Bitcoin: inside the encrypted, peer-to-peer digital currency

By Thomas Lowenthal | Published about 12 hours ago

Bitcoin—a pseudonymous cryptographic currency designed by an enigmatic, freedom-loving hacker, and currently used by the geek underground to buy and sell everything from servers to cellphone jammers. No, this isn't a cyberpunk artifact from *Snow Crash* or *Neuromancer*; it's a real currency currently valued several times higher than the US dollar, the British pound, and the Euro.

Bitcoin is a virtual currency, designed to allow people to buy and sell without centralized control by banks or governments, and it allows for pseudonymous transactions which aren't tied to a real identity. In keeping with the hacker ethos, Bitcoin has no need to trust any central authority; every aspect of the currency is confirmed and secured through the use of strong cryptography.

Over the last few months, Bitcoin's value has risen by an order of magnitude as the sagas of Wikileaks and Anonymous (among others) have highlighted the limits of a financial system which relies on centralized intermediaries. With a current estimated market capitalization of about $100 million, Bitcoin has recently graduated from a theoretical techno-anarchic project patronized by libertarians and hackers to a full-fledged currency prompting comment from technologists and economists. At the time of this writing, one Bitcoin (BTC) is worth about US$15.

So how does Bitcoin work? Is it really secure? And is it here to stay—or just another digital currency fad? Glad you asked.

Complexities of cryptographic currencies

The problem with purely digital currencies is that of double-spending. Economists in the audience will note that digital products like a movie or a text file are *non-rivalrous*. If you have a copy of my pseudo-trip-rock band's new MP3 album, there's still just as much MP3 to go around for everyone else who wants one. That's not a problem for files, but it is a problem with currency, since the whole point is that there's a limited supply. If you use a dollar at the grocery store today, you can't go out and spend that same dollar at a bar tomorrow.

The usual solution to the double-spending problem is a trusted intermediary. PayPal makes sure that you can't spend the same dollars twice by deducting them from your account before they get added to someone else's account. Visa, MasterCard, and every other bank and payment processor do the same. However, this centralized approach is the one that enigmatic creator Satoshi Nakamoto specifically tried to avoid in the original Bitcoin design. The idea was to use cryptography to create verifiable transaction records without the need to trust anyone but your own calculations.

The Bitcoin solution uses cryptography and an open transaction register. Whenever you spend a Bitcoin, you cryptographically sign a statement saying that you have transferred the coin to a new owner and you identify the new owner by their public crypto key. Whenever they need to spend the coin, the new owner uses his private key to sign it over to some further owner. As soon as a transaction takes place, the recipient (who has a very strong incentive to ensure that you don't spend the coin twice) publishes the transaction to the global Bitcoin network. Now every Bitcoin user has incontrovertible evidence that the coin has been spent, and users won't accept that coin from anyone but the new owner.

Mining and make-work

As a digital currency, Bitcoin suffers from a tangibility problem. Unlike other currencies traded online, you can't go to a bank and withdraw physical coins, so what are they? More importantly, where do they come from? Coins are essentially agreements between all the Bitcoin nodes to accept a particular coin as currency. They are created gradually according to a precise protocol in order to reward those who contribute and maintain the network, control the rate of creation of the currency, and maintain the integrity of the transaction list.

In a process known as mining, individual Bitcoin users attempt to generate new coins by checking the integrity of the transactions list. They confirm the previous transactions and attempt to solve a difficult proof-of-work problem which involves exhaustively trying different solutions. There are a very large number of such potential solutions, so the likelihood of finding the solution depends how many other people are looking for it and how much computing power you devote to the problem. The first client to find the solution announces its good fortune to the whole network and earns a little reward for itself in the form of some shiny new Bitcoins.

By finding the newest solution to the proof-of-work problem, a Bitcoin client confirms the history of previous transactions and moved the transaction register forward, allowing new debits and credits to form part of the next block that can be mined to earn more coins. Future coins can't be mined in advance, because the computation to find the new block (and hence create new Bitcoins) relies on the the chain of previous blocks and the history of transactions since the most recent block.

