Next-Gen P2P Network

A New Generation of Peer-to-Peer Electronic Cash System

FordCoin

FordCoin

FordCoin were born for the future

FordCoin are created for speed, privacy and security. FordCoin has made great technological innovation and upgrading from speediness, security and privacy to Bitcoin. Bitcoin is prone to network congestion due to transaction speed problems, which leads to transfer delays and greatly affects the faster circulation speed worldwide. FordCoin has achieved perfect upgrade on the basis of Bitcoin technology and integrated into lightning trading. The transfer speed is 10 times faster than Bitcoin. FordCoin, also known as Black Hole Coin, is the first black hole technology introduced in the world. Bitcoin can be traced up by address, which can easily expose privacy and account security. FordCoin is introduced.The world's first innovative black hole technology, address can not be traced upwards, the ultimate protection of user account privacy and financial security.

Use FordCoin to make instant, private payments online or in-store using secure open-source platform hosted by thousands of users around the world.The Birth of FordCoin: Bitcoin is accepted by more and more people in the world as a digital asset to store and use, but its transfer speed is not conducive to the current world's fast-paced payment mode. In view of the painful point of Bitcoin transfer speed, technology upgrading is carried out on the basis of retaining the advantages of Bitcoin."Science and technology lead development and innovation to change the future" and "make payment faster and easier", this time for the upgrading of Bitcoin technology and the support of Banking Circle, the world's largest B2B payment company.

Make Global Payment Faster and Easier

Global Payment Integration is Coming

Next-Gen P2P Network

Science and Technology Lead Development
and Innovation Change the Future

At FordCoin’s core is a unique fully-incentivized peer-to-peer network. Miners are rewarded for securing the blockchain and masternodes are rewarded for validating, storing and serving the blockchain to users.
Masternodes represent a new layer of network servers that work in highly secure clusters called quorums to provide a variety of decentralized services, like instant transactions, privacy and governance, while eliminating the threat of low-cost network attacks.

FordCoin Advantage

Next-Gen P2P Network

1

Constant quantity

A constant number of 21 million, fair and just, everyone can participate in mining free of charge;

2

Production halving rule

The number of blocks produced per minute decreases by half year by year, and the difficulty coefficient increases year by year. The total mining has been completed in 40 years.

3

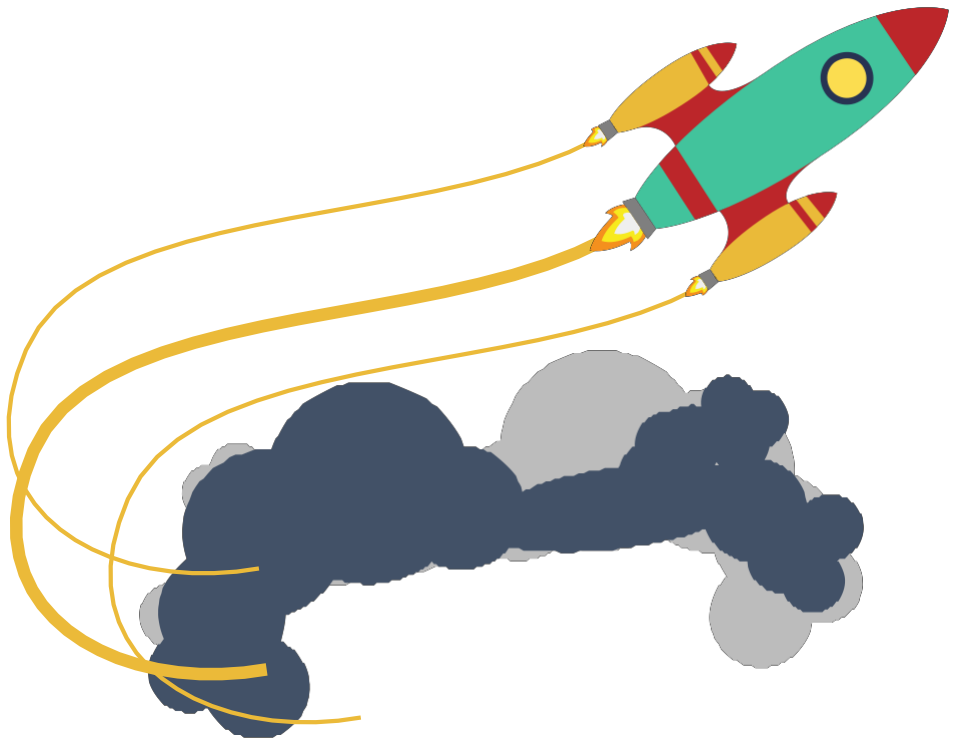
Decentralization characteristics

Decentralization features and algorithms, no one can manipulate currency value, data can not be tampered with, code open source, transparent and open;

