A Survey of Cryptocurrencies: general workings & security

Matthew Beary, mfbeary (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download

Abstract

Cryptocurrencies seek to replace or supplement traditional currencies to facilitate transactions without trusted third parties, while making certain cryptographic guarantees. Removing reliance on a trusted party incurs certain challenges in both payment confirmation and anonymity. The strength of cryptographic guarantees via proof-of-work can ensure that the system remains consistent and accurate in the long-term, but problems can arise in short-term payment confirmation.

Keywords

Cryptocurrency, crypto, currency, Bitcoin, BTC, blockchain, de-anonymizing, double spending, altcoin

Table of Contents:

1. Introduction
2. Purposes and Uses of Cryptocurrencies
3. Basic Functionality of Cryptocurrencies
   A. The Block Chain
   B. Difficulty of Removing Transactions
4. Adoption as a Currency
5. State of the Bitcoin Network
6. Information Propagation
   A. Possible Improvements
7. Possible Attacks
   A. Double-Spending
   B. De-Anonymizing
8. Conclusion
9. Works Cited
10. List of Acronyms

Introduction

Cryptocurrencies have emerged over the last several years, claiming to be an alternative to traditional forms of currency. This has caused a bit of an uproar across the world, as these currencies have been seen as anything from a worthless scam to a viable, secure alternative. Since the technology is relatively new, it may still be several years until their viability is truly made clear.

As with any protocol or program, cryptocurrencies face problems that are not seen with traditional currency. Things such as program errors, malicious network members, and simple communication delay can cause problems within a network. These must each be countered or mitigated, or the currency itself can become entirely worthless overnight.

Purposes and Uses of Cryptocurrencies

Cryptocurrencies can be used for many purposes, both positive and negative. On the one hand, they can represent a simple way to transfer funds long-distance, without the need for intermediaries, transaction fees, and conversion fees to the local currency. On the other hand, relative anonymity can make such currencies a haven for illegal transactions and money laundering [Brezo12]. As intermediaries are often unneeded in these networks, lawmakers lose the ability to use middlemen as regulatory agents [Marian14]. These same sorts of issues can be found in any sort of directly-traded currency, including physical ones such as the US dollar.

Private transactions can have many positive effects, in addition to the negative effects espoused by many governments. For example, supporting a cause or group when there could be backlash for doing so or when intermediaries refuse service. One notable instance of this was when major credit card companies and PayPal halted transactions to WikiLeaks under pressure from the US government [Greenberg10]. WikiLeaks was able to continue taking donations over that time, via Bitcoin [Greenwald12], as there was no intermediary which could be pressured.

By removing third parties, cryptocurrencies can enable long-distance transactions without the fees usually associated. For example, PayPal charges start at 2.9% plus $0.30 per same-currency transaction [Paypal14]. Credit card companies charge transaction fees at roughly similar rates [Martin14]. However, there are often fees associated with exchanging a cryptocurrency for a fiat currency (such as Euros or US dollars) similar to exchanging one fiat currency for another.

Basic Functionality of Cryptocurrencies

Cryptocurrencies seeks to remove trusted third parties in its transactions. Since value is not kept in physical tokens, it must use some method to ensure that transactions can be verified. To do this, it uses a combination of public-key cryptography and public announcements. All transactions consist of the sender signing a hash of the receiver's public key and the sent coin's previous transaction hash. This hash is then announced publicly.

Many cryptocurrencies are designed to have a finite amount in circulation. For example, the Bitcoin protocol will cap the market at 21 million Bitcoins (BTC). This makes them more resistant to inflation, and more similar to stocks from a trading perspective [Bhatt14].

With public transaction announcement, privacy may come into question. However, the accounts in a cryptocurrency network consist only of a public-private key pair. This means that a person cannot necessarily be connected with their accounts. As we will see, however, there are still some issues with anonymity.

The Block Chain

Consistency in cryptocurrency networks is maintained via a proof-of-work chain, known as a block chain. It is the public record of all transactions that have taken place thus far. These transactions are broken up into blocks, which are signed by nodes in the network. The hashing in these blocks is done as a Merkle Tree [Rosen14].

A block is only considered valid if the hash of the block and its nonce begin with a certain number of zero bits. This means that to sign a block, a node must find a nonce that creates such a hash. This proof-of-work is a cryptocurrency's answer to the Byzantine Generals problem, making votes determined by processing power as opposed to another method which would be easier to overpower, such as proof-of-stake [Nicolas14].

