Blockchain: Trust in and with what?

Clément Jeanneau,
cofounder of Blockchain Partner

Abstract:
As the Internet has done with information, blockchains decentralize value. Cybernauts can, on a blockchain, create and exchange assets with other, selected cybernauts almost instantaneously without any third party's permission. Uses of this technology are now springing up in various fields. However they imply trusting a technology that often seems complex and has been controversial. Trusting a blockchain depends on understanding its principles, its new features and — beyond the praise without caveats for this innovation — its limits.

In October 2015, *The Economist* devoted its front page to a topic not familiar to the public: the blockchain, described as a machine for creating confidence.[1] This cover story launched a frenzy about an innovation with possibilities and limits that have, since then, often been poorly perceived. Seen as complex, even obscure, blockchains have become the archetypical "buzzword" stirring up excitement among some but irritation among others. Nouriel Roubini, an economist in the latter group, even wrote about a "*fraud*" and the "*most overhyped and least useful technology in all of human history.*"[2] Nothing less! This very cleaving opinion is evidence of the disproportionate reactions, laudatory as well as severe, to blockchains.

More than ten years after its invention and five years after its entry in the media, this technology deserves a less impassioned analysis. Can we trust blockchains, which claim to do without a trusted third party? If so, for what concrete uses? These questions are addressed herein.

A misunderstanding from the very start

The topic of blockchains was food for worms from the start, whence all the controversy. There is no consensus about how to define a blockchain. This is a matter not just of the choice of the words for describing this technique but also of this technique's perimeter. For instance, although a blockchain is a decentralized database (shared by all users and operating without a central, controlling authority), not every decentralized database is a blockchain. To be one, the database has to have supplementary characteristics, but the list of these characteristics is a subject of debate. A typical example: is a decentralized database a blockchain if the permissions for reading or writing in it are reserved for specific parties? Most players in this sector will answer "Yes, potentially", but on condition that we talk about a "private blockchain". However purists will answer "No". For them, a blockchain is meaningful only in a "public" version with permissions open to all.

[1] This article, including quotations from French sources, 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. All websites were consulted in June 2021.

[2] In his article "La grande escroquerie de la blockchain", *Les Échos*, 30 October 2018, available at https://www.lesechos.fr/idees-debats/cercle/la-grande-escroquerie-de-la-blockchain-143986.

The grounds of trust: A consensus protocol

This is not a minor issue. Confidence in a blockchain depends on how information is written to it and managed. It thus depends on what is called the "consensus protocol" — how the parties on a blockchain agree about recording and managing its data, in particular about how to authenticate the data. This protocol is the very ground that enables this machine to produce (or not) confidence. In brief: if the consensus protocol is deemed weak, confidence in the data will be flimsy; if it is robust, confidence will be strong.

The blockchain with what is widely considered to be the most robust consensus protocol is the very first one. Invented in 2009, Bitcoin reflected the deficit of confidence resulting from the financial meltdown. Its consensus protocol is based on an algorithm called "proof of work". To summarize, this algorithm relies on the work done by others, entities and individuals. These so-called "miners" compete with each other to solve as fast as possible a complex mathematical problem for the purpose of confirming a transaction on the blockchain. The first to solve the problem receives a financial reward. The transaction then validates this registration of data on the chain (like a ledger or registry). Each transaction is thus associated with a (small) set of data.

Why was Bitcoin novel at the time of its invention?

Confidence in the Bitcoin blockchain stems from the unusual combination of a technological layer (the consensus algorithm, asymmetric encryption, a peer-to-peer network and a distributed registry) with a layer of economic incentives. In short, it is more profitable for a party with strong computing power to take part in the network's activity (by trying to validate transactions) than to attack it (by trying to commit an act of piracy, which is out of reach of nearly all entities). The more computing power an entity has, the more chances it has to be the first to solve the mathematical problem and win the reward for validating a transaction. Were we to apply the too overused word "revolution" to blockchains, it could more appropriately be applied to this combination. The Bitcoin blockchain is not infallible, nor is any information system. To borrow the words of Gérard Berry, a major French computer scientist, a "*system is secure not when it cannot be attacked — which is theoretically impossible — but when attacking it costs too much.*"[3] This principle underlies the Bitcoin blockchain, now one of the safest of all public blockchains.

This does not mean that the Bitcoin blockchain is ideal in every aspect. Among its principal disadvantages, mention is often made of its high energy consumption and, too, its bit rate for validating data. For the sake of security, this rate is slower than the rate on other blockchains. In fact, no blockchain is "better" in an absolute sense. Everything depends on the criteria that users deem important in relation to their needs.

Nor does this mean that the Bitcoin blockchain was a totally new invention. Its anonymous inventor, going under the pseudonym of Satoshi Nakamoto, had dug through decades of academic research. Nearly all of Bitcoin's technical components came from research studies published in the 1980s and 1990s.

[3] DE LA PORTE X. (2016) "Le Grand Entretien — Gérard Berry: L'ordinateur est complètement con", 21 November, available at https://www.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE7684/gerard-berry-l-ordinateur-est-completement-con.html.

Digital scarcity, the first product of blockchains

Bitcoin's originality derived from a combination of elements that had never been associated with each other. Bitcoin was not the first cryptocurrency, but it was the first to incorporate the idea of a consensus algorithm for preventing double spending (spending the same coin twice). Had this problem not been solved, there would not have been any confidence in bitcoins.