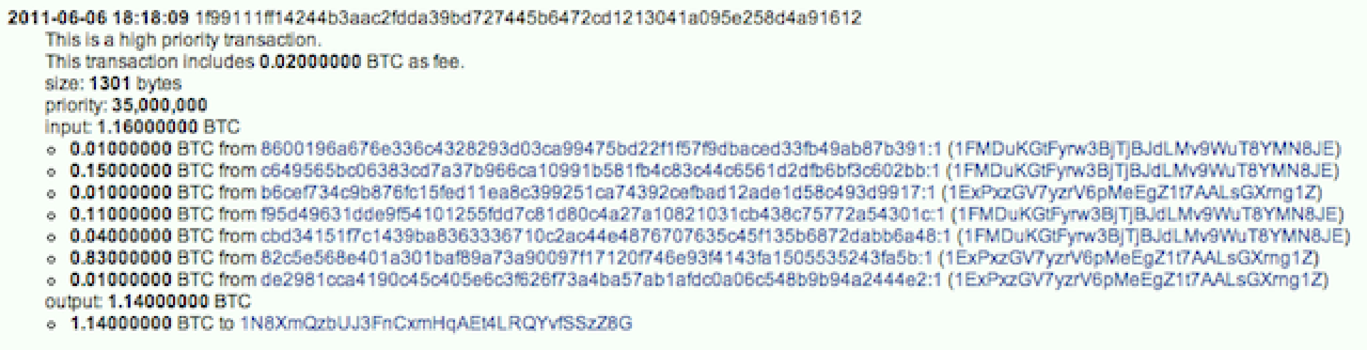
The number of new coins generated per block gradually decreases over time. It started out at 50 BTC, but will dwindle to zero sometime in future when all 21 million coins have been generated. Fortunately, coins can be divided down to the eighth decimal place, which may prove increasingly useful if their value grows.

A Bitcoin explainer

What's a few coins between friends?

One of the difficulties with a novel currency like Bitcoin is adoption and valuation. The same was true when the greenback paper dollar was first introduced, and it's a real problem with any means of exchange. After all, a currency is little more than something useless but rare which everyone agrees to trade for useful things, whether apples or assault rifles. National currencies have the advantage that governments demand them in taxes and require them to be accepted, which provides both a particular market and a high rate of adoption.

So, why would anyone exchange their hard-won dollars for Bitcoins, or accept Bitcoins in exchange for real products like a carton of milk or a subway ride? As a currency, Bitcoin has a number of desirable features which are not found together in any other currency. Cash has features like anonymity and eminent portability, but also comes with the downside that you have to physically move it from place to place to use it. Credit cards and other trust-based electronic currencies can be used instantly over any distance, but you have to attach your real identity to the purchase.



```
2011-06-06 18:18:09 1f99111ff14244b3aac2fdda39bd727445b6472cd1213041a095e258d4a91612
      This is a high priority transaction.
      This transaction includes 0.02000000 BTC as fee.
      size: 1301 bytes
      priority: 35,000,000
      input: 1.16000000 BTC
      o  0.01000000 BTC from 8600196a676e336c4328293d03ca99475bd22f1f57f9dbaced33fb49ab87b391:1 (1FMDuKGtFyrw3BjTjBJdLMv9WuT8YMN8JE)
      o  0.15000000 BTC from c649565bc06383cd7a37b966ca10991b581fb4c83c44c6561d2dfb6bf3c602bb:1 (1FMDuKGtFyrw3BjTjBJdLMv9WuT8YMN8JE)
      o  0.01000000 BTC from b6cef734c9b876fc15fed11ea8c399251ca74392cefbad12ade1d58c493d9917:1 (1ExPxzGV7yzrV6pMeEgZ1t7AALsGXmg1Z)
      o  0.11000000 BTC from f95d49631dde9f54101255fdd7c81d80c4a27a10821031cb438c75772a54301c:1 (1FMDuKGtFyrw3BjTjBJdLMv9WuT8YMN8JE)
      o  0.04000000 BTC from cbd34151f7c1439ba8363336710c2ac44e4876707635c45f135b6872dabb6a48:1 (1FMDuKGtFyrw3BjTjBJdLMv9WuT8YMN8JE)
      o  0.83000000 BTC from 82c5e568e401a301baf89a73a90097f17120f746e93f4143fa1505535243fa5b:1 (1ExPxzGV7yzrV6pMeEgZ1t7AALsGXmg1Z)
      o  0.01000000 BTC from de2981cca4190c45c405e6c3f626f73a4ba57ab1afdc0a06c548b9b94a2444e2:1 (1ExPxzGV7yzrV6pMeEgZ1t7AALsGXmg1Z)
      output: 1.14000000 BTC
      o  1.14000000 BTC to 1N8XmQzbUJ3FnCxmHqAEt4LRQYvfSSzZ8G
```

