The Bitcoin transaction system

Lodewijk André de la Porte

June 30, 2012

Abstract

The cypherpunk movement is all but dead. Bitcoin [8] is a full peer-to-peer system for gaining consensus upon transactions. It can be used for various purposes, anywhere consensus is required the bitcoin system can be of great help. It has been applied to form a currency, called Bitcoin, and an alternative for DNS infrastructure, NameCoin. It has also been proposed in application to several other problems where value can be used against spam and there is a need for (eventual) consistency.

1 Cypherpunk movement

The cypherpunk movement started in the late 1980’s, driven by technological progress and the potency of cryptography. This potency is often underestimated, it helps to remember that cryptography was classified as munitions in America. Many cypherpunks still consider crypto a weapon of sorts. The goals of the movement are, as with any movement, slightly vague but the common element is the use of technology to improve democracy and personal freedoms, often through protection of privacy with cryptography. Standpoints defending common availability of cryptography fall usually within the cypherpunk mindset. The paranoid way of looking at society as a large tracking mechanic often warrants tinfoil hats comparisons and causes an anti-government mantra. Software such as BitTorrent, PGP, TOR, SSL/TLS, OpenSSL, MojoNation, crypto.cat, Tahou-LAFS and Bitcoin and precursors are typically cypherpunk products. [7]

2 An abbreviated history of what money is

Core to the cypherpunk philosophy is a trust model without truly trusted components. The so called "Trusted Computing Base" is nonexistent or permits for as large as possible failure. Money is an example of something that everyone uses, yet many people do not understand why it works. There was a time when it was more clear, every coin itself was worth the metal it contained. That made coins heavy and expensive, there has also been trouble with the exact size of coins and re-minting with a lower quality of metal. Once law became stable enough engaging in contracts for trading an amount of metal for a token became more useful than carrying the metal around. These tokens were bills or coins. One should note that the amount of metal present at the organizations engaging in contracts would usually not suffice for trading all tokens. There would be enough tokens to remain in circulation to warrant that difference. When governments made these contracts they also made, or had for metal currencies, additional law that required people to accept these tokens, "legal tender" laws. This made the tokens more useful as they could be spend everywhere. In fact they would hardly ever be exchanged for gold. This realization has more recently led to the dropping of what is called the "gold standard" where country would exchange the tokens for gold. Since the demand for gold and its unfair distribution created an unnecessary fluctuation in economies this was a reasonable thing to do. A currency is now denominated not in promises of gold, promises as the country had to guarantee it would have the gold, but instead in other currencies to be exchanged through trade with third parties. At its introduction this caused economic boosts, in no small part because the government could inject capital to its desire. This new kind of token-only currency is called fiat money and is the de-facto standard at this time. How money is valuated is said to correspond to the countries whom print it, these is a certain trust they will not mint large quantities of it and that the money will be useful. The amount of "overminting" seems to relate to a countries debt, as money is often digital it need not be minted to be spend. One notices the situation complicates in situations such as a shared currency like the Euro, or when a country other than the one to mint it uses a currency as a
national one. The recent banking crisis and the "evaporation" of money likely relates to banks being able to borrow towards each other thus creating tokens for fiat money, essentially a promise of a fiction, and abusing their ability to in-transparently deal with complex loans and money contracts, like mortgages.

3 Cryptocurrency incentive

One day we send messages by scribbling them down upon papers and carrying them towards their recipients. It is clear the advantage of digitally transmitted money over carried money is huge, due to its value even more so than with messages. That is why it is being done for decenia now. In Europe the Single Euro Payments Area has successfully harmonized most of the European interbank transactions and debit cards [4]. E-Banking lets practically everyone perform digital transactions for casual reasons over the Internet, whereas virtual payment methods like iDeal, Mister Cash, Direct eBanking, EPS, MyBank, etc. assist companies in accepting and streamlining digital payments. Let it be clear that digitally transacting money is a common business.

Cypherpunks are however not easily satisfied. There is a fundamental flaw in the way digital money operates now. To help you find it we will discuss a case study. A politically motivated group has been collecting information that was not intended to be collected at all. Their conviction being that no information should be hidden as that would damage democracy, after all how can you decide about something you do not know about? This organization published, with as much media coverage as they could get, as much information as they could warrant to publish. This includes diplomatic messages passed between governments, interrogation techniques used, etc. A certain organization, the USA, did not much like those documents being spread around and tried everything they could to stop it. The rigorous application of encryption for anonymous submissions, TOR for anonymous contact and very careful reproduction of documents to take away stenographic methods of identifying the one that leaked the data made stopping them impossible. So instead the USA made, means undisclosed, major payment processors like VISA and MasterCard halt transactions towards the organization. This stopped donation flow nearly completely. The organization is called WikiLeaks. Its founder, Julian Assange, is now the world's most wanted and known cypherpunk. Neither Julian nor WikiLeaks have every been prosecuted, instead they are economically sanctioned.

