Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 44 (2015) 527 – 536

Procedia Computer Science

2015 Conference on Systems Engineering Research

An Architectural Assessment of Bitcoin

Using the Systems Modeling Language

Nicholas Roth*

Abstract

Bitcoin is an emerging crypto-currency, which is wrapped in mystery and controversy. The goal is to transform how we transfer payments. The current approach for sending money from one remote party to another is via bank deposit and transfer by check or bank transfer. PayPal and other services were developed to provide faster payments to verified individuals, but each layer in the transaction adds time, cost, and/or risk to the transaction. Users of this new digital currency proclaim the benefits of security, anonymity, and efficiency for making transactions.

The functionality and structure of the Bitcoin Network is complex and often attacked for not being a suitable replacement for currency. An independent understanding can be developed of the composite Bitcoin Financial Systems of Systems architecture by considering the challenges any System of System would face. A functional analysis, employing the Systems Modeling Language (SysML), is performed on the Bitcoin System of Systems architecture to help gain an understanding of the structure and functionality, and how that relates to the key actors and use cases, for determining if the users' expectations are aligned with the architecture.

Peer-review under responsibility of the Stevens Institute of Technology.

Keywords: Bitcoin; crypto-currency; SysML; System of Systems

* Nicholas Roth. Tel.: +1-256-513-9876;
E-mail address: nroth6@gatech.edu

Peer-review under responsibility of the Stevens Institute of Technology.
doi:10.1016/j.procs.2015.03.066

1. Introduction

Bitcoin is an electronic money system (EMS) [1] that was created to exchange units of currency called bitcoins, sometimes referred to BTC [2]. Many electronic money systems have existed and had success in the past [3], but Bitcoin differs in that it is a new and unique cryptocurrency with mechanisms that try to mitigate costly challenges to an EMS. A cryptocurrency uses cryptographic controls to eliminate the need for a central authority's involvement in transactions, which removes the risk that they might manipulate the supply of currency, or feel compelled to mediate on disputes. The upper bound on the amount of cryptocurrency units is known and carefully controlled to mimic a scarce resource, such as gold [4].

1.1. Heritage

Bitcoin became popular at a period in time where distrust in government, due to the handling and impact of the Financial Crisis of 2007-2008, was at an all-time low of 17% [5]. Poor government regulation, over regulation, complicated financial products, and investment bank behavior have all been blamed for the crisis [6], but the common theme among the explanations is reliance on an inherently imperfect central authority.

The Cypherpunks were a group that believed a better alternative was to rely on software because it "can't be destroyed" and "a widely dispersed system can't be shut down." The group had a history of utilizing software to provide "a guarantee", with "physics and mathematics, not with laws," due to their distrust in central authority [7][8]. This distrust in government was confirmed as a result of the Edward Snowden National Security Agency leaks in 2013 [9]. The Cypherpunks mailing list was a means of organization for central authority concerned individuals, including Julian Assange. They defined their purpose as:

> *"…dedicated to building anonymous systems… Privacy is necessary for an open society in the electronic age… We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy…We must defend our own privacy if we expect to have any. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money"* [10].

The Cypherpunks' efforts in electronic money began with Digicash in 1990, which resulted in a failed commercial offering. The real step towards what Bitcoin is today was Adam Back's development of the hashcash proof of work (POW) function in 1997. This function was applied by Hal Finney to develop a reusable proof of work (RPOW) as a form of money [11], which was used in Wei Dai's B-Money Proposal [12], Nick Szabo's Bit Gold proposal [13], and finally, Satoshi Nakamoto's Bitcoin proposal [14].

1.2. Architecting Non-Reversible Transactions

Satoshi Nakamoto, a pseudonymous author, published the foundational specification for Bitcoin and developed the initial Bitcoin implementation. The architecture was designed to achieve non-reversible, cash-like transactions by removing the third party. He reasoned that traditional electronic payments falter by requiring a third party, which cannot avoid mediating disputes, and will inherently increase overhead and transaction costs [14]. The generalized financial system of systems, in Figure 1, shows the common components that exist in such a system, including governments, banks, an interbank network, debit/credit aggregators, central banks, and a core central bank network. It is the business and political interests and their control of storing, exchanging, and producing more currency that the central authority concerned individuals dislike about the system.

