Greencoin: The Future of Cryptocurrency

Wang Yong Chan
wangyongchan@gmx.com

1. Introduction

Since the inception of the internet, organizations have relied on the transfer of real-life commodities for digital assets. This paved the way for the dot com boom and the explosion of computer technology. The human race relies on the power of computer science and the flow of information via the internet more everyday. Digital currency has ruled the internet since birth and still does. Credit cards, gaming companies and live streaming services all rely on forms of digital currency usually backed by big banks. Then in 2009 a global financial recession suffocated the Earth and as the economy retracted, the original crypto punks invented an alternative to the established hegemony. A fungible publicly available ledger utilizing math and cryptology to ensure greater security than any printed currency. For over a decade Bitcoin has had a %100 success rate as it was designed to. Unlike other currencies which rely on the issuer for ethicacy, a cryptocurrency relies on mathematics. While all advances in digital technology can lead to growth in the human race, none as much as cryptocurrency. The concept of a global commanding currency immutable by any actor would give financial security and access to all people. This would divert the worst consequences of large scale economic downfall, similar to what occurred in 2009 and again in 2020. Bitcoin was revolutionary but lacks scalability to become a commanding global currency simply due to unnecessary and confusing redundancies in the protocol. The future of cryptocurrency lies in a simple scalable protocol that promotes minimal computer processing usage and instantly verified, fee free transactions.

What is needed is a simplistic protocol designed for the user. Bitcoin's blockchain technology and proof-of-work system complicate the protocol for the average user. While communication with computers always requires learning and cryptology is mathematically intensive, complicating the process while introducing transaction fees and incentive to maximize power usage is harmful to scalability. Bitcoin will never become the global currency that cryptocurrency has the capability of becoming if it takes 10 minutes and $5 USD to verify a transaction when the network is stress free. Cryptocurrency should give incentive for every user to participate and provide free and instant trusted transactions. This may not be a simple creation but the idea behind the currency can be. There is an intangible truth behind the math and science which makes

cryptocurrency possible. This truth is eroded when users are expected to provide transaction fees when they are willing to provide a minimal amount of processing power to the system. Meanwhile gigantic crypto farms have led to the banning of mining by the government of China, the country most invested in cryptocurrency. Any one farm could run the entire Bitcoin network twice over or faster on a server-to-client protocol. This is not inherent in peer-to-peer networking and can be remedied with a protocol that gives each user the capability to participate in the network however much they want. This new cryptocurrency is named Greencoin because of the color's correlation with business and our environment.

2. Protocol

Protocol is the process behind a cryptocurrency. A cryptocurrency is just the acclimation of users that choose to follow the protocol. If the user base decides to update the protocol, then the cryptocurrency would fundamentally change. The integrity of the user base is reliant on the acceptance of the protocol and disagreements in the protocol can lead to major forks in the coin like with Etherium Classic and Etherium 2.0. The concept behind the protocol for Greencoin is a scalable global cryptocurrency to become a world-wide standard. This means the protocol should be fundamentally inclusive for the greatest number of users. Transaction fees, congested networks and high power requirements are all exclusive. Greencoin should be supplied to the system simply to accommodate a growing user base and should be distributed evenly among all holders of the coin. Transactions should be free and instant with a reliance on the user base to supply the processing power necessary for the network to operate. Greencoin delves into the fundamentals of what a perfect cryptocurrency protocol would look like and does not rely on schemes like proof-of-work. Instead every user is given equal opportunity to participate in verification of the network.

