1

Non-centralized Architecture

The blockchain and the distributed registry technology allow us to solve the problem of certification of the transaction chain, without using a centralized system, to a trusted third party.

The term "decentralized", frequently used to refer to the blockchain or its applications, does not seem entirely appropriate to refer to the blockchain architecture. Indeed, decentralization is a movement from the center to sub-entities. In political science, for example, decentralization is a process by which entities, generally local, are given their own powers previously held by a central power, unlike deconcentration, a process by which the central power delegates powers at the local level to its representatives.

The blockchain architecture is not decentralized; it is part *ab initio* of parallel centralized or partially decentralized models, so the terms "distributed" or "non-centralized" seem more appropriate. The term "non-centralized" was preferred for this book because it explicitly marks an alternative to a centralized model and avoids a debate that has no place in this book between decentralized and distributed systems.

This typology, which is very frequently used not only on blogs [EAG 17] but also in books on the blockchain [RAV 16],

is generally associated with a diagram that presents the difference between centralization, decentralization, and distribution, based on a book by Paul Baran on distributed systems [BAR 62].

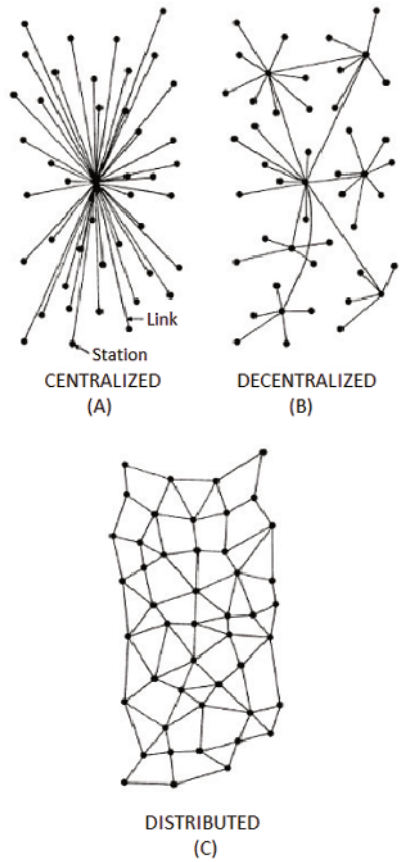

Figure 1.1. *Paul Baran's distributed system typology. Source: [BAR 62, p. 4]*

The diagram depicting centralization shows only one central point, the decentralization diagram shows a central point and several central sub-points, and the diagram on distribution shows one distribution mode among others, with a connection between the nearest nodes only (see Figure 1.1).

This schema is, wrongly, regularly used to present the blockchain as a decentralized model and to contrast the blockchain with distributed registers (of which the Bitcoin blockchain, for example, is a sub-category). The authors, using this schema to demonstrate that blockchains are decentralized and not distributed generally, later indicate that what makes the strength of a decentralized system compared to a centralized system is that there is no central point and that if a node fails the system persists[1]. Based on this schema (and on the concept of decentralization in general), this approach is wrong; there is indeed a central point and if it is missing, the system no longer works.

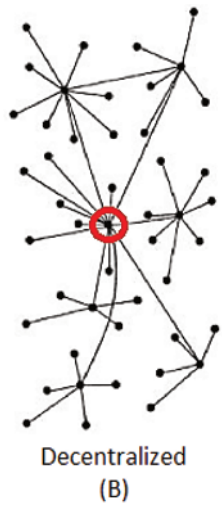

Figure 1.2. *Decentralized system. For a color version of this figure, see www.iste.co.uk/quiniou/blockchain.zip*

To repeat this diagram, the centralization point is surrounded; if it is faulty, none of the central sub-points are connected anymore.

1 See, for example, [RAV 16, p. 3]: "Bitcoin […]. It is also decentralized because if one node fails, the network is still able to operate".

It should be noted that the use of the notion of decentralization in the blockchain ecosystem has become widespread with Ethereum and smart contracts. For example, the Bitcoin seminal document did not refer to it and used the notions of peer-to-peer and lack of central authority, which is fundamentally different [NAK 09]. Vitalik Buterin, the founder of Ethereum, also indicated on his blog that there was confusion about the use of the notion of decentralization in the blockchain ecosystem and that the above-mentioned schema was "unfortunately too widespread" [BUT 17].

Blockchain networks, such as Bitcoin, are actually designed according to a particular form of distributed architecture, a peer-to-peer architecture, which could be transcribed by the diagram below. It is this network architecture, in which all nodes theoretically have a copy of the registry and participate in consensus, which is referred to in this book as the "non-centralized" architecture. All points or nodes are connected or potentially connectable to each other directly.