The block chain itself contains several anti-fraud measures. Each block includes the previous block's hash, which makes altering a block significantly more difficult as its successors are added to the chain. The longest chain is always used, which ensures that the network is in agreement [Nakamoto08]. If two blocks are created at the same time, the chain briefly forks. The first fork to be built on becomes the correct chain.

There are various incentives used for the work done to sign blocks. One method of doing so is for newly-created coins to be added to the node signing each block. Another possible incentive is transaction fees.

Difficulty of Removing Transactions

The difficulty of removing transactions from the block chain increases significantly as more blocks are added. This is because enough valid nonces must be found to make the fake chain at least as long as the currently-accepted chain. Table 1 shows the percentage of computing power within the network, q, required to have a 0.1% chance of altering block z from the end of the block chain and is based on a table from page 8 of [Nakamoto08]

Table 1: difficulty of removing transactions

q	z
10	5
20	11
30	24
40	89

Adoption as a Currency

Bitcoin and other cryptocurrencies are beginning to seriously face the question of adoption as a currency. While there are certainly cons to adoption of cryptocurrency (especially from a taxation standpoint), there are many reasons one may be adopted.

The early adopters of a cryptocurrency will generally have specific reasons for doing so. They may simply be a tech-savvy person who already has sufficient equipment, and tries the currency out of curiosity. They may also be interested for political or philosophical reasons, as cryptocurrencies can cut out many middlemen. The relatively anonymous nature of cryptocurrencies is also a boon to black market traders. Finally, cryptocurrencies can make several aspects of microtransactions easier for online games [Luther13].

There are several reasons a new currency can gain ground once it has a sufficient base of early adopters. One common way throughout history was for a government to introduce a currency, enforcing a fixed exchange rate with existing currency [Luther13]. Another is simple network effects - once several people accept a currency, it becomes more useful to have that currency. Finally, hyperinflation can make people flee an old currency for an alternative.

Whether or not a cryptocurrency is considered a currency can also have profound legal effects. For example, the US Department of the Treasury's "Financial Crimes Enforcement Network" determined that since virtual currencies could be exchanged with & used as a substitute for legal tender, it counts as a form of money transmission [MiddleBrook14]. This means that financial laws written to deal with issues such as money laundering and Ponzi schemes can apply to cryptocurrencies in the US. This has led to several subpoenas over the last few years [Varriale13]. On the other hand, the IRS (Internal Revenue Service) does not classify Bitcoin as a currency - it is considered a property [Hill14]. These issues and more led the Government Accountability Office to release a report highlighting the lack of a real legal definition that can be applied to virtual currencies [McLeod14]. These conflicting regulations cause issues for the usability of Bitcoin by businesses

At this point few cryptocurrencies have bases beyond the early adopters. However, it will be interesting to see how continuing financial issues across the globe effect this.

State of the Bitcoin Network

The network of a cryptocurrency as a whole is also an interesting topic. Bitcoin, as one of the oldest cryptocurrencies, has had the most thorough investigation of its network.

Since Bitcoin (BTC) can be sent in increments of 10^{-8} BTC, small transactions are common. The majority of payments are in the sub-BTC range, as each BTC tends to be salable for several hundred US dollars. In 2011, it was measured that 84% of transactions were less than 10 BTC [Ron11].

At this point, the high prices for Bitcoin could partially be explained by their scarcity. In addition to have a maximum number which will go into circulation, the vast majority of BTC are sitting in accounts which have not sent any transactions in a great while. Among other things, this could include early-adopters who have since forgotten their account information, along with block-signing nodes whose operators have yet to use their newly-minted BTC. It was measured at one point that 78% of the total BTC in circulation belonged to dormant accounts such as these [Ron11].

In addition, it is frequently encouraged for users to take additional steps to protect their anonymity. This can be seen in the network, as transactions are frequently sent via several intermediates [Ron11]. In addition, users frequently have many accounts in order to decrease the likelihood of their transactions being linked. This can have varying amounts of success, as we will explore later.

