Blockchain Technology, Challenges and Opportunities

Vijay Mathur, Ravinder Yadav

Abstract - **Blockchain technology [1] poses a daunting challenge to democracy. It allows both participatory and decentralized governance, but is also the expression of unbridled liberalism, the enemy of democracy. In this paper, we are attempting to provide an overview of Blockchain, its characteristics and the challenges and opportunities of Blockchain technology.**

Index Terms: Blockchain, Decentralized, Distributed ledger, Smart Contracts, Cryptocurrency

I. INTRODUCTION

At a time of the crisis of confidence and dissatisfaction with third parties and traditional mediators, institutions, banks and States, blockchain technology, which carries the promise of disintermediation and transparency, seduces and intrigues. The term “blockchain” appeared in 2008 and since then we have seen a growth in projects based on this technology. It is often presented as a breakthrough innovation, as important as the birth of the printing press or the Internet. Its potential impacts could revolutionize our economic systems and our ways of exchanging: the blockchain is capable of profound transformations in many fields of application. It can both represent a threat, either in its intentions or in its use, by creating systems of trust based on mathematical laws which would overcome democratic requirements or an opportunity for democracy, if it is used well. Above all, this technology holds the promise of new governance, locally and globally, based on innovative principles: collaboration, decentralization and transparency. States and the European Union are keenly interested in the evolution of blockchain technology and its potential for the social economy. The European Economic and Social Committee is currently preparing an own-initiative opinion on the issue of blockchain and the social economy, which should be adopted in July 2019.

Blockchain designates a block chain [2] on which information of all kinds is stored. Blockchain is generally defined as "technology for storing and transmitting information, transparent, secure, and operating without a central control body". Blockchain is a distributed ledger technology, or DLT (Distributed Ledger Technology), which groups digital systems that record asset transactions and their details in multiple locations at once. Blockchain is the best known DLT technology. A blockchain constitutes a database which contains the history of all the exchanges made between its users, and this, since its creation.

Vijay Mathur, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India

Ravinder Yadav, Department of Technology, Shivaji University, Kolhapur, Maharashtra, India

To represent it, the image of the general ledger is frequently used: the blockchain can be compared to a vast public register integrating all the exchanges made by its users since its creation. One of its main features is that it cannot be changed. The blocks are protected by several innovative cryptographic processes which make modification impossible. This is what gives this technology its transparent nature: you can only add operations, but not modify or delete them, they are tamper-proof. This technology is based on a decentralized peer-to-peer system: the data is not hosted by a single server but distributed between users, without intermediaries. Part of the users hold copies of the blockchain, which is therefore found everywhere in the world. These hundreds of copies are constantly updated simultaneously. Unlike traditional databases, which are administered by centralized operators, the blockchain is administered collectively, by all the nodes of the network. These nodes all obey the same computer protocol, which defines the procedures to be followed, as well as the conditions to be respected to update the database.

Concretely, blockchain technology takes the form of a register which lists data, generally transactions, grouped in blocks linked together. A block is simply a set of information put together, and the blocks are linked together irreversibly (by chains). Each block is validated by the nodes of the network, user-validators called "miners". Once validated, the blocks are time-stamped and integrated into the block chain, accessible to all users. The transaction is then visible to the receiver as well as the entire network. Minors are paid via tokens. The only way to modify the blockchain is to add a block: it is not possible to change an existing block or modify the chains.

II. CHARACTERISTICS OF THE BLOCKCHAIN

Several characteristics [3] are associated with blockchain: disintermediation, traceability, transparency, distributed consensus, indelible, distributed structure, resilience, security and trust. All these characteristics constitute the innovative potential of blockchain. The main characteristics of blockchain technology are:

A. Disintermediation

Blockchain technology allows trading without the control of a third party. The validation and the addition of a block result from a consensus between the user-validators, which rests on the possibility of verifying their validation work and which makes control by a reference institution unnecessary. All is done without the intervention of a central authority, users operate monitoring and control each other, ensuring the certification of backups and their consistency. The trusted third party, a bank for example, is traditionally the only way to ensure that a transaction is

valid, that is to say that the data (most often money) has actually been transferred from person A to person B, and that person A is therefore no longer in possession of the initial data. Blockchain allows trust to be based solely on technology and on the possibility for everyone and at any time to control operations and their validation. Trust is distributed here and no longer requires an intermediary.

