10 BITCOIN MYTHS

EDUARD DE JONG, GEERT LOVINK
AND PATRICE RIEMENS

Amsterdam, November 2015

Pigs will fly, but not in the next 100 million years.
—Johan Sjerpstra

1. 'Bitcoin is a Peer-to-Peer System.'
In order to transfer value from one Bitcoin account to another, the owner of bitcoins uses the services of a collective of operators known as 'miners' who validate the transaction on the Bitcoin distributed database also known as 'the ledger.' The relationship between these operators and an individual user, i.e. owner of bitcoins, is hence one between merchants and customer and not one of equals. Only miners are, and then only operationally speaking, peers, since they all perform the same software program. However, they are also, and mostly, in competition which each other because they need revenue to pay for the equipment they operate. Also, any time an update to the database is made, only a single miner is actually adding the transaction records with Bitcoin value transfers to the ledger, and gets the financial rewards for doing this. In this way, the incentive for miners to support each other is limited, and one cannot speak of a peer-to-peer relationship in the traditional sense.

Over the time Bitcoin has been operational the inherent hierarchical relation between miners and users has become more pronounced by an ever rising technical and financial barrier to becoming a miner. Investments and operating costs of the necessary equipment rise in tandem with the continuously increasing difficulty of adding a new record to the database that is built into the Bitcoin protocol.

Conclusion: Bitcoin is not a peer-to-peer system, but an online merchant-customer transaction market place.

2. 'Bitcoin does Away with Intermediaries and Fees.'
To make a payment using bitcoins a Bitcoin user needs a 'Bitcoin exchange' and these exchanges charge a fee. The sole exception is if the user is a data base operator (a.k.a miner), having aggregated some bitcoins by mining and exclusively pays other users who have decided to accept and keep bitcoins.

There is an other intermediary in Bitcoin, the operators of the distributed data base, the Bitcoin miners. A miner also needs to charge for its labor and expenses. For the time being, a miner is rewarded with newly created bitcoins, that is why updating the database is called 'mining'. By design, the available amount of bitcoins that can be mined is restricted, and it is expected to be exhausted somewhere around 2040. After exhausting the lode miners can only earn money by explicitly charging a fee.

Conclusion: De-facto, Bitcoin users need to engage services of intermediaries and do pay fees for their transactions.

3. 'Bitcoin is an Alternative Currency.'
An alternative currency, by definition, is designed to _entirely_ displace and replace existing currencies. Complementary currencies intend to _partially_ displace and replace existing currencies, usually in a local setting.

By design, Bitcoin is an alternative currency. Real world observation however, shows that most transactions in bitcoins translate, either at the point of purchase, or at the point of sale, in transactions in existing currencies. Only miners can create bitcoins, non-miners need to acquire them, usually by way of purchase.

In practices Bitcoin transactions are often intended to avoid high transfer fees or bypass local restrictions in making international payments. In such cases, bitcoins are purchased, swiftly change hands, and are just as fast converted again in another currency. In this 'cash-in cash-out' scheme Bitcoin operates then as a facilitator in the circulation of existing currencies and not as a replacement of these. Cash-in cash-out has been shown the most common mode of operation in bitcoins. A Bitcoin transaction can also be speculative in purpose, to hoard bitcoins expecting a raise in their value. In this case Bitcoin can be considered an alternative to other currencies, comparable to a speculative investment in dollars or in commodities, like iron ore, gold or grain.

Conclusion: Bitcoin does not actually operate as an alternative currency.

4. 'Bitcoin is Not a Fiat Currency.'
In practice, acceptance of Bitcoin payments takes place before the (irrevocable) recording of the transaction in the distributed database. That is, without formal confirmation of its validity. Apparently, the parties involved in payments in bitcoins _believe_ in their eventual recording. The payee therefore trusts the _eventual_ availability of received funds.

This looks distinctly similar to the way traditional instruments of payments, such as coins, banknotes and bank transfers, operate. The users trust, based on experience and social convention, the correct operation of the system such that received funds are available for further spending. This 'systemic trust' in traditional, fiat, currency is underpinned by a mix of technical features such as hard to copy bank notes, fraud detection software in financial institutions and government imposed and enforced regulations.

Conclusion: Where in practice the 'systemic trust' in Bitcoin is no different from that of traditional currencies, Bitcoin operates _de facto_ as a fiat currency.

5. 'Bitcoin is Anonymous.'
The central database with transactions in bitcoins is publicly accessible. This is an essential Bitcoin design property to, at least in theory, allow any party to participate as processing node (miner) in order to get involved in updating the distributed database. The parties in a transaction are identified by unique numbers, and a payment transaction is linked through this number to the transaction wherein the spend value was received.

But as most Bitcoin transactions effectively constitute a payment in traditional currency at one end or the other, or both, they involve well known parties that exchange bitcoins for and against these currencies, the Bitcoin exchanges. Hence, payments in bitcoins can be traced as the value flows between these exchanges. Identification to the humans involved in a payment, e.g. by law enforcement, are therefore _potentially_ possible.

Conclusion: Bitcoin is not an electronic form of cash and does not protect privacy.

6. 'Bitcoin is Secure and Cannot Be Hacked.'
Security for electronic payments has several parts: first to make sure that only the rightful owner can make a payment, secondly to make sure that the intended recipient actually receives the moneys paid and finally that only money can be paid that is actually owned by the payer and hence can not be spend twice.