4

Lightning network

Lightning network, block speed 1 minute a block, transfer speed is 10 times faster than Bitcoin;



5

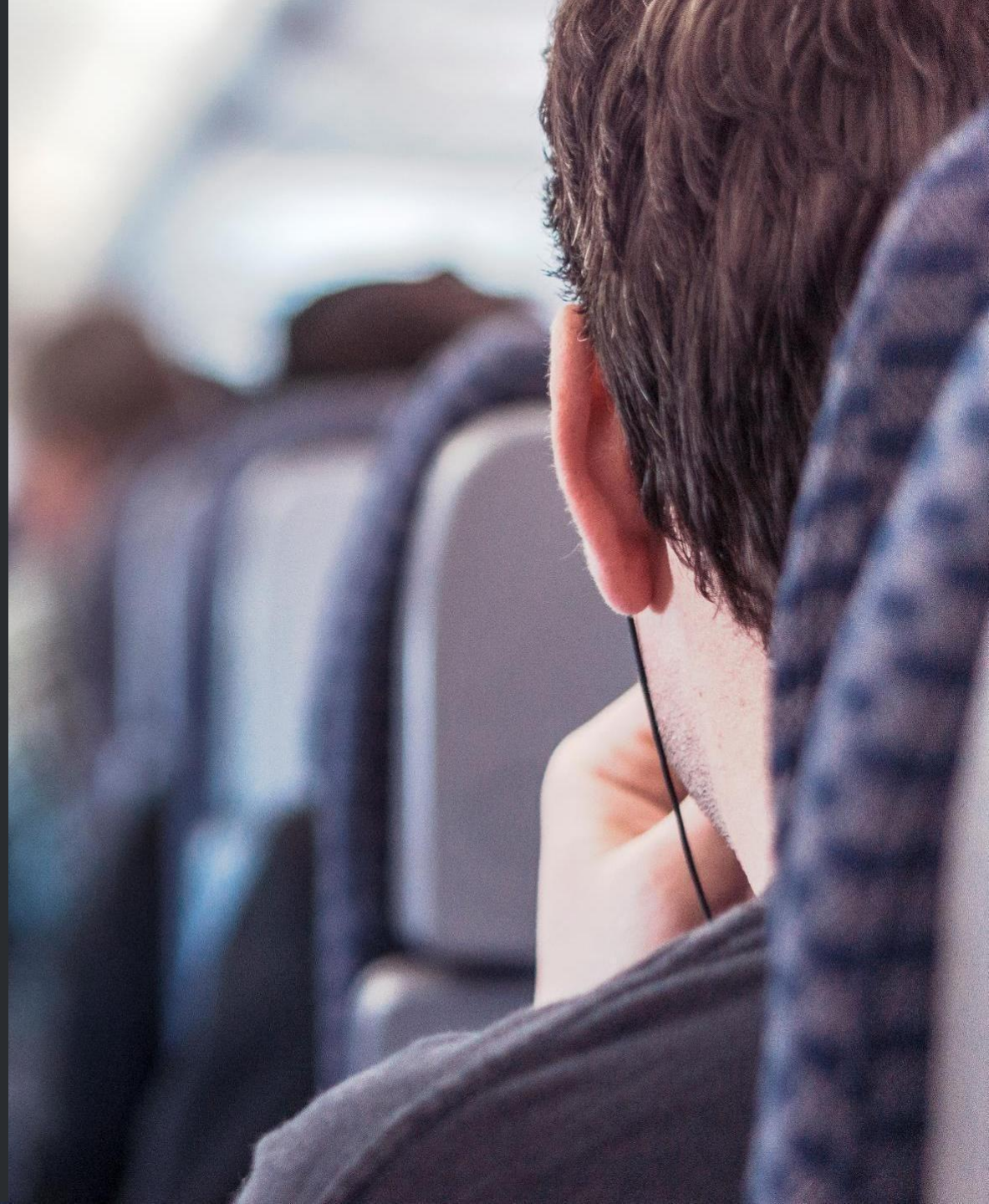
High anonymity

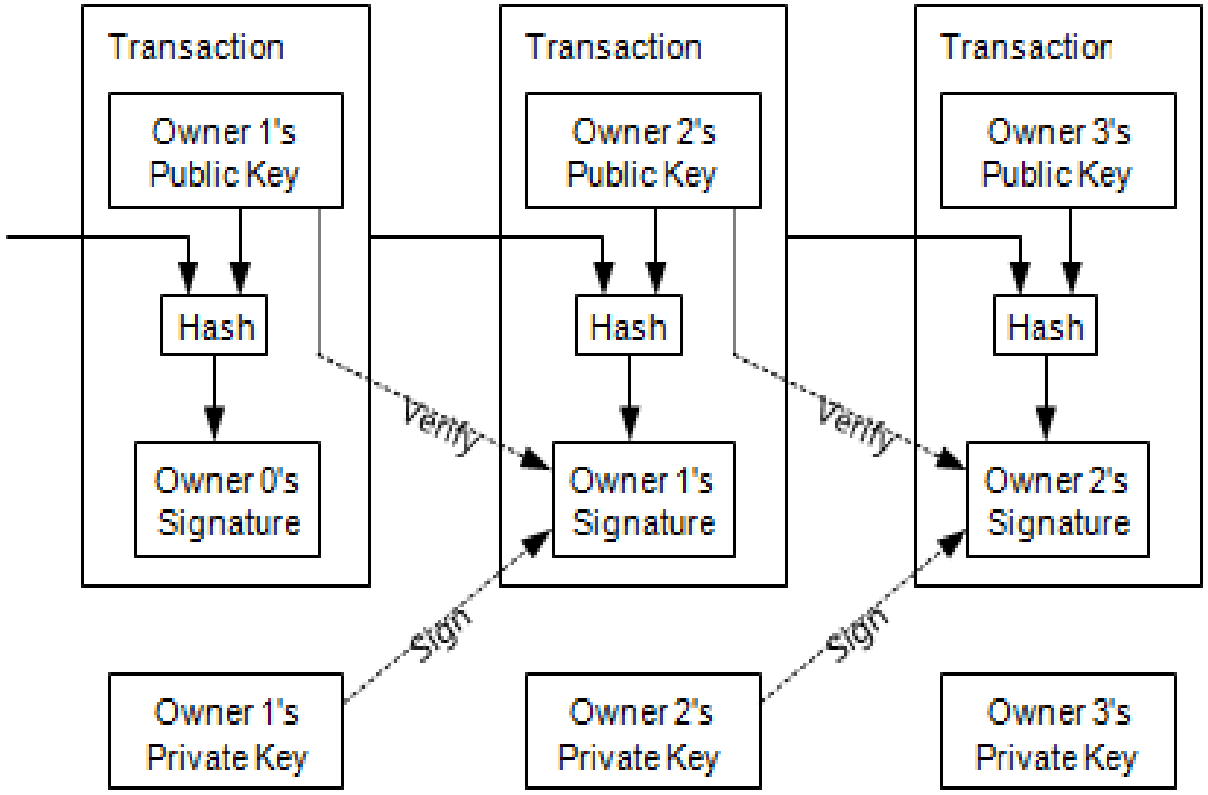
Its anonymity is upgraded on the basis of Dashi coin technology. At present, it is the only one that uses Ring Signature + Dual Stealth Address + zk-SNARK (ring signature, double-key stealth address and black hole technology). Bitcoin can track transaction records and trace up the source block. Fordcoin is highly anonymous and cannot go back to its source. Compared with other currencies, it has bigger future development goals, and has had various natural advantages since its birth.

Introduction

Next-Gen P2P Network

Businesses on the Internet rely almost entirely on financial institutions as trusted third parties to handle electronic payments.
Although the system works well for most transactions, it still has inherent weaknesses based on trust model.
An electronic payment system based on password certification rather than trust allows any two willing parties to trade directly without requiring a trusted third party.
Computatively irreversible transactions will protect sellers from fraud, and conventional custody mechanisms can be easily implemented to protect buyers.
A solution to the double overhead problem of generating transaction sequential computation proof using point-to-point distributed timestamp server is presented.
As long as honest nodes control more CPU capabilities than any collaborative attacker group, the system is secure.





