NDCoin and Cryptographic Currency Application

Sathvik Palakurty

07/18/2014

Table of Contents

Abstract

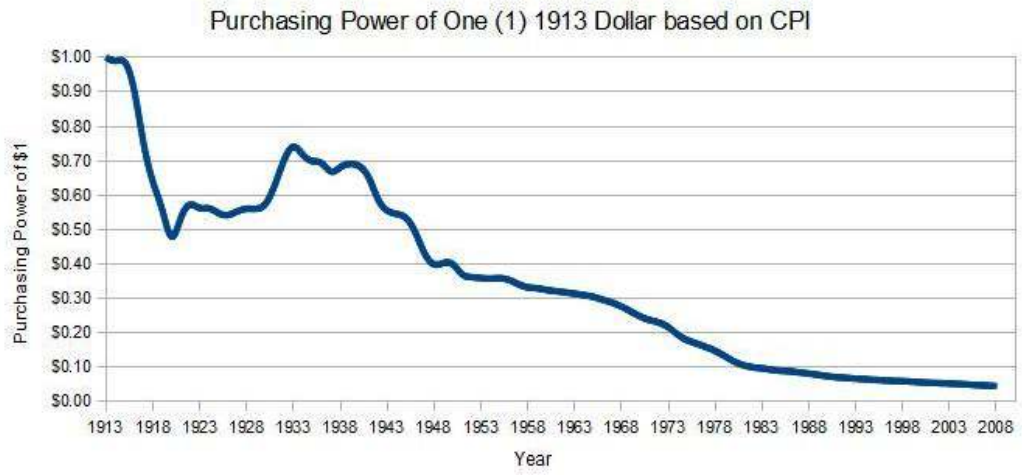
In this paper, we will investigate Bitcoin and Bitcoin related technologies as well as novel technologies that will aid in the implementation of NDCoin, a new cryptocurrency that allows for one to make an incomplete transaction request with a non-deterministic problem. Along with the reasons why cryptocurrencies are needed and the revolutionary technologies brought forth by Bitcoin, we will discuss hashing and other cryptographic technologies. Therefore, the bounty of NDCoin is given to whichever node finds the solution to the problem the fastest. The integrity of the solution is double checked by the system to ensure that the node is honest. To ease the amount of computational effort needed for a node to verify a non-deterministic problem, various technologies like zk-SNARK (were explored. We will also view the different methods including running a Turing machine on encrypted data to obfuscate the execution of the code to protect the customers data. A brief introduction to PitCoin, a currency that allows public trading of stocks with no centralized authority, will also be provided.

Why digital cash?

In a day and age where we already have credit and debit cards, digital cash might seem redundant. However, cash money offers certain benefits over the use of electronic means of transferring funds. Digital cash does not ideally require a middle man meaning that the costs of transaction are negligible allowing for small transactions as opposed to credit cards which require the merchant to pay swipe charges limiting the use of virtual money to larger transactions. Cash itself is anonymously transferrable and hard to trace. Cash can be accepted in confidence with minimal trust. For example, one can check the validity of the bill by verifying watermarks; however, the validity of a cashier's check or a credit card requires the use of a central authority. Lastly, the transactions are irreversible. However, digital cash can be more useful than physical cash given that the limits of distance are removed. One can make long distance transactions immediately with minimal risk and hassle. Digital cash offers encrypted storage as opposed a wallet or a safe which requires less work to obtain the money. It allows for the use of backup copies and adds non repudiability because one cannot deny a transaction as they can with paper money.

Fiat Currency

A fiat currency is one that a government has declared to be legal tender, but is not backed by a physical commodity. The value of fiat money is derived from the relationship between supply and demand rather than the value of the material that the money is made of. Historically, most currencies were based on physical commodities such as gold or silver, but fiat money is based solely on faith. Due to fiat money not being linked to any physical reserve, there is a possibility of the money becoming worthless due to hyperinflation if the government prints more money. Most modern paper currencies are fiat currencies which hold no intrinsic value.



Past Digital Cash Restrictions

The double spending problem arises with the ability to make multiple copies of digital cash. If one were to send the same copies of the digital cash to two separate merchants to spend it twice, then digital cash fails to mimic the security of tangibility that real cash provides. If the viability of the cash, whether it has been spent yet or not, must be checked with a central authority, there is a central point of weakness given that one must invest trust in authority.