In order to implement a peer-to-peer network such as this a precise protocol is required however the concept behind the protocol can be simplistic. This is like Bitcoin and the proof-of-work model. While the concept behind requiring an attacker to have greater than %50 of the processing power of the entire network to successfully attack the network might be simple, the implementation of this is complicated for any lamen. While the implementation behind Greencoin is complicated, it's up to the computer literate population to help educate other users and communicate with the network. A well designed application is necessary to the adoption of the coin so that users do not need to know the intricacies of the protocol to participate. While large institutions like Coinbase provide platforms for users to purchase digital currency, a real cryptocurrency would

provide an open-source community created application for buying and utilizing the coin. An all-in-one application is optimal for an involved user base. If participating in the verification of messages is as simple as turning on an application and connecting then the user base will easily grow. Bitcoin requires multiple applications and a specific environment to function as a network node. Greencoin strives to provide a single application from which users can send transactions, connect to the network, verify transactions and assist with the connection of new users without requiring understanding of protocol specifics.

The fundamentals behind Greencoin are similar to those of any cryptocurrency. These specifications are standard cryptology and are optimal for a functional cryptocurrency with the mathematical capabilities of the time. Each user creates a Private Key using ECDSA (Elliptic Curve Digital Signature Algorithm) over a prime field from which they also create a Public Identifier (Generally stored as a hex encoded string of an x and y point consecutively). Messages are signed using the Private Key and verified with the Public Identifier to ensure authenticity. Each user also connects to a small number of other users in order to create the network and pass messages to the user base. Networking standards are also implemented to ensure that messages cannot be sent that destroy or intentionally hurt the system. Greencoin documentation of protocol is precise and all applications used should be open-source community driven projects. Greencoin operates with TCP on port 39933. The first Greencoin was started at 12:00AM PT(Pacific Time) 1/1/2022 by:
68abb56693f3c234180dcbde88cf70ca63994b14b79d5de0f955eb88c365701ehb15d48e5d6b52539c5d08eaab1addcb432f58adc816d721474b046113fd17cfeh.

3. Locations

The first tool that Greencoin utilizes which is new to cryptocurrency is the concept of location and age. The network operates by sending messages through the system based on conceptual mapping of the system. This is accomplished by relating each user's Public Identifier with a unique location based on the order of the location. The order of the locations define the age. Locations are strings of integers separated by periods. They are based on the user's location that created the new user by sending coin to a new Public Identifier. Locations are indexed from 0. The first location is 0 with 1 being the next youngest location and new user, then 2, then 3 and so on. New locations from the integers after 0 are indexed from 0 following a period and the previous location. For example, if the user at location 1 created a new user, they would be 1.0 and if location 1 then created another user they would be 1.1, then 1.2 and so on. A location's age is evaluated as the

number of periods in the location. For example location 5 would be age 0 and location 1.0 would be considered older than 5 even if 1.0 originated earlier than 5.

Locations are assigned directions based on their relationship with other locations. There are four different directions; up, down, left and right. These directions determine how messages are sent throughout the system. Directions are also either primary or secondary, meaning connections between users can be classified in 8 different categories; primary up, secondary up, primary down, secondary down, primary left, secondary left, primary right and secondary right. Not every location will have one of each of these connections however users should maintain one of each connection if it exists. This means the system operates best with each user having a maximum of 8 connections. Primary connections are considered closer than secondary connections. If a primary location exists but the user is not connected then the connection can be replaced with another secondary location, with the closest of the two locations serving as the primary connection.

Each of the four types of locations have different parameters and each can only have 1 primary location or less. Locations to the left are younger in age. For example location 3 is to the left of location 4.5. The primary left location is the parent of the user. For example the primary left location of 4.7.8 is 4.7. Locations up and down have the same parent as the user and the same left locations. Locations up have a smaller end value and locations down have a greater end value. For example location 5.30.42 is up from 5.30.50 and location 7.13 is down from 7.9. Primary up and down locations are the end values directly before and after. For example location 6.8 has a primary up of 6.7 and a primary down of 6.9. Locations to the right are descendants of the user and the primary right location is the first descendant. For example location 4.7.8 might have a right connection with location 4.7.8.61.6 but the primary right location is 4.7.8.0. Not every location has an up, down, right and left location especially if the right or down user hasn't been created yet. Also locations whose last value is 0 will have no up locations and integers have no left locations. Finally, a primary left connection must also correspond to a primary right connection.

