Universal Currency [UNIT]

UNITCOIN a decentralized, peer-to-peer digital currency.

Abstract

In the age of globalization, things are changing rapidly. In the past decade, technology has an unavoidable role in our lifestyles. In adjusting to the changing technology is essential in order to meet with people lifestyle in the age of globalization. The exchange system of Unit Coin fulfills people in the globalization age through technology using Algorithm SHA-256, which are cryptographic hash functions designed by National Security Agency or NSA hashing data for the Unit Coin system and Unit Coin can be both Proof of Work (PoW) and Proof of Stake (PoS) taking the role as a drive to ease peoples lifestyles in the age of globalization. For those holding Unit Coins, they can use them as a medium for the exchange and a medium for services similar to other currency used to exchange goods and services in the daily life.

Origin and Importance

In the age of globalization, things are changing rapidly. In the past decade, technology has an unavoidable role in our lifestyles. Adapting technology to people's daily life is important and in order to meet with people lifestyle in the age of globalization. Adapting the Blockchain technology is therefor important for people of current age. In general, making of any transactions or agreements between individuals or organization, both parties had to have a medium in a form of person or organization as a third person to witness the existence of those transactions or agreements in case one day any of the parties breaches the mentioned contract, this medium will help as prove. An obvious example of a medium is the bank, which always served as a medium of the financial transactions, but the existing of the medium is not limited to only the financial business, but also covers all types of business. The issue of making these transactions or agreements, from the technological perspective, organizations always had agreement storage or transactions data in the digital form so far, whether it is files or recorded into the database and each party making these transactions or agreements had to keep their data, but as the old technology is not designed to guarantee that the stored data between both side's individual or organization is always correct as the same and there is a possibility that one of the parties may alter their copy of the data, so the person served as the medium must store these data to be compared later. Blockchain is a technology substituting these mediums. Making transactions between individuals and or concerned groups can be completed directly without any mediums. Also the data can be used in the digital form, making the transactions fast. Besides, the Smart Contract can also be used to push the process as the standard determined in the mentioned agreement. This guideline greatly creates the capability for the work process, also eliminates the time and cost of the transaction and because each transactions are recorded continuously and indefinite, the examination can be done throughout the lifetime of the asset. This is even more important if the original data is necessary for the investigation of the assets' validity. Each transaction will be investigated within the network by using complex encryption and investigated freely. Hence the precision of the data is assured and this credible data is one of the important grounds of making a use out of internet of things: IoT, which is a work progress connecting current assets through the internet controlled in a closed system.

To summarize, the benefits of the Blockchain are as follows:

1. High transparency , it can be inspected retrospectively
2. No possible corruption, because the data cannot be altered
3. When the transaction or agreement are stored as data, analyzing these data to enforce to comply with those agreements or transactions can be done automatically and can also be adapted for other type of use such as notification for the nearly expired agreements etc.
4. No medium needed for the making of these transactions or agreements, this saves a great amount of both time and expenses.

Therefore it is right to conclude, that Blockchain can be adapted for many above mentioned activities needing the transparency and credibility etc.

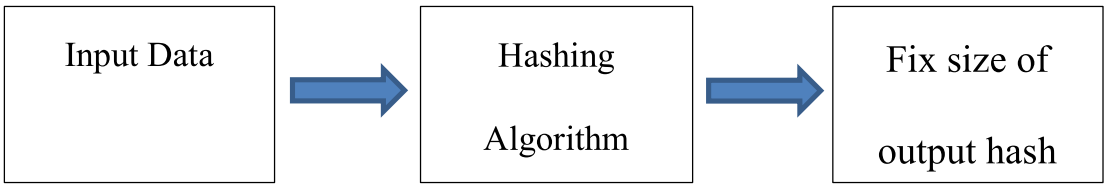
Principle of Unit Coin Creation

Unit Coin comes from modifying Source Code Bitcoin to support the Proof-of-Stake work, but can still work as Proof-of-Work. So Unit Coin is in the form of Pow/PoS Hybridge.