Bitcoin

This cryptographic currency provides solutions to the past digital cash restrictions. To make an electronic payment system that is trustless, it uses cryptographic proofs and allows two people to communicate directly with each other without the use of a third party. Just like cash, Bitcoin transactions are nearly impossible to reverse allowing the sellers to be protected from frauds that are common with credit cards. Bitcoin provides a solution to the double spending problem by utilizing a timestamp that is irrefutable. Also, unlike fiat currencies, the total number of Bitcoins that can ever be generated is about twenty one million allowing the users to have confidence that their currency will not hyperinflate. Future regulations on Bitcoin and other cryptocurrencies in the state of Florida is determined by the Office of Financial Regulation, to whom Dr. Frank, the IRP sponsor, is presenting on possible recommendations for regulation or lack thereof. Precedent was recently created by the release of a draft of New York's financial regulations on Bitcoin.

Transactions

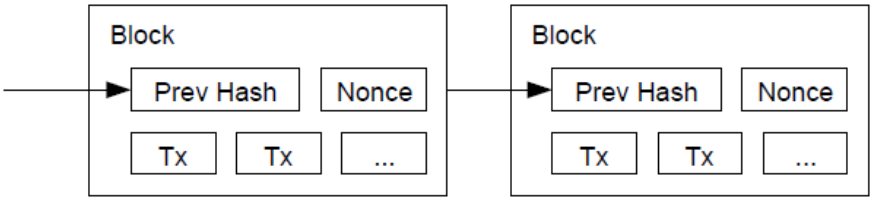
Rather than a particular serial code attached to the coin identifying the coin, a coin is marked by a chain of digital signatures. Every time a transaction is made, the person that currently owns the coin will hash[1], the previous transaction and attach the public key of the person receiving the money to the end of the coin. This allows one to verify who had the coin and the order of ownership. To verify that the coins have not been double spent meaning that there are not two or

[1] Hash - an algorithm that yields the same result for a given input but is nearly impossible to reverse to see the output even given the hashing function because this function is not one to one

more chains of ownership for the path of a coin, a new way of time stamping transactions was devised so that the only one transaction holds merit, the one that came first.

The Blockchain

A block of items or transactions are hashed at given intervals. The validity of a transaction can be verified to see if it was included in a block. If the transaction was included in a given block, one knows that the transaction was made at that time. The next block includes the previous block's hash in the input to its hashing function as well as a block of transactions. Therefore, each block and the following blocks reinforce each other. To utilize this method of maintaining time in the system, one needs to use a proof of work system. The proof of work system is to find a given hash for a certain nonce that yields a given number of zero bits at the beginning of the hash. One would need to increment the nonce till they find a certain number of zero bits. Once the nonce is found, the block is added to the blockchain. If one would want to change the blockchain, in other words, change a transaction or reverse one, they would need to redo the work to find the nonce that satisfies the number of zero bits at the beginning of the hash. However, as more blocks are added to the chain, one would need to expend more computational work because they would need to find the nonce that satisfies a given block which requires a change as well as all the following blocks because the following blocks take the previous block's hash as part of the hash function's input. Because nodes always consider the longest chain, the integrity of the blockchain is maintained even if someone were to replace a block.



Dynamic Difficulty

The difficulty of adding a block to the blockchain is increased or decreased based on fluctuations in hardware and increasing technology. If too many blocks are being produced at any given time, the number of zero bits required increases meaning that there is a lower probability of one attaining a value of a hash that satisfies the required number of zero bits. This means that as time increases, due to the inevitable evolution of technology, it will be more difficult to add a block to the chain.

Attacks to System

The brute force attack is when the attacker submits a transaction to the network indicating that he has paid the merchant while mining a blockchain fork that involves double spending. The merchant sends the product after a certain number of confirmations, the merchant sends the product that the attacker bought. Then, the attacker releases the blockchain fork that allows him to regain his money. He will have to provide more computation power than the rest of the network combined. The attacker controls more than half of the network's hashrate, since the

probability of success of the attack is dependent on the percent of the network hashrate, the probability of success becomes one. This is because the attacker can produce blocks faster than the rest of the network. His blockchain would be the one accepted by the network because he blockchain will be longer than the chain generated by the honest network. The more confirmations a transaction has, the more computationally expensive the attack will be; however, no number of confirmations can prevent the attack ideally. When analyzing incentive, a company which holds 51% of Bitcoin is very unlikely to double spend given that it would cause people to lose interest of trust in Bitcoin effectively causing the value to drop.