Information Propagation

Information propagation in the Bitcoin network, as well as several other cryptocurrencies, follows the following protocol [Decker13]:

1. receive a block from another node
2. verify that the hash of the block is valid and correct
3. verify that each transaction hash within the block is valid
4. send "inv" messages to each neighbor, alerting them of a new block
5. if the neighbor does not have the block, it will send a "getData" message back
6. the block is sent

This can be visualized as shown in Figure 1, which is based on Figure 2 of [Decker13]:

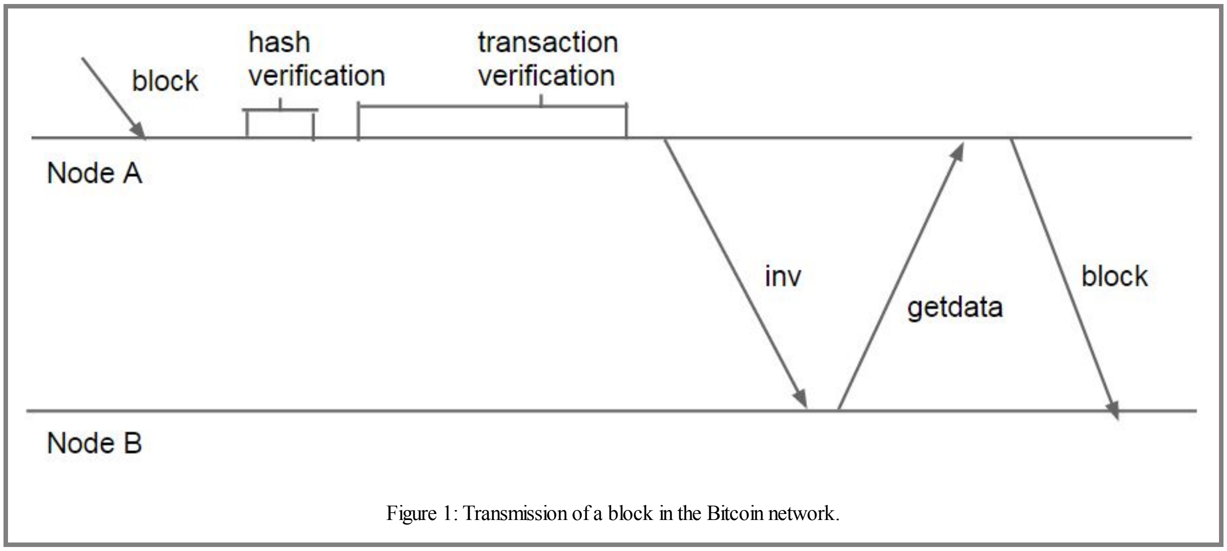

Figure 1: Transmission of a block in the Bitcoin network.

Possible Improvements

There are several possible ways this information propagation could be improved, which would allow for faster confirmation of payments, reduce wasted effort by nodes attempting to find hashes for old blocks, and make removing old payments even more difficult [Decker13]. All three of these methods are compatible with the existing default Bitcoin protocol.

Firstly, the "inv" message could be sent after the block hash is verified, but before the transactions are verified. Since the proof-of-work is checked in the block hash verification, this still provides a large barrier against denial-of-service attacks.

Another option would be to immediately forward "inv" messages, while not sending the entire block until after its hash has been verified. This allows the "inv" and "getData" roundtrip with Node B (in Fig. 1) to happen alongside Node A's download and verification of the block. The downside of this would be that Denial of Service attacks could become easier to mount - a node would need to detect when its neighbors are sending "inv" packets for which they cannot provide a block, and stop forwarding that neighbor's messages. Figure 2 shows the transmission of blocks with both immediately forwarded "inv" messages, and blocks forwarded after the block hash check.

