Bitcoin-based altcurrency Protocols : A Survey

Nur Hasan

Northeastern University
nur858@gmail.com

8 August 2013

Abstract

Bitcoin, the first truly decentralized cryptocurrency system was launched in 2009. Since inception, it has seen widespread adoption as a censorship-resistant donation system by organizations including Electronic Frontier Foundation, WikiLeaks, and Freenet. The system relies on peer-to-peer network built using free software. The unique infrustructure allows pseudonymous users to make financial transactions stored in public/global ledger record. Being fully decentralized, user's financial activity in bitcoin system is completely free from intervention and censorship by any government sponsored monitoring organization. This paper explores recent research activity on bitcoin and some newer protocols based on it.

Keywords: Bitcoin, Litecoin, PPcoin, Zerocoin, Namecoin, Primecoin, Domain Name System, Cryptography, Freicoin

I. Introduction

In 2008 pseudonymous developer satoshi nakamoto introduced a concept which he called peer-to-peer electronic cash system.The system is decentralized, works over peer-to-peer nerwork. Since this system does not rely on central authority and conventional trust based model, it is completely free from government intervention and censorship. the convergence of pseudonymity, transparency and decentralisation in one single cash system is something technological libertarians waiting for. Bitcoin understandably created stir among activists pursuing cryptography in service of empowering civil liberties.

II. Namecoin

At the pick of the Cablegate case in December 2010, the whistleblowing website WikiLeaks was severely crippled by attacks that revealed its vulnerabilities. DNS provider everyDNS stoped providing domain name service. Amazon removed it from their webhosting. This spree of denial of service was consequently upheld by PayPal, Visa, Mastercard and Bank of America denying it of all kinds of financial services. In this series of hectic events, Electronice Frotier Foundation(EFF) came forward and took part in protest against censorship on Internet. They took this opportunity to avocate for several free software tools that are censorship resistant. Along with some well known tools like Tor and Dot-P2P, they endorsed an electronic cash system that very few heard about before: Bitcoin, a decentralized digital currency (Palmer, 2010; Reitman, 2011). EFF viewed Bitcoin as a tool that has potential to evade centralized financial services, and ensure privacy and anonymity which these financial institutions exploit for political purposes.

EFF activist director Rainey Reitman spoke about Bitcoin for the first time in a public gathering, a WikiLeaks protest rally In San Fransisco in December 2010. Bitcoin solved a part of the censorship puzzle. The other part, the

DNS system was still a compromise of internet freedom. In 2010, Appamato described a Bitcoin like domain name system (BitDNS), and later internet activist Aaron Swartz touted similiar idea as a counter example of Zooko's triangle. A few months later in April 2011, it was implemented as Namecoin that can bypass ICANN's hierarchical DNS, offering itself as a strong framework for online freedom. Namecoin is an alternative distributed Domain Name System(DNS) based on Bitcoin Technology. It works by creating a new top level domain outside of ICANN control and makes internet censorship practically impossible. It extends Bitcoin to support transaction for registering, updating and transferring domains.

Like Bitcoin, Namecoin is also a peer-to-peer sysytem. It is based on the assumption that majority of participants is honest and the system cannot be controlled by a single state or company. Any changes/transactions to the namespace of the rightful owner of a domain with public key signature are distributed to all the peer-t-peer users. Inclusion as part of a block in a decentralized public ledger called blockchain, verifies that the transactions are authentic. Inclusion process involves a proof of work system where all the nodes in the system search for a small enough hash value with predefined property in a process called mining.

When the small enough value is found, the winner is credited with a set number of namecoins as reward, and the hash and the transaction information is added to blockchain. The reward amount initially was 50 coins and is programmed to decline exponentially every 4 years. Every block in the blockchain is timestamped. So after several subsequent hashes have been added to the blockchain, the transactions and registrations are considered to be irreversible. Because the would require attackers to come up with new set of hashes which would require an infeasible amount of computing power.

Dot-BIT is the first project using namecoin, and is building a domain name system using .bit as TLD. As of July 2013 there have been 78549 .bit domains registered. .bit is the first and only TLD of the so called Domain 2.0 namespace. The actions necessary to register a new domain or to update existing one are built into the Namecoin protocol by means of the new transaction types.

There are three types of Namecoin transactions:

name_new This operation costs 0.01 Namecoins(NMC). This constitues a fixed cost pre-order of a domain.

name_firstupdate This operation in effect registers a domain making it publicly visible.

name_update This operation is used to update, renew and transfer a domain.

Namecoin is merged mined with Bitcoin. Merged mining is the act of using work done on one blockchain on more than one other chains through a relation called auxiliary proof-of-Work. The hashed value to be mined contains:

coinbase Bytes that uniquely identify coins mined in current block.

merkle root Bytes that cointain history of all transactions.