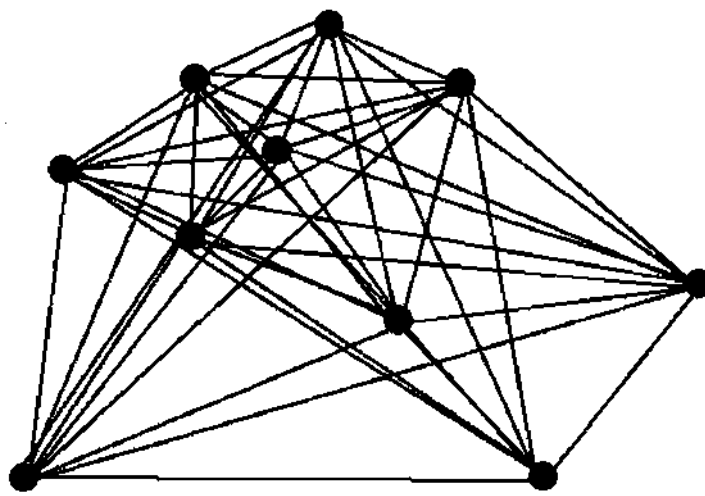

Figure 1.3. *Non-centralized egalitarian system*

Nevertheless, certain trends, such as the development of private blockchains, the concentration by certain groups or miners' pools of the computing power used to generate consensus, or the concentration of crypto-assets in a few portfolios, raise questions about the maintenance, in practice, of the non-centralization of certain blockchains.

A schema that more accurately transcribes a blockchain network could, therefore, be as follows:

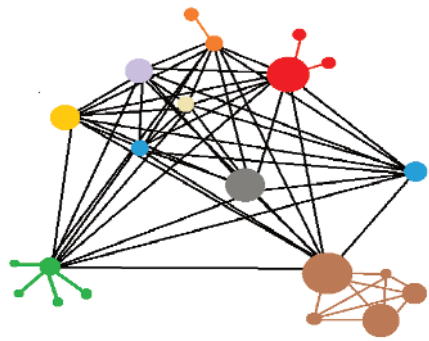

Figure 1.4. *A non-centralized system with variable and multi-level weighting. For a color version of this figure, see www.iste.co.uk/quiniou/blockchain.zip*

While certified timestamping of transactions and operations represents the initial and main use of the blockchain technology (section 1.1), these non-centralized ledgers also combine encryption and verifiability, anonymity and transparency (section 1.2) in a new way. Some usage implications can be discussed on the basis of this non-centralized architecture and its primary characteristics (section 1.3).

1.1. Certified timestamping of transactions, operations, and events in a non-centralized registry

The primary use of the Bitcoin protocol is to allow the bitcoin to be transferred from one portfolio to another or,

more accurately, from one key address to another, as well as to allow timestamping and certification of the transaction from the storage based on a distributed network.

A distributed registry or blockchain is based on a peer-to-peer network and a consensus algorithm that allows the duplication of the content stored and validated on the different nodes of the network.

1.1.1. *The network of nodes: the peer-to-peer architecture*

Nodes are connection points to the distributed network, nodes are peers, and nodes are equal connection points. In the Bitcoin network, full nodes download blocks and transactions and validate or invalidate them according to Bitcoin rules.

In the Bitcoin seminal document, the operation of the Bitcoin network is presented as being based on these nodes:

The steps to run the network are as follows:

1. New transactions are broadcast to all nodes;
2. Each node collects new transactions into a block;
3. Each node works on finding a difficult *proof of work* for its block;
4. When a node finds a proof of work, it broadcasts the block to all nodes;
5. Nodes accept the block only if all transactions in it are valid and not yet spent;
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

With the increase in computing power required for the proof of work, mining pools have been formed with an entity

operating as an administrator of the complete node and third parties assigning their computing power to this node.

It is these peer nodes and their common functioning that make the architecture of blockchains non-centralized.

1.1.2. *The timestamping system*

A timestamping system allows the Bitcoin proof-of-work system to operate and adjust the difficulty of mining the blocks.

Figure 1.5 represents, in the Bitcoin founding document, the block aggregation and timestamping system in the Bitcoin network:

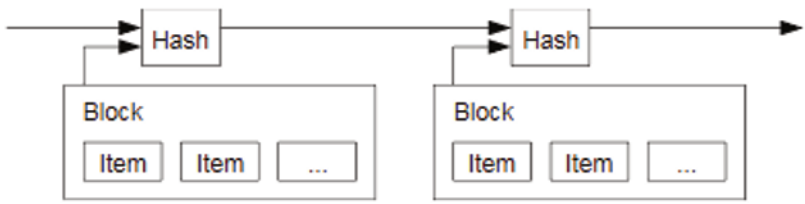

Figure 1.5. *Bitcoin timestamping system. Source: [NAK 09, p. 2]*

Mined blocks are timestamped and then published within these networks of non-centralized blockchain nodes, such as the Bitcoin blockchain. During mining, the miner's computer tool (mining rig) indicates the time at which the mining of the block begins. This time is expressed in Unix time, i.e. in seconds, since January 1, 1970.

This timestamping is at the heart of the proof-of-work system. If the computer clock is dysfunctional or deliberately incorrectly set, the block will be rejected beyond a certain margin of error. The block date must be greater than the median of the last 11 validated blocks and less than the

adjusted date from the node network plus 2 h. The time-stamping system of the Bitcoin blockchain is based on non-centralization of the network. Therefore, the timestamping of the Bitcoin protocol is only approximate and works by reinforcement, relying on previous block time-stamps and verification by the node network.