Transactions

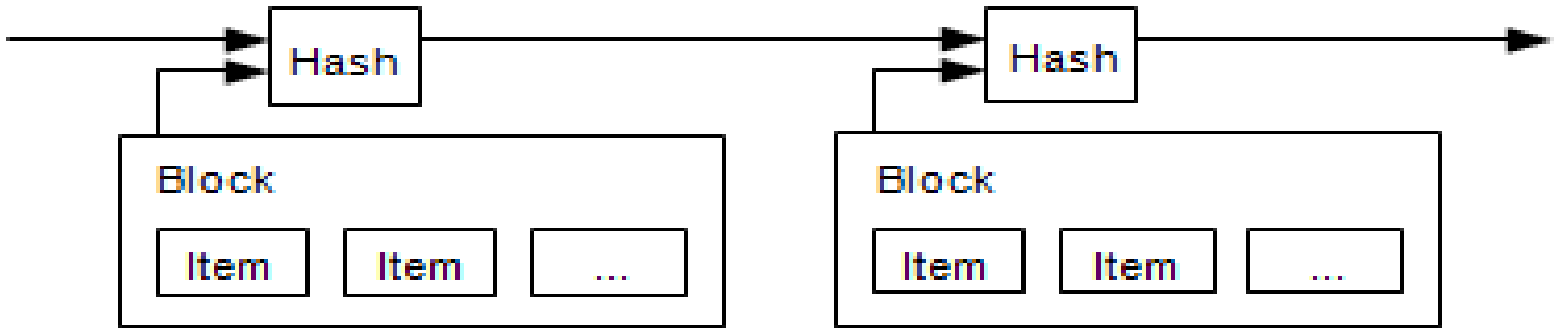
Next-Gen P2P Network

We define electronic coins as digital signature chains.
Each owner transfers the coin to the next owner by digitally signing the hash value of the previous transaction and the public key of the next owner and adding it to the end of the coin.
The payee can verify the signature to verify the chain of ownership.
We need a way for the payee to know that all previous owners have not signed any early transactions.
For our purposes, the earliest transactions are the most important, so we don't care about future double consumption attempts.
The only way to confirm that there are no transactions is to know all the transactions. In a mint-based model, the mint knows all transactions and decides which one comes first.
In order to achieve this without a trusted party, it is necessary to publicly announce the transaction [1].
We need a system in which participants agree on the order in which they receive the transaction.
The payee needs to prove that at each transaction, most nodes agree that it is the first to receive.

Timestamp Server

Next-Gen P2P Network

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5].
The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash.
Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



Proof-of-Work

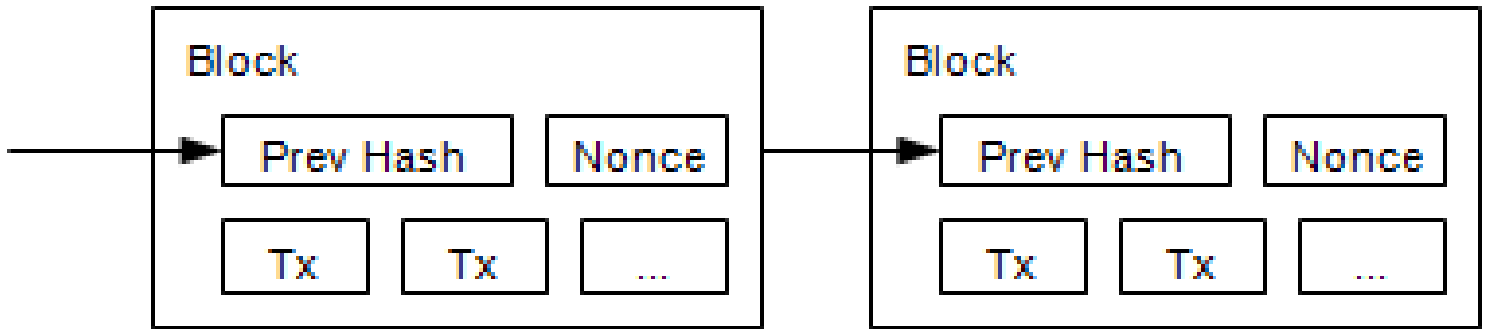
Next-Gen P2P Network

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof- of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.



Network

Next-Gen P2P Network

The steps to run the network are as follows:

1)New transactions are broadcast to all nodes.
2)Each node collects new transactions into a block.
3)Each node works on finding a difficult proof-of-work for its block. 4)When a node finds a proof-of-work, it broadcasts the block to all nodes.
5)Nodes accept the block only if all transactions in it are valid and not already spent.
6)Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof- of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.
New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

Incentive

Next-Gen P2P Network

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block.

This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.

The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins.

