



ISSUE PAPER

# ISSUE PAPER ON BLOCKCHAINS

*afnic*

ISSUE PAPER

## WHAT IS A BLOCKCHAIN?

A **blockchain** is a recent invention that allows a group of actors who do not trust each other (or who do not even know each other) to nonetheless reach an agreement on a common **operations ledger**. The ledger in question contains an ordered list of the transactions between the actors.

Blockchains are known in particular for their use in the Bitcoin payment system. But they have many more applications than the world of finance. Before they existed, an agreement on a list of transactions almost always required a third party that all the actors had to trust. Since their invention, that agreement can be completely peer-to-peer, without a central authority.

## /// INTRODUCTION

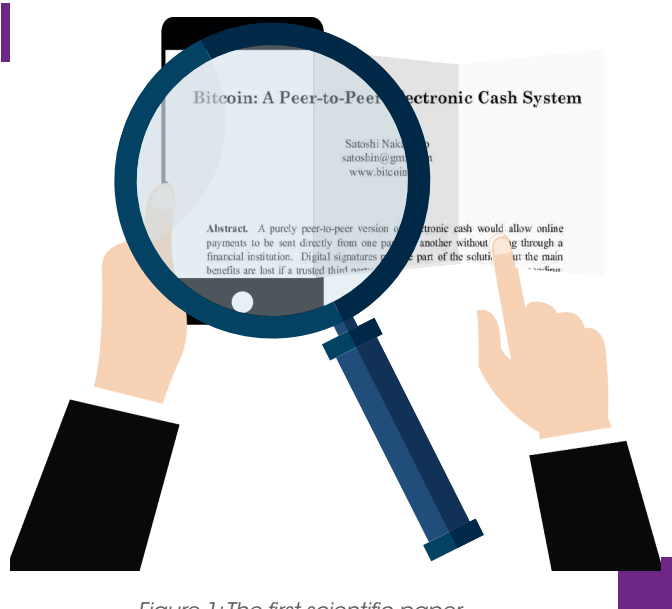


Figure 1: The first scientific paper describing a blockchain in 2008

Potentially, a blockchain can therefore replace all of the instances in which that central authority has no other purpose than to serve as an intermediary. This phenomenon, which is sometimes called «uberizing Uber» or, more amusingly, «blockchainization» is often cited in discussions about the practical consequences of the blockchain.

Technically speaking the chain is a remarkable invention and, socially, challenges well-established situations. As a result, highly exaggerated statements have sometimes been made, attributing powers to the blockchain that it does not have. The purpose of this [Afnic](#) issue paper is to explore possible uses of blockchains, especially in registry activities.

## WHAT IT CAN BE USED FOR?

A priori blockchains have very many applications: every time the various actors used a central authority, it could have been replaced by a blockchain.

### An obvious example is a currency.

Since the Middle Ages, a currency is typically guaranteed by a State (the central government). With the blockchain, a currency can be designed with no central authority, which is the case of Bitcoin, the technology that launched and popularized the idea of blockchains. There are many motivations for these «distributed» or «peer-to-peer» currencies: they avoid having to trust authorities that the actors do not approve, facilitate micro-payments on the Internet, have reduced transaction costs, etc.

After the currency, another service that is often centrally managed is that of **management of names** (create, delete, etc.) in a namespace. For example, the user names of a social network are centrally managed today by the company that has the infrastructure of that social network, making it possible in particular to ensure the uniqueness of those names. But this centralization also gives the company too much control: for example, it has the power to close accounts on the basis of a simple notification, without any real verification. The blockchain provides an alternative: the registration of names on a «first come, first served» basis can be done using a blockchain. As a result, there is no central authority that can delete accounts, and censorship becomes much more difficult.

An example very close to this is the registries of **domain names**. They register domain names, essential for the use of the Internet. But they also have the power to delete them (as in the Sci-Hub case). We can therefore consider replacing those registries by a blockchain, in which the transactions are the creations of domain names.

