Virtual Ziggurats and Digital Bazaars

The Contractual Regimes of Bitcoin

This text sets out to show a chain between the many aspects of Bitcoin as a regime of exchange to a regime of contraction-based transaction. These aspects are Bitcoin’s status as money, its different and shared functional properties with other types of money, its distributed nature and its structural integrity, as well as its, close to societal in nature, contract that governs its slow development. Added onto this chain is the advent of Bitcoin-based marketplaces where the goal is to include the transactions themselves in Bitcoin’s block chain – the foundation of this digital regime of exchange.

Long historical lines are drawn between Bitcoin and the cultures of Mesopotamia in 3000 BC. The attributes of the monetary system used there is the antithesis of Bitcoin when it comes to the dichotomy of centralization/decentralization, but evinces strong similarities concerning the relative unimportance of material tokens. A further shared trait is traced, one that is likely to prove revolutionary in the future: the intimate connection between the monetary system itself and the transactions performed using it.

*This is an early draft, with potential problematizations still being considered*

1. High-priest Nakamoto

The key realization was that there’s no difference between modern culture and Sumerian. We have a huge workforce that is illiterate or alliterate and relies on TV – which is a form of oral tradition. And we have a small, extremely literate power elite […] who control society because they have this semimystical ability to speak magic computer languages.

N Stephenson, Snow Crash

In “Bitcoin: a Peer-to-peer Electronic Cash System”, written under the pseudonym Satoshi Nakamoto in 2008, a system was laid out that would allow for online payments to be sent directly from one party to another without going through a financial institution. In January the following year Nakamoto released a computer

1 Nakamoto p1. The real identity behind the moniker Satoshi Nakamoto has always been an intriguing conundrum. Based on the fact that the original article consistently uses “we” one would conclude that it was a collective of individuals, though the wording could have been chosen to evoke an air of respectability, or simply to obfuscate the identity further.

Recently Australian entrepreneur Craig Wright tried to mathematically prove that he was Satoshi Nakamoto. Though accepted by some, the mathematical evidence was also heavily criticized by crypto specialists. It seems this conundrum will not be laid to rest as Wright seems to have ended his attempt. On his website, drcraigwright.net, he posted the following on may 5th 2016:

I’m Sorry, I believed that I could do this. I believed that I could put the years of anonymity and hiding behind me. But, as the events of this week unfolded and I prepared to publish the proof of access to the earliest keys, I broke. I do not have the courage. I cannot. When the rumors began, my qualifications and character were
implementation under open source license, with the first transaction of Bitcoin taking place a few days after release.\(^2\) Since then Bitcoin has grown exponentially and is seen as both a boon and a threat.\(^3\)

The rules in bitcoin were designed by engineers with the express purpose of getting rid of the need of trusted third parties. Its code reflects an ethos of decentralization and a distrust in single authorities. Rather than storing transactions on a single cluster of computers, Bitcoin is a network wherein the transaction log is distributed across all participants.

2. The Money Status of Bitcoin

There is an ongoing and quite philosophical debate about what Bitcoin is, or rather what it should be regarded as. That it has perceived value is obvious since it is used in transactions, but whether it can be understood as some form of good or commodity that can be treated as property has been the subject of some debate. This debate will not be continued here. Rather, the focus will be on the subject of Bitcoin’s qualities when used as money.\(^4\)

2.1. Is Bitcoin money\(^5\)

Defining what is money and distinguishing it from what is not money is a delicate problem. This delicacy arises from the fact that there are many different functional qualities that we expect from money, but for something to be recognized as money, it doesn’t need all of these functional qualities, nor does each such quality need to be fulfilled to one hundred percent. If you list all the functions we associate with money, there are probably none of all the things we recognize as money that can be said to be “perfect money”. If one matches Bitcoin against the functional factors below, one finds

\(^2\) Currently the code-base for Bitcoin is managed and developed through the Github code depository by computer developers mostly in a volunteer capacity. Decisions are taken through a consensus-driven process.

\(^3\) More than a 100,000 stores accept Bitcoin as payment while regulators in many countries have taken a variety of steps such as imposing licensing requirements on some firms involved in the bitcoin market, issuing warnings to consumers, banning financial institutions from using it or outright banning the use of bitcoin completely. IMF pp24-35.