Bitcoin Intrinsic Value

Although Bitcoins are not backed by physical commodities or gold, some argue that Bitcoin does have intrinsic value in that it can be used to verify that one possessed a certain document at a given time. Given that the block chain is an irrefutable timestamp, the contents of a certain document can be hashed and broadcasted to the network allowing one to declare to the network, the possession of a set of information. However, NDCoin[2] will provide greater intrinsic value given that the currency can be used to employ computational power from the network.

SHA256

Designed by the National Security Agency and published by the National Institute of Science and Technology in 2001, SHA256, standing for Secure Hashing Algorithm 2 – 256 bit, has an output of 256 bits. With the output, unlike encryption, there is no way that one can obtain the input of the hashing function. For SHA256, there are 2^{256} possible outputs given that the output is always 256 bits; however, there is no definitive limit to the number of inputs because hashing algorithms, in contrast to encryption, do not have a 1:1 mapping function. Application specific integrated circuits have been developed to quickly hash using the SHA256 algorithm contributing to a large difficulty rise in the Bitcoin network. For newer coins, given that the hash rate is very high for ASICs used for SHA256, this might discourage the average consumer.

input	61 62 63
hash	ba7816bf 8f01cfea 414140de 5dae2223 b00361a3 96177a9c b410ff61 f20015ad
input	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
hash	248d6a61 d20638b8 e5c02693 0c3e6039 a33ce459 64ff2167 f6ecedd4 19db06c1
input	One million of 61
hash	cdc76e5c 9914fb92 81a1c7e2 84d73e67 f1809a48 a497200e 046d39cc c7112cd0

Examples of hash function inputs and outputs

Scrypt[3]

There is a growing rise of alternative currencies employing the scrypt hashing algorithm. Since the scrypt algorithm takes a longer time to hash any given input, the hash rates are naturally

[2] Currency to solve non-deterministic problems in a trust free manner

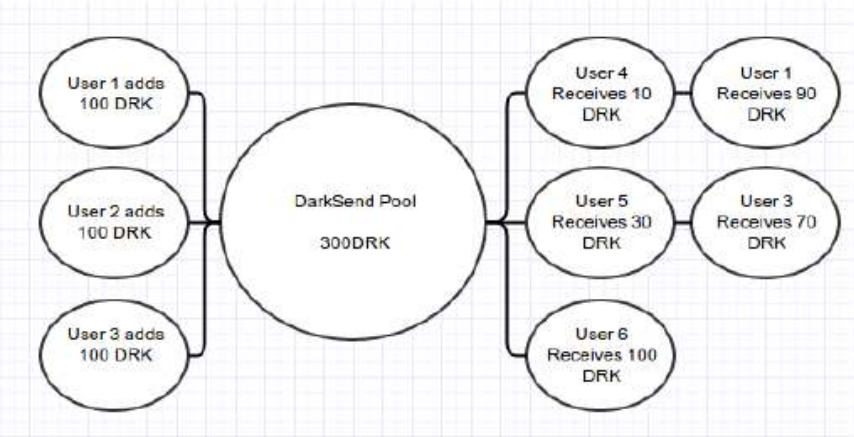
[3] Although traditionally this hashing algorithm was hard to generate ASICs for, new chips are recently anticipated in the market.

going to be smaller. However, the unique part about scypt is its ability to discourage the use of application specific integrated circuits (ASICs). This allows the smaller consumers to mine with their graphics processing unit. Although some hardware has been developed for scrypt, the ideal mining of scrypt coins requires huge amounts of memory or RAM. Depending on the business plan for NDCoin, one must either use scrypt or SHA256. However, it is notable that some currencies employ a chain of hashing functions providing more security.