Mathematical researchers have verified, based on the history of the blocks of the Bitcoin blockchain, whether this precaution was necessary and have identified that out of 500,000 mined blocks up to November 2017, 13,618 blocks had dates earlier than the previous block and 1,000 of these blocks had an earlier date of more than 10 min [BOW 18].

The main objective of this timestamping system is to check the integrity of the mined blocks and adjust the difficulty of calculation. However, this timestamping system, despite its approximate nature, may have other uses and may make it possible, for example, to prove a prior art in a transaction or operation.

1.1.3. *Recording of transactions and other operations*

The Bitcoin blockchain is a transaction-oriented registry like a general ledger. The Bitcoin blockchain is not, as such, designed to store data other than that required for transactions; nevertheless, a text box has been provided for each block, which is the coinbase text (not related to the Coinbase exchange platform).

For example, it is in the text cornerbase of the initial block (genesis block) that the founder of Bitcoin inserted a reference to an article in *The Times*: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", to date it, i.e. to prove that this initial block was not prior to the date of this article (and that there was, therefore, no pre-mining) and, according to some commentators, to include Bitcoin in the line of cypherpunks or in opposition to the financial world.

The coinbase text is defined by the miner who discovers the block. However, since a consensus between miners[2], known as "BIP: 34", this text-based corner must contain the size of the block. It is no longer possible for a miner, wishing to have their block validated and integrated into the blockchain, to insert only the text of their choice[3].

The coinbase text is not the only way to integrate text or other data into the Bitcoin blockchain. It is also possible, at least for the moment, to code the text as false public keys and pay transaction fees. Since the recipient key is not valid, the transaction will be considered as an Unspent Transaction Output (UTXO) and stored in the block that will then be validated. There are other methods to record data in the Bitcoin blockchain, such as the OP_RETURN or Data Hash w/ Sig method. These have their advantages and disadvantages, particularly in terms of available storage size and decryption mode [SWA 17].

The OP_RETURN method is a meta-protocol of the Bitcoin protocol dating from February 2014, making it possible to name Bitcoin fractions. The objective of the OP_RETURN method was to replace the other methods, which were considered inadequate. Initially, it was possible to store 80 bytes per OP_RETURN, then the storage capacity was reduced to 40 bytes before being reduced to 80 bytes and then to 220 bytes in 2018. This practice is referred to as coloration, and these Bitcoin fractions are called "colored coins". This method allows the designation of fractions of Bitcoin held to be changed to, for example, associate them with an interest in property. A fraction of Bitcoin can, thus,

---

2 In summary, for a consensus to be reached between miners on the Bitcoin blockchain, a minimum number of miners must apply the rule so that it is established; thereafter, blocks that do not follow the rule are considered invalid and the miner does not receive the reward linked to the block.

3 https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki.

be colored to be a software license, a reproduction right of a work, a property right on a computer, or shares of companies. Specific portfolios are required to interpret and read the number of colored corners associated with an address.

In the Ethereum ecosystem, there is also a system of coloring or designation – it is the creation of tokens. But beyond the creation of tokens, i.e. in a way the coloring of the Ether, it is possible on the Ethereum blockchain to execute basic programs, called smart contracts. These smart contracts make it possible, for example, to govern an organization operating with tokens with voting rights or to set the rules for raising funds in Ether, known as Initial Coin Offering (ICO), by setting, for example, a financing ceiling, a token/Ether ratio, and a financing campaign duration. These blockchain features go beyond the strict timestamping of transactions.

Neither Bitcoin nor Ethereum was designed to be general storage systems. The records made correspond in principle to traces of transactions or operations. Other projects, such as Storj, have this general storage objective and are looking to develop distributed cloud computing services. Storj is described in its white paper as a "protocol that creates a distributed network for the formation and execution of storage contracts between peers" [WIL 16]. To ensure the confidentiality of data stored with a peer, the data are encrypted before being transferred to the peer performing the storage. Thereafter, a proof of recoverability system can be activated by the person who made the deposit to ensure that his or her data are still stored.

Figure. 1.6 shows how the Storj system ensures that data, documents, and files are encrypted before they are communicated to the network.