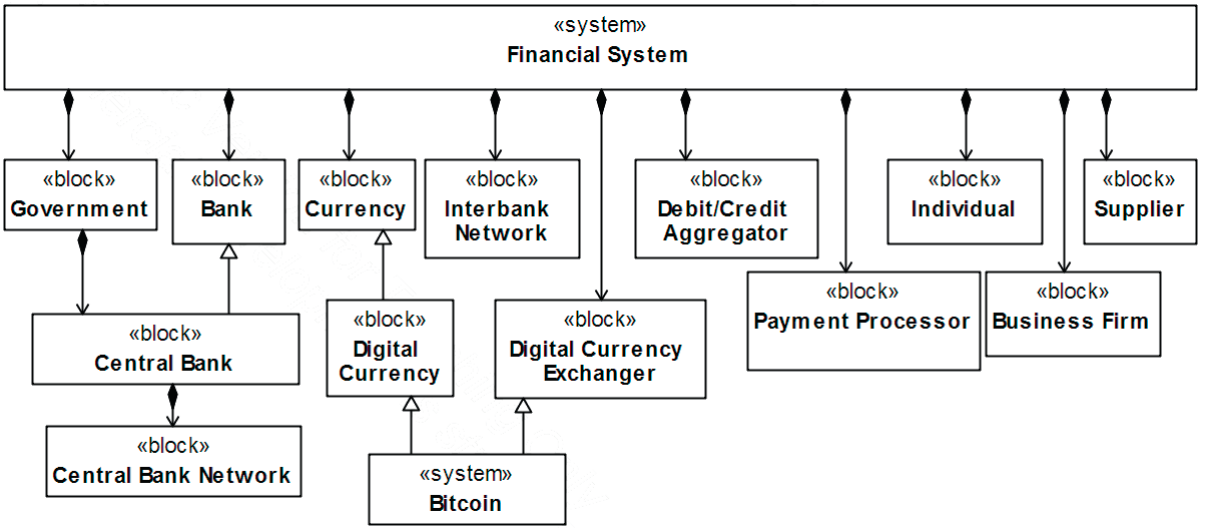

Figure 1. - Financial System

The POW is the capability that removes the need for a central authority in a transaction, and therefore, the risk that the transaction could be reversed. By implementing the POW functionality into a decentralized processing network of incentivized nodes, Bitcoin can achieve non-reversible, hard transactions. These hard transactions operate in the same manner as an exchange of physical currency would.

The goal of the architect was for the Bitcoin Network to process payments at a lower cost [14] than comparable services, such as PayPal or Western Union, by cutting out steps in the process. This paper will conceptualize the key structural and behavioral elements of this Bitcoin Financial System of Systems (SoS) (also referred to as Bitcoin SoS), to include the core Bitcoin Network and the services that are built on top of it, using Systems Modeling Language (SysML). The purpose is to investigate the alignment of users and their fundamental requirements to the direct and indirect qualities of the SoS.

For sake of communication, a simplified key to SysML notation is provided in Figure 2, below:

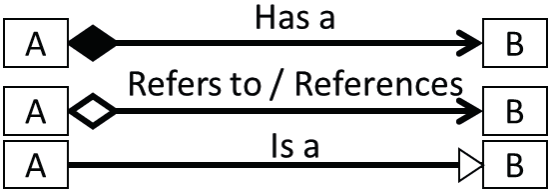

Figure 2. - SysML Relationship Key

2. Bitcoin Architecture

The Bitcoin network could be viewed as the key component of a specialized financial system, the Bitcoin Financial System of Systems. It is an alternative to the traditional system, which is built around large banks and their interbank network. This SoS, which includes the Bitcoin Network, the foundation that supports it, the e-commerce stores that utilize bitcoin processing software, and the payment processors is depicted in Figure 3. The key concepts of Bitcoin are outlined in the following sections.