Darkcoin

Although Bitcoin provides some privacy in that the public addresses cannot be tied to one's identity, Darkcoin seeks to improve the inherent problem of privacy brought upon by publishing the block chain publically. Employing a technology which is named DarkSend, small transactions are merged into larger anonymous ones. The system takes a set of random transactions made by regular modes and elects a master node randomly. The master node is then the one that makes the transaction meaning that there is no way to indicate whose money the node had and how much each of the regular nodes are spending. To defend against malicious users, DarkSend uses a collateral system in which 0.1 DRK ~ 1.3 USD is given to the payment nodes, the last nodes to create a block. If the suspected malicious user puts an input but refuses to complete the transaction or leaves the network, the payment node will get the collateral that the potentially malicious node had to put up when making a transaction. These payment nodes will be ones that are monitoring the network for wrong doing. The use of the collateral system allows the payment nodes to get return for the work that they have expended when monitoring the system. Since transactions are grouped into larger transactions, all the transactions are added up to a denomination of money, similar to cash. This means that one cannot discern any information based on the size of the transaction. Although the master node seems to have a disproportionate amount of power compared to regular node, to insure that the transaction will not be lost if the master node loses connection or is a dishonest user, a slave node will be elected. On top of all the existing anonymity features, a given user can choose to push their money through the DarkSend pool meaning that they send their money to themselves. This will take up space in the pool and increase the overall speed and anonymity of the network because transactions can be more efficiently be paired into larger transactions of a certain denomination. Unlike other popular cryptocurrencies, DarkCoin uses X11[4] for proof of work rather than SHA256 or Scrypt. This prevents the use of ASICs to mine in the short run. X11 is a string of 11 different hashing function where the output of one hashing function becomes the input of the next hashing function.

[4] A combination of blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo hashing algorithms



Transactions are made in round w and all transactions are anonymous

Ethereum

Unlike other crytocurrencies, Ethereum is a platform for decentralized applications. The goal is to distribute the consensus from a single authority figure to a network. This allows individual developers to make applications that can easily be implemented in the Ethereum platform. Providing only the abstract for currencies, in its bare bones, it functions like any other currency like Litecoin; however, one can create a contract account which executes a given set of code when a transaction is made. Although the transactions are all made in ether, one can use the ether to do a large variety of things. Existing applications of Ethereum, which is to release in December of 2014, include NameCoin, which allows reservation of domain names, and BitVote, that allows elections to be held on a distributed consensus network where corruption is less likely. Applications of Ethereum extend to a wide variety of the already existing coins given that it can replace Dogecoin. Outlined in the initial white paper of Ethereum was an idea for cloud computing; however, the idea is different from NDCoin in that there is no description of economic motive for mining nodes to compute for the person that hires the job. However, there was an indication that the nodes that are computing would have to put forth a security deposit before they are allowed to compute on a given job to discourage them from cheating. Another innovation of Ethereum is that each transaction has a given amount of gas and the rate at which the gas is consumed when a transaction is made to a contract account, to ensure that the contract code does not require excessive steps that overload the node.

Turing Machine on Encrypted Data

A Turing machine is simply a machine or algorithm that uses parameters that are predefined to yield a result from a set of input variables. Currently there are many options to compute on encrypted data including fully homomorphic encryption, Yao garbled circuits, functional encryption and attribute based encryption. The common model that is employed by all the technologies stated above takes a given input x and encrypts it into a cipher text. Then the algorithm which one wants to execute is converted into a cryptographic representation, which is called an evaluation key. The evaluation key can then be used to run the encrypted input yielding an encrypted or unencrypted output. In Yao garbling, a given algorithm, represented as a Boolean circuit, gets converted to a garbled circuit which corresponds to the evaluation key of

the algorithm. The garbled circuit is similar to a regular circuit; however, the gates have a string of binary. The input is garbled into a binary string. Then the algorithm can be evaluated in encrypted form. The need for a Turing machine to compute on encrypted data is brought to light when one looks at the simplex algorithm. This is an algorithm that runs very quickly under most instances but sometimes runs exponentially slower. Given that the encrypted key of the algorithm, represented as a circuit, is very large because it must consider even the inputs that rake exponential time to run. The use of Turing machines will allow a short definition for the evaluation key in encrypted form. However, the use of Turing machines will leak information about the time required to process a certain input. This slightly weakens the encryption scheme of fully homomorphic encryption. We can employ this method of computing on encrypted data to protect to the information given for computation by the customer to the node that is calculating in NDCoin.

