Blockchains:
The challenges to a rollout of this technology

Ilarion Pavel, engineer from the Corps des Mines (Conseil Général de l'Économie, de l'Industrie, de l'Énergie et des Technologies) & Laboratoire de Physique Théorique (École Normale Supérieure)

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
The rollout of blockchain technology encounters several technical problems related, in particular, to scalability, latency, liquidity, electricity consumption and security. But it also must cope with societal, legal and regulatory difficulties: users' behaviors, privacy, public perceptions, taxation, liability, etc. These challenges are reviewed; and a few solutions, suggested.

Blockchain technology appeared in 2008 as a full-fledged part of Bitcoin, the cryptocurrency and payment system for encrypted transactions, which operates without a central authority on a peer-to-peer network (NAKAMOTO 2008). All transactions are validated by nodes in the network and recorded in a public leger (the blockchain) that, it is claimed, cannot be falsified. In a language shift, the word "bitcoin" has come to refer to both the unit of value of this electronic currency (the bitcoin, BTC) and the underlying technology as well as the network on which it operates. Likewise, "blockchain" has come to refer, all at once, to the ledger, the technology and the network.[1]

Equipped with powerful means of computation, certain nodes (called "miners") in the network validate, register and secure transactions. The latter are grouped in blocks, which are then linked to each other to form a blockchain. The first "miner" who manages to solve a difficult cryptographic problem as its "proof-of-work" adds the last block by date onto the preceding block. Once the block has thus been "mined", the miner receives bitcoins for his success; and the new block is diffused to all nodes in the network.

Like other forms of currency, bitcoins can be traded for fiat money, products or services via electronic transactions using software installed on a personal computer or mobile terminal, or using a Web application.[2]

From the start, alternative cryptocurrency systems have imitated bitcoins. These "altcoins" use the same techniques but with optimizations. Blockchain techniques have been successfully used to launch "altchains", alternative chains for applications other than electronic currencies, such as managing resources or contracts. The scope of blockchain technology, originally devoted to financial transactions alone, has widened. A few hundred altcoins and altchains are now thriving. "Blockchain 1.0" refers to whatever has to do with the electronic currency and its operations (issues, transfers, payments), whereas "blockchain 2.0" refers to all other financial and economic applications (shares, bonds, futures contracts, loans, mortgages, intellectual property rights, "smart" contracts); and "blockchain 3.0", to applications outside the financial and economic spheres (in public administration, health, science, culture and art).

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

[2] The technical aspects are much more complicated. See, among many other references, ANTONOPOULOS (2015).

Bitcoins are the most widely used cryptographic currency in the world. The volume of transactions using them is busily expanding.[3] Bitcoin technology and the alternatives (altcoins and altchains) are probably going to transform the financial sector and the economy. As they are rolled out, they will encounter several technical difficulties, not to mention regulatory, legal and societal challenges.

Technical hurdles

Scalability: Insufficient capacity for handling transactions

The size of a bitcoin block was deliberately limited to one megabyte (MB) in order to fend off the denial-of-service attacks that could occur if someone malevolently created big blocks and then diffused them over the network so as to cause congestion and paralyze traffic.

Moreover, the time for mining a block was set at approximately ten minutes. Decreasing this interval would increase the frequency of "forks". Forking occurs when two miners mine two different blocks simultaneously. Depending on the transmission time (latency) in the network, the two blocks might reach miners in a different order: the one block first for some but the other block first for others. This causes the blockchain to fork into two chains. In practice, the two sets of miners continue mining blocks and adding them onto the two forked chains until the one chain becomes longer than the other. When this happens, the longer chain will be validated; and the other chain, abandoned. The more forks in a network, the more vulnerable it is to "51% attacks", a point of security to be discussed.

Increasing the block size and decreasing latency has the effect of increasing the number of "orphan blocks", which have been mined but not added to the chain. For example, two blocks, though mined one after the other in the same chain, might arrive in reverse order at a node in the network. The second block is the orphan. It is temporarily placed on hold while waiting for the first block to arrive.

Owing to these limitations on the size of a block and the latency time between two blocks, the Bitcoin network is only capable of managing seven transactions per second (tps). This is much lower than networks such as Visa, which handles an average of 2000 tps, with a peak capacity of up to 56,000 tps.

Eventually, as the number of transactions increases, it will probably take more time to validate them, whence higher transaction costs. A user normally pays for each transaction, this fee going to the miner who has managed to solve the cryptographic problem. The higher the fee, the more the chances that the transaction will have priority for being added to the next block to be mined.