4. Networking

The network consists of users and their connections to other users based on location. The closest connections are always prioritized to form a complete network. Users can accept messages from anywhere as long as the message follows the protocol allowing for the connection of new users. Messages are only sent to primary or secondary locations based on type of message. There are four different types of messages and the

type is referenced as the first letter of the message. The four types of messages are; (T)ransactions, (D)irect message, (R)eciept and (H)ourly update. Each message contains a header of 32 bytes with each header starting with one of the four letters denoting the message type, followed by the age, then location, then a period, then the size of the rest of the message and then a period. The message header is always directly followed by the coin count which is the total number of Greencoin. The coin count is used to ensure no message is sent through the network twice. Headers can be shorter than 32 bytes but not longer. An example header and coin count could be D2.1.5.4.300.154

Transactions are sent to every user in the network once. To accomplish this, transaction messages are sent left then up as far as possible then sent to every primary down and right connection. If a primary down or right location exists but the connection does not then the message is sent to the next closest connection. Transactions received from the right or down connections are sent to the left or up if no left connection exists. Transactions are only processed after being received from the left or up connections and only after they've been repeated to the primary connections. Transactions are written as a header containing the location the transaction originated from followed by elements all separated by periods. The first element following the coin count is the Public Identifier of the user followed by the coin the user is sending. Then comes as many outputs as wanted with each output consisting first of the output location followed by the output Public Identifier then the coin for that output. The final element is the signature using the Private Key of the message following the header. An example transaction would be: T LocationAge. InputLocation. BodySize. CoinCount. InputPublicIdentifier. InputCoin. OutputLocation. OutputPublicIdentifier. OutputCoin. OutputLocation. OutputPublicIdentifier. OutputCoin. Signature.

Transactions are checked against a built ledger and then the ledger is updated if the transaction is verified. When the transaction is verified, the transaction location is sent a receipt. Receipts are sent exactly like direct messages yet may be picked up by new users to help build a ledger. Receipts and direct messages are first sent left then up until the farthest left elements of the locations are matching. The message is then sent along the primary path following the same elements to the right until the target location is reached. Direct encrypted messages can be sent throughout the system yet it is not recommended unless necessary because all messages take some processing power. Simply send a message with a message header starting with D and then the target location and message size followed by the encoded message using the target location's Public Identifier. Receipts are sent with a message header starting with R followed by the target location then size. After that comes the Public Identifier of the user who sent the receipt, then the message they verified and a signature of the message using their Private Key. Finally

receipts are appended with a signed ledger from the last hour. An example receipt would be: R LocationAge. InputLocation. Size. CoinCount. InputPublicIdentifier. VerifiedMessage. Signature. SignedLedger.

Every hour one new Greencoin is added to the system proportionately throughout the user base. The new coin is added by dividing each user's individual coin count by the total number of Greencoin then adding that number to their coin count. Since the first Greencoin was created at 12:00AM PT 1/1/2022 the total count of Greencoin can be calculated by counting the number of hours since the first Greencoin and adding 1. The network goes through an update every hour when a new coin is created. Users add the new coin proportionately to every entry in the ledger and then know users send an hourly update to the network. Known users are the fundamental to the network and allow for some users to maintain the entire ledger while others maintain only a random allocation. Known users actively maintain the entire network by accounting for every Greencoin and providing the processing power necessary to verify every transaction. Known users create a hash of their ledgers when a new coin is created and deliver it to the network via an hourly update. Every user maintains a list of the known users whose hashes match to provide for new connections. Hourly updates are distributed in the same manner as transactions and are written as an H followed by the sender's location age, location and body size, then coin count, then the sender's Public Identification followed by their ledger hash and Private Key signature of the Public ID and hash. An example hourly update would be: H LocationAge. InputLocation. Size. CoinCount. InputPublicIdentifier. LedgerHash. Signature.