\(^4\) Bergstra and Weijland distinguishes between possessing “moneyness” and being “money-like” with the measuring the level with a system is suitable to being used as money while the latter’s functionality only partially resembles money, pp8. In their report from 2012 on cryptocurrencies, the European Central Bank called Bitcoin, similar to conventional money but not money. The report noted among other things that Bitcoin lacked a clear connection to existing currencies as well as a central authority in charge of the amount of money available, pp21.
that Bitcoin is not perfect money, but in many functional aspects it is better money than other things whose status as money is taken for granted. To this picture must be added that money cannot strictly be defined through its functional qualities, but also through its history; something that has been accepted as money is likely to be continued to be accepted as money because of social inertia. This logic is not without its limit however. There are a non-trivial number of functions associated with money, and it is not necessary for something to possess all of these functions perfectly in order to be seen as money, but something with none of these properties is not ever going to be a viable candidate for being considered as money. Following this logic, no thing that once was used as money but at a later stage loses all of these functional properties will be able to retain its status as money merely on the back of social inertia.

In the very current and heatedly ongoing debate about whether Bitcoin is money or not, a hefty portion of the arguments seem based in social acceptance, particularly acceptance by the large traditional actors such as central banks and state treasuries. To use an example, this debate is quite akin to the one found regarding the role being played by the recognition of other States concerning the issue of Statehood status in International Law: While the discussion about what role the recognition by established actors itself plays in a constitutive sense is a philosophically fascinating one, this text will not consider recognition by other entities as hard criteria, or constitutive, of Bitcoin’s status as money.

3. Money without money in Mesopotamia

It is interesting that the nascent issue of whether Bitcoin is money or not is mirrored in the question of whether money was used in the ancient cultures of Mesopotamia - the oldest organized States known in the history of Mankind. Both these questions seem perfectly natural because they both highlight the surprisingly complex problem of defining money and distinguishing it from that which is not money. Like the States in

---

5 According to Luhmann, over time a successful system of money becomes closed to its environment in the sense that it produces its own elements and its own internal structural changes, making it a self-referential and self-perpetuating system. Luhmann p350.

6 In the International Monetary Fund’s staff discussion note of 2016 a negative approach is taken to all virtual currencies’ status as money in stating: “While money can be created by private parties (for example, banks) as well as central banks, it must generally be denominated in a currency issued by a sovereign authority, and must be intended to serve as a generally accepted medium of exchange within that state.” While still holding the door open by stating: “monetary systems and the legal concept of money have evolved substantially over time and will continue to change in the future. VCs should thus not be judged solely based on their current characteristics or on how they compare to current monetary regimes.” IMF 2016 pp11-16.

7 Constitutive Theory maintained that recognition by other states was itself a criterion of Statehood while the Declaratory school considered it to simply be the recognition of the fact of Statehood constituted by other more objective factors (traditionally territory, population, government, sovereignty). Since 1991 this doctrinal debate is largely considered to be over, and Declaratory Theory is now officially considered to the correct school of thought, but recognition does in practice play a crucial role when it comes to the viability of a budding state. See further Lowe pp 160-166.
ancient Mesopotamia, the digital network of Bitcoin lacks an easily perceptible tangible coinage.

What has given rise to the debate about whether money existed in Mesopotamia is the fact that for many centuries they lacked coinage: archaeology finds use of coinage at the end of their Achaemenid period (aka the First Persian Empire), around 300 BC. However, Mesopotamia had been a hub of trade at least since the third Millenium BC and was well connected by routes to the Mediterranean, the Indian sub-continent, further Asia and quite likely with East Africa as well.\(^8\) Did they lack money during this long time, did they use primitive forms of barter economy? Most certainly the answer is in the negative. The archaeological evidence challenges the importance of coinage and lets us glimpse an economy where fairly advanced aspects of economy were used without a formal system of coinage.\(^9\) Initially the system of documentation was likely invented at and managed in the, for Sumerian culture so central, Temple structures. The Temples, and the Ziggurat-dominated Palaces of Sumerian rulers that modeled themselves on the Temple organization were gigantic, complex industrial institutions with staffs of thousands where shepherds, weavers and spinners rubbed elbows with dancers and clerical administrators.\(^10\)

Innovative financial instruments as *interest-bearing loans* likely arose from a need to finance the caravan trade, managed through the hub of the Temples. The central government kept balanced accounts divided into three basic sections: assets, expenditures and balance.\(^11\) The administration of debt and assets was a highly centralized affair, because of the lack of a system of coinage, which would have provided a decentralized mechanic for keeping track of wealth outside of the Palace and Temple administrations.\(^12\) In many ways, the concept of money in ancient Mesopotamia should seem distinctly familiar to the modern eyes of someone long accustomed to manage their assets without actually dealing with, or in any way handling, either bills or coins.

