Bitcoin: A cryptocurrency

Vairaprakash Gurusamy[#1], Darshak Akbari[#2], Jay Pipaliya[#3]

Research Scholar, Department of Computer Applications, Madurai Kamaraj University, Madurai, India

BCA Student, Department of Computer Applications, Marwadi University, Rajkot, India

BCA Student, Department of Computer Applications, Marwadi University, Rajkot, India

Abstract: A cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transaction to control the creation of additional units, and to verify the transfer of assets. Bitcoin, created in 2009 was the first decentralized cryptocurrency. These are frequently called altcoins as a blend of alternative coin. Bitcoin and its derivatives use decentralized control ad opposed to centralized electronic money and central banking systems. The decentralized control is related to the use of bitcoin's block chain transaction database in the role of a distributed ledger. Decentralized cryptocurrency is produced by the entire cryptocurrency system collectively, at a rate which is defined when the system is created and which is publicly known. In centralized banking and economic systems such as the corporate boards or governments control the supply of currency by printing units of or demanding additions to digital banking ledgers. In case of decentralized cryptocurrency, companies or governments cannot produce new units, and have not so far provided backing for other firms, banks or corporate entities which hold asset value measured in it.

Keyword: Bitcoin, Digital Currency, cryptocurrency.

I. Introduction

Although people refer to bitcoin as a decentralized digital currency, I prefer to think of it as an electronic asset, to sidestep questions around which government backs it and who sets the interest rate, which are often a mental block in understanding bitcoin. As an electronic asset, you can buy bitcoins, own them, and send them to someone else. Currently (Sep 2015) there are around 14 million bitcoins that have been created, increasing by 25 bitcoins every 10 minutes or so, with an agreed limit of 21 million, the last of which should be created a little before the year 2140.

Why we use bitcoin ?

1. Bitcoin payments - Payments of bitcoins can be made from one person to another, irrespective of geographical location or jurisdiction.
2. Potential users - Some communities are underserved by banks due to the cost/benefit of the brick & mortar banking model and regulatory cost; some international transfers are unreliable, or can take many days, with manual processes and faxes being used as part of the plumbing.
3. Price volatility - Just like other currencies, bitcoin’s price fluctuates. Bitcoin’s price is more volatile than a lot of currencies (though the volatility is decreasing), so if you account for your wealth in your local currency.
4. Conversion - Just like other currencies, if you have one currency (say, Pound Sterling), and you want to convert it to bitcoin, you need to find someone to exchange it with.
5. Maintain cynicism - You may hear of bitcoin being ‘fast’ and ‘free’ or ‘low cost’. While that is true when you are strictly in bitcoin, it’s worth maintaining some cynicism and thinking about the costs involved in the ‘on’ and ‘off’ ramp getting from sovereign currencies into bitcoin and back.

Blockchain Technology

One can think about the block chain as ledger of transaction a physical ledger is typically maintainted by a centralized authority not by market participants the block chain however is a distributed ledger which resides on each participants device. Each individual copy is updated in real time whenever a transaction is completed. The device of each participant or user is usually referred to as a ‘node,’ which forms part of a network of nodes.

The blockchain is unique because every node must authenticate every transaction in the network. This is why when a new node joins the network, the entire record of transactions is downloaded onto its system (for Bitcoin, this process now takes over 24 hours). From then on, it will join the other nodes in updating the ledger as and when new transactions are authenticated. The process of authentication is based on advanced cryptography, and is widely considered to be secure in and of itself. Hence, participants do not need to rely on a third party for transparency and authenticity. The blockchain ensures the transparency and integrity of transactions purely through mathematics, and not trust. The type of transaction varies depending on the application of blockchain technology. In Bitcoin, for instance, each transaction is a transfer of a certain value of Bitcoin between participants, and every transaction is recorded on the Bitcoin blockchain.

Architecture of Bitcoin

The distribution of data works on a peer-to-peer basis, rather than client-server. Peer-to-peer is like a gossip network where everyone tells a few other people the news (about new transactions and new blocks), and eventually the message gets to everyone in the network. This is as opposed to client-server is more like a conventional organization where a boss tells subordinates the news, and the boss is a central point of reference, and potential failure. One benefit of peer-to-peer (p2p) over client-server is that with p2p, the network doesn't rely on one central point of control which can fail.

