Bitcoin: an open source currency and more

Carlo Piana [a]

(a) Founder, Array; attorney (Avvocato) in Milano

DOI: 10.5033/ifosslr.v9i1.120

Abstract
The emergence of a cryptocurrency in the digital domain went unnoticed for years until the general press started to cover Bitcoin's more than tenfold raise in price in the space of a few months in 2017. Earlier on, technical and legal discussion revolved around one of its fundamental building blocks, but Bitcoin is more than the blockchain or an investment object. It is a revolutionary open source artefact that is bound to change the way we consider currency, as well as a proof-of-concept for how parts of international trade could disfranchise banks and other institutions as payment service providers.

Keywords
Law; information technology; Free and Open Source Software; currency; cryptocurrency; blockchain; fintech

During the last part of 2017 Bitcoin has achieved relevance in mainstream media. The debate is focused on "is it worth buying?"; "is it a scam?"; "is it a currency or commodity?"; "is it safe?". These are all legitimate questions but they miss an important trait of Bitcoin: it is open source, peer-to-peer, standard-based distributed technology.

The degrees of freedom in the Bitcoin phenomenon certainly goes beyond the software but the software plays an important role. The fact that Bitcoin is not controlled by any party but instead requires the implicit consensus of users is of utmost importance. It is possible that Bitcoin will never be used as a large-scale distributed currency. However, one fundamental component has definitely already attracted the attention of many, and it is the **blockchain**. Apart from its use as a component of crypto-currencies the concept of distributed ledger based on blockchain has become a highly regarded object of large investment by the technology industry.

The blockchain is important and it has many interesting applications in areas like "fintech" but focusing solely on this overlooks other interesting aspects of the emergence of Bitcoin.

Bitcoin in two simple words: ledger and blockchain

I have read many descriptions of Bitcoin that avoided tackling the technology behind it. These descriptions left the odd feeling that most authors had not made a serious effort to understand the underlying foundation. At the same time, there are so many intricacies that any attempt to explain it can easily get lost in the details and become unhelpful to the non-technical reader. I attempted to

strike a balance in the most relevant economic blog in Italy and – thankfully – the reception of the article by both inexperienced and experts readers was quite enthusiastic.[1] This small achievement makes me sufficiently bold to venture into a similar explanation in this article.

Bitcoin does not exist in the physical world. It is a **unit of account** in a transactional accounting system, otherwise known as a "**ledger**". In a ledger, a party enters records of active (income) and passive (expenses) movements. How much "money" an account holds depends on everything that has been credited to it, less everything that has been spent from it. All movement (after the first one, bear with me for a while, I will explain) have a debited account and a credited account – actually one *or more* of them. When all the credit is spent, the account will show "zero" unless it receives credit and will not be permitted to spend more. The system only permits fully funded expenditures.

This is similar to running a bank account. Imagine the scenario where we have Alpha Bank logging an expenditure on Alice's account, and Beta Bank logging an expenditure in Bob's account. Alice will have a corresponding reduction in her balance, Bob will have a corresponding increase in his, minus any wiring charges applied by the originating or destination bank. This transaction requires two banks that mutually recognize their wiring instructions as money. Each bank gives credit to the other if the transaction is genuine. If Alice's account is not sufficiently funded, Alpha Bank will pay for the transaction regardless, so if bank authorising the transfer is actually opening credit to Alice. The banking system has regulatory requirements and laws that create this trust, lead by an overarching central bank and a system that ensures the balance of all transactions is credited to each bank and that all operations are reflected by the banks' balance sheets.

You trust the compliance and reliability of the regulatory framework between two banks. It requires that banks can only loan within certain limits and under certain conditions the state guarantees the deposits in case of bankruptcy of a bank. In other words, the system and the law create **trust**. Trust about the fact that an entry in an accounting system accrues value that can be later spent to buy goods or services, without any physical object of intrinsic value to vouch for that transaction.

Now, let us remove the banks from the picture and consider the foundation of Bitcoin. In a situation without banks, who guarantees that Alice has money, that she has not spent it, that the transaction credits value that can actually be spent, and that double spending is not allowed? In this simplified framework we have two possibly reciprocally unknown peers, we lack the traditional mechanisms of facilitating and assuring a transaction. How can we operate without a trusted third party? The solution lies in a complex system of peer-to-peer software and algorithms conceived to provide public trust because all transactions are public and apparent to everybody. In this scenario there is no trusted party as with traditional transactions. Instead trust is provided by having many public "eyes" making forgery computationally impossible.