### 4. The Functions of Money

As stated above, not everything is a good candidate for money; its fundamental function function is to constitute a medium of exchange by keeping track of debt and value. In order to perform this function well, several properties can be identified that each facilitate the over-arching purpose. Obviously, money can fulfil other agendas than to act as a

---

\(^8\) Powell 1996, p225  
\(^9\) Ibid, p238  
\(^10\) Graeber, p64  
\(^11\) Powell 1977, p25  
\(^12\) Money signifies not only value lodged with an individual or other entity, but also the opposite of value: *debt*. Anthropology confirms that debt as a social organization technology precedes the invention of the material tokens to measure it. Bratton, pp335-336.
medium of exchange and thus not all of these properties will be viewed as desirable if a different agenda’s perspective is adopted.

A) The first property that comes to most people’s mind is that the amount of money must be **limited or at least scarce** and it should not be an easy task to add to it by producing more money or falsifying its tokens. This is an ancient problem known from stories about landlocked cultures using seashells as money: as soon as an easy route to the sea is discovered, the system is understandably weakened. Connected to this, money needs to be as an easily **identifiable** from other things. To aid in transactions, this identification should preferably be possible for a normal consumer to perform without access to specialized tools or facilities. To further grease the wheels of trade, money should be divisible. easily and preferably without limitation. Though digital management of transactions has removed the coarse division inherent in minted currency, but still has to relate to such concepts as ‘cents’ and thus run into round-off problems. Obviously non-legacy digital money systems do not suffer from these. Traditionally, in order to achieve **divisibility** one had to have access to tokens of many different denominations, something that could conflict with the ideal of money being **easy to carry around**. From a user perspective, money should require no additional space at all and be possible to transport anywhere. It is desirable that all such transportation can be done **securely**; that even during transportation the risk of losing your money is minimal. A related function of money that is equally desirable is the function of not losing money to banks through transaction fees, merely because you have undertaken said transportation. US Dollars and gold metal possess this property and are today therefore used as money internationally.

Though it might seem counter-intuitive, money should preferably have no value and functions outside of being a medium of exchange – it should **lack intrinsic value**, i.e. be impossible to consume or use for either sustaining life or enhancing the experience of it. If not, then its value will be partly dependent on how these external functions are valued on the market, not on its qualities to provide a function of exchange on that market.\(^13\)

B) **Non-volatility** is a highly desired property of any medium of exchange since risk minimization is desired. A close connection to political sensitivities does of course provide an increased risk of tampering with the value of a currency, a story born out by our knowledge of both ancient Mesopotamia to the modern independent central banks. But volatility is also influenced by various maturity factors, such as the size of its user base and length of time in use.\(^14\) A closely-related property is **resilience**, the ability to

\(^13\) The quality of having no intrinsic value is dependent primarily on whether the money in question already possesses stable value that is preserved over time. If these qualities are not present, having some intrinsic value becomes a positive quality since it provides for less volatility. When Swedish central bank, the Riksbank, back in 1740 was freed from the silver- and copper-foot, they lacked the insight or political will to adopt policies to maintain monetary stability, with drastically negative effect for the Swedish economy, resulting in an exodus of 3000 workers per year – a considerable loss for a country whose total population had yet to reach two million. Arnberg p245-247.

\(^14\) An anecdotal observation: Bitcoin has long been seen as an “anti-currency”; when trust in large governments such as the USA or China has waned, then Bitcoin has surged. At the time of writing, Bitcoin has had a long and fairly stable climb to around 440 $ when it suddenly exploded last night (may 30) due to Chinese investors wanting to move capital outside of China. Speculations are high as to what prompted this sudden increase.
withstand, preserve or even increase value over cycles of economic change – what is often named monetary stability. Tied to this we find the issue of having a large base of users, a property desired in its own right but one that also has a positive effect on resilience. If the money is easily exchanged for rival currencies, what is termed liquidity, then the user base is grown by proxy.

