Digital Assets Cryptocurrencies and Blockchain

Primavera de Filippi

4. Digital Assets Cryptocurrencies and Blockchain

Primavera De Filippi[1]

The interplay between blockchain technology and the law raises important questions and challenges. At the same time, we can look to fit the technology into a particular regulatory framework and see the opportunities that blockchain provides as a regulatory technology itself.

First, it is important to note that blockchain is a particularly difficult technology to regulate, especially due to its decentralized and persistent nature. The fact that a blockchain exists on the Internet, a global network that does not account for national boundaries and is very difficult to shut down, means that as long as there is one node that holds one copy of the blockchain, it is possible to replicate the blockchain. There is no single point of failure or control.

Its technical design is tamper-resistant, such that it is very difficult to manipulate the content, and therefore, to modify the information once it has been stored in the blockchain. It is inherently transparent by definition because it relies on distributed consensus, so every participant must be able to verify the accuracy and legitimacy of the transactions. It is also non-repeatable. Once a transaction has been executed in the blockchain, because it is signed by the private key by the person who has executed it, the person can hardly deny having executed this transaction. The majority of public blockchains are pseudonymous, meaning

[1] Primavera De Filippi is a permanent researcher at the national center of scientific research in Paris, in a faculty associated with the Berkman Klein center for internet and society, at Harvard University.

everyone can participate in the network without having to identify themselves to other particular operators. Finally, the most sophisticated and modern blockchains deploy *smart contracts*[2], guaranteeing execution. With smart contracts, one can be sure that a particular software will always execute as it has been codified, and that no third-party can influence the execution of that software.

The first cryptoassets to emerge from the technology were cryptocurrencies, independent of any central bank or government structure. Such freedom led to a dynamic ecosystem of designs. **Zcash** and **Monero**[3] built their foundations like **Bitcoin**[4] but added some layers of anonymity and financial privacy on top of it. Then came **Ethereum**[5], a general-purpose blockchain that enables layers of codifying and programming tokens to achieve a particular purpose. Unlike a traditional application that runs on a centralized server controlled and operated by the person maintaining it, **Ethereum** introduced the possibility of creating applications that are run in a distributed manner by all nodes in the network, with the code executed in a deterministic manner, so everyone knows exactly what will happen.

2016 saw an explosion of new types of cryptoassets, boosted by widespread use of the ICO.[6] The business model of many new applications was tokenization: creating their own cryptoassets specifically designed to run with a particular

---

[2] Smart Contracts are computer protocol designed to facilitate negotiation between unknown parts without intermediation of a central authority.

[3] Zcash and Monero are private, decentralized, open-source cryptocurrency that respect the anonymity of those involved.

[4] Bitcoin is considered the world's first decentralized digital currency.

[5] Ethereum is a decentralized platform for smart contracts and decentralized applications using blockchain technology. On this platform there is the cryptocurrency called **Ether** used in smart contracts

[6] Initial Coin Offering – ICO -unregulated method of raising funds for new ventures or cryptocurrency projects.

blockchain or the application deployed on top of a blockchain. The cryptoassets have defined functions and values, and the proliferation of many new typologies led to a wide variety of distributed applications.

The original typology is, of course, cryptocurrencies, which used to be called **Altcoins**[7], essentially a cryptoasset that is inherently associated with the functioning of the underlying blockchain to which it is associated. **Bitcoin**, **Ethereum** and **Dogecoin**[8] are all such tokens that are intrinsically part of their particular blockchain, and their value is inherently dependent on the supply and demand of the desire for people to purchase these tokens.

The ICO boom led to utility tokens, a new type of token not inherently associated with a particular blockchain but rather with a decentralized application on top of a blockchain. Utility tokens offer access to the services provided by a particular application deployed on a blockchain. The value of utility tokens is a combination of use value (the value of access to services) and market value (the speculative value independent of its use value).

