BITSOAR

The Digital Currency that Prepares the Future

2017.11.10

INDEX

The 4th industrial revolution and the block chain

What makes the existence of digital encrypted currencies such as bitcoins possible are the block chains. This infra utilizing the Crypto-technology and distributed networks, "proved that keeping public transparent records online safe is possible Also, many experts had foreseen, the blockchain to become a phenomenon that would shake the global market. It's almost like reminiscing on the advent of the internet, and the impact Yahoo, Netscape had in the world, through electronic searches, electronic transactions, emailing etc.

Every single individual involved in a specific transaction, is the one certifying for the validity and safety of the blockchain through its distributed network. There is no room for falsification, counterfeit, or similar. The transactions are shared, transparently with the public. In comparison to the past, now we can make this possible with less computing resources. The AI, and IoT technologies, when connected, create a communication system among objects, enabling automated tasks to be performed, and that's when. Blockchains will play a valuable role.

Blockchain Technology Status

Since the very beginning the Blockchains were public and available to everyone and also known as Public Distributed Ledgers. But as bitcoin has shown us, the public distributed ledgers do carry a set of technical and empirical problems. Especially, the fact that a network where pretty much everybody in this world has access too, maintaining and managing it requires a plethora of resources, how for withdrawals the internal/inside information is publicly available, the slow speed and the name of the parties involved in a transaction etc. There is a downside to it.

This is why, the Private blockchain, that operates around financial institutions only, with a limited number of participants in a network is getting this much spotlight. It doesn't need to have a massive unrealistic computing power, to maintain its network's safety, but it is able to also keep up with the in real time transactions and account managing. This private blockchain is also known as the certified distributed ledger. This new system can resolve all the problems public

blockchains carried as well as offering an effective management system.

BITCOIN?

2009.01.03 Satoshi Nakamoto develops the world's first encrypted digital currency. Bitcoin's currency unit is the BTC. Unlike any other currency, it's the first one to allow fast and safe P2P transaction, without the intervention of the government, centralized banks or any type of financial institution, also unlike conventional currency that can be printed at the wish of the government, its distribution volume is limited to 21 million. Every ten minutes, 50BTC is mined and the mining reward has been reduced to a 4 year-cycle.

- First ever bitcoin produced: 2009. 01. 03 (reward 50BTC)
- First block reward halving: 2012 .11 .28 (reward 25BTC)
- Second block reward halving: 2016 .7. 10 (reward 12.5BTC)
- Third block reward halving: 2020 .7 .(Predicts) (reward 6.25BTC)

Also, bitcoin uses a distributed logging and decentralized system, that guarantees
The transparency of its transaction, much more than any other financial institution. Anyone would have access to this public distributed transaction log system, and verify the details.

As of 2017. 11.05, one 1BTC was traded for 835 million KRW. It has a fluctuating price value , and in 2015.01 it plunged to 29.000 for 1BTC. When it was at its peak back 2013, it had even reach a million KRW for 1BTC. In 2017.05. 25 it suddenly went up to 422 million KRW for 1BTC. And in the same month on the 27th, went down to 270 million KRW. 2017, 06 remained a bit stable, selling around 320 million KRW. And in 2017.07.16 it faced the hard fork crisis, plunging down to 220 million KRW but it picked right back up, on the 1st of August, when the hardfork took place, going up to 320 million KRW, and up. Afterwards, reached up to 500 million KRW, and in 2017 10. 05 ~06 , in just one day, it went up about 800.000 KRW, and the highest peak was around 650

million KRW.

The Importance of BITSOAR

The biggest flaw of bitCOIN is that it isn't safe, there is nothing regulating it, no legislation, policies, regulations etc. even with the undeniable fact that is a revolutionary digital currency. Especially for commoners, the use of bitCOINS is complicated.

BITSOAR is a digital currency, that aims to compensate for bitCOINS flaws. By providing safety and simplified usage of it. Therefore, BITSOAR can only add more value to bitCOINS technology and currency value.

BITSOAR Developmental Policy

BITSOAR is unbelievably perfectly safe, it has engendered the structural features of bitCOINS. And to enable the safety environment for its use, a BISOAR platform had been additionally created.

Total amount of BITSOAR to be issued: 3,980,000,000 BSR

The amount to be issued has been already decided, after the inflation comes to a termination, there is no chance its value would decrease.

BSR (Participant) (Foundation), (Operatior), (Miner), (User)

• The participant, plays the role of establishing and spreading BSR's proper policies. When we say proper it refers to a set of rules that will prompt an increase in value and stimulate transactions.