An anonymous Bitcoin transaction

Bitcoins combine the advantages of the two methods. Using Bitcoins, I can buy a racy t-shirt from Tibet and computer time from China without either merchant knowing who I am, or my bank knowing what I bought. This is useful not just for those purchasing questionable items (the downside of anonymous currency flows), but also for those who don't want merchants, banks, or card companies to be able to build up detailed profiles of their life, likes, and habits.

Since they're useful, some people want to use Bitcoins. Since some people want to use them, merchants have an incentive to accept them in order to attract the business of those customers.

This simplified economic model is not uncontested. Ars tech policy contributor Tim Lee has publicly criticized Bitcoin's economic model, both from the point of view of external market forces and over the internal incentive structures inherent to the protocol. Tech and economic policy commentator Jerry Brito provides a counterpoint, emphasizing Bitcoin's decentralizaion, which makes it very hard to control, but concedes that it is very hard to distinguish between a currency bubble and currency value.

Bitcoin's anonymity has already attracted Congressional attention. Sen. Chuck Schumer (D-NY) this weekend blasted Silk Road, an online drugs outlet that allegedly relies on TOR to obfuscate Internet traffic and Bitcoins for payment. "It's an online form of money laundering used to disguise the source of money, and to disguise who's both selling and buying the drug," Schumer said.

Further reading

- Original Bitcoin paper by Satoshi Nakamoto (bitcoin.org)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

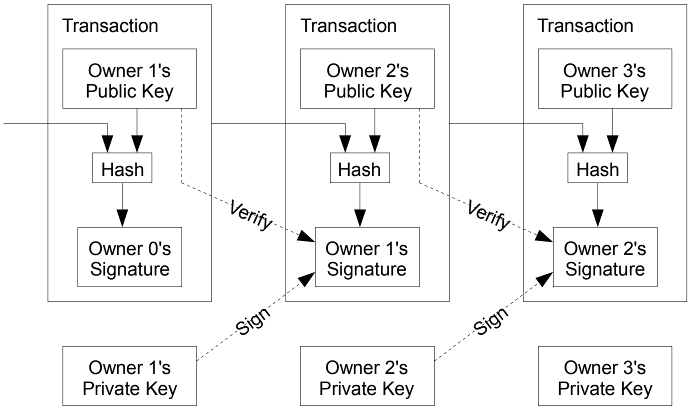
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

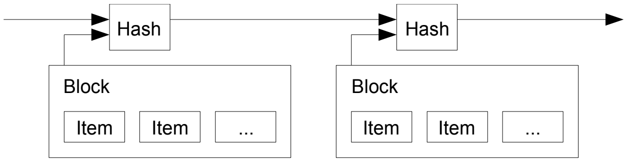


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

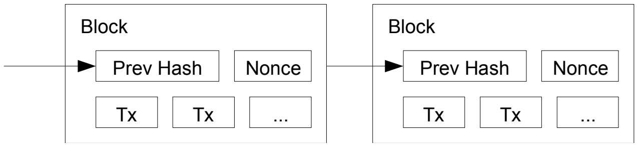
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to 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.