He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Reclaiming Disk Space

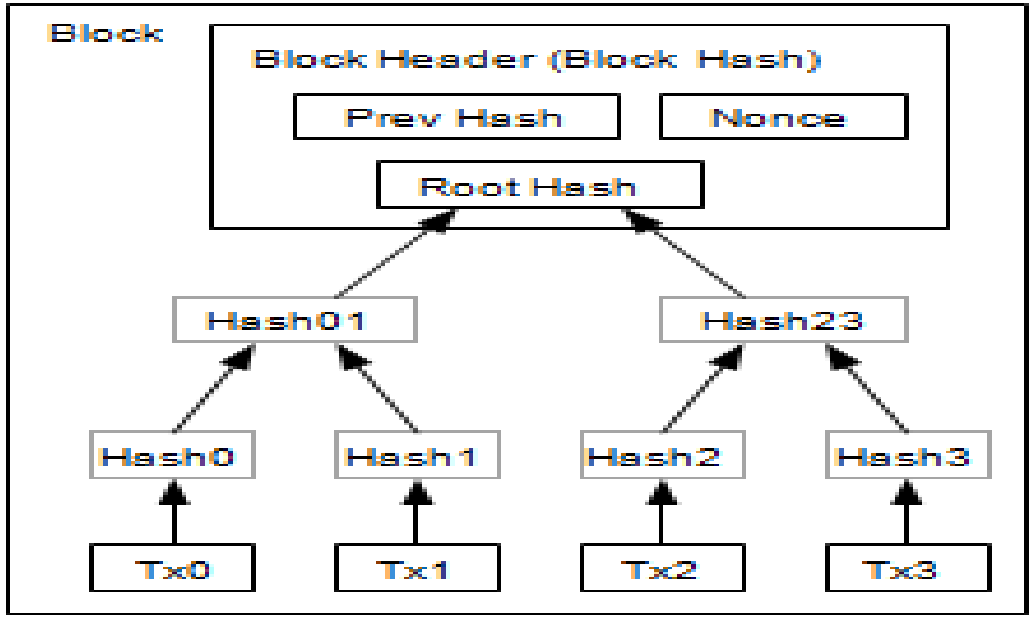
Next-Gen P2P Network

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space.

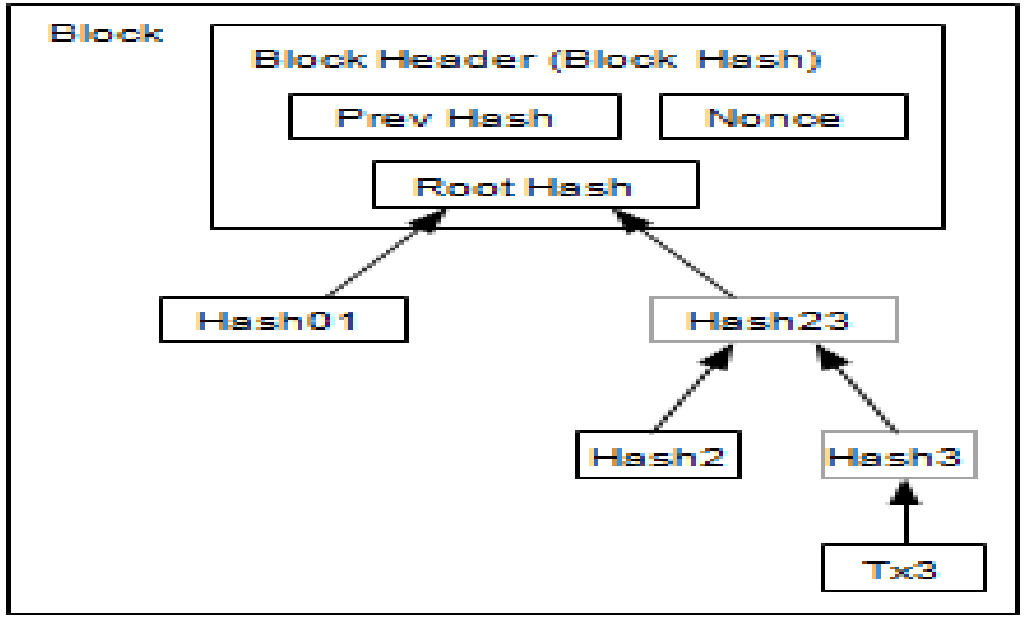
To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree.

The interior hashes do not need to be stored.

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Simplified Payment Verification