Design concept and UNIT COIN related technology

Unit Coin uses Algorithm SHA-256, same as Bitcoin, SHA256 is one of the encryption giving us new data called data hashing. Data hashing is to change various data, any data in the digital form of bit with the definitely fixed size.

Work Principles for converting data of SHA-256



SHA-256

Benefit of using SHA-256 to hash data

1. It is a one-way hash function; de-hashing the old data is not doable

2. For the purpose of mining; as SHA256 is suitable for Proof-of-Work mining
3. Suitable for the building of Wallet Address; as the building of Wallet address must consist of 2 items, which are:

    3.1 Public Key

    3.2 Private Key

    Usually the Public Key has very long data, so the Public Key needs to be shorten first. One of the shortening process of the Public Key is to hash with SHA256, therefore the Public Key that has been through the shortening process will be in short and easy to understand form and we call it the Wallet address. [Example of Public Key]: 0244 86EA 42E1 879B 4CD9 EACC 0672 3AC3 324C 2A3C 1E33 1C46
    28E7 ADF6 7FFE A878 DF

    [Example of wallet address]: PWexasVupBvgyBAbGFMQaGV7TinSHqj2TM

Unit Coin is both Proof of Work (PoW) and Proof of Stake (PoS)

Proof of Work (PoW)

Proof of Work is a set of rules or protocol set by a group of developer of those coins. The main purpose of the creating them is to protect DDos (distribute denial-of-service attack) attack or an attack with multiple computers sending request to attack the one server with the aim of over-working the server and crash. Currently, the Proof-of-Work is an idea that has been genius and wisely adapted for Bitcoin by allowing trustless and distributed consensus trustless system and distributed consensus enables you to send the money to anyone without needing any banks or any third person. For long distance money transfer and the receiver needs the money immediately, you may need the banking system or Visa, MasterCard and PayPal, as they always record the transaction data of the customers in the user account. An easy example that can be explained is if Mr. A sends money to Mr. B for the amount of 100 Baht, the medium or trusted party will key in the data into the system that the bank account of Mr. A has 100 Baht less while the account of Mr. B is increased by 100 Baht. This is the function of the third party system, which they have to trust. However, in Bitcoin and other Crypto Currencies, each person keeps a book bank or ledger (Blockchain) of everybody in the world who uses those coins, so there is no need to trust any third person anymore.

Using Proof of Work for mining

Proof of work is “Criteria Requirement” which needs power to process in the computer or in other words mining. This power to calculate or mine is used to create and records the trustless transactions (also called Blog) on the distributed ledger called Blockchain.

2 Objectives of the mining

1. Used to inspect the transaction made newly or to protect the fraud from the money payer such as “twice payment”
2. To create new digital coins by rewarding working miners

When transactions are made, these happen in the background system

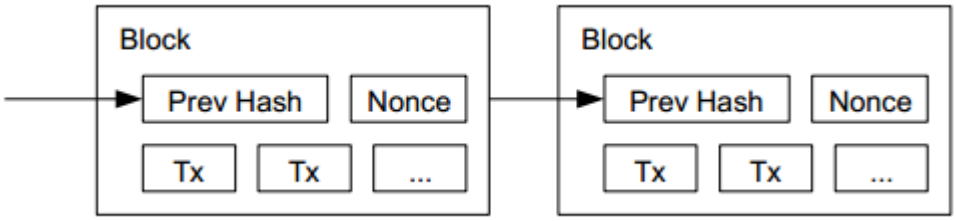
- Transactions are bundled and stored in a data collector called a blog.
- Many minors will check whether those blogs are real or not.
- In doing so, minors must resolve mathematical equation called the problem of proof of work
- The award will be given to the first minor solving the equation and successfully closed the blog
- Blog keeping the inspected and closed transaction will be kept in Blockchain

The feature of this mentioned equation is its imbalance or easily explained they have to be made hard to solve yet easy to be inspected on the network. This concept has different other names such as CPU cost function, client puzzle, computational puzzle or CPU pricing function.

Minors on the network must compete with each other to solve the mathematical equation which is never to be solved by any other way than to brute force. Therefore it takes somewhat long time and hard to mine.