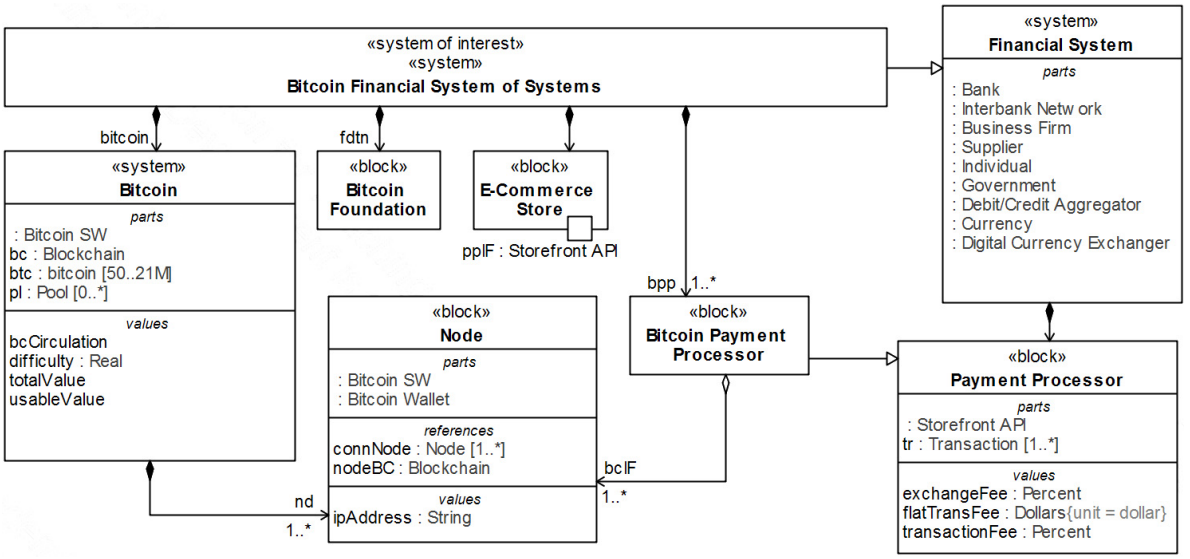

Figure 3. - Bitcoin Financial System of Systems Architecture

2.1. Transactions

The first key concept of the Bitcoin network are the **transactions**. The electronic coin is passed from owner to recipient by writing the transaction into a distributed ledger to form a non-reversible history of all transactions. The system uses asymmetric cryptography to allow the payee to verify that the payer (who must sign the current transaction) is the recipient of the bitcoins in the connected past transactions. Any recipient can check this chain of transactions back to the creation of the bitcoins. This verification process proves that the person paying owns the transferred currency, which is not possible for something like PayPal.

2.2. Blocks/Blockchain

The second key concept is the aggregation of transactions by time into a chain of **blocks**, each including a timestamp. This chain of blocks forms the distributed ledger, called a **blockchain**. A unique hash is then generated for each block, which could have only originated from that specific block, and then is widely published to the network. The global availability to the network allows anyone to verify that the transaction must have occurred at a set moment in time by simply verifying the hash [14]. Figure 4 shows the composition of many transactions into a block, and blocks into a blockchain. The block contains a tree hash of the composed transactions and the hash of the previous block. The compositional nature and references to previous blocks is what creates the chain of history. The hashing function and reference to a specific bitcoin wallet writes the transaction from payer and payee into the blockchain history.