The possibilities for dealing with these limitations are to increase the block size (by a coefficient of two, or even more), reduce the time between two blocks and latency time (which would lessen the problems related to forking) (CROMAN *et al*. 2016). The altcoin Litecoin operates with 2.5 minutes between two blocks; the altchain Ethereum, with 17 seconds. In addition, radical solutions could be imagined, such as redesigning the Bitcoin protocol (EYAL *et al.* 2015), but they would require a consensus among the parties involved (in particular miners). Another possibility would be to design protocol stacks at a level above the Bitcoin protocol, in the form of "smart" contracts. These stacks allow for millions of transactions per second via payment channels of which only the code at the start and at the end figure in the blockchain, as in Lightning (POON & DRYJA 2016) and TumbleBit (HEILMAN *et al.* 2017).

[3] For statistics on bitcoins, cf. https://blockchain.info/.

Too much latency

Latency refers to the time needed to circulate a block from a node in the network toward all users. This takes, on the average, twelve seconds. By forty seconds, 95% of the nodes will have received the block (DECKER & WATTENHOFER 2013). This is long compared with the Visa Card network (where the latency is a few seconds) and even longer if we imagine using blockchain technology to make safe applications for the Internet of things (IoT), which will be made up of connected devices that are permanently interacting, nearly instantaneously.

Lowering latency time requires modifying the Bitcoin protocol or adding protocol stacks at a higher all level.

A blockchain's size

The size of the Bitcoin blockchain, currently set at 115 GB, has been growing fast — increasing by 50 GB over the past twelve months. Downloading the blockchain on a computer takes several days, on condition that there is enough free memory on the hard drive.[4] Nonetheless, improvements in computers and Internet connection speeds will probably keep pace with increases in the blockchain's size.

Besides, users have the choice between a full node (containing all the blockchain) or a client ledger. In the first case, they validate transactions and blocks, and then transmit the information to other nodes. In the second, they download only the headers of the blocks, thus reducing a thousand times the size in comparison with a full node. Nonetheless, the client ledger relies on full nodes to carry out a transaction. In addition, users have the choice to be Web clients; the Bitcoin network is then accessed via a browser connected to a server that is a trusted authentication authority.

The lack of liquidity

Bitcoins were designed to be a currency with the money supply set at a maximum of 21 million BTC. They are issued as a reward to the first miner to mine a new block. Designed into this system from the very start, this reward is intended to encourage mining. It initially amounted to 50 BTC, but is halved for every 210,000 mined blocks (approximately every four years). By 2140, the reward will be less than the smallest bitcoin currency unit, the "satoshi". The currency will no longer be issued, and miners will be paid transaction fees only.

According to some economists, issuing less money is deflationary. The bearers of this currency would probably be tempted to use bitcoins as a store of value rather than as a medium of exchange. Another problem is the bitcoins dormant on the blockchain — in the electronic wallets of users who have lost their private keys. For these reasons, the BTC would increase in value; and given the constant money supply, the liquidity of transactions should decrease (especially in a deflationary environment).

The reply to these criticisms is that a bitcoin is divisible into very small units, the smallest being the satoshi, 10^{-8} BTC. In case of deflation, the currency could shift (one or two decimals) toward lower values. Besides, some altcoins (*e.g.*, Litecoin or Dogecoin) have lower values; and the Bitcoin system could fall back on them to complete transactions and ward off deflation. There are even altcoins (*e.g.*, Blackcoin, NXT, Peercoin or VeriCoin) with an unlimited money supply.

[4] For a full node, the recommendation is 125 GB on the hard drive, 2 GB of RAM and an Internet connection speed of at least 400 kB/s. *Cf.* https://bitcoin.org/en/full-node

Deflation has a notorious reputation, since it is associated with a sharp drop in demand and can trigger a major economic recession. Our current financial system uses a fiat money with nearly no limit on printing new banknotes. In case of deflation, banknotes can be printed to increase the money supply and jumpstart demand. In the Bitcoin system, deflation would result not from a sharp drop in demand but from a limited stock of coins — a preset limit. This limit will be gradually reached but will not automatically set off a financial crunch.

Electricity consumption

To mine blocks and thus validate transactions, miners must solve difficult cryptographic problems that require a huge number of computations and, therefore, a considerable supply of electricity for computers and cooling systems.

The difficulty of the cryptographic problem does not depend on the quantity and value of transactions, but on the arrival of new miners, who are drawn by the prospects of earnings and are equipped to enter this competitive marketplace. The profitability of their mining depends on the price of electricity converted into bitcoins.