The foundation of Bitcoin or similar systems without trusted or known peers is the **blockchain**. As suggested by the name, the blockchain is a chain of blocks which are continuously created and which contain the **ledger**. The latest block and all predecessors contain (nearly) all transactions that have ever occurred. The ledger is not a seamless log, it is a database made of chained blocks of text that are widely replicated and distributed. These blocks are created in a peer-to-peer network that is **public and open** both because everybody can *read* it (by downloading the entire blockchain from one or more peers), *and* because anybody can contribute to *creating* it. By downloading and reviewing an updated copy of the blockchain any peer can safely tell the balance of every account by checking all inbound and outbound transactions.

1 The blog was published by Econopoly, which is the avenue of publication of external writers of the largest Italian economy newspaper, Il Sole 24Ore. The article attracted 400,000 reads only in its first day of publication (a Sunday). http://www.econopoly.ilsole24ore.com/2017/12/17/bitcoin-bolla-o-souffle/ [Italian]

How the blockchain is generated (in Bitcoin)

On average every ten minutes a block is produced and distributed. The block is linked to and depends on the previous one. The main payload of each block is a list of (un)**validated transactions**. As soon as the block containing them is accepted as part of the blockchain, those transactions become validated and final.

"Validated" means that the transaction originates from a sufficiently funded "account" and has been signed with a valid unique private key. Given these conditions it shall prevail against any subsequent conflicting transaction, resolving cases of double expenditure. Trust that the transaction is irrevocable is therefore achieved only when it is integrated in the blockchain.

But **who creates those blocks**? Interestingly in Bitcoin and similar blockchain-based technology this can be anybody who has invested sufficient resources to "mine" the next block in the chain. This is where things get really interesting.

The activity of creating blocks is called "**mining**". Mining reflects the idea that – as with gold – blocks are figuratively dug out of the ground. The creation of the blocks is an expensive and rewarded task in order to ensure that incentives to take over the blockchain for nefarious reasons are counterbalanced by the effort it would require to overspend the rest of the network and accomplish such result. The more computing power needed to create a block, the higher – by a factor of many millions – the collective effort put into being the first one to publish a new block. In order to be *half sure* (50% chance) to create a specific new block you would have to provide at least *half* of this collective computing power.

This race makes it highly unlikely that somebody would take over the process as too many parties have a competing interest.

Who holds the checked flag to tell that you have been successful? "Nobody" and "everybody" are both acceptable answers. To be accepted your proposed block must meet two basic conditions: to be formally impeccable (including containing only valid transaction) and to show proof to have solved a **mathematical puzzle**. In other words, you must show a **proof-of-work**, a decision made not by a person but by the protocol itself, which is designed to rapidly resolve any potential dissent.

The puzzle, the proof-of-work, is a kind of treasure hunt, where any solution brings you to the next puzzle, and you can start solving the next puzzle only after the previous one has been completed, so no significant head start can be achieved by any one party.

The block is formed of pure text, arranged in a pre-defined way. One of the parts that must appear in the block is **a string that uniquely identifies** the previous block. This string is mathematically calculated using a **public, open algorithm** called a "hashing algorithm".[2] The hashing algorithm, if applied to a block, irrespective of the length of the originating block, gives a fixed-length hexadecimal[3] string called a "hashing footprint" or simply **hash**. It is computationally easy to calculate the hash from the originating block. Because this is a deterministic algorithm anyone with the same originating block will obtain the same hash. It is almost impossible that two different blocks could originate the same hash if the hash is sufficiently long (the possible combinations are 16^{64}).

The algorithm is designed so even inconspicuous variation in the originating block will generate a significantly dissimilar hash. An example could provide a more graphical explanation:

The quick brown fox jumps over the lazy dog

2 Bitcoin uses SHA-256, a hashing algorithm contributed by the NSA.
3 it contains numbers from 0 to 9 and letters from a to f

Generates the following hash:

c03905fcdab297513a620ec81ed46ca44ddb62d41cbbd83eb4a5a3592be26a69

By changing the capitalization of the first letter of "The" the hash changes to:

1153a4080f1fcb04425aa0b841c2b14606fe6df25d9076d2a1face2d5af57129

It is impossible to mathematically calculate how the originating block must be changed to obtain a hash with a given content. The only way to obtain such information is to "*brute force*" the result.