In the Bitcoin sphere a payer uses a password to initiate a payment from her computer. The password unlocks a private cryptographic key stored on the computer to send cryptographically protected messages to be recorded in the Bitcoin database to make the payment. Yet, computers can be hacked, and a hacker can gain control of the private key and hence initiate a fraudulent payment. A loss of the private key, for instance by a crashed hard disk, does not just lose access to the money, it actually loses all the moneys controlled. Indeed one of the design features of Bitcoin is that payments, once made, cannot be reversed or recalled.

For the ordinary user, this represents a much higher level of risk than in traditional banking, where losing the bank card or PIN does usually not result in losing the whole balance held in the bank account.

On the functional side, the operators of the processing nodes in the distributed implementation of the shared Bitcoin database use a protocol to agree on the next version of the database. This is required to correctly incorporate the payment transactions made since the last update. The software in each of the processing nodes must verify the correctness of the transactions by inspecting previous transactions where the payer has received the value to be spend. Yet, servers can be hacked (e.g. with a virus) and the continued operations can therefore not be guaranteed.

By design, the blockchain protocol does not guarantee that all past transactions remain stored for ever or can be available to each of the processing nodes (miners) for inspection in a fail-safe way. The protocol does also not guarantee that a processing node actually verifies the transactions it records. The blockchain protocol cannot prevent that fraudulent transactions get recorded, and does not provide a way to remove or correct fraudulent transactions.

Conclusion: using Bitcoin is more risky than the traditional payment infrastructure.

7. 'Bitcoin Operates Without Trust.'
Bitcoin literature is adamant that the Bitcoin set-up successfully substitutes 'objective' 'algorithmic' trust for less reliable, because human error and trickery-prone, 'subjective' institutional or political trust.

As described previously, the blockchain protocol used to synchronize updates to the Bitcoin central database (or ledger) does not guarantee the correctness of the updates made. Most processing nodes that update the database, use the same open source implementation, the Bitcoin 'miner' program. This program includes verification of transactions, but transaction verification by the miner program might be compromised either accidentally, by a software bug, or maliciously, e.g. by a virus, or by a miner intent on undue gains. Users engaging in Bitcoin transactions implicitly trust that the miner programs continues to operate correctly, that the equipment is protected against virus attacks and that the miners will not subvert it.

Also, protection of the stored value at the level of the individual owner is not very strong in the Bitcoin set-up. As a consequence, Bitcoin service providers have emerged offering enhanced payment security, in the form of managing their clients' wallets. This service can be provided both online and with physical tokens like smart cards. Making use of 'wallet providers' evidently entails trust in the continued correct and honest operations of the online service or of the physical device.

Conclusion: Bitcoin substitutes one form of 'subjective' trust in traditional institutions for another in new organizational forms.

8. 'Bitcoin is Politically Neutral.'
British prime minister Margaret Thatcher, in a famous 'last words' speech against the Euro, affirmed that decisions about money and currency are all essentially political in nature. In this context politics must be understood as more than what politicians do, essential politics is about the citizens and the state they live in. The decision that is embodied in Bitcoin's design to limit the issuable volume of bitcoins to 21 million units can only be seen as political.

Other characteristic Bitcoin features, such as it rewards for early adopters and big operators, its essentially deflationary and hoarding-inducing nature (also due to the designed scarcity of bitcoins), its rejection of regulatory oversight and consumer protection and of state intervention generally, all resonate with political beliefs of 'techno-libertarians'. Conversely, it is difficult to imagine how Bitcoin could effectively function in a capitalism-unfriendly political dispensation.

Conclusion: like any other monetary system, Bitcoin, in its technical design reflects explicit or implicit political choices.

9. 'Bitcoin is a Sustainable System.'
The whole Bitcoin set-up is, and especially the functioning of the distributed implementation of its central database with the compute-intensive blockchain protocol, is dependent on increasingly sophisticated and trouble-free network infrastructure resulting in an ever increasing consumption of resources. This clearly is at variance with the ever more forceful, and inescapable calls for less consumption, foremost in the energy sector.

Conclusion: Bitcoin does not fit well in the required transition to sustainability. This contrasts with traditional financial institutions that can reduce energy consumption a pace with improvements in IT technology.

10. 'Bitcoin Can Scale to World Size.'
Both the limited number of possible units of bitcoins and inherently severe technical limits to the operational speed of the blockchain protocol pose such insurmountable obstacles to a global economy that would run exclusively with bitcoins. In the absence of governance of Bitcoin, even a technical modification to increase transaction capacity are very hard to implement.

For consumer payment transactions, for instance, it is hard to conceive how the blockchain protocol in Bitcoin can be made to operate effectively at the same speed and volume as systems maintained by, e.g., VISA, Mastercard, AmEx, JCB and such.

As shown in Argentina or Greece Bitcoin can be useful in some specific situations. In these cases it has been a mediator between traditional monetary systems. For Bitcoin to 'scale up' to a true global scale, while maintaining (a semblance of) stability and security would for quite some time to come require such large amount of resources as to defeat any short or medium term perspective of attainability.

Conclusion: As Yanis Varoufakis, the economist and former finance minister in Greece, formulated it: 'Bitcoin is not capable of "powering" an advanced, industrial society.'

—

The authors thank Boudewijn de Kerf for a quick review, while keeping full responsibility for the substance of the argument.