The Bitcoin blockchain is based on an unprecedented combination of several innovations (in game theory, cryptography and computer science, to mention but a few fields). These made it possible to do what had never been done: send a unit of value on line from one party to another without any duplication nor the intervention of a trusted third party. In other worlds, this blockchain produced the possibility of "digital scarcity". When cybernaut A sends a file (text, image, sound, video) to cybernaut B, he is sending, in fact, a copy, since the initial file remains on his terminal. With Bitcoin, it has become possible to send peer-to-peer digital scarcity, thus without going through a central authority (*e.g.*, a bank).

A blockchain is to value what the Internet is to information

Why is this important? Because what holds for Bitcoin holds for many other digital assets that can be exchanged on a blockchain (whether bitcoins or other cryptocurrencies such as its principal alternative, Ethereum). These assets, which any cybernaut may create, are called "tokens" — in relation to the idea of "tokenization", of creating (on a blockchain) a digital representation of assets (stock, bonds, real estate, etc.).

Ultimately, a blockchain is to value what the Internet has been to information. The Internet has made it possible to decentralize information by giving every cybernaut the unprecedented power of publishing and exchanging information instantaneously with any- or everyone without having to ask for permission. A blockchain makes it possible to decentralize value: any cybernaut may use this new power to create an asset of value and exchange it with any cybernaut he has chosen (nearly) instantaneously without needing a third party's permission.

Confidence in what uses?

Our interest in blockchains as a generator of confidence very much depends on our interest in their uses. As explained, the very first use was for the creation and exchange of digital assets without middlemen. This is what the public has retained about cryptocurrencies, and with what firms have been experimenting in recent years for applications in finance and real estate (in line with the idea of tokenization). For instance, the banks Santander and Société Générale started experimenting in 2019 with tokenizing bonds on the Ethereum blockchain.

Managing digital assets on a blockchain allows the parties to the transaction to skip intermediaries, since the processes of emission and exchange are automated. Accordingly, firms can reduce costs, constraints and delays and, for certain operations, limit the risks related to a counterparty. These uses are part of the rationale of optimization for players in finance. In addition, they might open new possibilities, such as making it easier for small businesses to gain access to capital markets or for new products and financial services.

Beyond finance: Other examples of applications

Finance and real estate are not the only fields concerned. The concept of digital scarcity — the very grounds of the ownership, portability and traceability of natively digital assets — opens new fields that a growing number of players can explore: in sports (the idea of digital trading cards of professional players, as proposed by SoRare, a promising French startup that has signed contracts with the big European soccer clubs), in luxury goods (the idea of "digital clothing"), in art and in gaming.

Far from digital assets is the more traditional use of a blockchain as a registry (or ledger). In this case, the chain serves to prove that digital documents or data existed at a given time. This application could prove useful in the field of intellectual property (in the form of a digital "Soleau envelope" as proposed by Datatrust) or as proof of the integrity of digital data or documents. This is the reason that blockchains are now being used to fight against fakes.

Various applications exist in the economy but are still poorly known. In France alone, we might mention: institutions of higher education that are using blockchains to certify diplomas (*e.g.*, ESCP and EM Lyon via the startup BCDiploma); groups listed in the CAC 40 (such as Renault, Natixis, Bouygues and Crédit Agricole via the Wiztrust platform based on Datatrust) that use the Ethereum blockchain to authenticate their press releases and thus fight against "fake" financial news; Kering, a multinational that has been using the Bitcoin blockchain for over a year now to register the digital certificates of authenticity of its Ulysse Nardin watches; or even organizations in social housing (*e.g.*, Immobilière 3F) or the construction industry (*e.g.*, Léon Grosse), which use the Bitcoin blockchain (via the platform ContractChain) to guarantee the conformity of contracts.

A private blockchain might also be of interest for organizing efforts between parties who do not initially trust each other and/or have problems working together: rival firms, distant partners, firms in the same value chain, entities within a single industrial group, etc. Thanks to the decentralized registry, which is technically distributed between all parties, the political problem of its ownership is settled.

At the Bank of France

A last use worth mentioning is the Madre interbank blockchain developed by the Bank of France. This private blockchain was rolled out in 2018. Till then, the Bank of France collected requests for the SEPA creditor identifiers sent by merchant banks for their clients' accounts; and it managed these identifiers. It decided to decentralize the registry, which has become a blockchain distributed between itself and the merchant banks. Each player thus has a transparent database without any more control over it than the others.

Furthermore, the Bank of France has used "smart contracts" — automatic programs that, integrated in the blockchain, contain reliable specifications (SIREN numbers, etc.) — to automate the process of assigning identifiers and recording them in the registry. This new system has reduced processing time from several days to a few minutes.

A digital economy… to come

In the immense majority of cases however, a blockchain is not of much more interest than a traditional database. This technology is not intended to become the standard for data management. It satisfies very specific needs, as pointed out. We should not lose from sight that it is not private (or closed) blockchains that deserve attention. Though of interest to organizations, private blockchains are the equivalent of intranets in relation to the open Internet. Based on the concepts of digital scarcity and tokenization, blockchain applications have meaning only if the blockchain is open, thus opening the way toward a new digital economy.

Despite advances in recent years, there is the need to facilitate uses, confidentiality and speed so that this economy can take off on a large scale. This will still take several years. It should not be precipitated to the detriment of requirements related to reliability, which are the price to pay for end users to actually trust blockchains.