A final example of an application that is well suited to blockchains is **the registration of works in order to prove their anteriority**. Imagine an artist who produces a video, but who cannot or does not want to publish it right away, but wishes to be able to prove later that s/he is indeed the author. There are traditional centralized solutions, requiring trust in an organization. Instead, a blockchain could be used. But to put their work directly in a blockchain would have two disadvantages: it could be expensive and could disclose their work (since the

chain is public, and readable by all). One possible solution is a hash. It is a simple mathematical operation that hashes a document of any size into a relatively short number. Hashing is not reversible (you cannot recover the original content from the condensate). One of the properties of the mathematical functions used is that a document cannot be produced from a given condensate. This means that if the condensate is stored in a blockchain, only the original author may, on the appropriate day, produce a document that matches it, proving that s/he was the person who recorded the

condensate. Several projects already exist to implement this idea.

It is this possibility of replacing, in whole or in part, traditional intermediary functions, which justifies the statement that blockchains could «uberize Uber». Behind this slogan, there is the idea that at least in theory, economic actors could interact without the need for a trusted intermediary.

However, there is no evidence that this is possible in all cases, or even that this is desirable.

**Thus, interacting directly via the blockchain would mean there is no recourse in case of litigation, or in the case of an operator error (see the examples below on the poor management of private keys). It is therefore likely that there will always be room for freely chosen intermediaries, perhaps with a more limited, redefined role.**

## /// A KNOWN EXAMPLE, THE BITCOIN

The first blockchain, and without doubt the most important today is that of Bitcoin. Bitcoin is a payment system. The only transactions possible are sending and receiving money (bitcoins). Money being a very sensitive and highly regulated sector, it is not surprising that Bitcoin has been at the center of several controversies, not always justified. For example, people have criticized the fact that the inventor of Bitcoin, Satoshi Nakamoto, was only known by a pseudonym, and that therefore Bitcoin could not be trusted. In addition to the fact that the argument boils down to not trusting the printed word because you

have never met Gutenberg, it also shows a misunderstanding of the blockchain mechanism: **the trust is not based on the chain manager (there is none) but in the visibility to all of its operation.**

Other criticisms made of Bitcoin focused on its «virtual» nature, as if real-life money were still made of gold, and guaranteed by the production of material objects.

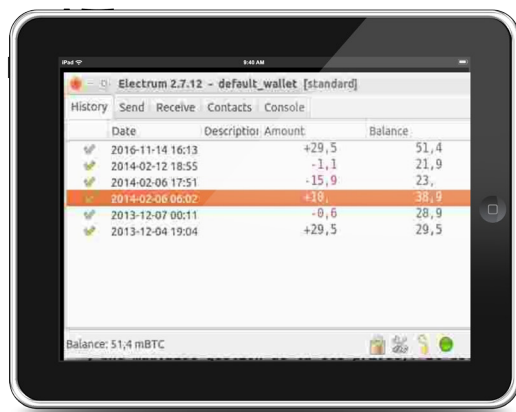


Figure 2: Bitcoin Electrum wallet

**But whatever one's opinion of Bitcoin, it does not necessarily apply to the concept of the blockchain. They can be used for many things, sometimes unrelated to money.**

## /// REGISTERING NAMES

The first example of the registration of names in a blockchain was the Namecoin system, another example was presented during the [2016 Afnic Scientific Council Day](#). Please note, we said that the replacement of registries of domain names was technically possible, not necessarily that it was desirable, nor that it would be adopted (lots of very good ideas have never met with success). Indeed, blockchains also have limitations (see below).

Afnic's work in monitoring and research in this area is long-standing. The [first presentation on blockchains](#) was given at a meeting of the Council of European National Top Level Domain Registries (CENTR) in Paris in 2014. The presentation by Afnic was on the Namecoin system, a variant of Bitcoin.

