Internet infrastructures and services

Stéphane Bortzmeyer,
engineer in the Department of Information Systems, Association Française pour le Nommage Internet en Coopération (AFNIC)

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
Descriptions of how to actually use the many applications proposed for blockchains are too vague to assess whether or not it is reasonable to use this new technology. Blockchains are not of use for any and every application. Herein, two widely discussed applications related to the Internet's infrastructure come under discussion: computer logs and registries. How to make a registry using blockchains? What are the advantages, problems and obstacles?

Since blockchains have become topical, countless articles and presentations have described their possible applications, often with very vague descriptions: "Lying about your diploma will now be impossible, thanks to blockchains"; "Health will be on a blockchain"; and so forth. This fuzziness makes it hard to talk about these applications, or to even see whether this technology is actually adapted to these problem areas.[1]

Herein, I would like, on the contrary, to discuss how blockchains might be applied to two basic services that are part of the Internet's infrastructure.

To work right, the Internet depends on a number of registries for seeing to it that certain resources are unique, and are properly managed and stored. A domain name, for example, has to be unique. Scarce resources, such as addresses using Internet Protocol version 4 (IPv4), must be severely rationed. The name and address of an organization that has a registered number as an autonomous system — a number indispensable to the Border Gateway Protocol (BGP) for exchanging routing information — must be recorded somewhere. The words "registry" or "register" refers to this service but also to the organization providing it. Before blockchains, commonsense was to have a single organization receive requests, decide (sometimes) whether they were acceptable, place the records in a data base and, in the end, issue public notices.

For instance, AFNIC (Association Française pour le Nommage Internet en Coopération) is the registry of the domain *.fr*. It sees to it that there will be only one *paris.fr* and a single *wikipedia.fr*, that it will be possible to find any domain-owner's name and address, and that these names "work", *i.e.*, that they will be properly listed in the Domain Name System (DNS, a protocol for using domain names). This intervention by a single organization places the registry under political pressure. Its legitimacy must be established (by the law for example); its decisions will be disputed; and the question will even be raised about eventually replacing it (evidence of this being the many debates about governance of the DNS root).

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

Besides registries, a second service that could potentially be placed on a blockchain is the upkeep of logs of various sorts. A log is a sequence of information in a given order that, once recorded, must not be modified. Here again, commonsense was to have a single organization keep the log and guarantee its integrity.

Many other services could, of course, be candidates for moving to a blockchain (like Twister, a rival of Twitter but entirely peer-to-peer); but since they are not part of the Internet's infrastructure, they lie outside the scope of this article.

Blockchaining registries

Thanks to a blockchain, parties who do not have confidence in each other can reach a consensus on the state of a register (registry or ledger), on its contents for example. What is important in this definition is: "parties who do not have confidence in each other". When everyone trusts a third party, traditional databases are better suited; and a blockchain would hardly make sense.

A blockchain can potentially take the full place of the registry. To its advantage, this would end controversies about the "politics" of the registry or its legitimacy. Before dwelling on the differences between theory and practice, let us look at the actual conditions for using a blockchain as a registry.

Namecoin has been used for several years now as a registry of domain names. This software, derived from the renown Bitcoin code, has its own blockchain, its own miners and explorers. Its programmers have added to the code the possibility for a new sort of "transaction": the registration of names and the association of data with them (just like the DNS allows for associating data, such as IP addresses, with domain names). Catchphrases such as "peer-to-peer DNS" are sometimes used to refer to Namecoin, but they are misleading. Namecoin has next to nothing to do with the DNS. The only common point is that both are systems for retrieving the data associated with a name. However Namecoin has a bridge whereby ordinary DNS clients can resolve Namecoin names via *.bit*, an unofficially registered top-level domain. Once equipped to resolve *.bit* addresses, you can access Namecoin names from ordinary software, such as your Web browser.

Other software for managing blockchains are probably better from a technical viewpoint than Namecoin. Such is case of Ethereum. Instead of requiring a modification of the blockchain software for each different application, it allows the blockchain to execute programs of any sort. Registry software could be developed and deployed on Ethereum.[2] Since the blockchain itself performs essential tasks, such as placing requests in the order "first received, first served", a registry of names on a blockchain is quite realistic. In fact, several already exist, such as EtherID or Ethereum Name Service. But let's take a look at the limitations.