When minors successfully solved the equations, it will be announced on the mining network that the crypto currency prize has been found as the protocol enabled.

From the technological technic, crypto coins mining is a step of inverse hashing as it determines the nonce to decrease the level of data of the blog from the defined level.



The stage determined is called difficulty, used to determine the challenge of the mining power, which means if higher power minor jumps into the network, the difficulty mentioned will increase. This duration for the closing blog and new blog is calculated efficiently. This stage will also increase the cost of new blog building or mining. It is to force the minor to upgrade their mining equipment for the balance of the general economy. Updating the difficulty will occur every 14 days and the setting of the difficulty to create new blogs is calculated for new blogs to appear every 10 minutes. Proof of work is not only used on Blockchain of Bitcoin, but also used in many other coins and Unit Coin is one of the coins that can be made proof of work.

What is Proof of stake in general?

Proof of stake is another different way used to inspect the proof of stake transaction. It is another algorithm and the objective is still the same as of proof of work, but the process to achieve the goal is different. The concept of proof of stake is from the Bitcoin Talk Forum in 2011, but the world's first coin is the algorithm called the Peercoin, which started to be used in 2012. After that, ShaodowCash, Nxt, BlackCoin, NuShares/NuBits, Qora and Nav Coin existed. What makes them different from proof of work, which normally the award are given through mining or solving the equation to confirm the transaction inspection and create the new blog. In proof of stake, creating a new blog is determined by the "richness" of the coin holder or in other words called stake.

Another difference is that coins using proof of stake algorithm are created all at once in the beginning and the amount of them will never ever change. That means that in the Pos system, there is no reward for creating new blogs. So the stake holder will receive fees instead which is not different than mining in proof of work where in order to find distributed consensus, minor needs a lot of electric power, referred to the information of 2015, building 1 Bitcoin consumes electric power of 1.57 American household electrical power consume and these electrical costs are paid in cash, That may cause problems in the economic value of cryptocurrency coins in the long term. In the latest research, the experts argued that the confirmation of the transactions of Bitcoin may consume the power usage of Denmark in 2020.
Every computer owner would want their computer safe from hacker attacks especially if it is about finances on your computer. So the question is, is proof of stake better than proof of work? Experts are concerned about this. Also, users in the community are skepticalTo use the proof of work, Hackers or persons with bad intention are guaranteed that they will never be hacked Due to expensive and high quality computer accessories.
In fact, to hack the system of proof of work costs a lot, which might be even higher than the amount intended to be stolen. By using the proof of stake algorithm can also prevent hacking as well. Without the adequate protection or sanctions, the proof of stake system may be easily penetrated and attacked.

UNIT Coin's Proof of Stake

Difference of pure proof of stake and proof of stake in unit coin is The proof of stake in the coin unit does not have all the coins, but the coins from the proof of work are kept And there will be a new coins made of this action is 1% of the coins kept per year. The Condition is to keep in the wallet for a minimum of 1 hour until a coin is generated in the system. It also does not include the conditions that must be competed who will be the coin generators in the network Based on the number of coins with every pocket.

Consensus Hybrid PoW + PoS System used in Unit Coin

Unit Coin is Hybrid PoW + PoS. Unit Coin holders are involved in determining the direction of the coin, Makin Unit Coin a coin that can truly be decentralized. Any experienced developer or Members who do not have any technical knowledge can offer improvements or new features and it is also possible to decide which direction the unit coins should be developed. In terms of technology

Unit Coin operates by voting mechanism which is Useful and flexible
(Using barcode keys and microblocks). To streamline the Hybrid PoW + PoS compliance program to be more efficient and flexible, So PoW and PoS are equally important in the Unit Coin ecosystem.
PoS mechanism also uses monitoring and counterbalance.
If there is no consistent network And Miner was suspected of being a fraudulent person, Major coin holders cannot vote for their mining. The PoS mechanism also allows the unit coin holder keep the coins in a wallet instead of the exchange which is ready to be traded and It also has a positive impact on the ecological system as the public will focus on the application of coin technology rather than short-term price fluctuations.