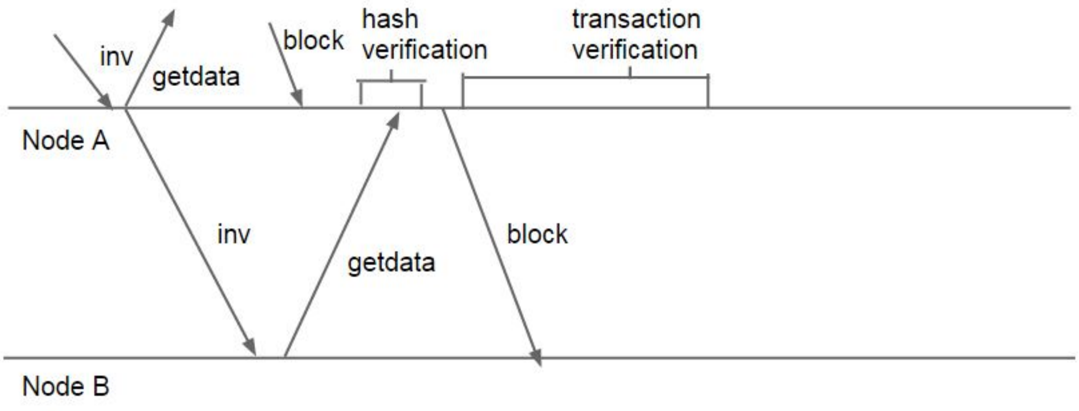

Figure 2: Alternate block transmission method

A third option would be to simply connect each node to more neighbors. The current default implementation has a minimum of 8 peers, and a measured average of 32 [Decker13]. By increasing the network's connectedness, the shortest path between from any node to any block's signer can be greatly reduced.

While there are more possibilities for improving the communication within the Bitcoin network, it has been shown that these three can greatly reduce the number of forked blockchains within the network [Decker13]. This decrease in forks allows transactions to be verified more quickly, and increases the reliability of the network by reducing wasted computing time.

Possible Attacks

The networks of cryptocurrencies were built to reach a consensus for the location of each coin in the network. However, this consensus takes a bit of time to reach, which may be vulnerable to exploitation. The consensus model also means that all transactions are publicly visible, which may allow for accounts to be linked with one another, and with their owners.

Double-Spending

Double-spending in a blockchain is spending the same coin a second time, before the block containing the first transaction is hashed. If the second payment is sent more widely than the first, there is a good chance that it will be the one considered valid by the network (as it arrived at more nodes before the first transaction did) [Karame12]. This is not such an issue for things like mail-order goods, but can be an issue in an area with quick turnaround, such as fast food. In the Bitcoin network, blocks are intended to be hashes on average every 10 minutes, but can take significantly longer. It has been shown that the default implementation is very weak to double-spending, and a 100% success rate can be achieved [Karame12]

While alternate currencies with shorter hashing times may be ideal for quick transactions, there are a few steps vendors can take to protect themselves. Simply increasing their connectivity within the network can help ensure that the correct transaction is spread quickly, and that they become aware of overlapping transactions more quickly. They can also set up additional nodes in the network, such that they have multiple locations able to see false transactions. Finally, the default implementation only forwards the first transaction received for any coin. This means that if the vendor's neighbors all see the correct transaction first, they will never forward the malicious transaction to the vendor. Changes to the network such that all transactions are forwarded would ensure that vendors can observe double-spend attempts against them [Karame12]

De-Anonymizing

As cryptocurrencies operate in an environment where all transactions are publicly visible, questions arise as to their anonymity. It has been shown that there are methods of reducing user anonymity by identifying accounts owned by the same person. If any of these accounts can be traced back to the user, then the anonymity of all accounts involved is removed.

Value merges are a common transaction in cryptocurrency networks. This is where one account sends all of its funds to a second account owned by the same person, in order to make a transaction that neither can fully afford. By looking at these transactions, the set of all accounts can be condensed into a much smaller set of users, with most users owning several accounts [Reid13].

The nature of peer-to-peer networking as used in cryptocurrencies can also cause some personal information to be leaked. When a transaction is made, the sender of funds sends a message to all nodes they are connected to, which in turn forward the transaction message through the network. However, by connecting to all peers, one can determine the sender's IP address by seeing which peer first sends the transaction message. This is a generally successful method of mapping public keys to IP accounts, as explored in [Reid13]

One final way to connect people to their accounts is simply by looking for other accounts they have set up. For example, many exchanges require both personal information and a public key to facilitate currency exchange. By using this along with the condensed set of users that can be found, many transactions are able to be fully de-anonymized [Reid13]

Conclusion

Cryptocurrencies could represent a new way to conduct transactions securely over distances, but have many problems to contend with. Between legal and technical issues, it may still be several years before their viability is apparent. However, many of their behaviors can already be observed.

At the base level, cryptocurrencies provide a way to remotely transfer funds without a trusted third party. This can be a great economic benefit, as it will cut out transaction fees and charges by intermediaries. However, this can also make them much harder to regulate, as the third party cannot be leveraged by governments.

As with any software, cryptocurrencies today have a few issues. While these issues might mean that they are not yet suited for quick transactions, they may be overcome by alternative protocols used by newer and less-well-studied cryptocurrency networks. In addition, properties of the block-chain can allow for information leakage, resulting in a loss of anonymity.