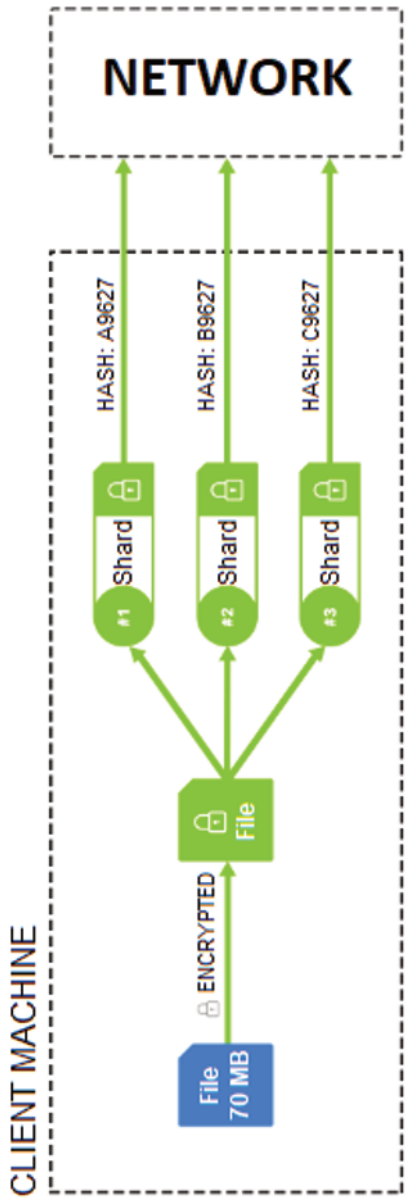

Figure 1.6. *Storj encryption system. Source: [WIL 16, p. 3]. For a color version of this figure, see www.iste.co.uk/quiniou/blockchain.zip*

The stated objective of non-centralized cloud computing projects, such as Storj, is to provide a solution that avoids dependence on high-cost storage companies and reduces the risk of unwanted data access. Storj acts as a storage intermediary between private individuals.

While the blockchain has an overall disintermediation effect for many activities (see Chapter 2), it also creates new forms of intermediation, as in the case of Storj.

1.2. Encryption, anonymity, transparency, and verifiability in a non-centralized network

The objective of many blockchains, starting with the Bitcoin blockchain, is to allow both user anonymity and transparency of operations. These two objectives may seem *a priori* intrinsically opposed but are in fact perfectly compatible. The concept allowing the junction between these two objectives is Zero Knowledge Proof[4].

This method of proof with zero disclosure of knowledge makes it possible to preserve confidentiality on certain information (civil status, business secrets, sensitive information, etc.) while proving a status, characteristics, property title, or even possession. From the point of view of the preservation of personal data or the protection of trade secrets, this method is particularly appropriate and effective. This explains why the first uses of the blockchain were deployed on the darknet for illegal transactions (drugs, weapons, etc.).

However, it is questionable whether this approach to user anonymity and transparency of operations adopted by public blockchains is compatible with regulations, particularly European regulations, on the protection of personal data and transparency.

4 See, in particular, [BAN 16a] and [MIE 13].

The comparative diagram of the Bitcoin founding document presents the fundamental difference between the traditional approach to transparency and personal data protection (referred to in the Traditional Privacy Model schema) and the approach adopted for the Bitcoin blockchain (referred to in the New Privacy Model schema).

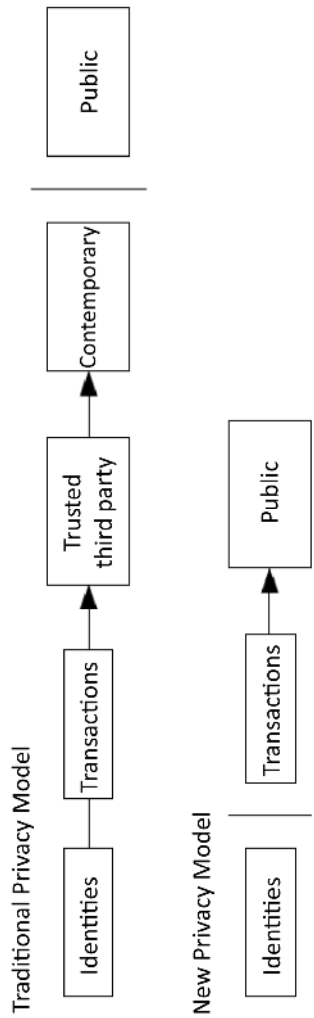

Figure 1.7. *Privacy Model schemas. Source: [NAK 09, p. 6]*

1.2.1. *A unique approach to transparency*

Transparency as currently conceived in law is transparency aimed at combating money laundering and the financing of illegal activities, mainly terrorism. In the European Union, the law applicable in this area has been largely harmonized by a 2015 directive[5], partially transposed, for example, into French law by the Sapin 2 law of November 8, 2016, and by Order No. 2016-134 of December 1, 2016.

These rules require financial institutions to collect information and verify the identity of customers; this compliance procedure generally takes the shape of forms, often referred to as Know Your Customer (KYC). The concept of transparency resulting from regulation is therefore focused on knowing the origin of funds and the identification of clients and intermediaries.

The issue of transparency is central to the blockchain protocols, but it is the transparency that is useful for user interaction and not the transparency that is useful for oversight bodies. The concept of dominant transparency in non-centralized systems is radically opposed to that defended by regulators. The transparency implemented in the majority of blockchains is the transparency of ledgers, allowing the reality of transactions to be verified. The objective is to be transparent on the running and existence of operations, and to be opaque on the origins of funds, the reasons for operations and the beneficial owners.

This structural incompatibility of the blockchain with the transparency rules of financial regulatory authorities explains the difficulties encountered with banks and the

5 Directive 2015/849/EU on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.

compliance efforts made by cryptocurrency exchange sites and ICO initiators, raising funds in cryptocurrencies. Indeed, banking and financial transactions are highly regulated and are based, in particular, on the identification and protection of consumers or non-professional investors.

ICO initiators who need to identify themselves in order to be credible to potential investors are aware that they must comply with some of the regulators' rules in order to be able to effectively convert the crypto-assets of their fundraising into foreign currency.