Accepting Hybrid PoW + PoS guarantees a price per unit of PoW as The cost of mining must be stable Because miners will not proceed to sell the unit medals received at a lower price than what they cost to mine.
In addition, the processing costs that are increased will increase the price of coins Reduces the problem of combining the PoS mechanism Hybrid POS / POW. It is a safe alternative to being attacked with 51% because it has PoW / PoS Hybrid work system, therefore It cannot control only the speed of the excavator.

Another advantage of using Proof of Work and Proof of Work is Unable to attack network by 51%. 51% of the attacks targets on the blockchain, this attack is usually done by Miner Or a group of mining workers controllers receive 50% with 51% attack. The intruder will be able to withhold the transaction, theoretically, coins can be used twice. This type of attack often occurs with new coins with low network intrusion prevention, Coins will be damaged by 51%. For example, Shift, Krypton, HTML5 and WildBeastBlock in the past With PoW and PoS shyroll. Unless the user has a most PoW hash rate and most PoS rates also find the parameters set by the Velocity system which is impossible to be attacked by the Espers with the Espus hybrid system. PoW attacks will cause chain change targets resulting in temporary block controls. At the same time, attacking the PoS blocks will require a tremendous amount of money.
With this system, Espus is a safe method for 51% Network Attacks than other Coins using PoW / PoS

Main advantages of Unit Coin

1. Energy saving. Can generate a new coin without turning on the miner.
2. Safe from 51%system attacks. Because of PoW / PoS Hybrid works, it cannot be controlled by the speed of the miner only
3. The appropriate amount of coins and coinage. There are new coins only about 250000 units per month, resulting in the amount of coins and prices in the appropriate range.

Unit Coin Features

1. Name: Universal Currency
2. Symbol: UNIT
3. Algorithm: sha256
4. Interest: 1% / year

5. Min age: 1 hour, no max age
6. Maturity: 15 confirmations
7. Total Coin: 210,000,000 UNIT
8. block 0-100 = 0 UNIT
9. block 101-210000 = 100 UNIT
10. block 210001-n = 5 UNIT
11. block size 4096kb
12. 60 second block time
13. pos start @ block 10001

Future Coin Unit Development Plan
Future Unit Coin will develop additional functions of coin for the Unit Coin. It uses the principle of OmniLayer. This will cause Unit Coin to have a layer that will break many other the coins and will solve the problems that developers agree to fit the coin and can make Unit Coin more acceptable to make Unit Coin accepted internationally in the future.

Conclusion

Unit Coin will use Blockchain technology has high transparency can be traced back from all parties; they cannot be corrupt because the information cannot be forged. When transactions or contracts are stored in the form of data, use of such information to enforce the contract or transaction is easy. Those can be done automatically. Unit Coin uses the same algorithm as Bitcoin, which is SHA-256 Algorithm.
The advantage is that one-way hash function cannot de-hashing, Suitable for creating a wallet address. Unit Coin is like a hybrid between Proof-of-Work + Proof-of-Stake and in the future will develop a further Function Coin that they can break the coin into many more coins and will solve the problems that developers agree to fit the coin and can make Unit Coin a reliable coin. In the future, Unit Coin coins will be accepted internationally. Therefore, Unit Coin is suitable for holding as crypto currency that can meet the needs of people in the future. It is a reliable digital currency, easy to apply. It is a medium to exchange goods and services with ease.

Reference

https://www.techtalkthai.com/introduction-to-blockchain-for-everyone-in-5-minutes/

https://www.techtalkthai.com/6-business-benefits-of-blockchain/

https://www.blognone.com/node/47074

https://blockchain.fish/bitcoin-address-2/

https://en.wikipedia.org/wiki/SHA-2#Pseudocode

https://bitcoin.org/bitcoin.pdf

Translation

https://medium.com/dcen/hashfunctionbitcoin-471f7c59440c

https://medium.com/dcen/hashing-algorithm-in-blockchain-367f09e043cf

https://questions.coincheckup.com/novacoin/what-is-novacoin-nvc/

https://siamblockchain.com/2017/08/13/proof-of-work-vs-proof-of-stake/

Translation