In 2014, the Bitcoin network consumed between 0.1 and 10 gigawatts (O'DWYER& MALONE 2014). At present, the most efficient ASIC (Application-Specific Integrated Circuit) on the market (AntMiner S9) consumes 1300 W for a hashing speed of 13 THash/s, in other words: 100 W per THash/s. All miners in the Bitcoin network perform, on the average, 4 million THash/s, thus consuming 400 MW. This corresponds to half the electricity generated by a nuclear power plant. Since some miners use less efficient tools, this consumption might be three to four times higher than what was previously calculated.[5]

This substantial energy cost must be compared with the potential savings that financial institutions could expect from replacing their centralized system of operations with a blockchain protocol. According to Santander InnoVentures (2015), blockchain technology could, by 2022, cut the costs of banking by $15 to $20 billion per year.

A valid criticism formulated against the Bitcoin protocol is that the proof-of-work system serves only to secure blockchains but that it would be worthwhile to put it to use for solving practical problems, as is done by Primecoin (which uses prime number chains and Cunningham chains), Curecoin (which uses protein folds) or Gridcoin (a proof-of-research system).

Security problems

The most serious security problem is the “51% attack”: a malevolent miner (or pool of miners) endowed with a high computing capacity could take over the blockchain and use it for double spending. This consists of paying for a product, taking possession of it and then deliberately causing a fork where the new chain invalidates the transaction and uses the coins obtained for acquiring a second product (whence “double spending”). If the attacker’s computing power is more than 51% of the total capacity of all miners in the network, the malevolent miner will be able to mine blocks in the new chain so that it becomes longer than the old one, which will, therefore, be invalidated.

[5] http://digiconomist.net/bitcoin-energy-consumption

According to probability models, it would not even be necessary to represent 51% of the network's total computing power: 30% would suffice. Given the Bitcoin network's total computing power however, it would be very hard for a single miner to reach 30%… but a pool of miners could. The pool's leader would build blocks to mine and then distribute them to pool members to do the mining. He could thus exclude certain transactions and include double spending transactions without other pool members having knowledge thereof.

A miner could also make a denial-of-service attack on other parties in the Bitcoin network by invalidating their transactions. After identifying the transaction to invalidate, he would re-mine the block containing it (by first removing the block). The transaction will be on hold as long as the attacker's computing power is dominant in the network of miners.

A defense against these attacks would be to modify the proof-of-work protocol. If the protocol required more computing power (in terms of CPU or RAM), the tools for computation would be more expensive. At present, the specialized ASIC has an affordable price.

Other malevolent attacks could have the goal not of fraudulently making a profit but of disrupting or even paralyzing the Bitcoin network by massively jeopardizing mining operations owing to a denial-of-service attack. This would require huge means of the sort probably only available to governments.

Insofar as the Bitcoin network's computing power increases, it will, however, be harder and harder to launch attacks.

Legal, social and regulatory issues

Users' behaviors and cybersecurity

In the conventional banking system, users can address the bank in case of errors, forgotten passwords, loss of a checkbook or of a debit/credit card…. Using bitcoins requires much more discipline from users. Losing the private key means losing the bitcoins on the addresses generated from it. There is no way to retrieve them. Several users have experienced this misluck when they changed computers or hard disks, since they failed to save, beforehand, their private keys.[6] Using bitcoins requires that users change their behavior patterns. Private keys and passwords must be kept; copies, made on USB devices or on paper (or even engraved on metal) and stored in different safe places.

A private key can also be stolen — the equivalent of stealing all the money available at the addresses in the electronic wallet generated by the key. In a world with ever more cyberattacks, the usual measures for making information systems secure must be reinforced. Software and antivirus programs must be updated. Users should not reply to dubious electronic messages and should not click on the attached files. Steer clear of suspicious Web sites; and do not download files from unconfirmed sources.

Another recommendation is to shun the on-line exchanges or wallets offered by Web client services, since they are not yet safe enough for depositing money. It is better to be a "full-node client" so as to obtain the whole blockchain. Another advice is to use several wallets. Limit transactions to small amounts when using (less safe) mobile terminals; and undertake transactions for larger amounts from a desktop computer (as a full-node client). Safety is also reinforced by using multisignature transactions from several private keys on different devices (desktop computer, smart phone…).