• The operator, is the one that makes sure regulations are followed. BSR and BSR System, are safely managed and administered by the operator. Especially, it listens to the complaints of customers and takes care of their inquiries and drafts a report about it.

• The Miner, plays the role of an actual customer using the BSR system. The miner would purchase the coins through the digital coin exchange market and exchange it for something else. Purchase items etc

• The user, is the real individual who'd be using the BSR system. The user would purchase coins from an official coins exchange market. Purchase items with the coins etc.

BITSOAR (BSR) Detailed Specifications

- Coin name: BITSOAR COIN
- Coin symbol (unit): BSR
- Total: 3,980,000,000 (line mining 3.68 billion)
- Mining type: 300 million
- Coin type: PoW
- Hashing Algorithm: X11
- Transaction rate: 10 TPS (600 TX per minute)
- Block size: variable (1MB to 4MB)
- Block time: 600 seconds (10 minutes)
- Number of block compensators: 50
- Number of blocks: 144
- Half-life: 1 year

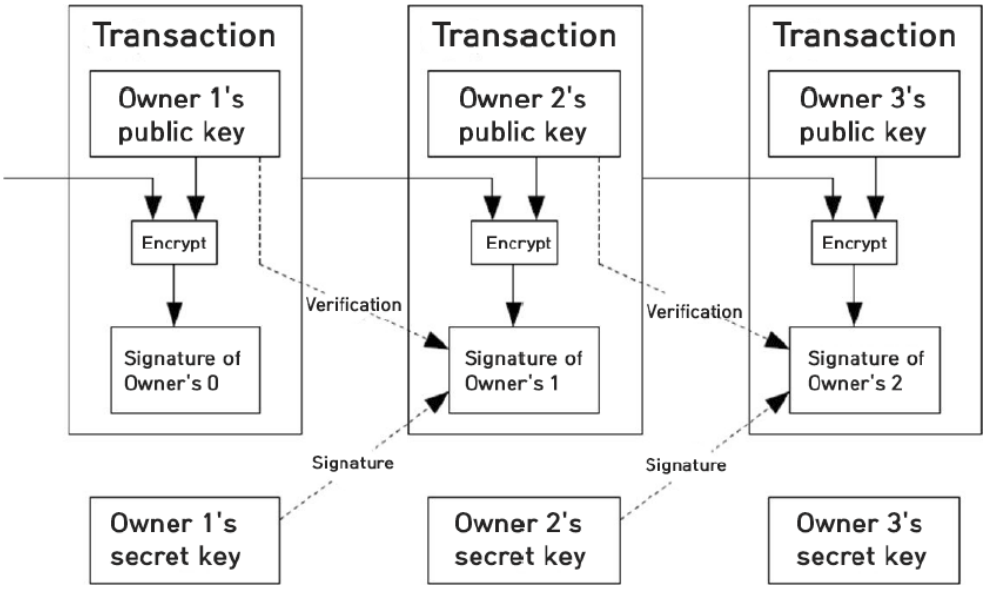
BITSOAR Hashing Algorithm

The X11, is a connected hash of algorithms that is used to protect cryptocurrency networks and used during proof of work analysis. It is called the chained algorithms because it utilizes 11 different algorithms. There are the Blake, bmw, groestl, jh, keccak, skein, luffa, cubehash,shavite, simd and echo.

X11 Algorithm Most Representative Coins below

BITSOAR Transaction

We consider the digital currency as connected to the digital signature.Each owner of a password key will send the transaction history with and attached public key to the next owner, then proceeds to activate the digital key, encrypted with personalpassword key.



The receiver of funds can view the transactions and public keys of all the digital signature chains Within the internal block system of BITSOAR, all transactions are saved, and each transaction comes with a digital signature and public key

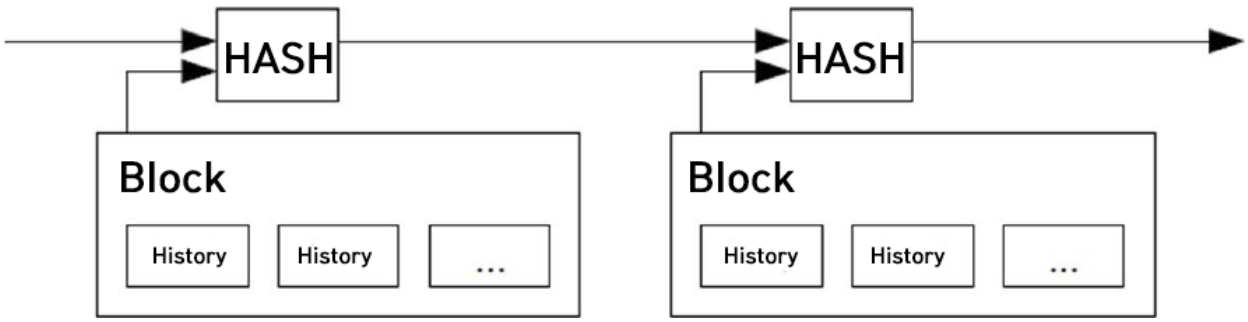
as a package. Therefore, all users of BITSOAR can see the list of transactions and verify them. When a digital signature is verified, the next can be checked.