The same applies to most cryptocurrency exchange sites or at least those that offer the possibility of performing currency conversion operations and transfers to and from bank accounts. Exchange sites that have made compliance efforts, such as the deployment of customer information forms (KYC) and bank accounts to carry out their activities, have a competitive advantage over other exchange sites that only allow the exchange of crypto-assets for other crypto-assets. The dollar-indexed crypto-asset Tether (USDT) is designed to limit the effects of the difficulty in accessing the traditional banking system for certain trading platforms. According to Tether's white paper, the company would hold as many dollars in reserve as there are Tethers available on the market[6]. Authorities, particularly in the United States, such as the Commodity Futures Trading Commission, regularly conduct investigations to verify the reality of this reservation.

1.2.2. *An advanced form of privacy by design*

Regulation on the protection of personal data has been strengthened at the global level, particularly in the

6 Tether: fiat currencies on the Bitcoin blockchain, "At any given time, the balance of fiat currency held in our reserves will be equal to (or greater than) the number of tethers in circulation," p. 4, https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

European Union, which is responsible for a universalist regulatory dynamic. The General Data Protection Regulations (GDPR)[7] came into force in 2018. These regulations reinforce the obligations placed on entities collecting and processing personal data, in particular, with regard to the collection of informed consent from data subjects, and make them responsible by requiring them to set up technical and organizational mechanisms to ensure compliance[8] and by introducing dissuasive sanctions[9].

Anonymization and, to a lesser extent, pseudonymization of personal data, i.e. preventing identification of the person whose data are being processed[10], and privacy by default and design, i.e. collection methods structurally designed to respect the privacy of users[11] are effective methods of protecting personal data implemented by this regulation and converging with the blockchain approach.

Indeed, public blockchains, particularly the Bitcoin blockchain, are structurally designed as devices allowing anonymous transactions between peers. Blockchains are generally intended to provide users with evidence with no disclosure of knowledge.

The encryption of asymmetric keys, i.e. the combination of private and public keys, is the central criterion for the anonymization of blockchain users. In the Bitcoin

7 Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

8 *Id* Art. 24. *Id*.

9 Art. 83: in some cases, up to 20,000,000 euros or, in the case of a company, up to 4% of worldwide annual turnover.

10 *Id*. Art. 4.

11 *Id.* Art. 25.

blockchain, the signature system works with a private key, a public key, and a Bitcoin address.

The private key is randomly generated and corresponds to a 256-bit number; therefore, there are two different 256 different private key possibilities, which makes the creation of duplicates of private keys unlikely, despite the lack of any centralized key allocation and makes it particularly difficult to identify a randomly generated private key.

From the private key, it is possible to calculate the 256-bit public key using the elliptical curve secp256k1[12], but the opposite is not possible in its current state. From the public key, it is possible to generate a Bitcoin address from the hash functions SHA-256 and RIPE®-160 and then from a base58check encoding, making decryption of the address particularly complex.

However, despite this encryption, the function of which is to make it impossible to identify the private key, the transactions carried out from different addresses appear and it is possible to draw up a history for the same Bitcoin address (or Ethereum, for example)[13], using blockchain history browsers.

In addition, the uses of the Blockchain ecosystem mean that many players, such as trading platforms or ICO platforms, ask users to fill in personal information in a customer information form (KYC) with their Bitcoin or Ethereum address, which makes it possible to link the two elements and, thus, to know the history of transactions made by a person identified from his or her address.

In addition, as mentioned earlier, it is possible to integrate messages into the Bitcoin blockchain, in particular

12 See, in particular, [BRO 10].

13 See, for example, https://www.blockchain.com/fr/explorer or https://etherscan.io/.

via the coinbase text or the OP_RETURN function, and some blockchains, such as Storj, are designed as distributed cloud computing services. Thus, it is possible to store data, including personal data, on the blockchain. However, one characteristic of the blockchain makes it difficult to make it compatible, despite the encryption of data, with the regulatory provisions on the protection of personal data, namely, the irreversibility of the blockchain. Indeed, when the data are integrated into a block, and if this block is validated, the data are in principle associated with the blockchain, as long as the latter works and the personal data cannot be deleted.

The only solution would be to make a hard fork, which incorporates significant protocol modifications of a pre-existing blockchain with rules that are not backward-compatible. Hard forks are generally designed to fix major bugs or limit the effects of hacking by retroactively erasing suspicious transactions in extreme cases[14], but such a solution does not seem feasible for only deleting personal data stored on a blockchain.

This irreversibility of the blockchain contradicts the right to withdraw from Article 16 of the GDPR[15] and the right to delete Article 17 of the same text[16]. Note that the creators of

14 A list of all the forks carried out or to come can be consulted on the website http://forks.net/list. Some forks give rise to the allocation of the crypto-asset to the holders of several crypto-asset, which is the case, for example, with the Bitcoin Private (BTCP) and has been allocated to both Bitcoin (BTC) and Zclassic (ZCL) holders.

15 Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), Article 16.