That payment should be prompt is another desired property of good money, but one that matters more or less depending on the context at hand. A consumer’s need for speed is high when buying a liter of milk, but less so when transferring money into a savings-account or buying a plane-ticket.\(^{15}\)

The functional properties listed under A) are such where Bitcoin excels by definition. Its weaker properties are found under B), though the currency is too new for anyone to know whether the system will prove resilient or not. The issue of speed in transactions is one where Bitcoin is currently locked to a ten-minute delay due to the need to build on the block chain in a peer-to-peer network.

One additional property that Bitcoin possesses that has not traditionally been viewed as a property of money, but that was present in the money-system of Mesopotamia, is programmability: a transaction in bitcoin can be coded into the currency itself. More on this later.

4.1. A Note About “Trust”
It is often said that money is a matter of trust, and Bitcoin has across various media been called a ‘trust machine’\(^{16}\). Trust is a complicated matter however and is a higher function of the properties listed above. For example: Mesopotamian money merited a certain amount of trust given its logically and physically centralized nature, where debts, value and transaction was centrally managed and thus could be verified. However, this centralized nature made it weak when it came to resisting devaluation because of overriding political interest, as in the case of the cancellation of consumer debts in Mesopotamia. On the other hand, a decentralized system based around a scarce metal such as gold could not be devalued in such a way, but trust in such decentralized systems where verification of the coinage could not was always vulnerable to different kinds of tampering with the coinage, such as debasing the metallic content. The Bitcoin system, being both logically centralized and physically decentralized seem to enjoy the best of both worlds with respect to these properties.

5. Old Money and New Money
The extraordinary feat managed by Bitcoin is to do without the physical Temple and manage a working physically-decentralized type of money through a peer-to-peer

\(^{15}\) Possibly discuss anonymity and fungibility as well.\

\(^{16}\) In 2015, The Economist used this term in its October 31st – November 6th issue.
Network. Some would say that the Temple is still there, only digitally distributed now, and that may in some sense be true. The Bitcoin system is unified, logically centralized and its underlying framework is maintained and developed by a sort of programmers’ priesthood.

But this should not lead to the Mesopotamian comparison where the priesthood, or ruler, could interfere with the ledgers and thus change the balance of debts and assets, which was done at intervals in Mesopotamian societies in order to compensate for some of the shortcomings of their economy: Since debt in ancient Mesopotamia seems to have been intimately tied to the debtor and his family, financial trouble led to the appropriation of possessions and in the long run to a form of debt-slavery. This would be almost impossible to break out of, since repaying your debts when you are bound to serve in a temple or in the household of some merchant must be an almost insurmountable obstacle. This state of things created strains on their society as Mesopotamian indebted would flee their lands and opt for an existence as brigands. The solution was from time to time to wipe the slates of the Temple clean, declaring all outstanding consumer debt to be void. The knowledge that such a jubilee would be declared from time to time affected the volatility and resilience of the monetary system in the negative and would doubtlessly have weakened its position if there had been alternatives available. This was obviously not the case in ancient Mesopotamia.

Such centralized and monopolized control over the system of money as exemplified here provides great economic and political power, and will inherently always expose such a central power to various pressures to use that control to rectify perceived economic or political imbalances - from the ancient temples of Mesopotamia to its modern counterparts in Frankfurt and Beijing, this remains a constant.

5.1. Centralization, Good Money and Bad Money

A formulation of Gresham’s Law: When a government overvalues one type of money and undervalues another, the undervalued money will leave the country or disappear from circulation into hoards, while the overvalued money will flood into circulation.

In 1976x Friedrich Hayek noted that to keep money non-volatile and resilient, it must be protected from politics, or at least it must be protected from the short-sighted and counter-productive instincts of elected officials. He noted the pressures a central power had always been subject to during the long history of money. Certainly, he did not want

17 Något om den limited liability corporation som social innovation här.

18 Graeber p65

19 This was very recently illustrated in the political negotiations between the Hellenic Republic and select member states of the Eurozone last year as the European Central Bank helped put political pressure on the Greek government by restricting the money supply to Greek Banks. Upon joining the Eurozone, the Greek treasure department had been required to permanently disassemble their Drachma printing presses, ensuring the integrity of ECB’s control of money, should Greece entertain the notion to opt out and return to their old currency.
to question that an independent central bank authority run by very intelligent people could not potentially do better than a gold standard or some form of automatic system, but in the real world he saw not the slightest hope that any institution subject to political pressure could ever act in such a manner.