- If a 3rd party had corrupted or not the log and data.
- If a 3rd party had engaged in transaction with a stolen ID
- If the official owner of the coin, had proceeded with the transaction or not

In order to issue a transaction, the public key and password are needed. BITSOAR uses an algorithm known as the elliptic curve cryptosystem(ECDSA), with a length of more than 256 beats. What is achieved with the ECDSA is that it can equal the level of security of RSA or ElGamel but shorter and faster.

Time Stamp Server

The solution we suggest is to start the Time stamp server. This server collects the hashes with timestamp, and is in charge of distributing the hash, just like newspapers for this type of Time Stamp transaction log, a clear data to prove a transaction Took at that specific time is needed. So. Each time stamp block would add the previous chain of transaction data, to the existent registry, and so on and on.



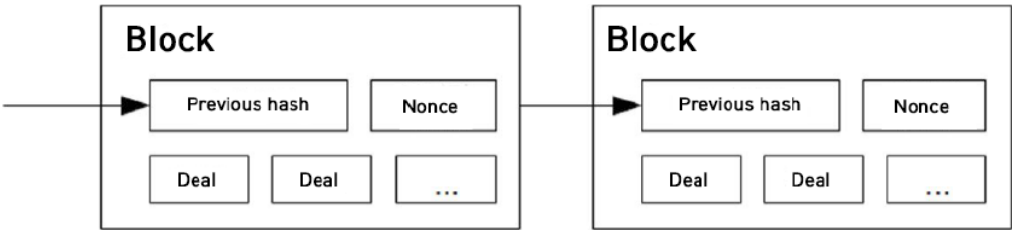
Proof of Work

To materialize the P2P based dispersed Time Stamp Network, we need to think of

how paper,Usenet posts are used. Maybe we need to use a similar system to that of Adam Back'sHashcash, a proof - of- work. This proof of work includes a similar algorithm to SHA-256,

includes the searching function for passwords starting in 0. On average, the time that it takesfor this process increases as the 0bit number requests continues to appear. In any case, it isverifiable just by carrying it out once the password hash. Time Stamp Network, through theproof of work method, it will consider increasing the temporary value of hash, nonce(temporary value) until all the block hash values sets at 0. When it arrives to the proof ofwork step, the block will set permanently unless it repeats the process. The following blockwill create a chain. Just to change a single block, the entire chain with all the blogs need togo through the same editing process. Also, it solves the problem of choosing the

representative for the proof of work process.



If it it's decided through a system where several IPs would gather to cast their vote, anyonecould access it and attack it. But, proof of work, is based on o
One vote per CPU. Multiple decisions appear in the longest chains, in other words, the effortis focused on the more crowded proof of work. If most of the computing power functionsoccur through honest nods, the honest chains are the ones meant to grow faster, and takeover the rival chains. In the past, to edit blocks, the attacker to make changes, he had toreverse the proofOf work from the target block and the rest that came after, and catch up with the currentChain of blocks iquestion and pass it. For the slow attackers, during the process, if newBlocks are added, as time goes by the more behind he would stay. Also as time

passes,

increase in hardware and to compensate for the increase in nod participation rat e

The proof of work's difficult will set at the average production number of blocks as a targetIf blocks are produced at a higher rate, then the difficulty level will go al ong