Two of the identified limitations of Namecoin involved the case of mass reservations of names for speculative

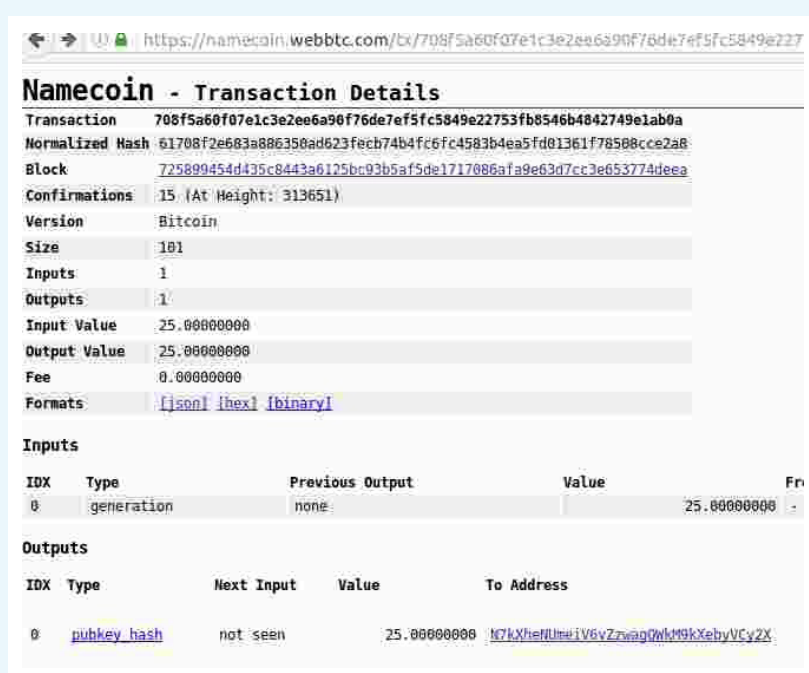
purposes (Namecoin names are very cheap, and almost all the interesting names have already been reserved), and the difficulty in managing keys by users: if they lose their private key, all their names are lost, and there is no recourse.

## /// A GENERAL CHAIN

If Bitcoin is certainly the best known instance of the use of blockchains, there are others, such as Ethereum. One of the latter's specific features is that the transactions stored in the chain

are not restricted to a small number of operations, but are programs written in a general-purpose language. Ethereum can therefore be used for a variety of applications. Thus, the example studied

during the 2016 Afnic Scientific Council Day was that of a registry of Internet names, developed on Ethereum.



Namecoin - Transaction Details					
Transaction	708f5a60f07e1c3e2ee6a90f76de7ef5fc5849e22753fb8546b4842749e1ab0a				
Normalized Hash	61708f2e683a886350ad623fecb74b4fc6fc4583b4ea5fd01361f78508cce2a8				
Block	<a href="#">725899454d435c8443a6125bc93b5af5de1717086afa9e63d7cc3e653774deea</a>				
Confirmations	15 (At Height: 313651)				
Version	Bitcoin				
Size	101				
Inputs	1				
Outputs	1				
Input Value	25.00000000				
Output Value	25.00000000				
Fee	0.00000000				
Formats	<a href="#">[json]</a> <a href="#">[hex]</a> <a href="#">[binary]</a>				
Inputs					
IDX	Type	Previous Output	Value	Fr	
0	generation	none	25.00000000		
Outputs					
IDX	Type	Next Input	Value	To Address	
0	<a href="#">pubkey hash</a>	not seen	25.00000000	<a href="#">N7kXheNlUeiiV6vZzwagQWkM9kXehyVCy2X</a>	

Figure 3: A blockchain: in this case a Namecoin transaction, accessible to all on the Web]

### /// WHAT IT CANNOT BE USED FOR

#### THE BLOCKCHAIN IS NOT A MAGIC SOLUTION TO EVERY PROBLEM.

For example, it is not suitable for storing large amounts of data, since the chain must be fully replicated on all machines in the peer-to-peer network. In November 2016, the Bitcoin system represented about 80 Gb of data. Storing only a hundred movies in high definition would more than double its size!

Nor is a blockchain suitable for large calculations (in the case of chains accepting arbitrary programs, like Ethereum), for a similar reason: the calculations must be performed on all of the machines, so that each can independently verify the result.

Finally, because of the public nature of a blockchain, it is not recommended to use it to store private data. Storing a condensate of these data, as in the example of registering intellectual works, is reasonable, but the data must not be written as cleartext.