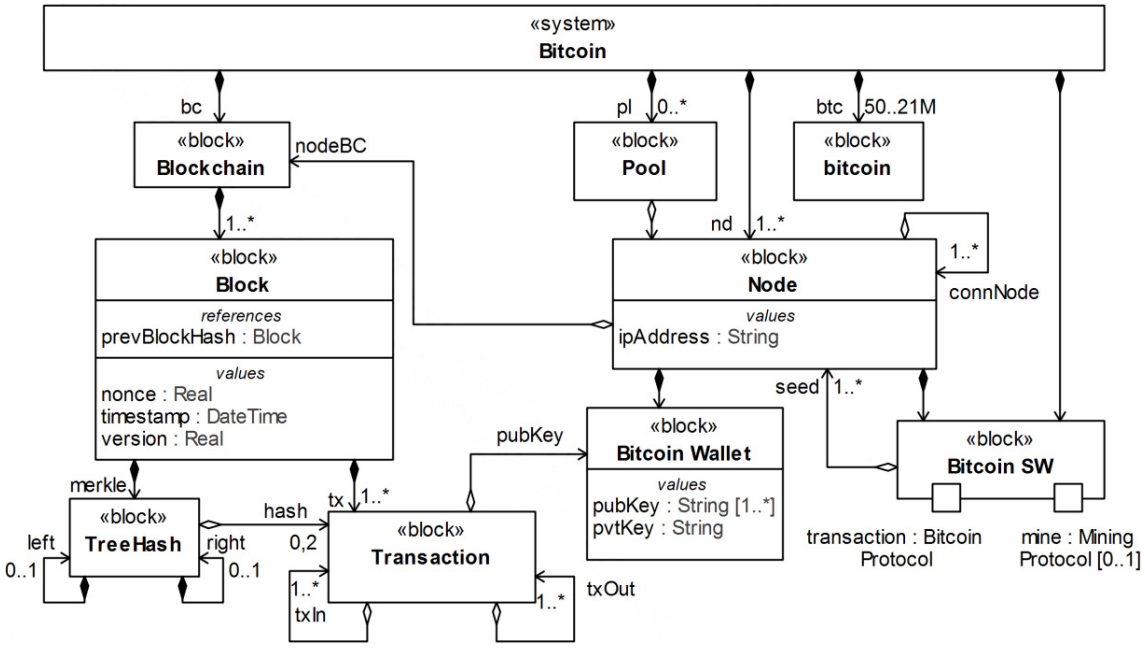

Figure 4 - Blockchain Data Model

2.3. Proof of Work

The third key concept is the **proof of work** scheme. By creating a system that requires real CPU cycles to create each block, the history of the blockchain can be protected. Because each block includes the hash of the previous block, an attacker would have to rebuild all subsequent blocks if they desired to modify the transactions that occurred within it. The work required to create a block varies in difficulty over time to make sure that a block is created on average of every 10 minutes. The processing complexity is introduced by requiring that the node adds a guess, called a "nonce," to the block of transactions. Each node increments the nonce each time they hash the block, until the resulting hash meets the predefined rare criteria of starting with a number of zeroes. The number of zeroes required is how the difficulty is adjusted over time as the processing capacity of the network changes [14].

2.4. Protocol

The fourth key concept is the decentralized **Bitcoin protocol**. The independent behavior of each node in the network is predefined for each node to continually request for and store the blockchain locally. Each node groups the current set of published transactions into a block, and race each other, through the previously described hashing process, to create the valid block. Whenever a node finds a valid block, it is announced to all other nodes, who then can assess the validity of the block. The other nodes stop trying to produce the new block at this point, and will begin on any outstanding or new transactions. Each node acknowledges the validity of the past block by incorporating the hash of it in the next block that is being worked [14].

A byproduct of the decentralized nature of Bitcoin is that it also has anonymizing characteristics. Each transaction can be seen as a unique id sending some number of bitcoin credits to another unique id. However, as [15] points out, a transaction consists of a grouping of input transactions to previous transactions. This grouping, along with knowledge of the individuals, gained from compromised money exchange websites or well-known public keys, could be used to deduce information about individuals or organizations.

3. Economics

3.1. Incentive

The reason that the nodes process the transactions and build on the block chain, instead of creating branches, is the potential reward for their work. Before a node begins working on a block, it is able to add an additional transaction to it called a generation or coinbase transaction [16] (noted inside Block on Figure 4). This special transaction is what adds bitcoin supply to the Bitcoin Network, but the protocol is developed to taper off this value exponentially. The potential for reward is what jumpstarted the Bitcoin Network and provides incentive until the network is established enough to support transaction fees. The transaction fee can be added to the transaction to make it more likely that a node will include a given transaction in a block. The approach moves network funding from inflation to transaction fees over time.

3.2. Transaction Value

The cost per transaction has increased significantly over time, due to the value of bitcoins increasing disproportionate to the number of transactions. Some point to this as an inherent inefficiency in Bitcoin, and others expect that market forces will balance this over time at the agreed market value of a Bitcoin transaction [17]. The high level objectives of specific types of researched users are related to the derived technical requirements in Figure 5. While there is overlap in user requirements, the General Consumer is going to have a different priority on any overhead that is primarily aligned with the concerns of the Central Authority Concerned user. Similarly, the Central Authority Concerned user may place a higher value on anonymity, and drive the cost of transaction higher than the general user would care for.