Another typology is governance tokens, which provide a particular set of privileges or decision-making power to those that hold them. The more of these tokens one holds, the more influence they have in the governance of a particular application. Governance tokens are not always transferrable, though some are. Their value is similarly a mixture of use value (in this case, the benefit of being able

[7] Altcoins are cryptoassets with some modification of internal parameters of the bitcoin network
[8] Dogecoin, created in December 2013 as a "joke coin" is a peer-to-peer open-source cryptocurrency.

to influence the governance of an application) and market value (if they are transferable, in terms of supply and demand).

Lastly, there are investment tokens, which basically represent shares and dividends from a particular organization, which can be either a traditional organization or a decentralized organization specific to a blockchain. Here the value of the token is essentially based on market value and dividends.

There was much debate as these tokens emerged about how their appeal was different from a traditional IPO, and there was a strong consensus that they are not the same because there is no company behind them. But as the space has evolved, many companies started using these tokens as a way of not selling shares, but still selling a particular investment. There was an explosion of scams, especially in 2017 and early 2018, due to a lack of regulation making it very difficult for investors to distinguish a serious project from a scam.

These new types of tokens actually have a symbiotic relationship with cryptocurrencies like **Ether** or **Bitcoin**, since people need to purchase these cryptocurrencies to be able to purchase these tokens; after all, one could not purchase the tokens with normal currency. This relationship has created wild speculative dynamics for the market value of cryptocurrencies: speculating on these tokens meant purchasing more cryptocurrency to purchase more tokens, up to the point where the bubble collapsed.

Another emerging speculative trend is in the domain of decentralized finance. Many fintechs use technology to optimize and create specific financial applications,

but they are traditionally banks or specific operators that control people's assets. The idea of decentralized finance is based on the principle that individuals maintain the custody and control of their own cryptoassets. Decentralized finance applications are hybrid financial instruments. On one hand, legacy instruments like existing currency or gold can be tokenized, issued, traded, and settled via a blockchain. On the other hand, cryptoassets are also being wrapped into a more legacy framework. Existing financial institutions and fintech applications enable the trading and settlement of cryptoassets on these legacy systems.

There are also different typologies of decentralized finance applications, each of which rely on blockchain technology to increase transparency and accountability and reduce operational risk. For instance, **Maker**[9] created a stable coin via a system of collateralized positions and a specific token that ensures the stability of the system. Other typologies are open lending protocols, prediction markets, and decentralized exchanges, which try to maximize liquidity in order to be able to transfer assets at any moment.

As always, new issues have emerged, such as when someone copy-pasted the code of **UniSwap**, a popular decentralized exchange, and added a token on top, creating **Sushiswap**. Of course, as soon as there is a token, everyone wants to acquire the token. Sushiswap managed to extract all the liquidity from UniSwap into their own liquidity pool. From a regulatory perspective, it is very complex to understand whether they have done anything wrong. It is unclear whether there is a

[9] Maker Protocol the smart contracts that drive the Dai, a cryptocurrency with a stable price.

claim for antitrust, or what kind of regulatory framework could prevent such activities, especially since such an easy transfer of liquidity from one system to the other is impossible in a traditional legacy framework.

There are all kinds of questions with decentralized applications. It's a similar situation to that of ICOs, which began entirely non-regulated, and governments needed to identify how to bring them under an existing regulatory framework. And it's also similar to the early days of the Internet, when its transnationality and decentralization made it difficult for the law to actually regulate the Internet itself. Certain operators and platforms, though, became dominant entry points for many online services. Thus, the regulators, instead of trying to regulate individuals on the Internet, focused on these online operators, shaping the architecture of the platform to indirectly regulate the individuals.

This solution cannot be replicated perfectly in the blockchain ecosystem, however, because the obvious intermediary or trusted authority that could be regulated by the law seems to disappear. The big question now is what levers can the law use to regulate, directly or indirectly, the operations on a blockchain network.

In a blockchain-based system, who are, if any, the new intermediaries? The developers could be held responsible and obliged to implement specific types of functionalities. This is easy for an online platform operator, who can simply change the code of the platform, but blockchain developers don't necessarily have that capability. A developer could modify the code, but if the software is not adopted by the network of users, the developer doesn't have much power.