This data is mixed to create a 'midstate' which is used as input to hashing algorithm. Namecoin mining is merged with Bitcoin mining by taking Namecoin 'midstate' and using it as coinbase for Bitcoin.

Like Bitcoin, there is a limit of 21 million of Namecoins and it takes 10 minutes to create a new block.

III. Litecoin

At the time of this writing (August'2013), a total of 11m Bitcoins have already been mined. It is getting even more difficult to earn new coins with time. People are solving this difficulty by throwing more computing power. They migrated from using computer processors to using graphics cards because of their huge number-crunching capabilities. For example, a CPU core can execute

4 (using a 128- bit SSE instruction) or 8 (using 256-bit AVX) 32-bit instructions per clock whereas a GPU like Radeon HD5970 can execute 3200 32-bit instructions per clock. In terms of GPU mining, AMD cards are preferred over NVIDIA cards due to their internal architectural differences that give AMD edge over NVIDIA. AMD designs GPU with many simple ALUs/shaders that run at a relatively low frequency clock. But NVIDIA design goes in opposite direction which consists of fewer more complex ALUs with high clock frequency. This design difference gives AMD advantage. For example:

- AMD Radeon HD 6990: 3072 ALUs x 830 MHz = 2550 billion 32-bit instruction per second
- Nvidia GTX 590: 1024 ALUs x 1214 MHz = 1243 billion 32-bit instruction per second

SHA-256 makes heavy use of 32-bit integer right rotate operation. This oeration can be implemented as a single hardware instruction on AMD GPUs(BIT_ALIGN_INT). But an NVIDIA GPU required three separate hardware instructions (2 shifts + 1 add) to do the same thing.

Together, these factors make AMD GPUs 3x to 5x faster when mining Bitcoins.

Hardware companies are pushing this computing limit even further by building specialised mining equipments using custom computer chips called ASICs (application-specific integrated circuits). ASICs are far more expensive than GPUs and CPUS, but they deliver minig capabilities into Gigahash range (comparing to 6-7 megahashes/sec on a Core i7 Mackbook Pro with 8GB RAM). As a result, GPU and CPU miners will alway be deprived with very high probability in this kind of ecosystem.

Partly because of this reason Charles Lee developed Litecoin. Litecoin has faster transactions (2.5 minutes as opposed to 10 minutes in Bitcoin). There are 4 times more coins (84 million) than Bitcoin. It uses Scrypt as proof-of-work. Scrypt is a sequential memory-hard function conceived by Colin Percival. Unlike SHA-256, Script is biased towards CPUs and GPUs, and against ASICs because of its memory-intensive computing. CPUs and GPUs are designed to work with variable amount of RAM whereas ASICs are not. They function on pure mathematical speed. ASICs are built to mine Bitcoin and can not mine anything else, but CPUs and GPUS are general purpose hardware. This could result in more CPU and GPU miners moving towards Litecoin mining instead of Bitcoin.

IV. PPCoin

Bitcoin's reward from mining is programming to decline exponentially. This may result in the decrease of incentive to mining and decline of miners as well. As the miners decline, the possibility of a monopoly increases which may leave the whole system vulnerable to a 51% attack. A 51% attack can take place when a single entity gains the control over more than half the mining power, which can allow this entity to double spend coins that a cash system must be able to protect against. PPCoin was introduced as a cure to this kind of risk. Its minting process and security model is built around a hybrid of proof of work and an alternative design concept called proof of stake.Proof of work only contributes to the initial part of the minting process and gradually reduces it signigicance as proof of stake takes over. In proof of stake, new coins are generated based on the possession of currency by the individuals.The possession of currency is estimated by another concept called coin age. Coin age is defined as the amount of currency times the holding period. In the hybrid proof of work/proof of stake design, blocks are of two types, proof-of-work blocks and proof of stake blocks. Special transaction in this new proof-of-stake block is called coinstake. In coinstake transaction, block owner pays himself consuming his own coin. In exchange, she gains privilege to generate a block for the network and mint for proof-of-stake. The first input of coinstake is called kernel and is required to meet

certain hash target protocol. The hash target that stake kernel must meet is a target per unit coin age (specifically coin-day). That means, the more coin age is consumed in the kernel, the easier meeting the hash target protocol.

Unlike Bitcoin, PPCoin Does not have a fixed money supply cap. The minting design attempts to mimick gold rather than Bitcoin. Gold does not have cap but it is known to be scarce. For many years, the annual inflation of gold is around 1-3%. Proof-of-work minting rate is regulated by Moore's Law which dictates exponential growth. But Moore's Law will eventually end. By that time, PPCoin will switch to Proof-of-Stake and maintain at most 1% annual inflation.