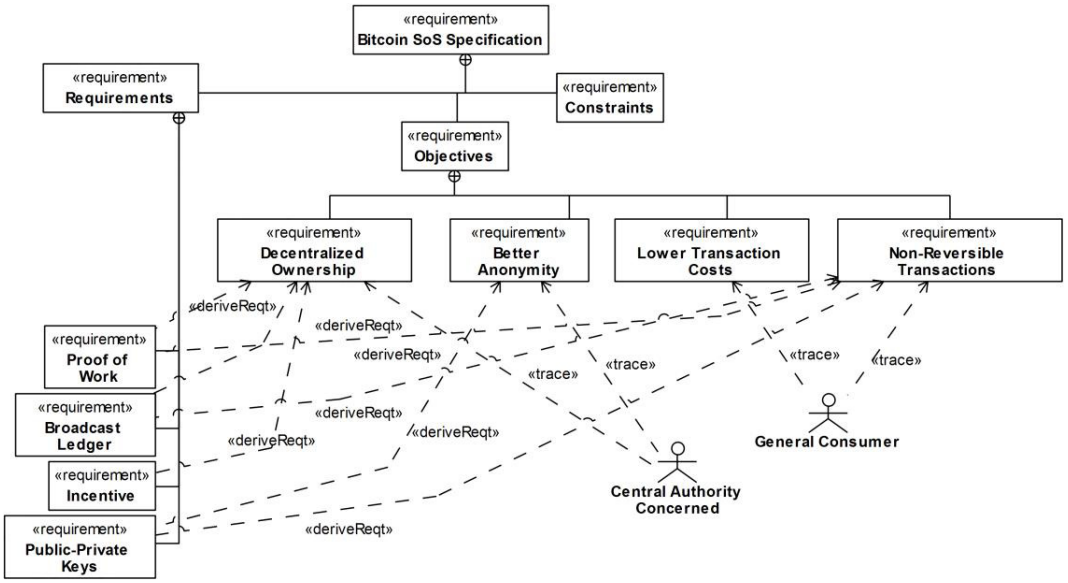

Figure 5. - User Objectives

SysML parametric diagrams can be used to identify how attributes of different system aspects may be related to each other through a set of equations. A simple example of a more complete cost of the transaction is modeled in Figure 6. The full transaction cost is a function of the total compute cost, the value of the transaction and the corresponding transaction fee, any flat transaction fee, and the cost to convert the bitcoins back into the primary currency. The cost can be defined, but it is up to the individual user class to determine if the value of the system benefits that matter to the individual are worth the additional cost. There exists no inherent guarantee that the cost will be lower than a traditional system in the same way that there is a guarantee that the transaction is non-reversible.

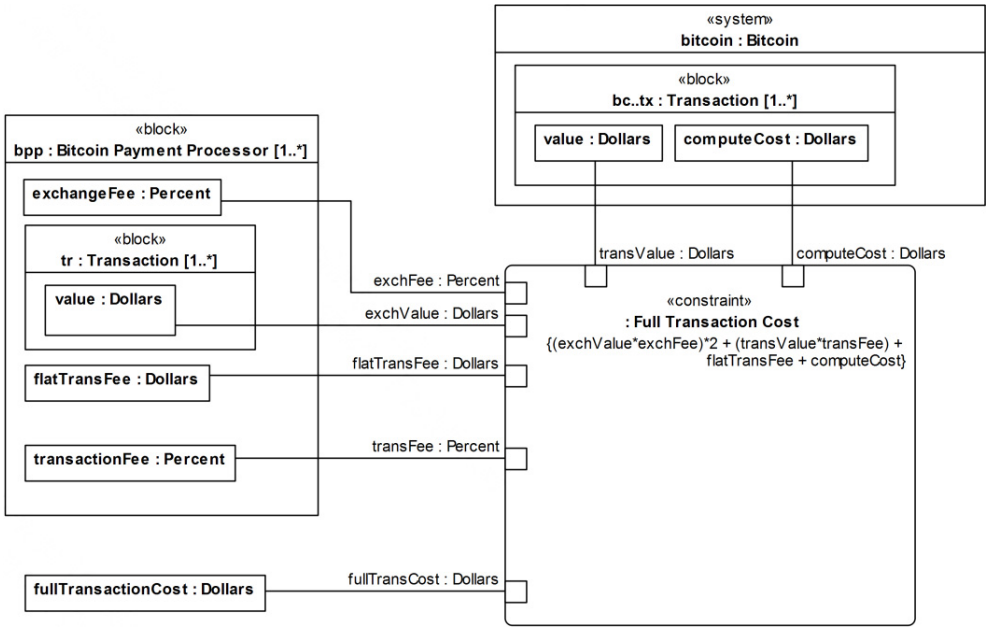

Figure 6. - Transaction Cost Parametric Model

3.3. Pooling

In [18], the author investigates the decentralized schemes and alternatives to form into pools (depicted in Figure 4) within the Bitcoin Network. The author finds that the POW difficulty in 2011 results in a 1.18% chance that a typical solo miner would receive a payment at any point during a day. As of February 2nd, 2014, [19] reports that the average time per block with solo mining is ~297.5 years. Because the difficulty increases exponentially, there is a high, and always increasing, incentive for nodes to form into mining pools. The mining pools concept provides some means to fairly group nodes that would otherwise be operating independently, so that their individual hash rate is more consistent. The higher hash rate increases the possibility that one of the nodes in the pool will produce a valid block over a given period of time. The result is that a less powerful node in a large pool will have a much lower variance [18]. A number of different pool and reward systems, such as Proportional, Pay-per-share, Slush's method, Geometric method, and other more advanced methods have been analyzed for fairness and the potential for abuse. Pooling is a large part of Bitcoin and most individual nodes are likely to be part of one, and is a critical behavior layered on top of the core Bitcoin standard that must be carefully considered [18].