Let us suppose that a participant must find a hash with two consecutive examples of the letter "a". She would probably attempt a few random hashes hoping to stumble into a valid outcome. In the example above I was successful in just two attempts. Let us make it harder, by asking that the matching string must be *at the beginning* of the hash. I can count how many possible combinations I have, knowing that only one valid combination among them: $16^2 = 256$ possible combinations. If the stakes are higher, the odds of winning must be lower. This is achieved by increasing the number of digits in the "winning" combination.

The challenge in Bitcoin mining is finding a block which has a hash lower than a certain value and therefore has with a certain number of leading zeros. Currently, this number is 16, which computes to 1 in $16^{16} = 1{,}844 * 10^{19}$ combinations, or *one in eighteen trillion trillion* combinations.

There is more. A miner must find a block that generates a sufficiently low hash, that is well formed to contain only valid actual transactions *and* that **contains the hash of the previous block**. That means that the process begins only after the previous block has been published, providing a average time to solve the puzzle limited to **10 minutes**.

This is hard-coded in the software. The protocol is self-adjusting, increasing the difficulty as soon as the blocks start to be generated at a faster pace. As such the protocol is conceived to resist both an anticipated increasing success (with more invested resources) and to Moore's law (computing power becomes cheaper and more available over time).

A (well) rewarded effort

Why should one invest the relevant resources required to solve such a difficult puzzle? This activity is **well rewarded**. The reward consists in an amount of Bitcoins and is how every past and future Bitcoin enters the system.

During 2017 Bitcoin has jumped over USD 10,000 per unit and is swiftly moving towards a valuation of around 20,000. Therefore the reward to obtain new coins is huge. Who arbitrates ownership? Since there is no tribunal, no central bank or other authority, the system is **self-governing**.[4] The first to achieve a result publishes the block. The result is swiftly propagated to all nodes. All mining nodes will then decide in a matter of milliseconds that it is time to move onto the next block. In the unlikely, but not impossible, case that two miners publish their own block simultaneously the blockchain spawns into two different **branches**. This means that nodes start receiving two different blocks for the next few places. Again, the software dictates that the longest chain wins, and since the pace will inevitably be different, as the branch with more computing power attached will outpace the other, eventually the weaker branch will die off because all the blocks in

4 "Code is Law here", literally. This is a quote by Lawrence Lessig, *Code is Law – On Liberty in Cyberspace*, Harward Magazine 2000. https://harvardmagazine.com/2000/01/code-is-law-html

the losing branch will be unable to spend their reward. This state of uncertainty has been experienced for up to an hour in the past (six blocks).

When a brand new block is created it carries freshly minted, or mined, Bitcoins. The miner will have associated her account to the Bitcoin and in the process will have generated a private key permitting her to spend the Bitcoins. This is via generating an outbound transaction with that block known as "entry point". The private key is the only enabler of this transaction. While the transaction is not authorised by a third party anybody can see where the transaction comes from and valid holder of the corresponding secret key, and this is all it is required to computationally assert trust.

The recipient of the transaction will have increased credit, and will use her own private key to make all subsequent transactions related to this and other credit. All these transactions are made available to all miners, and these miners will collect and place them into their candidate blocks.

The amount of awarded Bitcoins **halves** at given intervals, therefore it will come a time when the generated Bitcoin will be below the minimum amount of Bitcoin that can be spent (one hundredth of a millionth of a Bitcoin, currently). As the Bitcoin yielding curve is logarithmic, there will ever be **21 million** usable Bitcoins.

As soon as we will approach the upper limit, what would be the reward, as the newly minted Bitcoins will only be issued in ever-smaller fractions? What would compensate the effort of making new blocks, and make sure nobody is in a position to game the system as soon as the proof-of-work will be less demanding?