[6] James Howells threw out his computer's hard disk, which had an electronic wallet containing 7500 BTC. *Cf.* www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site

Privacy

We often hear that bitcoins are an anonymous currency, since transactions take place without the communication of personal information. A transaction contains the addresses of the parties involved, which are generated from public keys (in turn, generated from a private key). From the address, it is possible to discover, via the blockchain, all the transactions corresponding to the address; but it is not possible to identity the person involved. However, if the identity of the person corresponding to a given address is divulged (following an unfortunate set of circumstances), all the transactions the person made using that address will also be disclosed.

Bitcoins are, therefore, a pseudo-anonymous currency. This is the reason for the recommendation to use several addresses and several electronic wallets — all of which represents a complication for users.

Public perceptions and societal changes

Bitcoins have been at the center of several affairs involving theft and swindling. Among the most notorious: in February 2014, the bankruptcy of Mt. Gox, a bitcoin exchange, after the "disappearance" of 774,000 BTC ($409 million);[7] and, in August 2016, the theft of 120,000 BTC ($72 million) from Bitfinex.[8] Public opinion tends to perceive Bitcoin as a network for money-laundering. This undermines confidence in the network.

Financial establishments usually "forget and forgive" certain errors to their customers after a certain time. They give a second chance to someone who made a mistake in the distant past. In contrast, a system based on blockchains "forgets nothing".

Lack of legal recourse

In a smart contract (Blockchain 2.0), users freely decide the rules to adopt, but transactions are irrevocable. Once set, the rules must be scrupulously followed; no deviation is allowed. This is a requirement of the technology itself, independently of what the parties to the transaction would like. The execution of a smart contract is efficient and riskless, since there is no way to circumvent it. The counterpart of this is, however, the contract's extreme rigidity. What room is left for human interventions? How to break or nullify a smart contract?

Taxation

In a decentralized "sharing" economy, whether based on peer-to-peer exchanges (such as Uber or AirBnB) or on platforms (*e.g.*, OpenBazaar) for bitcoin payments, it becomes practically impossible for governments to tax transactions. What can authorities do to bring in taxes?

[7] www.theguardian.com/money/us-money-blog/2014/feb/25/bitcoin-mt-gox-scandal-reputation-crime

[8] http://fortune.com/2016/08/03/bitcoin-stolen-bitfinex-hack-hong-kong/

Conclusion

Blockchain technology could add an economic, financial layer onto the Web. It allows for a decentralized system of payments and transactions, for transfers of assets, and for the formulation and execution of smart contracts. Its scope of application could extend beyond the financial sector and the economy as such.

As with any new technology, the rollout of blockchain technology will encounter obstacles and limits. It is up to the community of its agents to find the means for moving forward.

References

ANTONOPOULOS A., *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (Sebastopol, CA: O'Reilly Media) 2015.

CROMAN K., DECKER C., EYAL I., GENCER A., JUELS A., KOSBA A., MILLER A., SAXENA P., SHI E., SIRER E., SONG D. & WATTENHOFER R., "On scaling decentralized blockchains, a position paper", *3rd Workshop on Bitcoin and Blockchain Research*, Barbados, February 2016. Available at: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

DECKER C., & WATTENHOFER R., "Information propagation in the Bitcoin Network", 10p., *13th IEEE International Conference on Peer-to-Peer Computing*, Trento University (IT), 2013. Available at: www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf

EYAL I., GENCER A., SIRER E. & VAN RENESSE R. "Bitcoin-NG: A scalable blockchain protocol", 21p., October 2015. Available at: https://arxiv.org/pdf/1510.02037.pdf

HEILMAN E., ALSHENIBR L., BALDIMTSI F., SCAFURO A., & GOLDBERG S., "TumbleBit: An untrusted bitcoin-compatible anonymous payment hub", 36p., *NDSS Symposium*, 27 February 2017. Available at:
https://eprint.iacr.org/2016/575.pdf

NAKAMOTO S., "Bitcoin: A peer-to-peer electronic cash system", 9p., October 2008. Available at https://bitcoin.org/bitcoin.pdf

O'DWYER K.J. & MALONE D., "Bitcoin mining and its energy footprint", 6p., Irish Signals & Systems Conference (ISSC) & China-Ireland International Conference on Information and Communications Technologies (CIICT), 2014. Available at:
https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf

POON J. & DRYJA T., "The bitcoin Lightning network: Scalable off-chain instant payments", 59p., 14 January 2016. Available at
https://lightning.network/lightning-network-paper.pdf

SANTANDER INNOVENTURES, ANTEMIS GROUP & WYMAN O., "The Fintech 2.0 Paper: Rebooting financial services", 20p., June 2015. Available via:
http://santanderinnoventures.com/fintech2/.