3.4. Acceptance as Money

A great amount of online effort goes into debating whether or not bitcoins can be considered money. This debate is primarily fought from various camps of economics and independent bitcoin fans. An interesting aspect of this debate is that the different sides have varying definitions of what money is. In this debate there are many that go back to the accepted key functions of money, which are to serve as "a medium of exchange, a unit of account, and a store of value" [20][21]. By some Austrian economist accounts, Bitcoin would not be considered money because it fundamentally isn't founded first as a medium of exchange.

In [20], Bitcoin is considered in the context of the evolutionary theories of money and how they become accepted. The idea presented is that medium of exchanges compete against each other based on their merits, and may excel in areas where another may fail. A summary of the key attributes identified in [20] are liquidity, store of value, and transaction costs. The transaction cost from Figure 6 being just one aspect of what makes a medium of exchange

successful. The general consumer and central authority concerned users likely would have differing opinions in what aspects they would compromise for the others.

4. Assessment

4.1. Systems Engineering Process Considerations

A System of Systems requires that the architect put thought into how the constituent systems fit within the whole, balance the SoS and system requirements, and plan for how the system will evolve over time. The architecture is broader than just a snapshot for how the system looks at any single point in time. This concept could affect current actions in preparation for a future state. The following core elements of SoS engineering are analyzed for how well they have been addressed by the Bitcoin System of Systems.

4.1.1. Translating Capability Objectives

The focus of Nakamoto is clearly outlined in the Bitcoin whitepaper for the system to be decentralized, make non-reversible payments, and to be trusted. The requirements derived from the objectives are to implement a decentralized ledger of transactions with timestamps, cryptographically signed transactions, proof of work, message broadcasting, payment verification by any node, and an incentive mechanism that self-adjusts as the network grows [14]. However, there is no specific capability implemented that will guarantee lower transaction costs, which is also described as a goal.

4.1.2. Understanding Systems and Relationships

The primary component that defines bitcoin is the interface that any node must implement. This is the framework that Nakamoto defines. However, while much time was spent anticipating future use or attacks, there was no concerted effort in the architecting by Nakamoto to address the SoS-level complexities that are seen today. There are automated traders such as Cryptotrader, payment processors such as BitPay, escrow services such as BTCrow, and bitcoin exchanges such as Bitstamp. There is unlimited potential for what kind of services or protocols that could be built on top of Bitcoin, so there will always be a SoS engineering role in reacting to the current trends.

All of the elements of the Bitcoin SoS will need to implement and stay up to date on the Bitcoin protocol, or integrate with an element that provides that function. Each higher level service will need to decide what level of involvement in the Bitcoin Foundation makes sense, based on the level of risk assessed for Bitcoin. The decentralized behavior of Bitcoin is designed to be resilient to attacks by incentivizing each individual Node into working together with the other Nodes. Since Bitcoin is developed as an open source project, it is important for each interested party to stay aware of changes in the Bitcoin protocol, so they make changes with the rest of the network. This may require a more proactive involvement than what similar electronic money exchange services might require.

4.1.3. Developing and Evolving a SoS Architecture

The Bitcoin Foundation considers changes to the Bitcoin Protocol through an open source environment. There should be a much more clear statement for how changes are developed, matured, tested, and implemented. The Bitcoin Improvement Proposal is the mechanism to suggest a change to the system, with the very first entry outlining the approach [22]. Currently, the strategy is to let market forces vote through their involvement in the open source project. This approach must be carefully watched, considering the failure and corruptions surrounding the Mt. Gox Bitcoin exchange failure [23]. The owner, Mark Karpeles, was also a founding member of the Bitcoin Foundation. His position could easily be seen as a conflict of interest for fixing any exploited technical aspects of the implementation. This organizational and human complexity is the kind of SoS-level concern that were not explicitly considered [14] at the origination of Bitcoin.

4.2. Architecture Considerations

4.2.1. Critical Elements

The proof of work function can be considered a critical element due to being on the critical path of meeting the system objectives. In this case, the cryptographic functionality that backs the proof of work is what provides the mechanism to protect against double-spending. The functionality is founded in the integrity of the proof of work system. Due to the decentralized nature of Bitcoin, it is possible that various nodes in the system will receive a subset of the transactions, and will create a new block that doesn't verify some set of transactions that have been created. Therefore, it is important that the engineers that are integrating their systems with Bitcoin are aware of the behavior of the proof of work function, and when they can interpret a transaction as verified. The software engineers would also need to be aware of the detailed nuances of the proof of work system in regard to their particular use.