### /// A (VERY) SHORT EXPLANATION



**This issue paper is not intended to be a complete course on blockchains. Nonetheless, this section aims to explain some necessary basic concepts. It will be the only technical part of the paper.**

A blockchain should actually be called a \*transaction chain\*, since it is an ordered sequence of transactions and operations. It is public: anyone can access the data in the chain, which implies consequences on privacy.

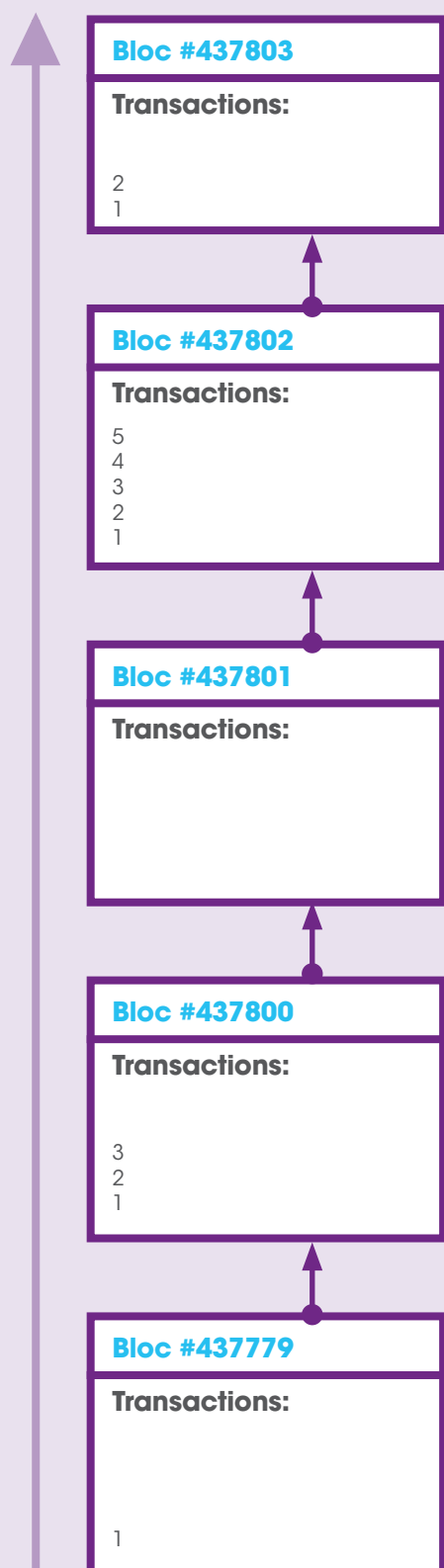
For various technical reasons, the transactions are grouped into blocks, and it is the blocks that are chained together. Here is a simplified representation of the Bitcoin system, the last block being #437803. Five blocks are shown here, the most recent being on top. Some include several transactions, block # 437801 comprising none.

Not only is the chain public, but it is maintained peer-to-peer, i.e. no machine has a special privilege. Everyone can add blocks (but cannot modify or remove existing blocks). To prevent unauthorized changes, the chain is secured by cryptography. In particular, all of the transactions are signed.

How can a distributed database that anyone can edit be trusted? Trust is based on the public nature of the software (all of it is free software), the algorithms, and the chain itself. Everyone can verify that everything has gone well according to the official algorithm, by running the software on their own machine.

**The blockchain is a concept, not a single entity. The best-known chain is that of the Bitcoin currency but there are many others.**

Figure 4: A blockchain (time flows from bottom to top)



## /// WHO DOES WHAT?

A frequently asked question on the functioning of the Internet is that of governance. **Who makes the decisions and how?** The same question applies to blockchains. Some say it works all alone, without any human intervention. But since blockchains run on physical computers, managed by real human beings, and is programmed by the same human beings, it cannot be entirely divorced from politics. Decisions are taken, choices are made, and everyone does not always agree, especially since the actors do not have all the same interests.

Two examples are often cited, the first being the debate within the Bitcoin community on a point that seems a technicality (increasing the block size) but actually raises Bitcoin orientation issues. The second is the debate that divided the Ethereum community in 2016 about what to do after the theft of numerous ethers. In both cases, decision-making mechanisms will have to be developed.