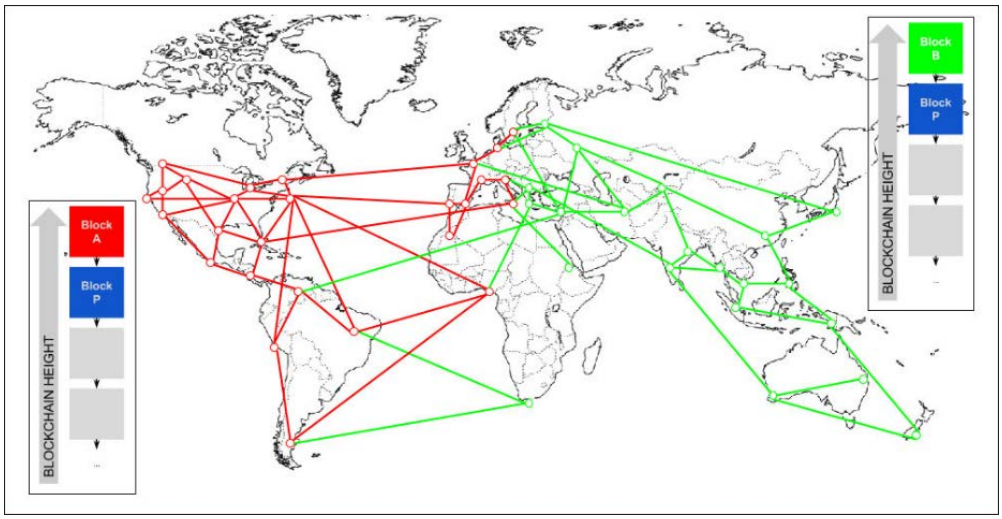
NETWORK

Network traffic occurs in the following way:

1) A new transaction details are sent to all nods.
2) Each nod gathers the new transaction details for the block.
3) Each nod performs the search for the proof of work that belongs to the block.
4) When a nod successfully acquires the proof of work, it sends it to the rest of the blocks.
5) The nods approve the block that was not used before.
6) The nods take the hash from this block as the previous one and through the process of creating the next blog it tells the block has been approved.

Nods moved to the longest chain and makes sure to maximize its growth.
When two nods from different versions inform about the next block at the same

Time



Distributed Block Chains (https://mastanbtc.github.io/blockchainnotes/consensustypes)

Some nods get the information from one of the nods. In this case, each nod would work on performing its function, and saves the information even though it's from a different source, just in case the chain gets longer.

If one side of the chain's proof of work gets longer then nods no longer work on that side and move tothe other side. It is not necessary for all nods to receive the information of the new transaction, eventhough these alerts are missed by nods, doesn't cause much troubles. If the information is missed and itbecomes aware of it, it can request the information on the next block.

REWARD

The firsts block of the transaction becomes, the first block that enables the creator to receive moneyand it comes a very special transaction. In this way, there is no need for a centralized entity, thereward is delivered to all nods that compose the network. It means the money to be distributedhappens early. Continuously adding

a set amount of money is like miners throwing in their entireresources so that gold can be supplied. In this case, computing power and electricity is wasted. In thereward system, there is a transaction fee. If the money that is being input is bigger than the amount to

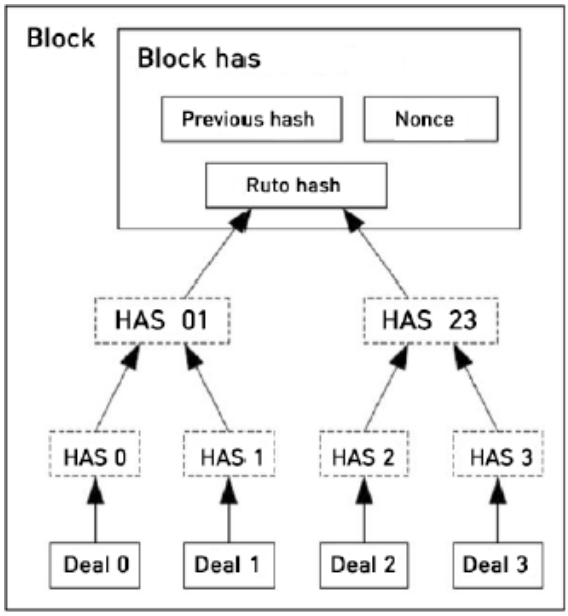
be printed from the transaction log, the different will become the transaction fee, and considered tobe an added value for the block that includes it. After the whole amount of money is distributed, youcan be free from the effects of inflation, this reward system makes it possible for the nods to honestlyparticipate and maintain in that way.