16 *Id*. Art. 17.

the blockchain are not the controllers; the controller is the person who requested the integration of this data into a block. The only sub-contractor is, virtually, the miner who acts as a validator host.

As for the entity who has created and deployed the public blockchain, but not designed it for such use and who has no power to edit, transform, or even delete the blockchain, their responsibility should not be engaged except after extensive reading of the regulatory texts. To hold a public blockchain creator liable in such a context would be like holding Microsoft liable for any database inserted in an Excel file. This could be different for private blockchains, where the nodes are controlled by the same entity or at least by a consortium composed of identified entities, generally linked together by convention.

There are also blockchains with reinforced secrecy protection protocols such as Zcash, Bitcoin Private, Monero, and Komodo.

Some of these protocols aim to ensure a maximum level of anonymity even to the detriment of the possibility of proving a transaction, such as Monero, a blockchain created in 2014 and based on the CryptoNote protocol using a ring signature system, making it possible for network nodes to prove the signature but impossible for them to identify the key used to sign it, the signature having been made by a set of keys and not just one [FUJ 07]. Monero is also based on a system of so-called stealth addresses, for single use.

Created in 2016, Zcash differs from Monero's model and is based on a system called the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, or zk-SNARK. Its objective is to allow anonymity through a zero disclosure proof system. Zcash offers users of its blockchain the option to make their transactions anonymous. These protected operations are called *shielded*. The Zcash team intends to

deploy other zk-SNARK applicators to generate evidence for complex operations[17].

1.2.3. *Blockchain and protection of trade secrets*

Public blockchains operating on zero knowledge disclosure evidence systems, such as Zcash, could in medium term represent powerful vectors for the protection of technical and operational secrets.

The protection of information and knowledge by secrecy has always existed in practice and traces of the protection of these secrets by law can be identified in Roman law in the context of actions brought against slaves who revealed their master's secrets in return for money [SCH 30]. Nevertheless, until recently, regulations on the protection of secret information were mainly focused on the protection of state secrets. In terms of protecting secret technical or commercial information held by companies or individuals, American regulations had a pioneering and international promoting role. The key regulation in the United States is the Uniform Trade Secrets Act (UTSA), which dates back to 1979 and influenced, in particular, the provisions of the 1995 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS-WTO), which aimed in particular to generalize the protection of undisclosed information[18] within WTO (World Trade Organization) Member States from a global trade perspective.

The value of certain technical or commercial information kept secret may be significant, and transactions involving it directly (assignment and licensing of patents or technology transfer) or indirectly (franchise, joint venture, or takeover of a company) may be difficult to achieve because of the balance

17 https://z.cash/technology/zksnarks.html.

18 ADPIC, Section 7 (Article 39): Protection of Undisclosed Information.

to be struck at the negotiation stage between disclosing elements of secrecy for its economic value and preserving secrecy in the event of failure of the negotiations [QUI 15].

In the European Union, regulations on the protection of secret knowledge were quite disparate and often implicitly integrated into protection against unfair competition, until the EU Directive 2016/943 of the European Parliament and of the Council of June 8, 2016, on the protection of undisclosed know-how and commercial information (trade secrets) against unlawful acquisition, use, and disclosure. Article 2 of this Directive defines the concept of business secrecy as follows:

> "'Business secret' means information that meets all of the following conditions:
>
> – they are secret in the sense that, in their entirety or in the exact configuration and assembly of their components, they are not *generally known* or *easily accessible* to persons belonging to the circles that normally deal with the type of information in question;
>
> – they have *commercial value* because they are secret;
>
> – they have been subject to *reasonable steps,* regarding the circumstances, by the person lawfully in control of them to keep them secret".

One of the peculiarities of the knowledge trade is the difficulty of proving ownership, possession [PAR 08, PEL 01, p. 290] or ownership of knowledge [BIN 17, p. 82]. The "reasonable provisions […] designed to keep it secret" to which the Directive refers in the definition of trade secrets is a crucial point in the protection, enhancement, and trade of secret knowledge. This approach echoes the approach of law and economics economists and, for example, Ejan Mackaay's

work advocating the protection and recognition of a right to trade secrets through the use of available legal and technical mechanisms, referring to the very pragmatic notion of creating one's own barriers: "build/mind your own fence"[19].

Blockchain, particularly blockchains with enhanced confidentiality, is a first-rate technique for enforcing rights over secret knowledge. Zero disclosure evidence and encryption are very useful tools for operations involving secret knowledge. It is, thus, possible with these technologies to create within the same organization or inter-organization levels of knowledge classification and access levels or to prove the possession (exclusive or not) of knowledge without disclosing its exact substance.

Nevertheless, the implementation of devices involving secret knowledge with high added value in a blockchain would require complex specific developments. As it stands, the main use of blockchain for trade secrets concerns the timestamping and encryption of trade secrets, in the same way as a Soleau envelope, a French instrument proposed by the National Institute of Industrial Property to prove a prior art while keeping its contents secret.