4. Proof-of-Work

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.

5. 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.

6. Incentive

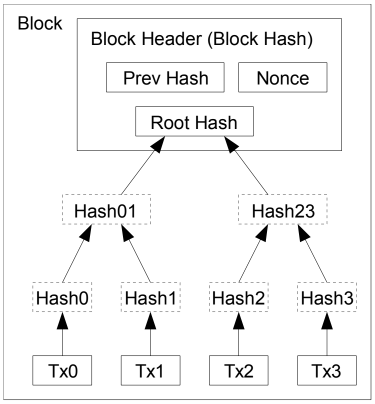
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. 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.

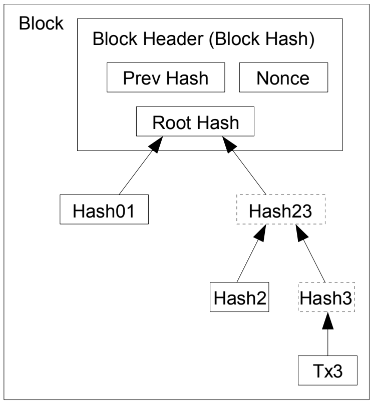
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to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

7. Reclaiming Disk Space

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.



Transactions Hashed in a Merkle Tree

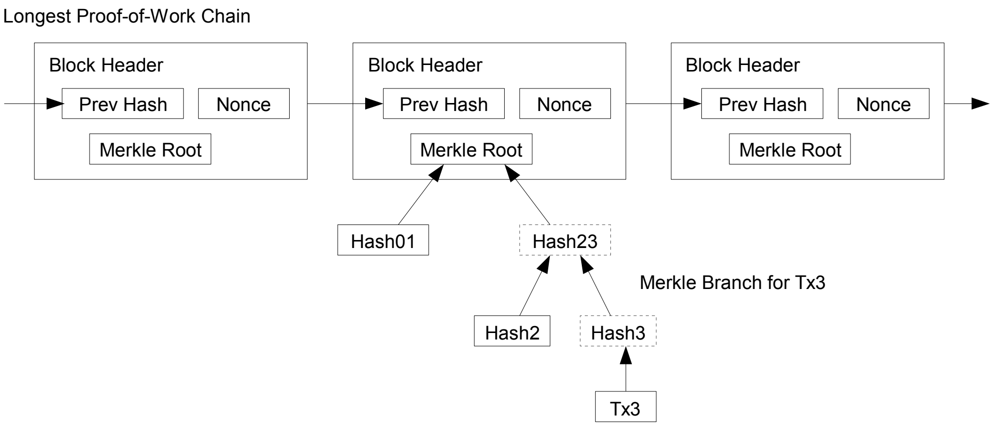


After Pruning Tx0-2 from the Block

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.

8. Simplified Payment Verification

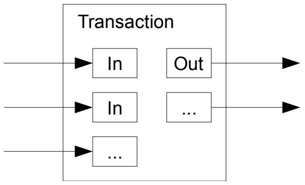
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction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

9. Combining and Splitting Value

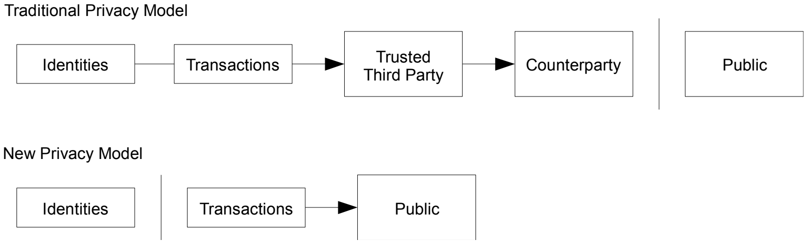
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous 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.

10. Privacy

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.

11. Calculations

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

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

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:

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

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:

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

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

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

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;
    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;
}
```

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
```

12. Conclusion

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

[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.