The flaw exposed here is the singular pressure points, the banks and payment processors, able to deny the flow of money. In this case it even permits a political economic blockade, even without legal basis. We are looking not for digital banking, we are looking for digital cash. Then may we call it digital money.

4 A systematic view to digital cash

A systematic view defines money as values being transacted. That means there has to be a personal total and a personal history of transactions. Personal total can be computed from transactions and needs not be tracked separately. Some mutual debt currencies implement only these transactions and trusts everyone in the community to keep his or her own debt as small as possible, thus providing infinite liquidity. This has not been made to be practical outside of small communities though. Bitcoin solves the coin minting problem through a process called "mining" a side product of the network on which we will talk more later. We wish to enforce a positive balance only system, as with cash no transactions can be made if one does not have the balance to fulfill it. And therefore need to somehow be certain one can spend an amount of money. In Bitcoin this is achieved by allowing transactions to have multiple in and outputs, where the inputs must be equal or larger than the outputs. From the latest transaction a single coin can then be tracked to its creation and this transaction chain can be known to be valid. This implicitly defines the one that owns the coin as the one that can transact it. Naturally we want to transact somewhere. Transact meaning to transfer control over the coin. This is a typical digital signing issue. A transaction consists of a coin identifier, here a set of previous transactions, and one or more target public keys. Then this transaction is digitally signed, locking it from adverse change and just as importantly proving the one that made the transaction has the private key to the public key the input transactions were last send to. In Bitcoin the public key is hashed, this provides extra defense against reversing that quantum computers may at some point do effectively. Inspiration for this systematic approach has largely been taken from b-money as described by Wei Dai [6].
5 Double spending

With this chain of transactions there is only a single real problem. When a transaction is used as input in more than one transaction its output can be used multiple times. I can produce a, perfect valid, sequence of transactions in which money ends up at Alice. I can also produce a chain that leads to Bob. Now Bob could, potentially, find out Alice already has control but that does not matter to Bob. Bob can also transact that money and thus owns it. This means we have now doubled a coin. This is clearly unintended. This could naturally be solved by only letting the first transaction, to Alice, count. Simply ignoring later transactions than the first. Now we have two problems. The first is to timestamp a transaction reliably and the second is to get conclusive enough evidence of being the first to receive a transaction. Both these things are trivially solved with a central trusted authority that stamps a transaction, too bad we cannot use those. Instead we create a chain of transactions, for effectiveness we actually creates chains of blocks of transactions, a so called blockchain. The links between blocks can be references to a hash of the previous block and a block height or dept number. The transaction earliest in the blockchain is the valid one. Now we need only find ways of building this chain in a distributed, functional manner.

6 Bitcoin mining

The problem with blocks is that if one could be created at any point in time, say with every new transaction, having the longest one would not be an achievement. We want to prevent block-spam as to make having the longest chain more difficult and more meaningful. It is easy to suggest something akin to a per person limitation of creating blocks, say a person may only create a block once in an amount of minutes equal to the user count. Sadly distributed per person identification is not technologically possible. Neither is it philosophically possible, is an organization a separate person? What about a robot? What about a full artificial intelligence? What about someone with multiple personality disorder? Or Star Trek Borg-like hivemind? Luckily a means of limiting spam in the virtual world has been explored by hashcash [2], the idea that a fee can be the solution to known to be difficult computational problem. So for every block we require something complex to be solved that relates uniquely to the block to be ”mined”. We call this Proof of Work, and it is essential to Bitcoin. In Bitcoin the proof is to find a nonce, a random data blob, to the block that makes its SHA-256 hash start with a certain amount of zeros. Fairly arbitrary, all will admit. But extremely effective. Computers have thus far had the amazing ability to adhere to Moore’s law [5], this will quickly reduce the amount of effort blocks cost, reducing them so far that spam might once again become a problem. Block production would grow linearly with use, another extremely unfavorable attribute. These problems have been solved by requiring the difficulty of the Proof of Work, the amount of leading zeroes, to be redetermined every so many blocks. Without this recalibration a block will be invalid. In the Bitcoin network it is set to recalibrate to one block every ten minutes, on average. This means the flow of blocks will be extremely steady. A transaction could still be reversed if someone were to swap the transactions in the blockchain by splitting the chain underneath the first of the transactions and proceeding with that forked chain. Should that fork ever become the longest blockchain the transactions will be reversed. That means the fork has to grow faster than the currently longest chain, recalibration of difficulty makes this effectively impossible. Recalibration however does not happen every block, in the Bitcoin network it does only every 2016 blocks or estimated 2 weeks. Meaning that someone with sufficient processing power might outrun the currently longest chain. The cost of that processing power becomes the certainty factor. It is therefore to the advantage of the network to promote a higher contribution to attempting to create blocks. Therefore it is possible, and for unusual transactions required, to place a bounty upon including a transaction in a block. The difference between input and output is assumed to be bounty and can be claimed by the block creator. To add some incentive and to solve the Bitcoin genesis problem described earlier a fixed reward is spawned in each block. The one to create a block may create a genesis-transaction towards himself of 50BTC. To get more reliable payouts people usually perform collaborate mining in so called pools that distribute earned Bitcoin proportional to work delivered towards finding a block. This amount will halve every so many blocks, causing the maximum amount of Bitcoins ever to come into circulation to be 21 million. This does not cause a fluidity problem as Bitcoins can be subdivided until eight decimal places, causing 2.1 quadrillion units to come into play eventually. It may seem that letting you computer do work lets you earn “free money”, in practice competition quickly drives out “casual” miners in favor of those employing specialized hardware. Such hardware can be a Field Programmable Gate Array (FPGA) that can be programmed to form a complex logic circuit, its capacity expressed in
quantity of logic gates. Such devices have a mass production advantage. Butterfly Labs has announced to be developing applied-specific integrated circuit (ASIC) devices and claims a 5500% improvement over presently excellent performance per watt [11]. So large an improvement seems excessive, put mildly, but ASIC should have at least a 2.5 times efficiency advantage over FPGA’s as gates are not multi purpose and as the name suggests the specialization allows for more performance gain. Let it be clear that SHA-265 hashing has become much more efficient due to the incentive to mine Bitcoin.