## /// 8. CONSTRAINTS

### KEY SECURITY



The security of the user's portfolio is based on asymmetric cryptography, in which the user has both a public key and a private key. The latter is used to authenticate transactions.

We must both prevent others from reading private keys and ensure that these private keys are correctly backed up, for example, to deal with a hard drive failure. This seriously complicates the use of blockchains for users! Of course, to solve the problem there are technical solutions (multiple signatures) and organizational solutions (the «notaries» to whom this work would be subcontracted) but they are still rare.

The first risk is that of the security of the machine that stores the keys. It is not easy to keep keys secret on a machine using a mainstream system infested with malware. Best practices include security good practices, and perhaps more high-tech mechanisms such as hardware devices for storing keys.

A celebrated example of the second risk was that of a [hapless Brit who had thrown away the hard disk containing his private key, thus losing 7500 bitcoins](#). There are several technical solutions to this problem, the main one being of course to have backup files.



## PRIVACY

It is sometimes said that Bitcoin is «anonymous». Actually, the correct term would be «pseudonymous». While a Bitcoin address does not directly identify a human being, it does however enable the traceability of all transactions related to that address. If one leak, a single leak, makes it possible to link an address and an individual, all of his or her Bitcoin business is disclosed. It is therefore no exaggeration to say that a Bitcoin address is close to personal data.

Several technical approaches have been tested to preserve the privacy of users of blockchains. They range from the use of mixers (services that receive several payments and mix them), to disposable

addresses (to reduce traceability), up to radically new solutions, designed for true anonymity, such as the Monero or Zcash cryptocurrencies.

In some cases, blockchains can protect privacy. For example, in the Internet name registration systems such as Namecoin,

a request for a name (the equivalent of a whois or DNS query) is purely local, made on a local copy of the chain, and therefore is not known by the other actors.



## DOUBTS ABOUT IMMUTABILITY

In theory, a blockchain is immutable. Once a transaction has been written, it is written for all eternity. This can be a good or a bad thing. The good thing is that it protects against arbitrary changes made by an intermediary. This is essential for trust. The bad thing is that it may conflict with the right to be forgotten. It also may

be difficult to fix bugs, as explained in the next section.

In fact, nothing is truly immutable. A blockchain after all is only a computer file and can always be changed. But this requires the consensus of a large number of actors, since the network has no

central management. It is this consensus that protects against arbitrary changes, while allowing the actors to change the rules of game from time to time, if there is a very good reason.

## BUGS



A good example of such a reason was the theft committed at the expense of the investment fund «The DAO» in June 2016, on the Ethereum chain. The rules followed by the chain had been modified to recover the stolen money.

In this case, the theft was possible due to a bug in a program (a contract) running on the Ethereum chain. Such a bug occurring in a program or in the software of the chain itself is more difficult to correct than a traditional bug, because

there is no central authority to decide to update the code or data. It is currently one of the factors of uncertainty for some chains, including those that enable the execution of any program.



### /// CONCLUSION

Blockchains are still new technology, so it is logical that there are many unresolved issues, and annoying problems. We must not compare them with mature technologies, but with, say, the state of the automobile in 1900: promising but difficult (and sometimes dangerous) to use.

# USEFUL INFORMATION

## To contact Afnic



Afnic  
Immeuble Le Stephenson  
1, rue Stephenson  
78180 Montigny-Le-Bretonneux  
France  
[www.afnic.fr](http://www.afnic.fr)



Tél. : +33(0)1 39 30 83 00



@AFNIC



[support@afnic.fr](mailto:support@afnic.fr)



Fax : +33(0)1 39 30 83 01



[afnic.fr](http://afnic.fr)

## About Afnic

**Afnic** is the French Registry for the .fr (France), .re (Reunion Island), .yt (Mayotte), .wf (Wallis and Futuna), .tf (French Southern Territories), .pm (Saint-Pierre and Miquelon).

**Afnic** is also positioned as a provider of technical solutions and services for registries and registrars. **Afnic** (the French Network Information Centre) comprises public and private stakeholders, including government authorities, users, and Internet service providers (Registrars). It is a non-profit organisation.



*afnic*