One drawback of PPCoin is that it is technically not decentralized as it required centralized checkpointing. Checkpointing is used to prevent any changes to the part of the block earlier than the checkpoint time. PPCoin's centralized checkpointing is used to defend the network until it matures, and to enable it to smoothly upgrade if any critical vulnerability revealed.

V. Zerocoin

Pseudonymity is the way Bitcoin offers privacy. Bitcoin transaction does not include user's name. Instead the only identity of users it includes is the public key. Already several academic works have successfully deanonymized Bitcoin transactions by building Bitcoin Transaction Graph. there are quite a few options to enforce stricter privacy model to evade this.

Use many Public keys a Bitcoin user can use different public keys for different transactions. This will make revealing identity harder.

Use TOR Tor provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis.Bitcoin can run easily on the Tor network.

Use Laundry There are services called laundries that take Bitcoins from users, mix them up, and return them back. It makes it very hard to trace transactions. Laundry is great when lots of users use it. But in reality, volume of users is very poor.

Zerocoin promises true anonymity in Bitcoin network. It is an extension to Bitcoin network that runs a separate anonymous currency designed to live side-by-side with Bitcoin on the same blockchain. Zerocoin is exchangeable with Bitcoin on a one-to-one basis.

A user can purchase Zerocoin by placing a special "Zerocoin Mint" transaction on the blockchain. Once the transaction is accepted by the Bitcoin peers, the same user can redeem the zercoin back into Bitcoins. She needs to embed the destination address into a "Zerocoin Spend" transaction, then sends it back to the network. During transaction verification process Bitcoin peers will treat Zerocoins like normal Bitcoin transfer. Redeeming Zerocoin gives user a completely different set of Bitcoins unrelated to what was Zerocoin minted for.This is why there is no way of relating Mint Transaction to its corresponding Spend transaction. Once a user converts her Bitcoins into Zerocoins, it is very hard to determine where she took them back out. Zerocoin is more like world's biggest laundry.

Zerocoin uses a combination of digital commitments, one-way accumulators, zero-knowledge proofs, and some extensions to the existing Bitcoin protocol. It also shares some similarities to a previous work by Sander and Ta-Shma.

A digital commitment allows one to commit to a chosen value or statement while keeping it hidden to others, with the ability to reveal the committed value later. This commitment scheme is designed so that a party cannot change the value or statement after they have committed to it.

A family of one-way accumulators is a family of one-way functions each of which is quasi-commutative (i.e. f(f(x,y1), y2) = f(f(x,y2), y1)).

zero-knowledge proof is a method by which one party (the prover) can prove to another

party (the verifier) that a given statement is true, without conveying any additional information apart from the fact that the statement is indeed true.

Zerocoin process starts by having have each coin commit to a random serial number. A fast commitment alogirthm wrap this number in a coin. The commitment process works like encryption, in that the resulting Zerocoin completely hides this serial number. At the same time the coin 'binds' the user to the chosen number. This random serial number is secret and only the user knows it.

To "Mint" new zerocoin, user needs to post the zerocoin to the network along with standard Bitcoin transaction containing enough Bitcoins to pay for it. The Mint Transaction adds some extra messages to the Bitcoin protocol. Since no change is made to existing protocol feature, Zerocoin transaction essentially is Bitcoin transaction with some extra data added to it. The peer-to-peer network will always accept it.

The "Spend" transaction is relatively complicated. To redeem zerocoin, the user first creates a transaction that contains the coin's secret random serial number which was created during "Mint" transaction. The user also attach to the transaction a zero-knowledge proof of the following two statements:

- The user previously posted valid zerocoin on the blockchain.
- The serial number attached to the "Spend" transaction is indeed the same number hidden in the zerocoin.

After a "Mint" transaction, Bitcoins which the zerocoin was minted for, cannot be accessed/used without publishing a "Spend" transaction for corresponding zerocoin.

VI. Primecoin

One of the disadvantages of Bitcoin is that its proponents often gloss over is the fact that its mining algorithm has little real world value. In order to add a new block to the Bitcoin blockchain, a Bitcoin miner must include a "proof of work", a number that is computationally difficult to find but easy to verify. The level of difficulty of finding proof is adjustable. It is obvious that mining will become harder with time. Number of miners will decline and the risk of 51% attack will increase. Bitcoin network will increase difficulty level to overcome the imminent threat. This is certainly an implication that growing amount of electricity burning will go on to make the network secure. For example, as of April 2013 the generation of Bitcoins was using approximately $150,000 USD per day in power consumption costs.

It has always been thought that something valuable can be done with this huge computing power. Some suggested that mining algorithm should have included SETI@home or folding@home. This way it would contribute to some of the world's most computationally-intensive projects. But the inherent problem with that thinking is that, participants will be more motivated by profit and will not bother with the actual purpose of those projects.