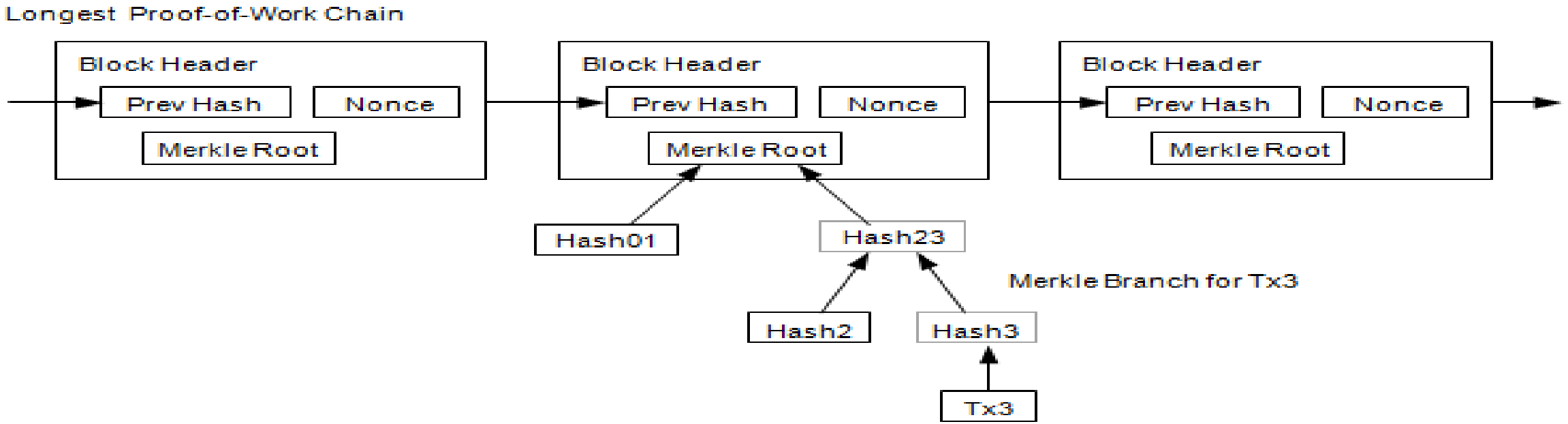
Next-Gen P2P Network

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in.

He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network.

One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.



Combining and Splitting Value

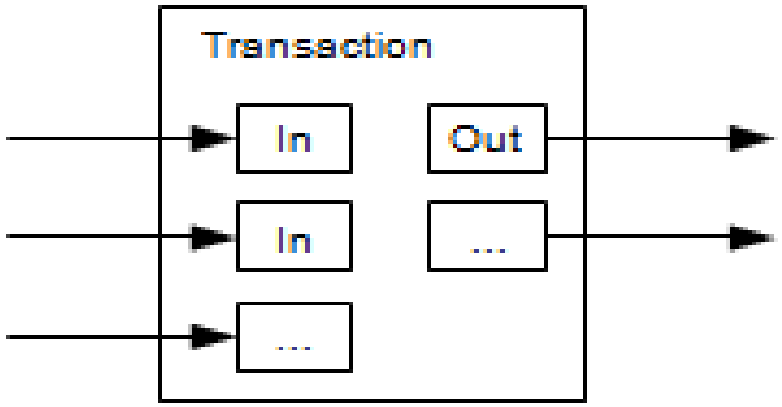
Next-Gen P2P Network

T Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer.

To allow value to be split and combined, transactions contain multiple inputs and outputs.

Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.



Privacy

Next-Gen P2P Network

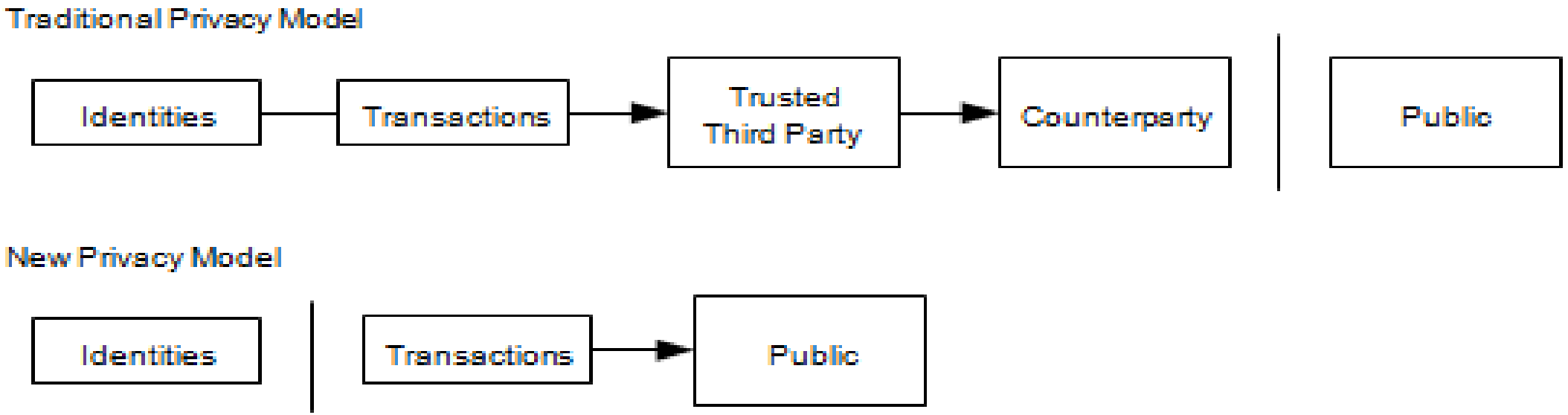
The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party.

