this is done to prevent stealing of already-transferred coins).

4. CloudCoin Governance

As opposed to mining for cryptocurrencies, CloudCoin runs on a network of RAIDAs, which are not freely accessible to the public for authentication. As such, the RAIDA has a governing body made up of what are called the “RAIDA Administrators.” RAIDA Administrators are extremely limited in their governing ability, and it was designed in this way to prevent the problem of hostile or corrupt governance from being able to take over the network.

4.1 The RAIDA is Static With a Few Exceptions

Remember that governance of a digital currency is only necessary if there are decisions to be made. The RAIDA was designed based on the Root DNS so that the code can be upgraded, and that only freedom-loving people could become Administrators. There are only two decisions that the RAIDA and the Root DNS need make that require governance:

1. Should the protocol be updated?
2. Who should be the RAIDA Administrators?

4.2 Should the Protocol be Updated?

According to Article 10 of the CloudCoin RAIDA Constitution, RAIDA Administrators are responsible for writing their own code and are free to use whatever software they like so long as it implements the protocol. The CloudCoin Consortium has provided free-of-charge to the RAIDA Admins three versions of the RAIDA code written in three different languages: C, Rust and C++. In order to eliminate the systemic risk of software failure, RAIDA Admins are encouraged to have no more than nine of them using the same code.

Although it is desirable for the protocol to remain stable, anyone can suggest modifications to the protocol. These changes can be made quickly if the person gets the support of the RAIDA Administrator thought-leaders and provides the funds necessary to alter the code. Many changes to the protocol have already been made based on suggestions from users.

4.3 Should an Administrator be Terminated?

The amended Article 18 of the RAIDA Constitution says that RAIDA Administrators are appointed for life and can bequeath their RAIDAs. The termination of RAIDA Administrators must be initiated by another RAIDA Administrator and the RAIDA Administrators must vote to remove that person. The Root DNS has shown that the administration of such a system can be very stable and without drama or threat. It should be noted that the United Nations and Telecom Federations have demanded that they control the Root DNS.

4.4 Who Should Become an Admin if a Position Becomes Available?

The amended Article 18 of the RAIDA Constitution says that RAIDA Administrators will elect new RAIDA Administrators. To be a RAIDA Administrator, one must be a world-class system administrator, pass a philosophical exam showing a belief in the values of freedom and, most importantly, agreement to the RAIDA Constitution.

4.5 The Role of Supporting Organizations

The CloudCoin Consortium may be misunderstood as central authority that make the rules and hire and fire. However, the CloudCoin Consortium has absolutely no control over the RAIDA, its Administrators or its software.

4.6 Can the RAIDA Administrators Work Together to Steal Coins?

Similar questions can be asked about the Root DNS Administrators:

- Can Root DNS Administrators make billions selling their nodes to adversarial groups or governments?
- Can the Root DNS Administrators create their own domains and make billions off of registrations?
- Can the Root DNS Administrators get rich by giving users false information so that they end up viewing advertisements?

They can, but over the last forty years of operation, they have not and it is unthinkable that they shall do so in the future. It would not make any sense to steal CloudCoins, as the reason for perceived value for CloudCoins comes from the trust of the system. Also, RAIDA Administrators earn CloudCoins by collecting abandoned coins. It would be wholly counterproductive to steal CloudCoins.

The RAIDA Administrators have not stolen any CloudCoins since the RAIDA's inception in 2016 and it is highly unlikely to happen future. It would also be nearly impossible for RAIDA Administrators to get away with stealing. RAIDA Administrators would need to recruit other Administrators in order to steal. The RAIDA Constitution states that anyone who suggests stealing CloudCoins will be permanently expelled as a RAIDA Administrator, and will no longer be able to collect lost coins. Any RAIDA Administrator who decided to organize such a theft would likely be tossed out before recruiting other Administrators in the theft. RAIDATech runs a support desk, and any reports of coins becoming counterfeit due to theft would be noticed immediately. Every incident where a user complains that coins have become counterfeit are thoroughly investigated by RAIDATech and the RAIDA Administrators. All previous incidents like this have been shown to be caused by bugs in the client software and not the RAIDA. The RAIDA Administrators are freedom-minded and have agreed to follow the terms of the RAIDA Constitution.

Here are some other questions need to be answered:

1. Can RAIDA freeze accounts? There are no accounts.

2. Can RAIDA steal money? No, because they have no desire to do that and it would be nearly impossible to orchestrate.

3. Who is responsible for keeping the RAIDA running? The RAIDA Administrators have signed a Constitution promising that they will keep it running.

4. Can the RAIDA be shut down? No. Like the Blockchain and the Root DNS servers, the RAIDA has Data Supremacy and cannot be brought down by hackers, governments, tech giants, AI, quantum computers, RAIDA Administrators or even its creator.

5. CloudCoin in the Market Ecosystem

CloudCoin has a myriad of different potential use cases. The initial proposed use case is as a medium of transfer. The design of the RAIDA allows CloudCoin to be more effectively used as a medium of currency than even fiat currency. As with fiat, value comes from the ability to transact, which is of course the biggest challenge with the adoption of any currency. The threat of monetary inflation by governments created the rise of Bitcoin and other blockchain-based currencies, which are used in millions of transactions, especially in nations suffering from hyperinflation. But there is demand in the marketplace for quick, fee-free, environmentally-sound transactions. Even electronic transfer of fiat, which is done by wire, ACH or other debit and credit service platforms usually charge a use fee, often times greater than 1% of the value of the transaction. CloudCoin is able to fill this void with seamless, free payment systems and applications that are capable of being brought to market. CloudCoin can easily be integrated with ATMs, credit cards and POS systems.