The blockchain is thus decentralized both politically (no one controls it) and architecturally (no central infrastructure). However, promising it may be, this extreme disintermediation can pose many problems. The lack of control and regulation by a third party facilitates litigious behavior such as, for example, the laundering of illegal activities. Likewise, there is the question of arbitration in the event of a dispute, given that there is no one, no institution to turn to in the event of a malfunction.

B. Transparency

Once a document is registered on the blockchain, this is enough to prove that the latter exists at time T and that it has not been modified. The blockchain is qualified as transparent because everyone can download it in its entirety and check its honesty at any time. All blockchain users can view current and past transactions. If transparency is ensured for transactions, user anonymity calls into question this characteristic. Indeed, possible anonymity on the blockchain can be used for fraudulent activities that are difficult or even impossible to detect and regulate.

C. Security

Decentralized hosting also makes blockchain a secure technology: it makes it almost impossible to delete all copies of documents, which exist on a multitude of servers around the world. The blockchain has great resistance, because all the data is copied to the different servers. This makes it resistant to cyber-attacks or state control. Indeed, if it is possible to attack one or more computers, it is more complicated to attack the blocks of information copied in all the computers connected to the network. This provides the blockchain with a high level of security. The blockchain is therefore considered unassailable and inviolable. However, this also makes it difficult to regulate.

D. Autonomy

The computing power and the hosting space are provided by the nodes of the network, that is to say the users themselves. There is therefore no need for central infrastructure. Within a blockchain, the infrastructure is no longer concentrated in the hands of an organization but is, on the contrary, dispersed in all the points of the network. A blockchain is therefore self-supporting and independent of third-party services. Blockchain is the underlying architecture of bitcoin cryptocurrency, which remains the best-known use case today. The first function of the blockchain was therefore the transfer of financial assets. But this technology is constantly evolving and is the basis of many other applications than a payment network. Today it is also used by other players and operations and data are not necessarily financial.

1) Smart contracts automatically execute actions validated beforehand by stakeholders: the Axa insurance group has, for example, tested the automatic reimbursement of delayed flights via this type of contract.

2) Electronic voting was tested by the city of Zug (Switzerland) in 201822.

3) The certification of copyright, as proposed by the start-up Mediachain which allows artists to deposit their creations on the database, while keeping control over them and their authenticity.

4) Product traceability offered by the Provenance platform.

5) The blockchain can be a tool for the implementation of digital complementary local currencies (MLC), like Lake Geneva, an MLC used in several French and Swiss municipalities. This makes it possible to better respond to the specific needs of the companies in the network and to guarantee better traceability.

6) It can also be used to set up more democratic systems of collaboration and governance, as we will see later in this note.

III. THE CHALLENGES AND OPPORTUNITIES OF BLOCKCHAIN TECHNOLOGY [4]

A. The stakes are technical Scalability.

Will the Blockchain protocols, which currently manage limited data, support the change of scale in the event of mass dissemination? The Bitcoin network, for example, processes a handful of transactions per second, compared to several thousand for a bank card operator. The blockchain's historical validation mechanism, with its multiple nodes and its cryptographic processes, is a source of slowness. Technical solutions go through less cumbersome validation mechanisms, but therefore less reliable.

B. The stakes are monetary and financial Volatility and speculation.

Built on blockchain technology, cryptocurrencies have multiplied in recent years: there are more than 1,500 today, with a total capitalization of more than 300 billion euros. But the great volatility of their prices prevents them from building sustainable economic models. The recent trajectory of bitcoin - with a surge in its price followed by a massive correction at the end of 2017 - has highlighted the speculative dimension of these crypto-assets. To combat this phenomenon, regulations comparable to those applied to the financial markets should be imposed, particularly with regard to price manipulation.

C. The stakes are security Failures and hacks.

Still largely experimental, the blockchain has been the subject of numerous hacks or bugs that undermine the promise of confidence and infallibility - even if the digital protocol of Bitcoin appears today unlikely to be faulted. Tension is emerging between the necessary streamlining of certification mechanisms and the weakening of blockchains. Fight against illicit activities. Cryptocurrencies also stand out for their ability - which varies with the degree of anonymity and traceability of transactions - to allow fraudulent payments (drugs, weapons, money laundering) or tax evasion. Fraudulent transactions would decrease in proportion but increase in absolute value. [5]The public authorities of many countries call for the strengthening of

policies to combat money laundering and the financing of terrorism (AML and KYC policies), by adopting the implementation methods specific to cryptocurrencies. Anonymity and traceability. The challenge is to reconcile - as with cash - legitimate expectations of anonymity, for the protection of privacy or business secrecy, and the objectives of traceability to fight fraud. Analysis tools are beginning to develop which allow operations to be traced beyond the pseudonym of transactions.