The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.

The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner.

The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.



Calculations

Next-Gen P2P Network

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block

q = probability the attacker finds the next block

qz = probability the attacker will ever catch up from z blocks behind

z {q / p if p}

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a poisson distribution with expected value:

□ z qp

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

∑ k ! ·{ 1 if k □z}

Rearranging to avoid summing the infinite tail of the distribution...

z □ke−□

z− k □

1−∑

k =0

k ! □1−□q / p□Converting

to C 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;
Tfor (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));
}
```

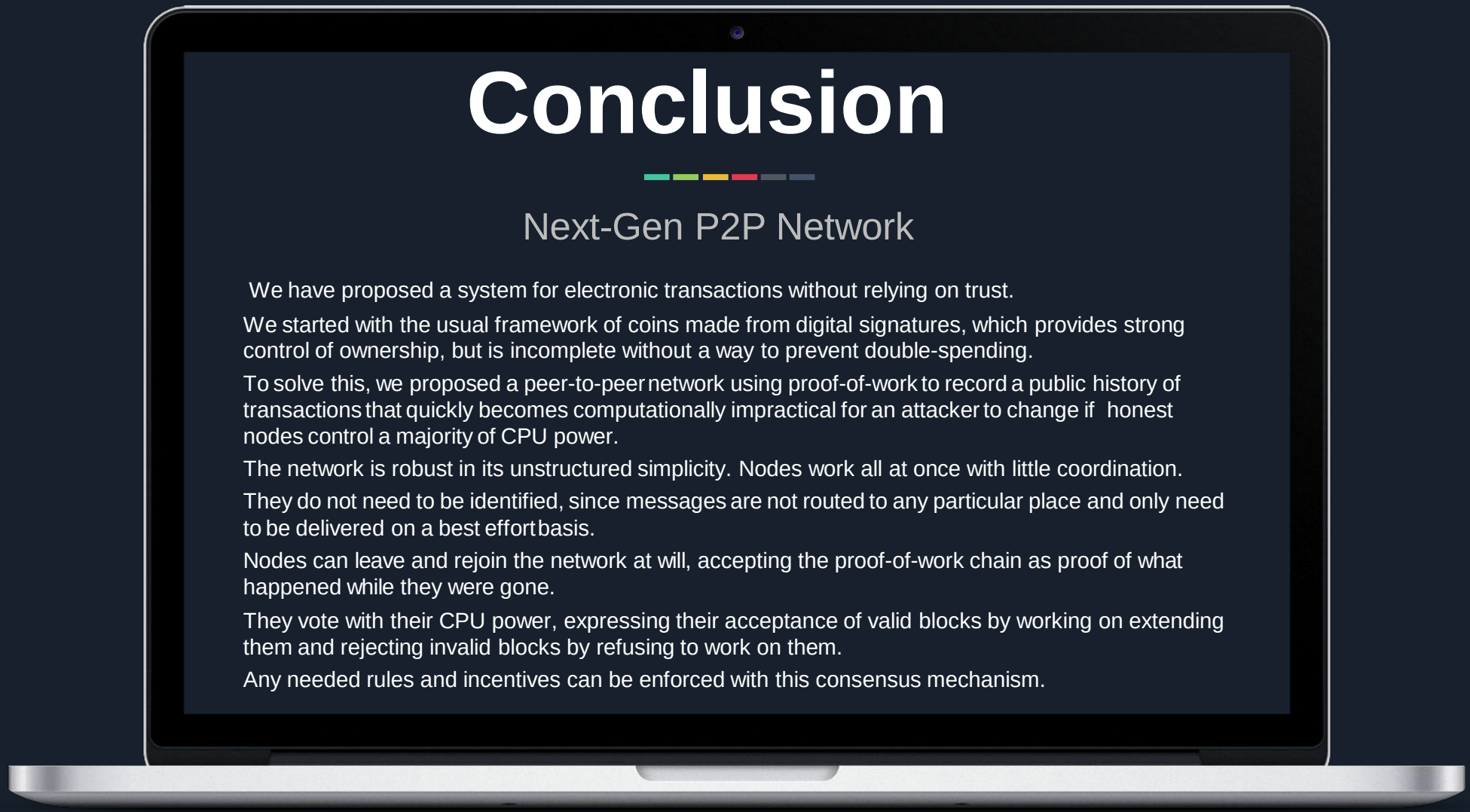
```
return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8  P=0.0000173
z=9      P=0.0000046 z=10      P=0.0000012
q=0.3
z=0      P=1.0000000
z=5 P=0.1773523 z=10 P=0.0416605 z=15 P=0.0101008 z=20 P=0.0024804 z=25 P=0.0006132 z=30 P=0.0001522 z=35 P=0.0000379 z=40 P=0.0000095 z=45 P=0.0000024
z=50  P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001 q=0.10 z=5
q=0.15 z=8
q=0.20     z=11
q=0.25     z=15
q=0.30     z=24
q=0.35     z=41
q=0.40     z=89
q=0.45 z=340
```


Conclusion
Next-Gen P2P Network
We have proposed a system for electronic transactions without relying on trust.
We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending.
To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.
The network is robust in its unstructured simplicity. Nodes work all at once with little coordination.
They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis.
Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone.
They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them.
Any needed rules and incentives can be enforced with this consensus mechanism.

References

Next-Gen P2P Network

[1]W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2]H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3]S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4]D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5]S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

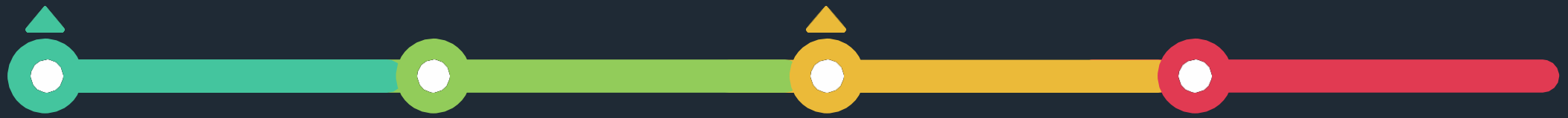
[6]A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7]R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8]W. Feller, "An introduction to probability theory and its applications," 1957.

Main Characteristics of FordCoin

FordCoin makes payment faster and more private.



De centralization

In a decentralized system, anyone is a node and anyone can be a center.

Distributed

FordCoin distributed ledger is a database shared, replicated and synchronized among network members.
Distributed books record transactions between network participants, such as exchange of assets or data. The arithmetic generated by distributed book-keeping technology is a powerful and subversive innovation.

