The Center on Capitalism and Society
Columbia University
Working Paper No. 91, August 2016

Blockchain Technology: What is it good for?

Dr. Saifedean Ammous
August 8, 2016

Abstract

This paper explains the functioning of "blockchain technology" and critically assesses its potential role in improving services in banking, contracts, and database systems. Comparing blockchain to the current best practice technology in these fields reveals several barriers to successful commercial implementation: Blockchain technology involves costly redundancies and irreversibility, faces serious scaling problems and significant barriers to complying with regulations, and is a security liability unless secured with its own freely trading currency. A survey of the state of the blockchain industry shows that in eight years since blockchain technology was invented, it has had no commercial applications other than digital cash. The paper concludes that a blockchain is a peculiar engineering design whose only advantage is in removing third party intermediation to allow for the creation of digital cash, and is unlikely to offer economic advantages for any commercial problem other than the one it was specifically engineered to solve.

Blockchain Technology: What is it good for?

Dr. Saifedean Ammous[*]

August 8, 2016

I. What is blockchain technology?

Blockchain technology is originally the name given to the design underpinning the operation of the digital currency Bitcoin. Bitcoin's creator never used the term "blockchain" in his whitepaper, and reading the paper one gets the distinct impression that the author was not introducing a new technology in the traditional sense of the term, but a software design drawing on several existing technologies to allow him to create a "purely peer-to-peer version of electronic cash".

The essence of Bitcoin's blockchain's operation is that whenever two network members transact, they announce their transaction to all network members (nodes), who record the transaction into a block with a limited capacity. Once the block is full, nodes simultaneously perform Proof-of-Work—mathematical operations that are hard to solve but whose correct solution is easy to verify. These mathematical operations are unrelated to the bitcoin transactions, but are indispensable to the operation of the system, as they force the verifying nodes to expend processing power which would be wasted if they included any fraudulent or invalid transactions. The first node that succeeds in solving a Proof-of-Work problem broadcasts the solution, along with the block of transactions, to all other nodes. Nodes can quickly and cheaply verify the accuracy of the transactions and solutions, and when 51% of the processing power of the network votes to approve a block, nodes begin recording new transactions to a new block, amended to all previous blocks.

The first node that solves the Proof-of-Work problem is rewarded with a specific quantity of the currency of the network. This reward makes verifying transactions potentially profitable, and leads to it being commonly referred to as 'mining', though 'verifying' is arguably a more functionally accurate description.

[*] Assistant Professor of Economics at the Lebanese American University and Foreign Member of the Center on Capitalism and Society at Columbia University. Preliminary draft. Kindly do not quote without author permission. Author correspondence address: sha2106@columbia.edu

Verifying the validity of a block's proof-of-work is far cheaper than solving it correctly, which makes determining the correct status of ownership of the currency both economic and lucrative. Functionally, Blockchain technology is a technology of *verification*: since it is far more expensive to solve the Proof-of-Work than to verify its correctness, honesty is the only strategy for profitability for nodes, and the outcome is a record that is undisputed by any of the members of the network.

The operation of the decentralized blockchain is entirely dependent on solving the Proof-of-Work, and voting on the validity of the blocks by nodes expending CPU. Transaction validity is not established by any authority, but by the consensus of the network members with the majority CPU. With this mechanism, Bitcoin has accurately recorded more than 140 million transactions in almost 8 years.

By 2013, several proposals and companies were promoting the idea of using blockchain technology without a digital currency underpinning it. In these 'permissioned blockchains' only preapproved members may commit data to the blockchain, which exists as a shared ledger between all participating parties. There is no Proof-of-Work calculation, as the veracity of the transactions is built on the members being identifiable and accountable to one another. To date, there exist no commercially deployed blockchains, but there are several well-publicized prototypes and proposals. The next section examines the three most common proposals for blockchain technology to assess their economic feasibility.

II. Potential applications of blockchain technology

An overview of start-ups and research projects related to blockchain technology concludes that the potential applications of blockchains can be divided into three main fields:

a. **Digital payments**: Current commercial mechanisms for payment clearance rely on centralized ledgers to record all transactions and maintain account balances. In essence, the transaction is transmitted once from the transacting parties to the intermediary, checked for validity, and accordingly both accounts are adjusted. In a blockchain, the transaction is transmitted to all network nodes, which involves many more transmissions and more processing power and time. The transaction also becomes part of the blockchain, copied onto every member computer. This is slower and more expensive than centralized clearance, and helps explain why Visa & Mastercard clear 2,000 transactions per second while Bitcoin can only clear seven. Bitcoin has a blockchain not because it allows for faster cheaper transactions, but because it removes the need to trust in third party intermediation: transactions are cleared because nodes compete to verify them, yet no node needs to be trusted. It is unworkable for third party intermediaries to imagine they could improve their performance by employing a technology that sacrifices efficiency and speed precisely to remove third party intermediaries. For any currency controlled by a central party, it will always be more efficient to record transactions centrally. Whether removing third party intermediation is a strong enough advantage to justify the increased inefficiency of distributed ledgers is a question that can only be answered over the coming years in the test of market acceptance of digital currencies. What can be clearly seen is that blockchain payment applications will have to be with the blockchain's own decentralized currency, and not with centrally-controlled currencies.