Finally special messages are utilized by users to connect to the network. Users connect to the system by sending special direct messages to the network. Users can send messages to users they know exist without being part of the network by sending the messages to a distant location but they cannot receive messages outside of primary or secondary connections. Users are expected to connect and disconnect from the network randomly so having a standard for connection requests and connection acceptance is necessary. Connecting also allows every user to securely build the current ledger and be confident in the veracity of it. Connection requests are created as direct messages and sent starting with D followed by the destination locations age, location and size of the body. This is followed by the coin count, location of the sender, then a period, then the Public Identification of the sender followed by a period then crequest(period). The sender then supplies the IP/Hostname open for the Greencoin application on the users port 39933 followed by the Private Key signature of the message body. After the new connection is made, the request recipient is expected to respond with a connection acceptance message. These are written the same as connection requests except crequest is

replaced with caccept and the IP/Hostname is replaced with a the most recent list of known users. An example connection request would be: D TargetLocation. BodySize. CoinCount. LocationAge. InputLocation. InputPublicIdentifier. crequest. InputIP/Hostname. Signature. An example connection acceptance would be: D LocationAge. TargetLocation. BodySize. CoinCount. InputLocation. InputPublicIdentifier. caccept. KnownUsersList. Signature.

Greencoin protocol is precise for the environment that currently exists but can always be updated by the community if there are major changes in the environment. Greencoin is created for end users and application developers both to have an exact and simplistic way to connect to the network. Transactions can be sent to the system from any location and the ledger can be built without the right connection in all cases. An example connection would be: a disconnected user sends a transaction, and a connection request to the primary up, down and left locations. The user creates three new connections up, down and left and receives three lists of known users, two match so the user selects those two assuming the third has an error. The user then collects all receipts and makes all secondary connections. The receipts of known users are used to construct the user base than the rest of the receipts construct the allocation of Greencoin throughout the ledger. Once the ledger is built the user judges the traffic on the network and allocates a random portion of the ledger equal to the processing power the user wishes to use. Every user verifies the transactions from their ledger, delivers all messages throughout the system and adds new Greencoin evenly throughout the system at the top of every hour. A transaction verification consists of checking the ledger for the input coin and input Public Identifier, checking the signature of the message, then checking the output locations and output Public Identifiers and then updates the ledger. The input coin will always move if the signature is correct so it is paramount the transaction writer correctly enumerates the location and Public Identifier because if the verifier of the transaction does not have the data on their ledger, they will assume the data is being kept by another user and not include it even if they are a known user. All users also maintain an updated list of known users from the previous hourly update and create a stamp for receipts every hour; a copy of the ledger at the time of the last new coin creation and a signature of the copy. To ensure the same message is not sent to users, a hash is made of each verified message and checked against each new message. By checking the coin count included in every message, the hash database can be emptied every hour. If the user can maintain a complete ledger they function as a known user by providing an hourly update message.

5. Conclusion

Greencoin's protocol utilizes specific logic that provides authentic and trustable ledger maintenance. Users choose how much of the ledger they want to verify and the health of the system is reliant on far less processing power than other cryptocurrencies. Greencoin removes the incentive for massive crypto farms and instead moves the creation of new coin to an investment in the current user base. Known users maintain the ledger and can instantly verify transactions based on their own processing power. Users do not require all transaction history to participate in the network and public databases maintained by the community can serve as collaboration on the authenticity of the protocol. In general, the process power of Greencoin comes from the users that input transactions. The users that send out transactions are expected to verify the receipts. Greencoin documentation is specific to provide application designers to have a unified approach in community applications which are necessary for any decentralized cryptocurrency. The product is the future of cryptocurrency; a scalable cryptocurrency that provides instant, fee free transactions to every user while using the most minimal processing power. The first Greencoin was created on 1/1/2022 at 12:00AM PT(Pacific Time) by:
68abb56693f3c234180dcbde88cf70ca63994b14b79d5de0f955eb88c365701ehb15d48e5d6b52539c5d08eaab1addcb432f58adc816d721474b046113fd17cfeh.