4.2.2. Redundancy

Proof of work functions are constantly being performed by all nodes part of the Bitcoin network. This critical functionality is what replaces the need to have a central entity that assumes the risk of transaction fraud. Each node being in a race with all others in creating a new block, incentivized by the possibility of being personally rewarded with a generation transaction. The incentive is what ensures that there is a high amount of redundancy available to process transactions. This orientation of nodes, combined with the randomized methodology that is used to connect to a subset of the other nodes on the network, creates a highly resilient and diversely connected mesh [24].

When expanding beyond just the core Bitcoin, systems are available that exchange currency with bitcoin, provide merchant services, bank-like functions for securing bitcoin wallets, or gambling. Issues have been encountered with particularly important functions, such as currency exchanges [23], which suggests there is a critical need to have redundancy in the systems that directly affect trust and confidence by the users. The confidence in the currency can be affected more than just by Bitcoin's technical foundations, but also by its liquidity [25]. As long as there is healthy competition and confidence, the system of systems will be robust to any single failure, change, or upgrade.

Another potential consideration for robustness is the capability to exchange out varying alterations (altcoins) to the Bitcoin protocol, shown in Figure 7. A merchant services company that offers the tools required to hook into the Bitcoin Network would require very little extra effort to add these altcoins. If Bitcoin and alternatives were simply viewed as a transaction medium, instead of a store of value, the actual value of each type of bitcoin compared to the other would be of less interest. This perspective would provide a platform for "transport-layer" currencies to compete against each other in reliability, stability, and cost of transaction, for added robustness at the SoS level.

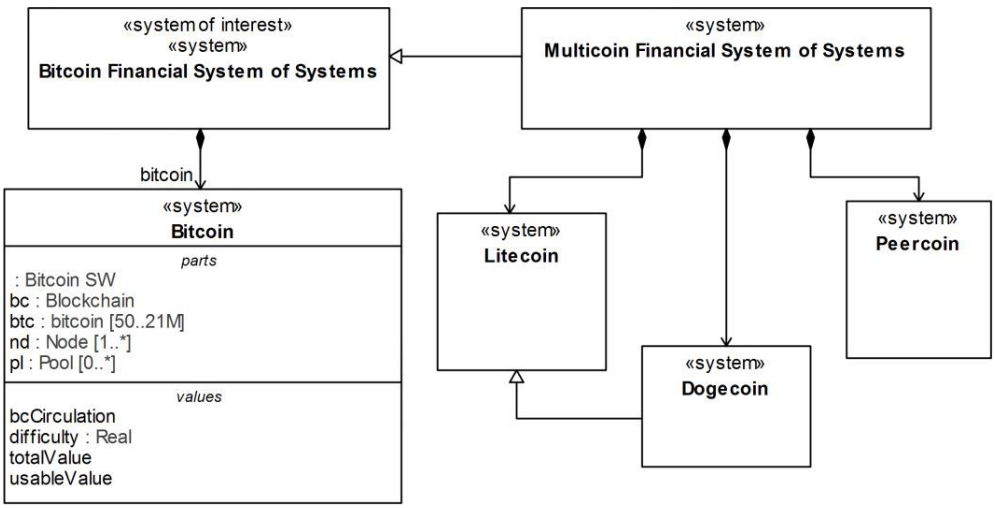

Figure 7. - Bitcoin-like Alternatives (altcoins)

5. Conclusion

Analysis was performed with SysML because it offers an established methodology for modeling any domain. The use of it is far from required to come to the same conclusions, but it provides a consistent framework to map most any domain into, offering an opportunity for systems thinkers to practice a generalized skill across many potential domains.

The requirements and use case analysis contributed towards identifying the different classes of users and how they might have differing interests into what makes a cryptocurrency personally valuable, while the structural analysis helped in building the body of knowledge for what technical and organizational components are in the domain, along with their attributes and relationships.

The analysis provides insights for identifying potential focus areas, plus a misalignment between the guiding SoS-level organization, the Bitcoin Foundation, and their support for an even playing field of competition between cryptocurrencies, in the same way that Bitcoin wants to compete against traditional options. There is potential to capitalize on differing approaches in deflationary or inflationary coin supplies [26] to provide robustness to the overarching goals outlined in the original architecture specification. These decisions are likely to not be in line with what is the best for Bitcoin or the speculative investors, but the entire system of systems could be better off for it.