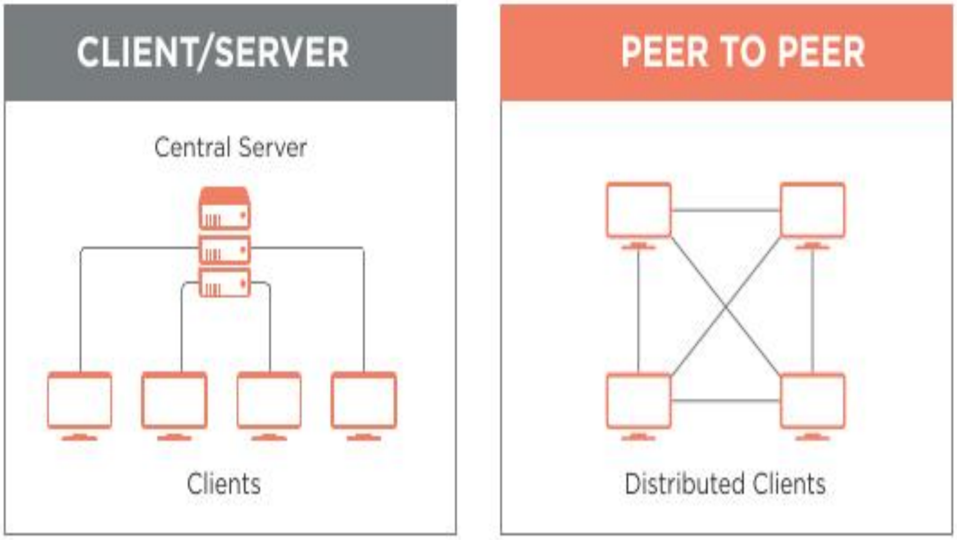


Fig 1. Architecture of Bitcoin

The term "bitcoin network" refers to the collection of nodes running the bitcoin P2P protocol. In addition to the bitcoin P2P protocol, there are other protocols such as Stratum, which are used for mining and lightweight or mobile wallets. These additional protocols are provided by gateway routing servers that access the bitcoin network using the bitcoin P2P protocol, and then extend that network to nodes running other protocols. For example, Stratum servers connect Stratum mining nodes via the Stratum protocol to the main bitcoin network and bridge the Stratum protocol to the bitcoin P2P protocol. We use the term "extended bitcoin network" to refer to the overall network that includes the bitcoin P2P protocol, pool-mining protocols, the Stratum protocol.

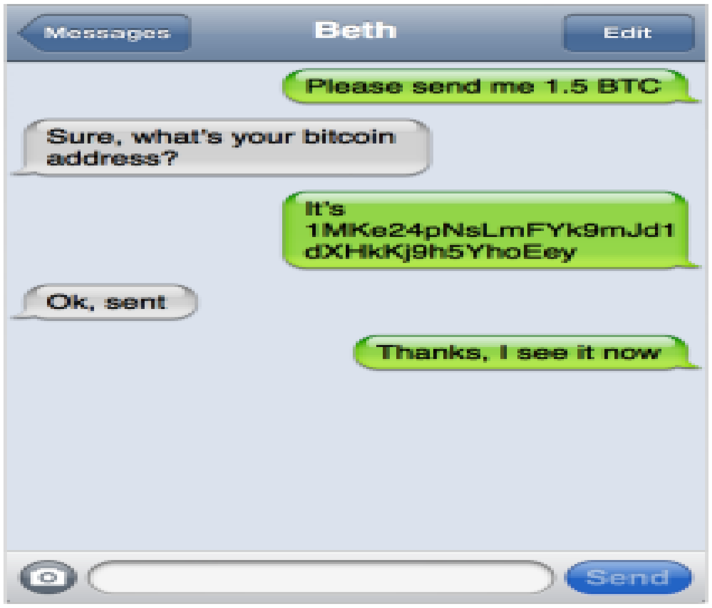
How are bitcoins stored?

Bitcoin ownership is tracked on The Bitcoin Blockchain, and bitcoins are associated with “bitcoin addresses”. Bitcoins themselves are not stored; but rather the keys or passwords needed to make payments are stored, in “wallets” which are apps that manage the addresses, keys, balances, and payments.

Bitcoin accounts: addresses

In banking you have *accounts* which keep pots of money separate; in bitcoin you have *addresses*. A bitcoin address is similar to a bank account number, with a few differences.

Here’s an example of a bitcoin address: 1MKe24pNsLmFYk9mJd1dXHkKj9h5YhoEey. Just like with bank accounts, if you want to receive a bitcoin payment, you need to tell someone your bitcoin address, so they know where to send bitcoins to. A typical conversation, which could be in person, or online, or on chat (Whatsapp/Skype etc) looks like:



Please send me 1.5 BTC

Sure, what's your bitcoin address?