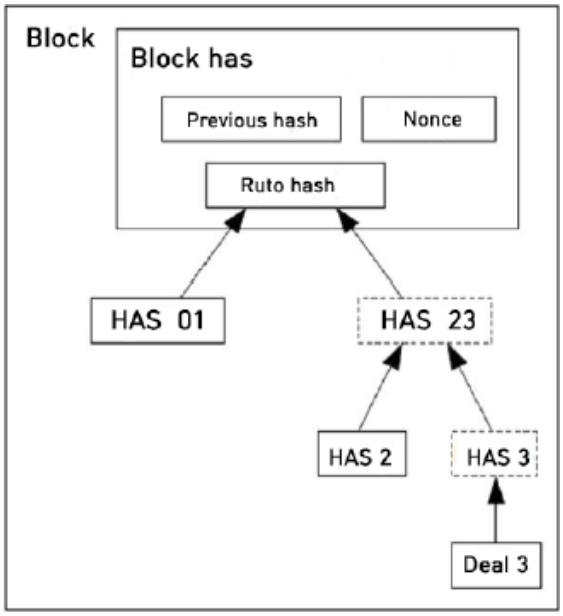
If an ambitious attacker decides that he could create a stronger computing power than the nods, hewould need to retract others' transactions or create new money. But if decides not to engage in suchbehavior, and instead of worsening the system status, if instead of causing on his own gain, he wouldhonestly participate in the system, He'd gain much more

Increasing Disk Storage

If the recent transaction data is buried within several different blocks, the old ones can be thrown away to increase storage capacity. In order to avoid pushing the block hashes to the edge and accomplish an easier task, the transaction data is hashed into a MerkleTree structure, only the root portion of the MerkleTree structure should be included in the block hash. The old blocks within the tree structure, cut out the branches and reduce its size, the lower portion hashes are no longer needed

to be stored.

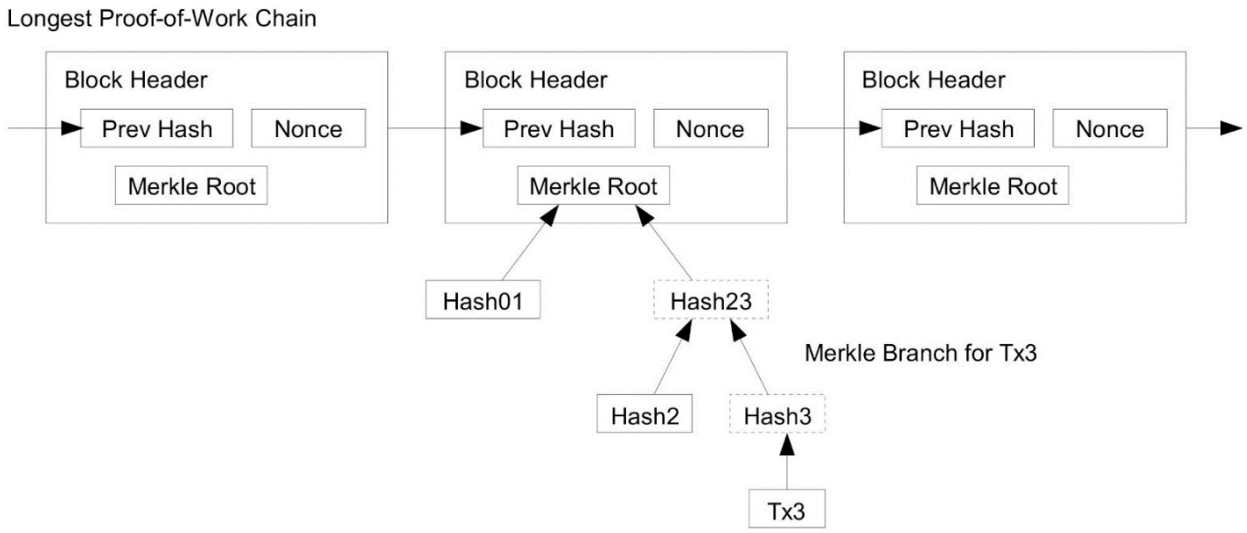




Simplified Payment Proof

It is possible to prove a payment has been made even though a nod from the whole network hasn't been used. If the user obtains a copy from the chain block's proof of work, and continues to request the network nods to send the confirmation of his long chain being the longest one.

Just by receiving a portion of the transaction data recorded in the MerkleTree is enough. He couldn't check the transaction details by himself, he can know only when the chain connects and the network nod approves it, and later with more blocks being added, it is known that it has been approved.