7 Politics

"And that’s actually how it works, and we never have any politics. That’s not quite true... we have other politics, but we do not have to worry about "commit access" thing." -Linus Torvalds in a presentation about git, a truly distributed version control system

A mechanism such as Bitcoin forces all policy to be made in protocol. Changes to the protocol need to be taken over by the rest of the community. Bitcoin is special among P2P protocols in that the most supported validation method takes precedence, only the longest blockchain is used, and that thus one can vote with hashing power. An extension was desired to allow escrow, a means of requiring a third party to agree upon a transaction. This is useful in trade where money can be payed but not used until a service or good has been delivered, effectively being held halfway to being transacted. As opposed to usual escrow the third party never owns the payment. There was discussion regarding how this extension should look. The extension would be incompatible, a transaction using it would be rejected by node that did not support it. This would cause the blockchain to fork. An IRC meeting was held to discuss the new extension on 14/02/2012 in which there was consensus to implement a specific method [1]. A vote was held, one could vote once per block. The extension was accepted with 770 votes for and 230 votes neutral with none against, the voting lasting 1000 blocks [3] or about 6.5 days. Note that this vote must be performed in some fashion, the blockchain would fork if the majority of miners would be against. Also note that this does not vote based upon miner count but on hashrate count, it is plutocratic. If the proof of work would be swapped with a proof of unique identity it could functions as a democratic vote.

7.1 Deflationary economy

A very controversial political decision inherent in the system is its limited supply. It causes deflation which is against the ideal in the Keynesian school of thought, that school promotes government interventions and inflation as a basis for growth. That school is the most popular the world round. The Austrian school is more focused upon a free market and prefers deflation. This school is much less popular in present day governments. It seems logical to prefer the second from a cypherpunk point of view, after all the free market is a self stabilizing idea whereas government intervention relies on humans and central authority to remain functional. The political choice for deflation would now require miner consensus to change. It is worth mentioning that gold itself is deflationary, although that depends on a much less certain supply. Further discussion of inflation versus deflation is outside the scope of this paper [9]. It is important to see that changing the way Bitcoin works requires a network consensus.

8 Other than uses for the Bitcoin system

The method for achieving consensus presented with the Bitcoin system is useful for many other purposes. A good example of how flexible it can be is the NameCoin network, that now implements the Dot-BIT project [10]. The project distributes aliases for the .bit TLD, allowing in a censorship free and distributed manner to create 1-to-1 aliases in the DNS system. NameCoin can be used for other types of key-value relations too and a hierarchical naming-structure is being developed to structure them. It has also been proposed for the central registration of papers, one could embed the title, hash and possibly magnet link to a paper into the blockchain. Thus "publishing" it at that point.

9 Good cryptographers write code

When someone claims "do not implement AES because you’ll screw up" do not listen. Yes you must never apply cryptography not thoroughly tested by yourself and others and even then will you make mistakes that you wish you could blame others for. But you only truly know it when you can code it, the best way to prove is to do.
References