Primecoin is the first altcurrency based on a proof-of-work that just does not burn electrictiy but also does something more important. Instead of SHA256 hashes, the Primecoin miners find long chain of prime numbers. The problem with using "finding next prime" as proof-of-work is that it gets exponentially harder to find next prime. But proof-of-work should be efficiently varifiable by all the nodes of the network. This disqualify Mercenne prime and qualify prime chains as proof-of-work for Primecoin. There are three specific types of chains that are of interest:

Cunningham chains of first kind Each prime is one more than double of the previous prime in the chain.

Cunningham chains of second kind Each prime is one less than double of the previous prime in the chain.

Bi-twin chains Each twin pair of primes are basically doubles of the previous twin pair.

Primecoin accepts these three types of chains as proof-of-work.

Primecoin uses the p-1 test in combination with the Euler-Lagrange-Lifchitz test to establish primality.

One of the properties of proof-of-work for cryptocurrency is non-reusability.Primecoin adds a restriction for this. For Primecoin, the origin of a "Bi-twin" prime is the average of the first pair in the chain. For single Cunningham chains, the origin is the average of first pair given the Cunningham chain's twin also exists. To ensure non-reusability, Primecoin requires that the origin of prime chain must be divisible by the hash of the block that the proof of work is for.

Like Bitcoin, Primecoin has adjustable difficulty. It uses remainder of Fermat test of base 2 as the difficulty indicator. For example, let k be the length of prime chain p_0,p_1,p_2, ...,P_{k-1}, r be the Fermat test remainder of the next prime in chain p_k. p_k/r is used to measure difficulty of the chain. The primechain length d is then computed with a fractional part: d = k + (p_k - r)/p_k.

Unlike Bitcoin, where transactions take 10 minutes to confirm, the Primecoin blocks are created at the rate of one per minute.

Like PPCoin, currency supply in Primecoin is governed by the natural simulation of gold's scarcity. Unlike Bitcoin, block reward or proof-of-work minting rate is not fixed but self-adjusting. It is determined by current difficulty in the network. The number of Primecoin released per block is always equal to 999 divide by the square of difficulty.

VII. Freicoin

All the Bitcoin protocol based altcurrenies seen so far, do not guarantee higher liguidity. Onwer of the coins can hoard them idle as long as they wants. This is where Freicoin differs from others. Friecoin is a decentralized currency based on Bitcoin protocol with some extra economic ideology included. This ideology is based on the writings of German merchant and economist Silvio Gesell. Freicoin introduces Gesell's concept of demurrage; the application of a carrying cost to money. Demurrage fee on money is designed to mirror the kinds of storage costs can be seen with other units of value. Gold must be stored. so must other assets, and they all cost money to hold. In Freicoin, the demurrage fee is set at around 5% per year. This will promote currency circulation and encourage sustainable investments.

Like Bitcoin, coins are mined in Freicoin by solving SHA256 problem. But the way miners are rewarded is different than other currencies. At the beginning, the total amount of currency in circulation will smoothly increase for approximately 3 years until it stabilizes at 100 million coins. During the initial 3 year distribution, part of the newly created currency is given to the miners in proportion to their contribution, starting at 30% and eventually decreases to 5%. The remaining currency is distributed through the Freicoin Foundation, a non-profit organization aiming to promote Freicoin and support a sustainable world.

VIII. Conclusion

Bitcoin has made significant progress in its adoption and usage since it was introduced in 2009. Other currencies based on Bitcoin are also doing very well. But still digital currencies are at their infancy. Their evolution over next few years will decide wether it will become integral part of global financial system or be rejected as another failed attempt.

References

[Nakamoto S., 2008] Bitcoin: A Peer-to-Peer Electronic Cash System

[King S., Nadal S., 2012] PPCoin: peer-to-peer crypto-currency with proof-of-stake.

[Percival C., 2009] Colin Percival. Stronger key derivation via sequential memory-hard functions.

[Barok D., 2011] Bitcoin: censorship-resistant currency and domain name system to the people

[Vinced, 2011] Namecoin a distributed naming system based on Bitcoin. Bitcoin Forum [online] (Published 18 April) Available at: http://forum.bitcoin.org/?topic=6017.0/

[Miers I., Garman C., Green M., Rubin A. 2013] Zerocoin: Anonymous Distributed E-Cash from Bitcoin

[King S., 2013] Primecoin: Cryptocurrency with Prime Number Proof-of-Work

[Ron D., Shamir A., 2013] Quantitative Analysis of the Full Bitcoin Transaction Graph

[Sander T., Ta-Shma A., 1999] Auditable, Anonymous Electronic Cash Extended Abstract

[Buterin V] Primecoin: The Cryptocurrency Whose Mining is Actually Useful. Retrieved from http://bitcoinmagazine.com/primecoin-the-cryptocurrency-whose-mining-is-actually-useful/.

[Freicoin site] How Freicoin Works. Retrieved from http://freico.in/how/.