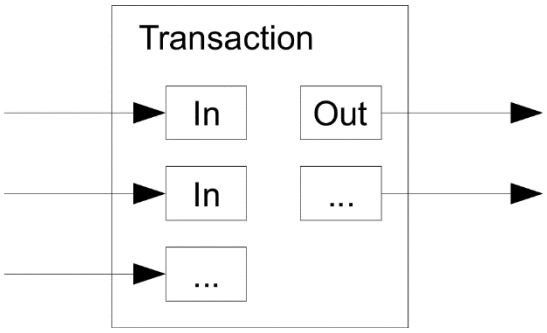
Because of these honest nods, the transactions that go through this are trustful as Long as the attacker's network doesn't take over. Network nods can confirm the transaction but the fact that in case the network has been taken by an attacker, it would continue to maintain its status within that fake network, therefore it is vulnerable. The only way to protect the user is to have him download the entire software for the block, and search for those blocks where the source is unknown or not valid, the nods could send out an alert message. Probably those who receive frequent payments would rather use an independent security system And faster approval methods.

.

Combination and Splitting Value

It is possible to manage funds independently but for minimal amounts it's a hassle. The transaction logs make it possible for multiple digit inputs and print outs. Most are to enter big amounts or others a series of small amounts. Therefore, there will be two different print outs. One print out will become unnecessary, one will consist of series of small number transactions, resembling change we get, when
we break a bill.

This is known as pan out,. It doesn't matter if one transaction depends on the bunch or the bunch among themselves depend on each other. There is no need to create a completely separate

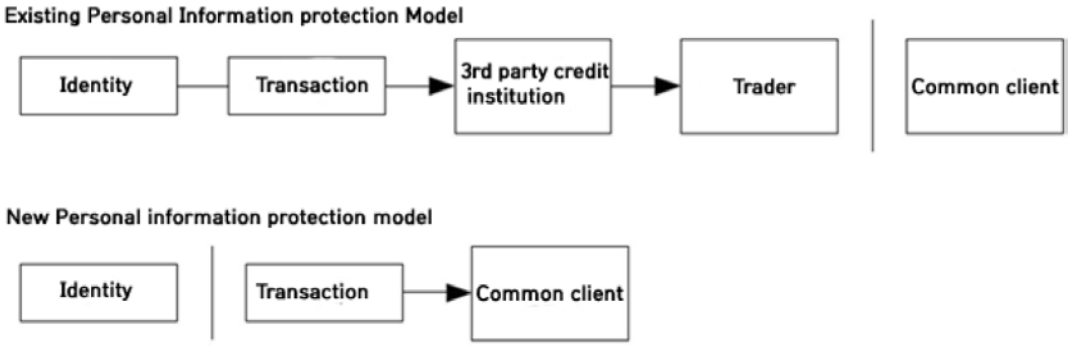


Privacy

The existing bank model limited the credit institution's the access rights regarding the parties' personal information, offering a partial protection of private information for the parties. Because all transaction details need to be open to the public, make this type of protection impossible.

But since the public key is anonymous, the flow of information is blocked and the

personal information can be protected. From the outside, it is possible to see how much are the transactions, but there is no way to identify the involved parties. This is concept is very like the ones that occur in the stock market. Additional safety measure is the fact that for every new transaction, a new secret key is issued, but for a transaction that has multiple keys, this connection itself reveals that it has a common source to all its transactions.



As an additional protective wall, to prevent from getting linked to ordinary owners, every transaction releases or issues a key pair. For the multiple-input transactions, some links are inevitable. It shows that is the same owner for the previous ones. If the key owner becomes known, and therefore, all the other transaction belonging to this key, can become public.

Calculation

Here's a scenario, imagine an attacker tries to produce a different chain's section to surpass the honest chain nods. Even though he succeeds, creating fake transactions or pretending to own those inexistent transactions will not be approved. The honest nods would identify these transactions as non- verifiable.

The attacker probably would try and get a refund on the most recent transaction and alter it. The honest nods' (Binominal Random Walk) chains produce one single block, is it called a +1 lead but if they fail and the attacker produces one, it is called -1.

Assuming the attacker could succeed in pretending to have funds he doesn't have is like the gambler's ruin Problem. Imagine this scenario, in which a gambler with infinite credit, starts the game while in debt, he is close to a winning, (Breakeven) that is like the attacker catching up to the honest nods. And we can put it in equation.

p = The probability of honest nods finding their next block
q = The attacker's nod in finding the next block
qz = z(numeric value) the probability of finding the next block fast

p > q if we assume that, then the probability of the attacker's block finding the block is equivalent to the probability of the number of blocks exponentially decreasing. If the attacker doesn't get lucky to find it first, the probability only decreases as time goes by.

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Now in a new transaction, let's think about how long will it take for the sender of the payment to not be able to make any changes to the transaction? The sender would have the receiver believe the payment has been made for a certain duration of time and after, the sender tries to retrieve the sent amount.