It's 1MKe24pNsLmFYk9mJd1dXHkKj9h5YhoEey

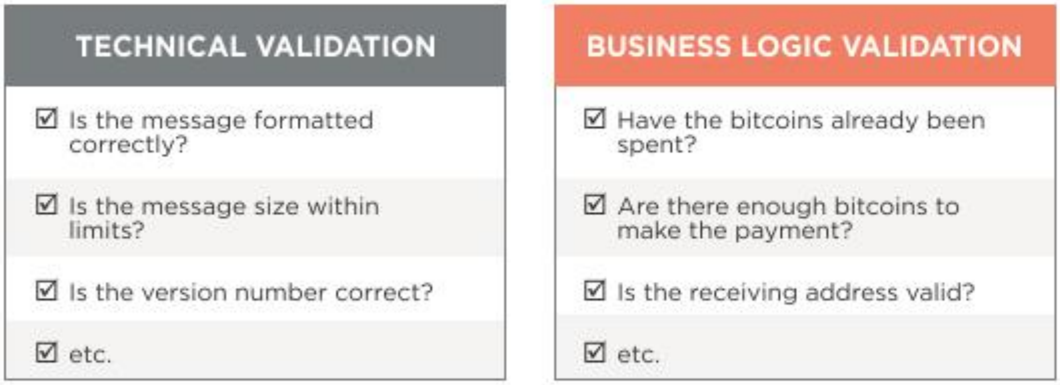
Ok, sent

Thanks, I see it now

Fig. 2 Bitcoin Payment Message

What happens when I make a bitcoin payment ?

1. which bitcoins you're sending
2. which address you're sending them from
3. which address you're sending them toValidators**.** When the first computer receives the instruction, it checks some technical details, and some business logic details (eg, does my payment attempt to create bitcoins out of nothing? Have the coins being sent already been sent elsewhere? etc).



TECHNICAL VALIDATION	BUSINESS LOGIC VALIDATION
☑ Is the message formatted correctly?	☑ Have the bitcoins already been spent?
☑ Is the message size within limits?	☑ Are there enough bitcoins to make the payment?
☑ Is the version number correct?	☑ Is the receiving address valid?
☑ etc.	☑ etc.

Fig. 3 BitcoinValidation

If these tests pass, then the computer relays it to others on the network, who each run the same validation tests. Remember on this network, computers can't trust each other so they have to run the same tests. Eventually all computers on the network know about this payment, and it appears on screens everywhere in the world as an "unconfirmed transaction". It is unconfirmed because although the payment has been verified and passed around, it isn't entered into the ledger yet.

Advantage of Bitcoin Technology

User Anonymity

Bitcoin purchases are discrete. Unless a user voluntarily publishes his Bitcoin transactions, his purchases are never associated with his personal identity, much like cash-only purchases, and cannot be traced back to him. In fact, the anonymous Bitcoin address that is generated for user purchases changes with each transaction.

Purchases Are Not Taxed

Since there is no way for third parties to identify, track or intercept transactions that are denominated in Bitcoins, one of the major advantages of Bitcoin is that sales taxes are not added onto any purchases.

Very Low Transaction Fees

Standard wire transfers and foreign purchases typically involve fees and exchange costs. Since Bitcoin transactions have no intermediary institutions or government involvement, the costs of transacting are kept very low. This can be a major advantage for travelers. Additionally, any transfer in Bitcoins happens very quickly, eliminating the inconvenience of typical authorization requirements and wait periods.

Mobile Payments

Like with many online payment systems, Bitcoin users can pay for their coins anywhere they have Internet access. This means that purchasers never have to travel to a bank or a store to buy a product. However, unlike online payments made with U.S. bank accounts or credit cards, personal information is not necessary to complete any transaction.

Conclusion

Blockchain technology runs the Bitcoin cryptocurrency. It is a decentralized environment for transactions, where all the transactions are recorded to a public ledger, visible to everyone. The goal of Blockchain is to provide anonymity, security, privacy, and transparency to all its users. However, these attributes set up a lot of technical challenges and limitations that need to be addressed.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no2, pages 99-111, 1991.
[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure, "http://www.hashcash.org/papers/hashcash.pdf, 2002.
[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
[8] W. Feller, "An introduction to probability theory and its applications," 1957.