Works Cited

C. Decker and R. Wattenhofer. "Information propagation in the bitcoin network," in IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, September 2013. Retrieved from http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6688704

Brezo, FÃ©lix, and Pablo G Bringas. "Issues and Risks Associated with Cryptocurrencies such as Bitcoin." SOTICS 2012, The Second International Conference on Social Eco-Informatics. 2012. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=sotics_2012_1_40_30101

G. Karame, E. Androulaki, and S. Capkun. Double-Spending Fast Payments in Bitcoin. In Proceedings of ACM CCS 2012, 2012. Retrieved from https://eprint.iacr.org/2012/248.pdf

Luther, William J. Cryptocurrencies, Network Effects, and Switching Costs. Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, forthcoming. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134, 2013.

Reid, Fergal, and Martin Harrigan. An analysis of anonymity in the bitcoin system. Springer New York, 2013. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4614-4139-7_10

Ron, Dorit, and Adi Shamir. "Quantitative analysis of the full bitcoin transaction graph." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013. 6-24. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39884-1_2

S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf.

Middlebrook, Stephen T., and Sarah Jane Hughes. "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions." Wm. Mitchell L. Rev. 40 (2014): 813-1158. Retrieved from http://je5qh2yg7p.scholar.serialssolutions.com/?
sid=google&auinit=ST&aulast=Middlebrook&atitle=Regulating+Cryptocurrencies+in+the+United+States:+Current+Issues+and+Future+Directions&title=William+Mitchell+law+revie
272X

Varriale, Gemma. "Bitcoin: how to regulate a virtual currency." International Law Review 32 (2013): 43. Retrieved from http://www.perkinscoie.com/images/content/1/4/v2/14234/08-20-2013-Bitcoin-IFLR.PDF.pdf

Marian, Omri Y., A Conceptual Framework for the Regulation of Cryptocurrencies (October 23, 2014). University of Chicago Law Review Dialogue, Vol. 81, 2015 Forthcoming. Available at SSRN: http://ssrn.com/abstract=2509857

Hill, Austin, "Bitcoin: Is Cryptocurrency Viable?" (2014). CMC Senior Theses. Paper 902. http://scholarship.claremont.edu/cmc_theses/902

Rosen, Elie, et al. "Bitcoin: An Empirical Study of Cryptocurrency." (2014). Retrieved from http://gdclark.com/wp-content/uploads/2014/08/FinalReport2.pdf

Nicolas, Houy. "It Will Cost You Nothing to'Kill'a Proof-of-Stake Crypto-Currency." Available at SSRN 2393940 (2014). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393940

Bhatt, Pramod Chandra P. "Whatâ€™s new in computers." Resonance 19.6 (2014): 549-569. Retrieved from http://link.springer.com/article/10.1007/s12045-014-0058-2

McLeod, Patrick. "Taxing and Regulating Bitcoin: The Government's Game of Catch Up." CommLaw Conspectus 22 (2014): 379-379. Retrieved from http://je5qh2yg7p.scholar.serialssolutions.com/?
sid=google&auinit=P&aulast=McLeod&atitle=Taxing+and+Regulating+Bitcoin:+The+Government%27s+Game+of+Catch+Up&title=CommLaw+conspectus&volume=22&date=20
5871

"PayPal Fees - For Purchases, Getting Paid and Merchant Fees - PayPal." PayPal Fees - For Purchases, Getting Paid and Merchant Fees - PayPal. N.p., n.d. Web. 23 Nov. 2014. https://www.paypal.com/webapps/mpp/paypal-fees

Martin, Andrew. "How Visa, Using Card Fees, Dominates a Market." The New York Times. The New York Times, 04 Jan. 2010. Web. 23 Nov. 2014. http://www.nytimes.com/2010/01/05/your-money/credit-and-debit-cards/05visa.html

Greenberg, Andy. "Visa, MasterCard Move To Choke WikiLeaks." Forbes. 7 Dec. 2010. Web. 23 Nov. 2014. http://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/

Greenwald, Glenn. "Prosecution of Anonymous Activists Highlights War for Internet Control." The Guardian. The Guardian, 23 Nov. 2012. Web. 23 Nov. 2014. http://www.theguardian.com/commentisfree/2012/nov/23/anonymous-trial-wikileaks-internet-freedom

List of Acronyms

- BTC = Bitcoin (the transactional unit)
- IRS = Internal Revenue Service

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at http://www.cse.wustl.edu/~jain/cse571-14/index.html

Back to Raj Jain's Home Page