1.3. The implications of a non-centralized model

The non-centralized model of the blockchain is based on a nodal architecture, with encryption and timestamping functions. The blockchain structurally allows the members of this distributed network to interact in a complex way

19 [MAC 99, p. 257]: "The logic of 'build/mind your own fence' is historically apparent, I submit, in property rights in land and other assets. It also appears to be part of the traditional trade secret law. If you seek remedies against a violator of your trade secret, you will have to show that you took the proper steps to keep the knowledge in question confidential. […] The law merely supplements your efforts at creating your own fence".

without having recourse to a central administration, a service, or sales platform on the Internet or any entity with legal or *de facto* authority or power. This non-centralized model allows many operations to be disintermediated.

1.3.1. *Limiting the risk of data loss*

Due to its network architecture of nodes, peers, recording, and replicating the ledger, the risk of data loss due to failure or hacking is lower in a blockchain than in a centralized system based on multiple backups. For example, some registry holders are not connected at the time of a blockchain attack, and the multiplicity of user configurations makes it even more complex to carry out a global attack on a blockchain network. The consensus mechanisms already mentioned also promote data integrity and availability.

1.3.2. *The lack of a central authority*

As previously indicated, the blockchain model can be termed as non-centralized rather than decentralized, since the blockchain does not result from a prior centralized model but is inscribed *ab initio* in parallel with it. Decentralization is generally reversible because the central authority only renounces it if it is specifically forced to exercise a power that it is not in a position to reclaim or, more generally, to reinterpret as falling within its field of competence. The central authority loses its status as a central authority only if it renounces the competence to determine the extent of its competence (also known as the Competence-Competence principle or Kompetenz-Kompetenz).

1.3.3. *Non-centralization and game theory*

Blockchains are not based on a central or even partially decentralized authority but on a distributed system with

weighted votes allowing positions to be taken to ensure the integrity of the blockchain and implement consensual improvements. In many ways, blockchains use game theory [VON 44], including John Nash's contribution to non-cooperative games [NAS 51], and the theory of incentive mechanisms [HUR 73], mainly for block validation algorithms and consensus.

With centralized registers, the central entity has, at least virtually, all the power to alter the content of the ledger in order to take advantage of it, which justifies the use of this type of register by individuals, mainly because of the authority exercised, the *de jure* or *de facto* monopoly or trust in the central actor.

With decentralized ledgers, such as blockchains, their use is explained in particular by the transparency and absence of errors in the register, due to the fact that actors with a validator role are encouraged not to compromise the protocol.

Many researchers in mathematics and logic are beginning to take an interest in game theory in the field of consensus building within blockchains[20]. For example, in the proof-of-work blocks, the "game" is designed in such a way that the miner designated to validate a block has no interest in trying to corrupt the blockchain by adding an invalid block. If the proof-of-work model corresponds to an incentive device for miners to create a block to obtain a reward, this incentive is coupled with a deterrent device to corrupt this block, the reward not being awarded or, more accurately, awarded on an alternative channel, which will be declared as invalid by the consensus of the miners, the latter having an individual interest in validating the authentic, uncorrupted channel.

These models for predicting and orienting the behavior of rational actors, particularly in the application of game

20 See, for example, [EYA 18, STO 18, KIA 16].

theory, are useful in a decentralized context but demonstrate their limitations when confronted with complex and evolving realities. Thus, in a model such as the Bitcoin blockchain, in the event that a group of miners holds more than 51% of the computing power due, for example, to centralization induced by heterogeneous electricity costs, the incentives inherent in proof of work may not be sufficient to preserve the integrity of the blockchain.

Incentive models are also the basis of Token Curated Registries (TCR). These token-based registers are designed to develop quality lists based on collective intelligence built on opinions expressed by people who are encouraged to build an informed and sincere opinion. This encouragement to give an informed and sincere opinion takes the form of a bet that an opinion will be that of the majority of the opinions expressed: to give an opinion, tokens must be bet, and if the opinion expressed is the one ultimately retained by the majority, a reward is granted from the tokens bet by those who have expressed a different opinion to the majority[21].

In this context of TCRs, if the participants' behavior is indeed guided by the incentive given to them, a rational actor will not seek to express their opinion but to express their opinion of the general opinion or of the majority view of the general opinion, which is still different[22].

Moreover, this mechanism does not prevent people from investing massively in the least likely outcome to win the tokens bet by rational participants who have expressed their opinion on the general opinion. This strategy can also be guided by a party with an interest other than obtaining the tokens obtained at the end of the vote, such as, for example, the indexing of one of his company's services in the register,

21 See, in particular, [SPA 18].

22 In psychology or behavioral economics, demonstrations linked to beauty competitors: [MOU 79, MOU 86, HO 98, NAG 99].

or the non-indexing of a competitor. This diversion strategy can be mitigated by allowing new votes to be triggered and by freezing the withdrawal of the tokens invested for a certain period. Indeed, it should be noted that since the value of the token is intrinsically linked to the quality of the register, if such behavior is detected on a register, the value of the token is likely to fall enough to destroy the potential gain and even part of the investment, before any conversion of the token, particularly if the investment or gain in token is frozen for a period of time.