NDCoin

NDCoin is a new cryptocurrency that allows one to submit an incomplete transaction to the network with a set number of conditions. The deadline for the transaction will be set such that if the no node can prove successful execution of a nondeterministic algorithm that is outlined in the condition of the transaction before the given time limit, the funds will be transferred back to the customer; however, if a node does manage to execute the algorithm and proves to the network that it has, then the public address to which the funds will be transferred to will be set to the that node which has found the solution to the nondeterministic problem. For computationally heavy tasks, zk- SNARK, a proof of computation that required no information, could be used which has a computationally expensive prover but a very quick verifier. Although currently this is not feasible because the generation of a prover is very computationally expensive, the need for a facile way to check the integrity of the solution is needed. However, if the customer accepted the solution provided by the node, the network can automatically accept the transaction given that the customer has no incentive to accept a false solution as true. The advantage of NDCoin over other cryptocurrencies is that having this currency has intrinsic value in that it can be used to buy computational power. Since the customer nor the solver can cheat by rejecting a correct solution or announcing an incorrect solution, this is truly trust free. However, the nature of the computation in some cases might be sensitive. Therefore, one can employ fully homomorphic encryption to allow for computation on encrypted data. To advance on that, one can employ a Turing machine to more efficiently execute a given encrypted algorithm given that the encryption key for FHE with Turing machine is significantly smaller than if one employs the conventional method. While NDCoin can revolutionize computation, one must consider the potential for abuse by black hat users. However, after brief investigation, the anonymity provided by NDCoin does not pose a greater threat than do the services already available for malicious activity today. Therefore, one does not need to additively worry about malicious use of computational power.

PitCoin

The current electronic trading platforms have many problems including the problems of opacity and mistrust since the participants of the market do not have access to the actual trading. They

have to go through a central authority figure. Also, it is a common practice to intercept incoming trades and place orders before the incoming trade to slightly raise the price. With the introduction of a cryptocoin, the participants have access to the actual trades; therefore, they can observe the trading activity on the network first hand. Due to this transparency, auditing to insure fair play becomes exponentially easier. Also, traditional trading allows one single point of weakness giving a target. Similar to what happened during the September 11th, 2001 attacks, a single authority indicates a single point of weakness. PitCoin works by allowing institutions to announce notes balances to the blockchain providing an irrefutable timestamp. The account holders directly add bids to the ledger rather than going to through an agency. There will be no absurd costs of trading since the mining fees are negligible.

The Future

With the introduction of new cryptocurrencies, there is a rapid decentralization of power where one no longer relies on one authority figure to dictate wrong and right. Given innovative solutions like NDCoin and PitCoin, the individual will no longer have to rely on large institutions but rather is empowered by distributed consensus.

References

A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. Mathematics of Computation, 61:29–68, 1993.

Ben-Sasson, Eli. "Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture." . http://www.ieee-security.org/TC/SP2014/posters/BENSA.pdf (accessed July 18, 2014).

Duffield, Evan. "Darkcoin: PeertoPeer CryptoCurrency with Anonymous Blockchain Transactions and an Improved ProofofWork System." . https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf (accessed July 18, 2014).

Frank, Michael. "Frank, Michael. Introducing NDcoin A Cryptocoin-Based Concept for Incentivized, Distributed Nondeterministic Computation. : , .." *Cryptowerks Inc.*.

Goldwasser, Shaffi. "How to Run Turing Machines on Encrypted Data." . (accessed July 8, 2014).

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." . https://bitcoin.org/bitcoin.pdf (accessed July 18, 2014).

National Security Agency. "Descriptions of SHA-256, SHA-384, and SHA-512." .

"You Say Bitcoin Has No Intrinsic Value? Twenty-two Reasons to Think Again. - Bitcoin Magazine." Bitcoin Magazine. http://bitcoinmagazine.com/12846/you-say-bitcoin-has-no-intrinsic-value-twenty-two-reasons-to-think-again/ (accessed July 18, 2014).