References

[1] “Electronic Money.” [Online]. Available: http://en.wikipedia.org/wiki/Electronic_money#Electronic_money_systems. [Accessed: 02-Feb-2014].
[2] “Vocabulary - Bitcoin.” [Online]. Available: https://bitcoin.org/en/vocabulary#btc. [Accessed: 02-Feb-2014].
[3] “PayPal.” [Online]. Available: http://en.wikipedia.org/wiki/PayPal. [Accessed: 02-Feb-2014].
[4] “Cryptocurrency.” [Online]. Available: http://en.wikipedia.org/wiki/Cryptocurrency. [Accessed: 02-Feb-2014].
[5] “Public Trust in Government: 1958-2013 | Pew Research Center for the People and the Press.” [Online]. Available: http://www.people-press.org/2013/10/18/trust-in-government-interactive/. [Accessed: 02-Feb-2014].
[6] “Financial crisis of 2007–08.” [Online]. Available: http://en.wikipedia.org/wiki/Financial_crisis_of_2007–08. [Accessed: 02-Feb-2014].
[7] “Cypherpunk.” [Online]. Available: http://en.wikipedia.org/wiki/Cypherpunk. [Accessed: 02-Feb-2014].
[8] “Schneier on Security: The Strange Story of Dual_EC_DRBG.” [Online]. Available: https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html. [Accessed: 02-Feb-2014].
[9] “Exclusive: Secret contract tied NSA and security industry pioneer | Reuters.” [Online]. Available: http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220. [Accessed: 02-Feb-2014].
[10] “A Cypherpunk’s Manifesto.” [Online]. Available: http://www.activism.net/cypherpunk/manifesto.html. [Accessed: 02-Feb-2014].
[11] “Reuseable Proof of Work System.” [Online]. Available: http://en.wikipedia.org/wiki/Proof-of-work_system. [Accessed: 02-Feb-2014].
[12] W. Dei, “B-Money,” 1998. [Online]. Available: http://www.weidai.com/bmoney.txt. [Accessed: 02-Feb-2014].
[13] “Bit gold.” [Online]. Available: http://unenumerated.blogspot.com/2005/12/bit-gold.html. [Accessed: 02-Feb-2014].
[14] S. Nakamoto, “Bitcoin : A Peer-to-Peer Electronic Cash System,” pp. 1–9, 2009.
[15] F. Reid and M. Harrigan, “An Analysis of Anonymity in the Bitcoin System,” Jul. 2011.
[16] “Blocks.” [Online]. Available: https://en.bitcoin.it/wiki/Blocks. [Accessed: 02-Jul-2014].
[17] “Bitcoin Is an Expensive Way to Pay for Stuff.” [Online]. Available: http://www.bloomberg.com/news/2014-01-02/bitcoin-is-an-expensive-way-to-pay-for-stuff.html. [Accessed: 07-Feb-2014].
[18] M. Rosenfeld, “Analysis of Bitcoin Pooled Mining Reward Systems,” Dec. 2011.
[19] “Blockchained Mining Profitability.” [Online]. Available: http://blockchained.com/profit/. [Accessed: 02-Jun-2014].
[20] P. Surda and P. R. Haiss, “Economics of Bitcoin : is Bitcoin an alternative to at currencies and gold ? by Peter urda Advisor : Univ . Doz . Mag . Dr . Peter R . Haiss.”
[21] R. V. co. Salam, *Everything You Need to Know About Bitcoin: VICE Podcast 027 - YouTube*. VICE.
[22] P. Todd, “Bitcoin Improvement Proposal 0001.” [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki. [Accessed: 02-Sep-2014].
[23] R. MCMILLAN, “The Inside Story of Mt. Gox, Bitcoin’s $460 Million Disaster,” 2014. [Online]. Available: http://www.wired.com/2014/03/bitcoin-exchange/.
[24] C. Decker and R. Wattenhofer, “Information propagation in the Bitcoin network,” *IEEE P2P 2013 Proc.*, pp. 1–10, Sep. 2013.
[25] “Bitcoin Exchange Mt. Gox Says Users Can Withdraw Cash.” [Online]. Available: http://www.bloomberg.com/news/2014-02-10/bitcoin-exchange-mt-gox-says-users-can-withdraw-cash-as-normal.html. [Accessed: 11-Feb-2014].
[26] C. arstechnica Farivar, “Dogecoin to Allow Annual Inflation of 5 Billion Coins Each Year, Forever.” [Online]. Available: http://arstechnica.com/business/2014/02/dogecoin-to-allow-annual-inflation-of-5-billion-coins-each-year-forever/.