Security secret key

FordCoin encryption algorithm has two kinds: asymmetric encryption algorithm (elliptic curve encryption algorithm) and hash algorithm (SHA256, RIMPED160 algorithm).

Autonomous and anonymous

With consensus-based mechanism, all nodes can exchange, record and update data freely and safely in a trusted environment, and no human intervention will work.

Next-Gen P2P Network, Why?

Next-Gen P2P Network

Technological upgrading is carried out on the basis of Bitcoin and Dashi coin technologies.

HighAnonymous Black Hole Technology

Ford coin is also called Black Hole Coin. Its anonymity is upgraded on the basis of Darth coin technology. It is the only one that uses Ring Signature + Dual Stealth Address + zk-SNARK (black hole technology). Bitcoin can trace back to the source area. Fordcoin is highly anonymous and cannot go back to its source. Compared with other currencies, it has bigger future development goals, and has had various natural advantages since its birth.

Lightning Quick Payment

Lightning network, block speed 1 minute a block, transfer speed is 10 times faster than Bitcoin.

FordCoin Block Chain Characteristics

Next-Gen P2P Network

Anonymous

Because the data exchange between the nodes of the block chain follows a fixed and predictable algorithm, the block chain network does not need trust and can exchange data based on address rather than personal identity.

Autonomous

Block chain adopts consensus-based mechanism, which enables all nodes in the whole system to exchange data, record data and update data freely and safely in a trusted environment. No human intervention is effective.

Openness

Block chain system is open, and any node can have the general ledger of the whole network. In addition to the private information of the data directly related parties is encrypted through asymmetric encryption technology, the data of block chain is open to all nodes, so the information of the whole system is highly transparent.

Tamper Proof

The information of block chain is recorded by all nodes after it is added to the block chain by consensus, and is correlated with each other by cryptography. The tampering is very difficult and costly.

Collectively Maintain

Block chain system is maintained by all nodes with maintenance function. All nodes can query block chain data and develop related applications through open interfaces.

Permissionless

No permission is required to indicate that all nodes can request any transaction to be added to the block chain, but only if all users consider it legitimate.

FordCoin

The Next-Gen P2P Network

Changing the Payment Habits of the World

FordCoin will be the black horse of digital currency with the technology of encryption, anonymity and fast trading at the bottom of rebuilding block chain.

Make Global Payment Faster and Easier.

FordCoin makes payment faster and more private.

www.fordcoin.org