Hayek’s suggestion was to allow for competition between different types of money. The problem lay not in the fact that states were issuing money; it lay in their power to limit the kinds of money in which contracts could be concluded or to set the rates at which monies could be exchanged. With open competition between different kinds of money, money-use would migrate to the money that possessed the best functional qualities; governments would be unable to conceal if their money was becoming bad would have to adopt sound long-term policies.

Many readers are presumably familiar with Gresham’s famous law that bad money drives out good money. This is true in the cases where we have two types of money with the same nominal value but where one one type of money lacks the level of intrinsic- or commodity value possessed by the second. The bad money will be preferred to be used in transactions, if possible, because it would be “a good deal” to get the same exchange for something that is less good. Hayek pointed out that this maxim only holds true only if the two types of money have to be accepted at a prescribed rate of exchange. If, on the other hand, people are free to exchange the different kinds of money at whatever rate they agree upon, then exactly the opposite will happen: good money will drive out the bad.

One only has to remember the way American Dollars were used when travelling beyond the Iron Curtain to realize the truth of this. Money that is considered to be good as per the qualities listed above will compete effectively if they are allowed to co-exist with other money that is perceived as inferior. The spirit of Hayek’s solution, to allow free monetary competition where good money would prevail, is very much alive in the circles around Bitcoin: not only do many Bitcoin evangelists believe that Bitcoin will

20 He was obviously not thinking of a an actual digital cryptocurrency, but the wording is nonetheless quite prescient.

21 Ibid p14.

22 Ibid pp17-18. By free competition Hayek does not mean that a state must allow other money than its own as legal tender when it comes to taxes; they are perfectly free to set these conditions as they see fit. True to form, his prescribed free competition is framed as the freedom from state interference.

23 One of the oldest insights into the mechanisms of money; named after a 16th century banker, the principle is mentioned back in ancient Greece by Aristophanes and later my Copernicus. It is occasionally referred to as Copernicus’ law.

24 Hayek p20.

25 Indeed it can be said that the theoretical roots of Bitcoin can be found in the works of Hayek, von Mises, Böhm-Bawerk, as well as other more modern authors who sympathize with the analyses of the Austrian school of economics. (Anecdotally: my own personal acquaintances who are computer programmers by profession tend to be quite “Austrian” in their views without ever having read one word of political writing. One can only speculate if this is related to them having acquired their highly sought-after skills mainly through their own effort and interests, with little formal schooling.)
prove superior to other national forms of money if allowed to compete on its own merit, they also hold that free competition between cryptocurrencies will result in a digital evolution that will give birth to better, or at least more well-adapted, money. In their words, the best bitcoins of the future may therefore not be Bitcoin.26

6. The Decentralized Nature of Bitcoin

So you think that money is the root of all evil? . . . Have you ever asked what is the root of money? Money is a tool of exchange, which can’t exist unless there are goods produced and men able to produce them.

– A Rand, Hunger and Freedom

As stated above, Bitcoin achieves something quite quite extraordinary in eschewing central control over money by lodging it in the physically-distributed structure of those who use the money. As opposed to the ledgers being kept by the Mesopotamian clerics and the central banks of today, the ledger that regulates Bitcoin must have two properties: it must be impossible to tamper with it, and in order to achieve this goal, it must be open to inspection by everyone and anyone.

This does of course raise the interesting question of whether governments will and are able to prevent Bitcoin transaction. Hendrickson et al find that in order to effectively do this, the government must control a sufficiently large part of the economy, and even in these extreme cases some transactions will effectively be beyond the reach of the state.27

6.1. Tech over Trust

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don’t care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.28

Satoshi Yakamoto’s solution to integrity and transactional tampering was in many ways ingenious: any “tampering” with the ledger establishes the official ledger. Thus there can by definition be no tampering, since any work done that is sufficient to establish the accepted ledger is the work that drives the system.

26 The risk of “forking”, so often dreaded in Open-Source projects, where one group of programmers split from the development team and continue developing the computer code in their own direction while still competing with the original project, is not seen as a weakness in Bitcoin, but rather as a potential advantage. Value would simply migrate to superior frameworks, it is felt.