IV. BLOCKCHAIN OPPORTUNITIES FOR THE SOCIAL AND SOLIDARITY ECONOMY [6]

The social economy intends to respond to the challenge of loss of confidence in institutions with an innovative solution: co-construction, which relies on the strength of proposals from citizens, placed on a footing equality with public or private authorities. However, collective intelligence and cooperation are not easy to implement, particularly due to the lack of systems of recognition and traceability of everyone's contribution, which can discourage spontaneous sharing of information and ideas. [7] Blockchain technology allows collaboration between users and can therefore be a tool for the emergence of collective intelligence, by experimenting with new practices of shared innovation and contribution. It can generate new co-creation platforms and allow individuals to come together and collaborate in an open and decentralized manner, ensuring perfect visibility and traceability of the added value provided by each, encouraging individuals to innovate and share their ideas. The consensual decentralization of trust that the blockchain allows the reinforcement of the effective coordination capacities of individuals.

V. BLOCKCHAIN OPPORTUNITIES FOR FINANCIAL SECTOR [8]

Blockchain technology is also a source of new funding opportunities, which are also more democratic, in particular thanks to the disintermediation through which the institutions which traditionally govern and dominate the financial system, such as states and banks, lose their power in favor of modes of more horizontal funding. Funding is one of the biggest barriers for social economy organizations, which face significant start-up costs, but cannot attract investment in the same way as traditional businesses. [9] The blockchain is shaking up the rules of the classic digital economy. Thanks to blockchain, it is possible to appeal to a large multitude of Internet users for financing, without recourse to a third party. There are already several crowdfunding platforms already based on blockchain technology.[10] Blockchain funding also solves the problem of confidence in the actual allocation of funds, due to its transparency.

VI. CONCLUSION

The emergence of virtual currencies, based on cryptographic protocols, raises questions about their status as money in the classic sense of the term. In this article, we analyze the case of bitcoin. [11]We show that today it does not satisfy the usual functions of money. Its acceptability as a means of payment is limited, its volatility is too high to serve as a store of value and it is not used as a unit of account. However, the collaborative and decentralized technology, the blockchain, used to issue this currency and settle transactions, has the potential to modify the centralized organization of payment and settlement systems. [12] The lack of intrinsic value and legal tender results in high price volatility which does not allow it to fulfill traditional monetary functions. On the other hand, the block chain offers opportunities to modify the centralized and intermediated practices of the financial markets. This possible development will be accompanied by the emergence of operational and legal risks that regulators will have to assess and monitor.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang -An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

[2] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen - A Survey on the Security of Blockchain Systems

[3] Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi, Gary Wills - Blockchain with Internet of Things: Benefits, Challenges and Future Directions

[4] Huaimin Wang , Zibin Zheng , Shaoan Xie , Hong-Ning Dai , Xiangping Chen- Blockchain challenges and opportunities: a survey

[5] Brett Scott, John Loonam, Vikas Kumar - Exploring the rise of Blockchain Technology: Towards Distributed Collaborative Organisations

[6] Eric G. Krause, Vivek K Velamuri, Tobias Burghardt, Denny Nack, Moritz Schmidt, Tobias-Micha Treder - Blockchain Technology and the Financial Services Market State-of-the-Art Analysis

[7] Sarmah, Simanta Shekhar. "Understanding blockchain technology." *Comput. Sci. Eng.* 8 (2018): 23-29.

[8] Wang, Yingli, Jeong Hugh Han, and Paul Beynon-Davies. "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda." *Supply Chain Management: An International Journal* (2019).

[9] de Kruijff, Joost, and Hans Weigand. "Understanding the blockchain using enterprise ontology." *International Conference on Advanced Information Systems Engineering*. Springer, Cham, 2017.

[10] Baliga, Arati. "Understanding blockchain consensus models." *Persistent* 2017.4 (2017): 1-14.

[11] Seebacher, Stefan, and Ronny Schüritz. "Blockchain technology as an enabler of service systems: A structured literature review." *International Conference on Exploring Services Science*. Springer, Cham, 2017.

[12] Holotescu, Carmen. "Understanding blockchain opportunities and challenges." *Conference proceedings of» eLearning and Software for Education «(eLSE)*. Vol. 4. No. 14. " Carol I" National Defence University Publishing House, 2018.