Then the receiver would receive an alert, but the sender hopes the alert occurs much later. The receiver would create a set of new password keys and right before the sender signs, the public key is sent. With this method, the receiver can protect himself from a possible malicious plan the sender must have had. When the payment is being made, the malicious sender would add other transaction information to create a chain at the same time, and the receiver Has a "z" number of additional blocks is added along with the transaction's block and wait until

The blocks connect. He can't know how far the malicious sender has gone but the honest blocks Are produced every hour and the attacker's potential advancement can be explained through the"poisson" equation, it is as follows: In order to calculate the probability rate of a sender to catchup (expected value), we have to multiply the blocks from that chain to the poisson distribution.

$$\lambda = z\frac{q}{p}$$

To calculate the probability rate of the attacker catching up, we multiply the Poisson equation (Poisson density) to Each and every single one of the blocks produced right at that moment. .

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

To avoid adding the infinite series from the formula, we translate the information into C language.

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

If you implement this in C language code

```
#include <math.h>

double AttackerSuccessProbability(double q, int z)
{
  double p = 1.0 - q;
  double lambda = z * (q / p);
  double sum = 1.0;
  int i, k;
  for (k = 0; k <= z; k++)
  {
        double poisson = exp(-lambda);
    for (i = 1; i <= k; i++)
    poisson *= lambda / i;
    sum -= poisson * (1 - pow(q / p, z - k));
  }
return sum;
}

```

The result reveals that depending on the value of "z" the exponential time's probability decreases.

BITSOAR Value-Increase Strategy

BITSOAR foundation adds value, safety and drafts strategies to prevent plummeting of prices.

First, The BSR Safety Strategy is as follows

- The foundation would acquire part of the coins
- Strengthening public activities for both parties

Second, Maintaining the BSR Strategy

- Paid and free issuing of coins
- Strengthening public activities for both parties

Third. BSR Investment Strategy

- Investment on BITSOAR

- Public and Welfare institutions' investment
- Opening Vietnam branch, to activate digital currency use locally
- Investment for coin activation process

We will put all of our efforts into increasing the value of BITSOAR and on the strategy to propagate it.

BITSOAR's Expansion Strategy

BITSOAR is a coin that has been strategically planned to coincide with the digital industrial revolution.

It goes along AI, Big Data IoT, shared economy, which are convergence/Integration Complex business trends that represent the 21st century. BITSOAR's platform has the merit of expanding BSR's value, and is an API for supporting the IT business.

Coin API' converting points to BITSOAR
DB sync API It can sync with a variety of DB's
Exchange Market API for managing local exchange market
Wallet API for developing wallets
Management API' for independent management
Test servers for Testing purposes

BSR was designed based on a flexible yet stubborn way, and programmed in a modern language that let's it have an outstanding expanding capability. These characteristics let it interact with a variety of different industries with ease, and at the end it'll lead the digital currency business to success.

BITSOAR (BSR) General Roadmap

BITSOAR(BSR) Team since it was established in 10.15.2015

1st Step : BSR Team Established	**2nd Step : BSR Specifications**
- Main business members organization - Research on Coin market - First draft for the coin white paper - Technical draft for the coin white paper - Technological draft for coin white paper - Opening seminar for coin white paper	- Defining coins - Defining mining coins - Definition of coin transaction - Definition of coin block and blockchain - Defining coin mining amount - Defining coin logo
3rd Step : Coin Engine Development(Trial)	**4th Step: ICO Operations**
- Coin mining module development - Coin transmission module development - Coin Wallet module development - Coin Signature module development - Coin management module development	- ICO roadmap -ICO legal, technological, organizational assess ment. - ICO Preparation of Presentation paper - ICO token issuing system development - ICO login system development
5th Step : Coin Engine Development(Commercial)	**6th Step : Coin Platform development**
- Coin mining module development - Coin transmission module development - Coin Wallet module development - Coin Signature module development - Coin management module development	- Transaction Server development - Blockchain Server development - PC/MOBILE WALLET development - Mining System Development - Application System Development
7th Step : Coin market registration	**8th Step : Coin foundation established**
- GitHub source registration - Mining service registration - Blockchain search service registration - API service registration	- purpose of foundation - defining main activities - drafting budget - drafting policies

BITSOAR

BITSOAR Foundation, is a nonprofit organization in charge of administering all the information referent to BITSOAR

The establishment of this foundations follows the following stages:

① Purpose, ② Name and location ③ Representative's information, ④ information on digital currency and bonds/stocks issuing ⑤ Policies and regulations ⑥ Directors meeting and guidelines ⑦Members of the board

of directors and policies ⑧Finance and accounts, ⑨Supplementary provisions

BITSOAR **Foundation's Mission**

The BITSOAR foundation aims to establish a systematic strategy in order to increase and expand the value of coins. In more details as follows:

BITSOAR branch establishment in Hochimin Vietnam

Rapid listing on the International Exchange Market

Listing on various international exchanges

Launching Global mobile wallet (multi-language support)

Establish global infrastructure (Russia, UK, Japan, China, Vietnam, Brazil, Mongolia, Paraguay, Thailand)

VISA card transaction availability for global payments

Open 1,000 branches in China and Vietnam

ATM installation in China and Vietnam scheduled

BITSOAR TEAM

The members that are working towards planning and making BITSOAR happen areas follow.

	**Sangdong Kim, CEO:** **Korea**, Inha Univ. He majored in computer science and was a representative of leading IT companies. He was awarded by the Ministry of Government Affairs and Communications and the Ministry of the Future Creation Sciences.
	**Attila Ferencz, Rumania, CIO:** **Rumania,** Cluj-Napoca Univ. He has worked as a professor for many years since he received his Ph.D. in Computer Science and worked as a senior researcher at Samsung Electronics R & D Institute and KT Research Center since 1999. He is currently working as a cryptographic specialist.
	**Sergei Kuratov, Russia, CTO:** Has 20 years of experience as a hardware and software architecture expert for large web services in USA, Israel, Japan, Korea, China and Spain.

Conclusion

BITSOAR can be traded nationwide, but also, it can be used for business. When listed in exchange markets for digital currency, civilians will also have access to transactions using it. It will enable synching with a variety of businesses and therefore, gains.Also, the staff and management of BITSOAR will go out of their way to deliver the safe and practical, the very best BISOAR service

References

01. Alt chains and atomic transfers:
https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949

02. B-money: http://www.weidai.com/bmoney.txt
03. Bitcoin, A Peer-to-peer Electronic Cash System:
https://bitcoin.org/bitcoin.pdf
04. Colored coins whitepaper: https://tinyurl.com/coloredcoin-whitepaper
05. Decentralized autonomous corporations, Bitcoin Magazine:
https://tinyurl.com/Bootstrapping-DACs
06. Ethereum: https://ethereum.org.
07. Ethereum Merkle Patricia trees:
https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-Patricia-Tree
08. Ethereum RLP: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-RLP
09. GHOST: http://www.cs.huji.ac.il/~avivz/pubs/13/btc_scalability_full.pdf
10. Intrinsic value: https://tinyurl.com/BitcoinMag-IntrinsicValue
11. Jae Kwon. Cosmos, A Network of Distributed Ledgers:
https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md
12. Joseph Poon and Tadge Dryja, Lightning Network:
https://lightning.network/lightning-network-paper.pdf
13. Mastercoin whitepaper: https://github.com/mastercoin-MSC/spec
14. Merkle trees: http://en.wikipedia.org/wiki/Merkle_tree
15. Mike Hearn on Smart Property at Turing Festival:
http://www.youtube.com/watch?v=Pu4PAMFPo5Y
16. Namecoin: https://namecoin.org/
17. Patricia trees: http://en.wikipedia.org/wiki/Patricia_tree
18. Paul Sztorc. Drivechain – The Simple Two Way Peg:
http://www.truthcoin.info/blog/drivechain/
19. Peter Todd. Tree Chains: https://github.com/petertodd/tree-chains-paper
20. Peter Todd on Merkle sum trees:
http://sourceforge.net/p/bitcoin/mailman/message/31709140/
21. Raiden. Raiden Network: https://raiden.network/
22. Reusable proofs of work: http://www.finney.org/~hal/rpow/

23. Secure property titles with owner authority: http://szabo.best.vwh.net/securetitle.html
24. Golden Master and Branch whitepaper: http:/www.gmbcoin.org/gmb-whitepaper.pdf/
25. Simplified payment verification: https://en.bitcoin.it/wiki/Scalability#Simplifiedpaymentverification
26. Smart contracts: https://en.bitcoin.it/wiki/Contracts
27. Smart property: https://en.bitcoin.it/wiki/Smart_Property
28. StorJ and Autonomous Agents, Jeff Garzik: https://tinyurl.com/storj-agents
29. The Bitcoin Model for Crowdfunding: https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/
30. Vitalik Buterin. Ethereum Sharding FAQ: https://github.com/ethereum/wiki/wiki/Sharding-FAQ
31. Zooko's triangle: http://en.wikipedia.org/wiki/Zooko's_triangle