27 Hendrickson et al p20.

28 Nakamoto section 2.
Transactions in the Block-chain

The ledger in Bitcoin is called the block-chain. Technically it is a distributed database consisting of a constantly growing list of transaction records arranged in “blocks”. Each such block contains a timestamp and is a function of the previous block. Actually, every block in the block-chain is a series of numbers that through a cryptographic function incorporates all the previous blocks combined with the latest one – all the way to the first block, the so-called Genesis Block.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block’s hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.29

Each new block of transactions gets tacked onto the existing chain in a process that provides the driving engine behind attracting computer power to the network and then uses this power to maintain its own integrity.30

An Example

Alice and Bob, of course, are exchanging an amount of Bitcoin. When they agree to do so through the Bitcoin p2p network, their transaction information is broadcast to the entire network. Through her public key encryption, Bob can verify the identity of Alice and that she has the Bitcoin, though he cannot verify that she does not try to spend the coin somewhere else simultaneously. But now everyone in the Network also knows, theoretically at least, that Alice and Bob are going to participate in this exchange. All the information that identifies Bob’s and Alice’s unique digital wallets, the number of bitcoin’s transacted, any contractual conditions set on the transaction as well as the optional transaction fee - it all becomes publically available information. The network now automatically rejects transactions that include the same Bitcoins and thus prevents them from going toward two separate ends, thus nullifying the risk of Alice double-spending, and double-crossing, Bob.

The same goes for the other transactions that happen in the network at this time. The collated product of all these transactions provide the basis for the next proposed block in the Bitcoin block-chain. Alice and Bob’s transaction is not finished until the next block has been accepted by the Network. That is, until a node in the network has solved the cryptographic puzzle generated from all the proposed transactions. Solving this puzzle takes a lot of computational horse-power. But once a node in the network has found the right solution, it is easily and quickly verifiable (see below for details). The node will broadcast its solution to the rest of the network and the other nodes can verify that the

29 Nakamoto section 4

30 This text does not address the issue of low integrity at the exchange level, such as when a third party that undertakes to exchange your assets to Bitcoin acts in a fraudulent way. Reference Mt Gox and the debate ensuing.
solutions is indeed correct; they will then cease trying to find their own solution to the puzzle and will start working on the basis of this new block in the chain – the block that incorporates Alice’s and Bob’s transactional record.

\[
\text{New proposed block} = f(AB \text{ transaction, } XY \text{ transaction } \ldots)
\]

At this point, the transaction is complete and non-reversible, all conducted directly between Alice and Bob.

6.2. Proof-of-Work Puzzles, Miners and the Incentive for Verification

To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.\(^{31}\)

As per above, each new proposed addition to the block-chain of Bitcoin is a result of the cryptographic combination of the new transactions in the network. This string of numbers provide the challenge in a mathematical puzzle - in Bitcoin this is a mathematical hash-function.\(^{32}\) The most important property of such a function is that it is hard to solve, but at the same time it is very easy to verify that the solution is correct once it is proposed.\(^{33}\) Anyone with computational power can become part of the Bitcoin network and try to find a “response string” of numbers that when combined with the challenge will solve the puzzle. These days only serious actors with huge farms of dedicated computers have a realistic chance of solving this puzzle before any of their competitors do.\(^{34}\)

\(^{31}\) Nakamoto section 4.

\(^{32}\) Unlike the other two traditional cryptographic algorithms, Secret Key and Public Key, the Hash function provides one-way encryption. In a good hash function, the only way to arrive at the data string that will recreate a cryptographic hash function’s output is to try a large number of possible data strings to see if they produce a match. The level of difficulty can be ratcheted up by increasing the number of bits required in the output. For example, finding the correct string in a 128-bit function can be compared to throwing a coin and having it land heads-up 128 times in a row. In effect, the computer has to \(2^{128}\) tries before finding the correct string. \(2^{128}\) is more than the expected number of stars in the known universe, including all known galaxies. See Northcutt.

\(^{33}\) Proof of work puzzles has been around long before Bitcoin. They can for example be used to dissuade email-spamming activity by requiring each sender to solve such a puzzle before being allowed to send an email. Solving a puzzle once is not a noticeable effort if you are only sending to a few recipients, but becomes insurmountable when you are an email spammer. Conversely, since the effort of verifying the puzzles require a fraction of the effort, the effort required by the service that asks for the puzzle-solution is almost negligible.