The CloudCoin Consortium has found a need for payments systems to exist in video games. And being that CloudCoin is able to be used as a crossover currency, it has a strong use case as in-game currency in video games in order to draw users to games it exists in, where CloudCoins can be exchanged for NFTs or other in-game elements.

6. Tokenomics

Token Design: CloudCoin is designed to be the perfect money. It is designed to have no inflation, 100% true privacy, instantaneous authentication, no fees, globally scalable, crossover-able into virtual reality and video games, easy to use, recoverable if lost, resistant to theft, quantum safe, and to also contain a Collectible Color NFT.

Proof (of coin Integrity): CloudCoin is the only coin that uses Proof-of-Authenticity instead of Proof-of-Work or Proof-of-Stake.

Total supply: 16,777,216 CloudCoins fixed. The number never increases except in the cases of "splits." Splits cause all CloudCoins to double for all users equally, so that the percentage of all ownership distribution of CloudCoins remains the same.

Token distribution: The original Legacy CloudCoins were minted by the CloudCoin Consortium in 2016. These coins were spent over a five-year development period ending in 2021. Legacy CloudCoins can now be converted into CloudCoin. It is estimated that there are over 30,000 CloudCoin holders at the time of writing.

Network Funding: CloudCoin is the only coin that is funded by the recovery of lost coins. Any coin not POWNed after five years is considered lost and can be recovered by the RAIDA Admins.

Fees: CloudCoin has no fees.

Governance: CloudCoin has no governance. See "The RAIDA is static with a few exceptions" above. The CloudCoin Consortium is a group that promotes CloudCoin but has no say over CloudCoin's administration.

NFT: Each CloudCoin has one unique color from the RGB color spectrum. This adds a non-fungible element to CloudCoins.

Primary Exchange Listing: BitMart.com (June 29th, 2022)

Starting List Price: $0.50 (50 cents USD)

Total Market Capitalization Based on Initial Listing Price: $8.4 Million

Number of Transactions: There have been over 671 million Legacy CloudCoins POWNed in the first six months of 2022. Note that CloudCoin POWNs coins using the RAIDA and does not have transactions. Transactions take place outside of the RAIDA Network.

Ticker Symbol: CC (Not to be confused with CCE which is the CloudCoin Ethereum token)

7. Summary

To date, the RAIDA has achieved the highest performance of any digital currency or payment system and has just enough centralization to allow for updates to the code. The RAIDA, like the Root DNS that it is inspired by, has never gone down. It is fast, scalable, energy-efficient and free. We can count on the RAIDA to dominate the future of digital currency.

8. The CloudCoin v.2 Project

The CloudCoin Project has been in development for the past five years. The original coins are now called Legacy CloudCoins. The new coins that were released June 26th, 2022, are now called CloudCoins. The only way to obtain the new CloudCoins initially is to exchange for Legacy CloudCoins.

All client code and protocols will be open to the public using the MIT Opensource license. This code is provided free of charge by the CloudCoin Consortium. This ensures that the CloudCoin can quickly be adopted by the global community. The exception is the RAIDA Server software which is protected by a patent (granted 12 May, 2020) to eliminate the possibility of thousands of copy-cat coins.

There is a fixed amount of CloudCoins with serial numbers 1 through 16,777,216. This is a three-byte integer that ensures that any serial numbers outside of this range are counterfeit. New coins cannot be created unless CloudCoin splits. If this happens, then all CloudCoins will be multiplied.

9. Acknowledgements

I would like to acknowledge all of the people involved in the development of the RAIDA. I would also like to acknowledge the CloudCoin Consortium and the Board of Directors for their efforts in reviewing and editing this paper.

About the Author

Sean Worthington is the CEO of RAIDA Tech where he develops technologies based on the RAIDA.

Prior to that, Sean has worked for twenty years as a computer science instructor at Butte College in northern California.

Sean is also the patent holder (USPTO #10,650,375, granted 12 May, 2020) of the RAIDA and author of Beyond Bitcoin, the Future of Digital Currency.

RAIDA Tech provides unhackable solutions for business. Learn more at **https://RaidaTech.com**

Contact Sean: CloudCoin@protonmail.com Skype ID: Sean_worthington@hotmail.com

References

[1] "Inflation in Zimbabwe Essay Example | Topics and Well Written Essays - 1500 Words", n.d. https://studentshare.org/history/1457991-inflation-in-zimbabwe.

[2] Downey, Lucas. "Digital Gold Currency (DGC)." Investopedia. Investopedia, September 13, 2021. https://www.investopedia.com/terms/d/digital-gold-currency-dgc.asp.

[3] [The Limits to Blockchain? Scaling vs. Decentralization.] Social Science Research Network. Cybersecurity, Privacy & Networks eJournal. Accessed 21 April 2019.

[4] Dale, Brady. "Everyone's Worst Fears About EOS Are Proving True." CoinDesk Latest Headlines RSS. Coindesk. September 19, 2019. https://www.coindesk.com/markets/2019/09/19/everyones-worst-fears-about-eos-are-proving-true/

[5] https://www.pearsonitcertification.com/articles/article.aspx?p=1708668