To start, blockchain technology does not allow for easily changing the policy adopted for recording blocks, unless it has a procedure for authorizing a trusted third party to do so. In that case however, the blockchain comes close to being a conventional registry — what the advocates of this technology want to avoid. If, for example, registration is "first in, first out", a more restrictive policy cannot be adopted. Most advocates see this as an advantage, since it shelters the chain from arbitrary decisions and passions. A blockchain follows a policy; but it is the policy that was adopted when the chain was launched and that cannot normally be modified. Users must be well aware of this and keep it in mind.

[2] I presented in detail software of this sort to the Journée du Conseil Scientifique de l'AFNIC on 11 July 2016: https://www.afnic.fr/fr/l-afnic-en-bref/agenda/182/show/jcsa16-journee-du-conseil-scientifique-de-l-afnic-2016.html

For this reason, a blockchain is probably unsuitable for allocating IPv4 addresses. Given their scarcity, new addresses are allocated only after a thoroughgoing examination. A blockchain is unable to manage scarce resources. As much can be said about the DNS root: a blockchain cannot easily limit the number of new top-level domain names (TLDs: such as *.re*, *.com* or *.pizza*). Were the current problems related to root names settled by using a blockchain, the trend in the creation of TLDs would be much different from what it is.

Another point worth making has to do with the lack of recourse for an appeal. A blockchain is designed to run automatically without human interventions. If you lose a conventional domain name (because you forgot to pay for it, or because it has lapsed and someone else is using it), you have the possibility of appealing to the registry (or a court). Such a procedure might be slow, complicated and expensive; but it exists. If you lose a name registered via a program that works on a blockchain, there is no recourse. You cannot argue with an algorithm! I had this unfortunate experience in September 2015, which explains why *bortzmeyer.bit* no longer works.

The security of what is recorded on a blockchain relies on two cryptographic keys (the one private, the other public). The private key is a secret to be strictly kept. A third party who makes a copy of it can do whatever he wants with the information you have registered. Given the quantity of malevolent software programs that run on any computer using Microsoft Windows, this risk is far more than hypothetical. If the private key is lost (and there are no backups, or if the hard drive where it is stored stops working), you can no longer modify your registered names or even renew your registration.

Once again, there is no appeal to an institution, as is possible if you forget your password on a website. As experience has taught us, users are not very good managers of cryptographic keys. In the future, techniques using hardware for stocking a private key will perhaps limit these risks but without fully eliminating them.

Blockchaining logs

Would it be possible and worthwhile to place logs on a blockchain?

There are public logs, such as the digital certificate log X.509 used by Certificate Transparency. Under the RFC 6962 standard, certification authorities are to publish on a log the certificates they have signed. This log allows for additions only, never for modifications or deletions. A Web browser can check the certificate received from a server against the log and verify that it has been recorded there. In addition, the owners of domain names can permanently access the log to verify that no false certificates have been issued. Certificate Transparency is supported by Google — logically since this firm has often been tricked with false certificates.[3]

Existing logs are managed by firms that limit writing permissions to “recognized” certification authorities. Could these logs be placed on blockchains? Of course; and that would eliminate the dependence on a private party. However no actual projects seem to be in the pipeline for doing so.

[3] Governments have had false *gmail.com* certificates made to intercept traffic with Google.

Conclusion

So, will the current registries, so important to the Internet's infrastructure, be replaced with blockchains? The choice is not binary, between a single traditional registry and a fully peer-to-peer system. Innovative arrangements could be designed, such as a blockchain with "notaries" who perform difficult operations (monitoring the blockchain, managing cryptographic keys, etc.) for their clients. Such a system would have as advantage that a domain name's owner would be free to choose a notary or to do without.

Separating a registry's various functions from each other has, in addition, the intellectual advantage of forcing us to think about the operations performed by registers of all sorts. In my very simplified explanation of blockchains, I did not mention backing up data, an essential operation. The data on a blockchain are automatically duplicated; but if all nodes in the network "disappeared", the data would be lost.

Evidently, the biggest challenge is for blockchains to be adopted. Namecoin, a small blockchain maintained by a few enthusiasts, has existed for several years now but has never really taken off. Several services (such as the resolution of public DNS names with *.bit*) do not exist anymore. Anyone — even someone with few skills — can soon enough create a registry of names on Ethereum. This is the Internet's very important, "permissionless" aspect. But will users recognize such a registry?