The reward is not only in the minted Bitcoin. There is an (optional) reward consisting of a **fee** that the parties in a transaction offer to those who publish the transaction in their blocks. The higher the fee the more likely it is that the transaction will make the ledger. A fee-generating transaction is (naturally) prioritized over the non fee-generating ones. Therefore, even in the future, a sufficient incentive not to meddle with the blockchain growth process should be guaranteed.

Who has invented it?

The crypto-currency christened "Bitcoin" was allegedly conceived by Satoshi Nakamoto – a pseudonym with no known author (or even authors) – who delivered the concept and the first iteration of the open source software tools. "Satoshi" published an academic paper to describe the working of the crypto-currency based on a distributed ledger, peer-to-peer network operating a blockchain and a private-public key pair system.[5]

Ththe system can be summarised as follows:

> *The steps to run the network are as follows:*
>
> 1. *New transactions are broadcast to all nodes.*
> 2. *Each node collects new transactions into a block.*
> 3. *Each node works on finding a difficult proof-of-work for its block.*
> 4. *When a node finds a proof-of-work, it broadcasts the block to all nodes.*
> 5. *Nodes accept the block only if all transactions in it are valid and not already spent.*
> 6. *Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*

5 The paper is available at https://bitcoin.org/bitcoin.pdf

Is it Currency or is it a commodity?

A commodity is a kind of good which is traded by its quantity and quality, not as an individual item. Currently, Bitcoin is traded as if it was a commodity, but this state of affairs is unusual because a commodity has an intrinsic value and is useful per se. Some commodities are consumable, which means that they naturally perish and must be consumed by a "best-before" date, leading to stock-keeping incurring a seizable fraction of their value. This is the case with oil, gas, frozen orange juice, barley and coffee. Other commodities are not naturally consumable and are traded over longer time periods, even indefinitely, since they are more easily stored.

Bitcoin as a commodity and as a high-yielding tradable object is therefore somewhat unusual. It may be regarded a perversion of the original system intent, because by its nature Bitcoin should have a *transaction* value rather than a value of its own. The success of Bitcoin is also one of its most striking current shortcomings. It is very difficult to use a currency whose value floats between wide margins day over day. This volatility impedes an important characteristic for a currency: to express an intermediate value by which, in an economic system, players can exchange currency against goods or services, allowing the recipient of the currency to consistently trade it with an equivalent value in goods or services. All the values on the market can therefore be coherently expressed in one single unit of measure that permits ta calculation of all relative "prices" (e.g., how many man/hours work is worth a car, how many movie tickets can I buy by selling a loaf of bread, etc.).

One of the basic functions of a currency is normally understood to be a reasonably stable **price system**. This is not always strictly true, with an example being that in Europe several hundred million people at once started using a totally new currency called the euro in a nearly zero-inflation zone. Many people continued making a mental conversion between the new currency to the old one, because their experience had stratified over the years, while the new unit did not hold much meaning for them. Nonetheless, the new currency was adopted before a new set of relative prices had sunk in older people's habits (some still make this conversion, which after nearly twenty years has very little meaning).

Therefore, it is not *essential* for a currency to represent such a social reference system, and this aspect of Bitcoin is not without precedent. An absolute role is also not played by another commonly recognised function: that of **accumulating value** for later expenditure. This important function is not well served in hyperinflation situations (e.g. the one currently experienced in Venezuela or Zimbabwe), when prices may significantly within the day. Of course even in these situations there is no doubt that the national currency is still a currency, albeit it cannot be kept for very long without losing its presumedvalue.

What makes a currency a currency (even an open source one)?

Bitcoin, as many other open source revolutions (Internet, Free and open source software, open content, open data, etc.) forces us to rethink what we know about economics from the perspective of openness and lack of control. It suggests that the time is right to reassess some about currency: that there cannot be currency without a legal tender emitted by a central bank. At least theoretically it has been demonstrated that an anarchic, uncontrolled, distributed payment system with a currency of its own *is possible*.

This is not the first time the concept of "currency" has undergone a re-thinking process. In ancient times, it was thought that a coin held worth because it had an intrinsic value, that of the materials it was forged from. Even back then, this was only half-true, as the implicit function of the coins was to represent an easily-accumulated, stored, transported and exchange token at conventional value in a shared prices system. The coining material had value but the value of an object still depended on the

perception of the parties involved in each transaction. Accepting the coin did not indicate interest in using the metal but rather to further exchange it against another item. This implied that the important value was not in the meal but rather in what it could accomplish as coinage.