1.3.4. *Oracles and decentralization*

There are several types of oracles and projects in this field, software oracles operating from certified sources on the Internet, hardware oracles operating with data collected by connected objects with sensors and declarative oracles operating with consensus rules [RAB 17]. In these different cases, the receiving blockchain must set up a mechanism (or game) to encourage entities to transmit correct information, through a reward and a system of validation by other entities within the framework of a consensus, for example. In this field, there are many projects such as Oraclize or Augur.

In the case of Oraclize, it is a solution that works with smart contracts from different blockchains (Ethereum, EOS, etc.) and allows requests to be made using TLSNotary, a system for auditing data and web browsing information (in https sessions) that works with a specific browser extension called PageSigner proving that data from the server have actually been received.

In the case of the Augur project, the Oracle system is particularly ambitious, since it makes it possible both to deeply decentralize the betting system and to deploy a predictive system based on collective intelligence, taking into account in particular the betting rates. In such a system, the

incentive to give a sincere opinion is the expected gain from the bets made, which is intended to guarantee, to some extent[23], honest participation in collective intelligence.

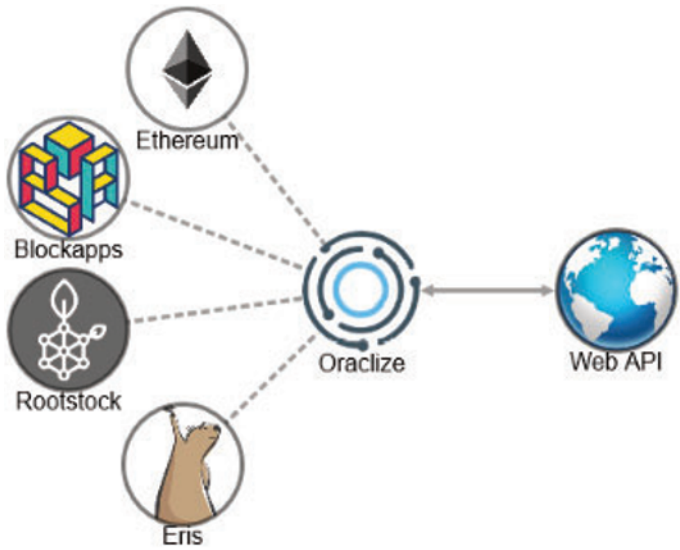

Figure 1.8. *Oraclize ecosystem. Source: http://www.oraclize.it/*

The Augur project is of real interest, but its implementation is likely to encounter legal obstacles that are difficult to overcome. In many countries, betting, especially online betting, is highly regulated, the type of bets available is very limited (sports betting and poker) and bets can only be placed by authorized operators. In France, for example, until recently, betting could only be offered by entities

23 If a system like Augur is indeed deployed on a sufficient scale, some entities wishing to certify their potential on purpose (communication, credibility with investors, lenders, insurers, etc.) could try to bias this system by betting massively for a favorable projection. Such a bias could even have a Pygmalion effect, a self-fulfilling prophecy, if a system like Augur is adopted on a massive scale.

benefiting from a state monopoly (Française des Jeux and Paris Mutuel Urbain). Since the opening to competition[24] in 2010, the regulatory authority has only approved about 10 operators. Other legal systems, often based on common law, are more flexible in terms of betting and some countries have also pursued a policy very favorable to this type of activity for reasons of economic attractiveness, as is the case, for example, in Malta and Gibraltar.

Beyond the limitation of authorized operators, attention should be paid to the types of betting that can be offered in a decentralized peer-to-peer system. One of the important reasons in many legal systems for limiting betting to sporting events is the absence of a significant impact of the outcome of such events on society in general and, therefore, of a rigged bet.

In a way, a transaction on a stock market can be assimilated for the investor to a bet on the future of the company or more precisely to a bet on the perception of the company's value in the future. In this field, which is less insignificant than sport, national regulations are generally very strict and punish market abuse. In France, Act No. 2016-819 of June 21, 2016, transposing European Directive 2014/57 of April 16, 2014, governs criminal sanctions for market abuse, including insider trading, price manipulation, and the dissemination of false information. In addition to the criminal aspect, the competence of the National Financial Prosecutor's Office, a specifically competent administrative authority, the Financial Markets Authority, has numerous enforcement powers, an extended right to information (in particular, in the event of a threshold being crossed) and may hinder or impose conditions on certain transactions planned by market participants. The main objective of this regulation is to create confidence in the financial markets and to make

24 Act No. 2010-476 of May 12, 2010, on the opening to competition and regulation of the online gambling sector.

this method of financing more fluid with the public, thus reassuring investors against behavior that distorts the result.

A decentralized, anonymous, and unregulated betting system in important areas of society could have deleterious effects. By making it possible to bet on an election, clinical test results, or someone's death in such conditions, this system could have many perverse and particularly dangerous effects. Such a system would also be harmful overall in terms of overall social performance because the easiest way to win a bet is for a protagonist to bet on their loss. However, betting mechanisms limited to certain areas could be implemented in a blockchain with less significant consequences.

With its decentralized architecture, the blockchain is a technology that shifts the control modalities of actors with a *de jure* or *de facto* monopoly to a neutral system that responds to pre-defined and transparent rules that can evolve according to the consensus of stakeholders. This observation makes blockchain a powerful vector for disintermediation.