b. **Contracts:** Currently, contracts are drafted by lawyers, judged by courts and enforced by the police. Smart contract cryptographic systems such as Ethereum encode contracts into a blockchain to make them self-executing, with no possibility for appeal or reversal, and beyond the reach of courts and police. "The code is the law" is a motto used by smart contract programmers. The problem with this

concept is that the language lawyers use to draft contracts is understood by far more people than the code language used by smart contract drafters. There are probably only a few hundred people worldwide with the technical expertise to fully understand the implications of a smart contract, and even they could miss glaring software bugs. This all became apparent with the first implementation of smart contracts on the Ethereum network, the Decentralized Autonomous Organization. After more than $150m were invested in this smart contract, an attacker was able to execute the code in a way that diverted around a third of all the DAO's asset to their own account. It would be problematic to describe this attack as a theft, since all the depositors had accepted that their money will be controlled by the code and nothing else, and the attacker had done nothing but execute the code as it was accepted by the depositors. In the aftermath of the DAO hack, Ethereum developers attempted to roll back their blockchain to reverse the attacker's transactions, and as a result the Ethereum network has split into two networks with two different currencies, one which confirmed the DAO attack, and another which reversed it. This "fork" raises questions about Ethereum's blockchain's claim to immutability. The processing power of Ethereum (the second biggest cryptocurrency) is small enough that a small central group of programmers can decide to reverse transactions because their contracts had bugs in them, and succeed in taking the majority of network hashing power with them. This also raises questions of the entire rationale of smart contracts, since it showed that they are not that unstoppable. Given that a blockchain can be rolled back, smart contracts have not replaced courts with code, but they've replaced courts with software developers with little experience, knowledge, or accountability in arbitrating.

The DAO was the first and so far only sophisticated application of a smart contract on a blockchain, and the experience suggests wider implementation is still a way off. All other applications currently only exist in prototype. Perhaps in a hypothetical future where code literacy is far more common and code more predictable and reliable, such contracts might become more commonplace. For the foreseeable future, demand will likely only be found for simple contracts whose code can be easily verified and understood by many. The only meaningful existing blockchain contract applications relate to simple time-programmed payments and multisignature wallets, all of which are performed with the currency of the blockchain itself, mostly on the Bitcoin network.

c. **Database & record management:** Blockchain is a reliable & tamper-proof database and asset register, but only for the blockchain's native currency, and only if the currency is valuable enough for the network to have strong enough processing power to resist attack. For any other asset, physical or digital, the blockchain is only as reliable as those responsible for establishing the link between the asset and what refers to it on the blockchain. There are no efficiency or transparency gains from using a permissioned blockchain here, as the blockchain is only as reliable as the party that grants permission to write to it. Introducing blockchain to that party's record-keeping is only going to make it slower, while adding no security or immutability, since there is no Proof-of-Work. Trust in third party intermediaries must remain, while the processing power and time required for running the database increases. A blockchain secured with a token could be used as a notary service, where contracts or documents are hashed onto a block of transactions, allowing any party to access the contract and be sure that the version displayed is the one that was hashed at the time. Such a service will provide a market for scarce block space, but is unworkable with any blockchain without a currency.

III. The economic drawbacks of blockchain technology

From examining the above three potential applications of blockchain technology, four main obstacles to wider adoption are identified.

a. **Redundancy:** Having every transaction recorded with every member of the network is a very costly redundancy whose only purpose it to remove intermediation. For any intermediary, whether financial or legal, there is no sense in adding this redundancy while remaining an intermediary. There is no good reason for a bank to share a record of all its transactions with all banks. There is also no legitimate reason for any bank to want to have complete records of other banks' dealings with one another. This redundancy offers increased costs for no conceivable benefit.

b. **Scaling:** a distributed network where all nodes record all transactions will have its common transaction ledger grow exponentially faster than the number of network members. Thus the storage and computational burden on network members will eventually become too large for network members to handle as the network size grows. Blockchains will always face this barrier to effective scaling, and this explains why as bitcoin developers search for solutions for scaling, they are moving away from the pure decentralized blockchain model towards having payments cleared by intermediaries off the blockchain. There is a clear trade-off between scale and decentralization. Should a blockchain be made to accommodate larger volumes of transactions, the blocks need to be made larger, which would raise the cost of joining the network, and result in fewer nodes, making the network more centralized. The most cost-effective way to have a large volume of transactions is centralization in one node.