At the end of the day, we can safely state that any kind of currency, from its users' perspective, is an **implicit contract**. When we buy something, the buyer and seller settle for a price attached to the currency as a value which is measured against all other values. Even when a price is fixed or imposed, individuals can still decide whether to trade for that price or not. The buyer and seller know the quantity of currency required to buy a certain quantity of goods or services. The worth of the currency emains implicit. If the price is not sufficient, the deal is not made.

A Dollar is worth a Dollar. An euro is worth an euro. If by magic everybody had ten times more Dollars, and prices, obligation or debt was equally increased, everyone's wealth would remain perfectly static.

The fact that a currency is **legal tender** is often cited as a reason why Bitcoin is not a currency. However, this holds dubious merit. "Legal tender" means that one cannot refuse payment of a debt made by offering that the assigned currency. Conversely, nobody can be forced to accept currency which is not legal tender unless settlement with that particular currency had previously been agreed upon. None the less, in certain countries, especially those suffering from high inflation, sometimes a parallel market expressed in a foreign and more stable currency appears, something called "**dollarization**" due to the frequent use of the US Dollar for such parallel trade. Often this dollarization is illegal, and even importing foreign currency is or outright illegal, or subject to tight control.

But using foreign currency is not illegal per se and a foreign currency can be chosen by the parties in a transaction to settle the dues originating from their relationship. In Italy, for example, the Civil code was issued during WWII addressed a period of strong autarchy imposed by a fascist regimebut conversely was quite liberal regarding the use of foreign currency. It allowed full address of obligations which are expressed in currency "which is not legal tender within the State". The debtor could offer to pay the equivalent of the chosen currency in the national legal tender at the exchange rate at the time when the debt is due (art. 1278). However, this legal option can be originally excluded by the parties, and this exclusion holds as long as the currency in which the obligation is denominated can be easily obtained. There is no reference to the fact that an alternative currency must be legal tender some country (the law does not mention "foreign", but just "not legal tender in the State") so the question of what happens outside the domestic jurisdiction in terms of legal tender is in fact irrelevant. The result is that currency which has no legal value can be treated as holding the same value as the legal tender. This holds true in general, as an obligation in foreign currency is treated as a monetary one, not as a barter, as would happen if it was a commodity.

It is therefore reasonable to conclude that Bitcoin was born as a system to provide a generally available, all-purpose payment system to transfer value between parties irrespective of the underlying obligation, which is ultimately the role of currency. It is, if used properly, money, in a manner that is not dissimilar to foreign currency.

Conclusion

Money is a fundamental element of a complex society. A complex society tends to have money and a denominated price system even in the absence or against the intervention of a State. It follows that money is what makes trade possible, trade is what makes a liberal society thrive, and therefore money is an item of critical importance. Controlling money is a way by which governments can help or hinder their citizens. Having a currency that can be used outside the banking and financial systems is an option that cannot be disregarded lightly or labeled dismissively as a "black economy."

Bitcoin is the first software-defined currency with a complete system of its own. Despite its many shortcomings, such as the environmental cost of making and maintaining it or the already discussed volatility, or the relative uncertainty of when a transaction is final, or the associated fraud causing significant losses, Bitcoin has been used and it is accepted in limited but not irrelevant cases for small to very large transactions as was originally intended. At times, it is used to find a workaround for payments in national tragedies, lack of democracy, nefarious governments, and it allows people to keep some space from illiberal constraints of dictatorship.

Bitcoin is open source and it inherently fits into the broader ecosystem of open technologies and solutions. It is based on publicly available, open standards and infrastructure suchas the Internet. It something that until a few decades ago would have been unthinkable. The question is where it will go next.

About the author

Carlo Piana *is an Italian attorney admitted to the Milan Bar. It has founded Array, a new concept law firm (Array is an array) which specializes in Information Technology Law and Free and Open Source Software in particular. External General Counsel of the Free Software Foundation Europe, is a member of the Editoria Committee of IFOSSLR and a member of the Council of the Legal Network, the initiative sponsored by FSFE to discuss under the Chatham Rule the bleeding edge of openness-related legal issues.*

DOI: 10.5033/ifosslr.v9i1.120