\(^{34}\) At the time of writing, May 29 2016, Swedish Bitcoin miner KNC has filed for bankruptcy, citing the high energy taxes of Sweden as the chief factor behind their inability to compete with their Asian counterparts.
The incentive for those who dedicate computer power to this effort is twofold: they can set one transaction of a mathematically-determined amount of Bitcoin to themselves, and they are also allowed to claim any of the rewards that the primaries have included in their transaction.\(^{35}\)

Trying to trick or in any way hack a system such as the one at hand cannot be done by attacking any one point in the system, since that is a weakness missing in a non-centralized system. Instead an attack has to be made against all the network and all the instances of the Block-chain in it, in essence you would have to out-compute all the other miners and the work previously made.

### 6.3. Summary

In short the block-chain is shared, trusted and public; qualities that by definition puts it outside of any single user’s control. The participants in the system collectively keep the ledger up to date: it can be amended only according to strict rules and by general agreement. The block-chain of Bitcoin prevents double-spending and continuously keeps track of transactions.

### 7. Old and New Priesthoods

This pride in having established a monetary system that does not have a Temple or a Palace, and thus the inherent integrity to resist political demands, is what makes it highly sensitive to discuss changes to the underlying architecture.

Changes to the codebase of Bitcoin are decided by consensus, in an informal circle of merit. Such a system is common in computer-developer projects, particularly Open Source, but brings with it its own difficulties and limitations concerning scalability.\(^{36}\)

### 8. A Return to the Merchant Temple

Though Bitcoin itself has many interesting properties, it is when used with an equally decentralized system of contract that its revolutionary potential shines through properly. Like in the Mesopotamian temples, there is a connection open between the monetary system itself and the contract of the transaction, a connection inherent in Bitcoin’s logical potential, but managed at a physically-decentralized level. Though any such decentralized trade-system involving programmable cryptocurrencies could draw on this

---

\(^{35}\) The ability to reward yourself with a new Bitcoin is sometimes referred to as mining. Mathematically, the system will "mine out" in 2050, when there are around 21 million Bitcoin in circulation. At that point, incentives will be provided by the rewards included. The optional rewards are sometimes called “miner’s fees” give the miners the incentive to prioritize your transaction when constructing a new block.

\(^{36}\) Avsluta detta v 25. Se Bernsteins artikel om diamanthandeln.
potential, this text will use the newly-launched OpenBazaar network to provide concreteness.

Touted as the next “killer app”, OpenBazaar is an open source project to create a decentralized network for peer to peer commerce online, using Bitcoin, without fees and restrictions on the types of goods.37

OpenBazaar is a different approach to online commerce. Its intention is to put the power back in the users’ hands. Instead of buyers and sellers going through a centralized service, OpenBazaar connects them directly.38

Let’s say that Alice is looking to sell her old computer. Using the OpenBazaar client application she creates a new product-listing of her computer with a type of detail exactly like what can be found on any e-commerce site, such as e-bay. When Alice publishes that listing, it is sent out to the distributed peer-to-peer network of other people using OpenBazaar and becomes searchable to all other thereon.

Let’s assume Bob is also on the network and finds Alice’s listing. If they both agree on a price, the client creates a contract between them both, and sends it to a third party called a moderator. The moderators are other human nodes on the OpenBazaar network who Alice and Bob trust in case something goes wrong. The third party witnesses the contract and creates a so-called multi-signature Bitcoin account that requires two of three people to agree before the Bitcoin can be released.

Bob then sends the agreed amount to the multi-signature address. Alice subsequently receives a notification informing her that Bob has sent the funds, and she ships the computer to him and notes that it has been shipped on the network. When Bob finally receives it he marks it as received on the network, which releases the funds from the multi-signature account to Alice.

Further interesting properties envisioned for this network are that with Bitcoin and its programmable property the inclusion of contracts readable to both humans and machine becomes possible. With these so-called “Ricardian contract”39, disputes in more advanced contractual arrangements can be resolved directly between two parties, or in cooperation with a mutually selected third party that needs only verify certain facts rather than render a more traditional judgment. Thus OpenBazaar aims to frog-leap the deeply embedded

37 Currently, online commerce means using centralized services. eBay, Amazon, and other big companies have extensive policies and charge fees for listing and selling goods. They only accept forms of payment that cost both buyers and sellers money, such as credit cards or PayPal. They require personal information, which can lead to it being stolen or even sold to others. Buyers and sellers are not always free to exchange goods and services with each other, as companies restrict entire categories of trade.