c. **Regulatory Compliance**: Blockchains with their own currency, such as Bitcoin, exist orthogonally to the law, as there is nothing that any government authority can do to affect or alter their operation, and the Federal Reserve chair has said it has no authority to regulate Bitcoin. Transactions will clear if valid, and will not clear if not valid, and there is nothing that regulators can do to overturn the consensus of the network processing power. Applying blockchain technology in heavily regulated industries such as law or finance, with currencies other than Bitcoin will result in regulatory problems and legal complications. Regulations were designed for an infrastructure very different from that of blockchain and the rules cannot be easily tailored to fit blockchain operation, with the radical openness of having all records distributed to all network members. Further, blockchains operate online across jurisdictions with different regulatory rules, making it difficult to ensure compliance with all rules.

d. **Irreversibility:** With payments via intermediaries, human or software errors can be easily reversed by appealing to the intermediary. In a blockchain, things are infinitely more complicated. Once a block has been confirmed and new blocks are being attached to it, it is only possible to reverse any of its transactions by marshalling 51% of the processing power of the network to engage in a 'hard fork' of the network, where all these nodes agree to move simultaneously to an amended blockchain. Blockchain technology, after all, is meant to replicate cash transactions online, and they will thus replicate the irreversibility of cash transactions, and not carry any of the benefits of custodial intermediation.

   In most likelihood, such a fork will never succeed if tried with Bitcoin, as it would require far too many disparate actors to agree and expend resources for no gain. After the DAO incident, it has become apparent that for any blockchain other than bitcoin, the network hashrate is small enough, and the designers of the currency influential enough, to overturn parts of the blockchain that they do not like. This means that blockchain technology's claim to 'immutability' is only really valid in the case of Bitcoin. For any other blockchain, the operators of the blockchain, or a regulatory authority, could in fact change the record. A blockchain that is alterable is a completely pointless exercise in engineering sophistry: it uses a very complex and expensive method for clearance to remove intermediaries and establish immutability, but then grants an intermediary the ability to overturn that

immutability. Current best practice in these fields contains reversibility and supervision by legal and regulatory authorities, but employs cheaper, faster, and more efficient methods.

e. **Security:** The security of a blockchain database is entirely reliant on the expenditure of processing power on verification of transactions and proof-of-work. Blockchain technology can best be understood as the conversion of electric power to verifiable undisputed records of ownership and transactions. For this system to be secure, the verifiers who expend the processing power have to be compensated in the currency of the payment system itself, to align their incentive with the health and longevity of the network. Should payment for the processing power be made in any other currency, then the blockchain is essentially a private record maintained by whoever pays for the processing power. The security of the system rests on the security of the central party funding the miners, but it is compromised by operating on a shared ledger which opens up many possibilities for security breaches to take place. A decentralized system built on verification by processing power is more secure the more open the system, and the larger the number of network members expending processing power on verification. A centralized system reliant on a single point of failure is less secure with a larger number of network members able to write to the blockchain, as each added network member is a potential security threat.

IV. Blockchain technology as a mechanism for producing digital cash

The only commercially successful application of blockchain technology so far is digital cash, and in particular, Bitcoin. The most common potential applications touted for blockchain technology, payments, contracts, and asset registry, are only workable to the extent that they run using the decentralized currency of the blockchain. All blockchains without currencies have not moved from the prototype stage to commercial implementation because they cannot compete with current best practice in their markets. Bitcoin's design has been freely available online for almost 8 years, and developers can copy and improve on it to introduce commercial products, but no such products have appeared.

The market test shows that the redundancies of transaction recording and proof-of-work can only be justified for the purpose of producing a digital cash and payment network without third party intermediation. Digital cash ownership and transactions can be communicated in very small quantities of data. Other economic cases which need more data requirements, such as mass payments, contracts and asset registry quickly become unworkably cumbersome in the blockchain model. For any applications which involve intermediaries, the blockchain will offer an uncompetitive solution. There cannot be wide adoption of blockchain technology in industries reliant on trust in intermediaries, since the mere presence of intermediaries makes all the costs associated with running a blockchain superfluous.

Good engineering begins with a clear problem and attempts to find the optimal solution for it, which not only solves the problem, but also does not contain within it any irrelevant or superfluous excess. Bitcoin's creator was motivated by creating a "peer-to-peer electronic cash", and he built a design for that end. There is no reason to expect that it would be suited for other functions. After eight years and millions of users, it is safe to say his design has succeeded in producing digital cash, and, unsurprisingly, nothing else. This digital cash can have commercial and digital applications, but it is not meaningful to discuss blockchain technology as a technological innovation in its own right with applications in various fields. Blockchain is better understood as a mechanism for creating digital cash. It is but a cog in the wheel of digital cash.