A focus instead on the miners and validators ensures that any change in the protocol of a blockchain is adopted or that specific transactions are censored. But the miners also do not have full powers; the blocks they choose still have to be accepted by the other nodes of the network.

It is a tripartite, polycentric system of governance, and none of those groups alone have sufficient power to influence the blockchain. Any impact on the network will require distributed consensus among all of them.

Still, there are new large and powerful operators who do not necessarily have more power than others, but in practice, they have a lot of power in the social and political realm around a blockchain community. Influencers, founders of a project, the technically savvy, those on social media: they all have power to influence the governance of these networks. Mining pools have tremendous power over which blocks should be mined and which transactions should be prioritized or censored. Large operators, such as cryptocurrency exchanges, blockchain explorers, or any commercial operator that people want to interact with, make impactful decisions, such as to follow a particular fork, that many users are arguably forced to follow as well.

There are three central figures, the core developers, miners, and validators, but many additional layers of social and political governance on top. Thus, it becomes much more difficult to regulate than the Internet, where **Google**, **Facebook**, and other operators we want to regulate are easily identifiable. It's difficult to govern many different actors at once.

At the same time, blockchain technology provides its own opportunity to regulate, bolstering the move from **FINTECH** into **RegTech**[10]. A system that harnesses the technological guarantees afforded by blockchain technology can help enforce traditional legal constraints.

It is important to distinguish between two types of equivalences. The traditional model of functional equivalence is to consider the electronic contract to be a functional equivalent to a paper-based contract. The idea is that a characteristic application of a particular technology can be held to be equivalent to another type of activity, which is itself subject to regulation. If there is equivalence between them, they are considered subject to the same rule. The question is whether smart contracts can be regarded as functionally equivalent to existing contracts, and whether the signatures for a transaction on a blockchain can qualify as an electronic signature. The other, more complicated concept of equivalence is regulatory equivalence, and here the question is not whether a particular technology or activity is equivalent to another, but whether there are alternative means to achieve the same regulatory objectives.

A good example to illustrate this dichotomy is the sale of tokens. Issuing tokens to the public could be considered, in certain circumstances, to be functionally equivalent to an IPO; a token sale would then be subject to the same regulatory framework as IPOs or security issues. But one of the specific regulatory goals that justify regulation is protecting investors from getting involved in scams and non-

[10] Regulatory Technology (RegTech)- new technology that uses information technology to improve regulatory processes.

transparent investments. If blockchain technology can reduce risk for investors, then even if it is functionally equivalent, there is also regulatory equivalence and therefore, some of the formalities that must be fulfilled by IPOs could be achieved via technological means, to the extent they have the same regulatory objective.

Another use of blockchain as a regulatory technology is regulatory compliance, either for privileged identity management or for auditing (i.e., automated reporting of executed transactions). If a party automatically provides a constant report on all transactions, it's easier to audit the operators. With such transparency, the operators can no longer pretend they made a transaction when they did not, and they cannot hide a transaction they in fact made, because everything was stored in and retrieved from the blockchain. One no longer needs to trust that the operator will act as a fiduciary institution in the interest of their client. The technology automatically enforces this. Hence, there is no possibility for the operator to breach their fiduciary duties.

Blockchain also affords traceability (recording every step of a process), and thus verifiability of execution. This is crucial for manufacturing, distribution, internal corporate processes, certifications, and many other applications. This also ensures the integrity of information and that data has not been manipulated, which has immense and cascading benefits.

Blockchain technology in so many ways helps promote regulatory objectives. This is, indeed, the interplay between rule of law and rule of code, which can conflict at times, but also be combined to create a more reliable system that instills confidence. The interesting challenge is to understand how existing law

enforcement can regulate these new decentralized applications and yet also come to rely on the technology to build back trust in their own institutions.

This is discussed at length in my book[11], so I thank everyone who reads it.

[11] De Filippi, Primavera & Wrigth,Aaron - *Blockchain and the Law: The Rule of Code*- USA Harvard University Press,2018