38 The Open Bazaar project was initially spun off from the Dark Market project. Elaborera från FF:s intervjum med projektansvarig!

39 Not to be confused with the English economist David Ricardo. These contracts were initially a format developed by Ian Grigg and Gary Howland as part of the Ricardo payment system. The over-arching philosophical goal is to provide a unified document that will work for both man and machine.
and highly involved “paper institutions” rather than wait for them to adapt themselves to a digital globalized world.\(^{40}\)

8.1. The Silk Road Revisited

Given the overarching historical comparison in this text, it is quite fitting that OpenBazaar was supposedly conceived of as a response to the shutting down of Silk Road – the infamous Internet marketplace best known for its abundant and varied supply of illegal drugs.\(^{41}\) However, the roots are only code-deep and the current development team inherited the code from the original developers who had left it chase other projects.

The ancient Mesopotamian temples were places of commerce, where goods were sold and purchased, business ventures were proposed and planned – all under the watchful eyes of the clerics who kept records in their ledger of how value changed hands, and to what purpose. In its physically-decentralized network, the OpenBazaar market aims at repeating the same process – by tacking each transaction and its contractual terms onto the ledger that is the Bitcoin block-chain.

The New Oracles and Digital Sharia

In this replacement temple of OpenBazaar its developers even envision a function called an Oracle. An oracle can be another person, a group, or even an autonomous organization governed only by self-sustaining code. Oracles can act as reporters on the state of any object or event in the future. They can thus provide the necessary data input needed to settle disputed contracts between other users. These users would have little or no interaction with the Oracle directly. Oracles can also serve as the escrow agent or moderators, where the future state of the object or event, which they report on, is the basis of releasing funds from multi-signature accounts to the appropriate party. Releasing funds would be done in cooperation with the winning party, since a multi-signature contract require two out of three parties to agree.

In line with the spirit of free competition even in money itself, OpenBazaar sees an open market for Oracles as a way to introduce competitive forces and diversity to improve the quality and range of data sources. Oracles can advertise what categories of objects or events they will report on, and why they are uniquely qualified over their peers. The Oracle’s reputation within the system will reflect how accurately they report correctly and cite reputable sources.\(^{42}\)

\(^{40}\) Szabo characterizes this development as a move from static to dynamic media, where software “literacy” will have massive impact on law and legal institutions.

\(^{41}\) This obfuscated market was hailed as a libertarian zone of free trade by its evangelists. It was shut down in October 2013 when a United States’ citizen was arrested by the Federal Bureau of Investigation and subsequently sentenced to life imprisonment.

\(^{42}\) Maybe a parallel to Sharia Arbitration here.
Back to Babylon

Just like The Temples that provided the hub of Mesopotamian trade were complex industrial institutions with staffs of thousands; where craftsmen, caravan-organizers and clerical administrators mingled, Bitcoin can be seen as a complex ecosystem with many actors making up that which has the potential to be truly novel and valuable. The various forms of alternative crypto-currencies that try to keep the cryptographic base around a block-technology but in a centralized form merely provide a new technological vessel for an ancient tradition of centralized money. The unique selling point of Bitcoin lies in its attempt to create a competing form of money that eschews the weaknesses inherent in a physically centralized system where the trusted party can always be put under pressure to meddle with the properties of its money. As a juxtaposition to established forms of money, Bitcoin is a more natural fit to decentralized markets such as OpenBazaar, without being a requirement for them.
Literature

Arnberg, J W, 1868 *Frihetstidens Politiska Ekonomi*, W. Schultz Förlag

Bergstra J, Weijland P, 2014 “Bitcoin: a money-like Informational Commodity”, Informatics Institute, University of Amsterdam


Bratton, B H, 2015 *The Stack: on Software and Sovereignty*, Massachusetts Institute of Technology


Grigg, I, “The Ricardian Contract”


Heidbrink, J, 2016 “Regelering, avreglering, omreglering – Privata avtal på infrastrukturmarknader”, *Festskrift till Ronney Hagelberg* pp. 51-68, Jure Förlag


Luhmann, N, 1995 *Social Systems*, Stanford University Press


Reports

European Central Bank 2012 “Virtual Currency Schemes”

International Monetary Fund, 2012, “Staff Discussion Note: Virtual Currencies and Beyond: Initial Considerations”