Crypto-Blogging

OpenTimestamps, IPFS, and NFTs for the blockchain era of blogging.

Marco Favorito
Sapienza University of Rome
favorito@diag.uniroma1.it
https://marcofavorito.me

April 5, 2021

Link: https://marcofavorito.me/blog/crypto-blogging

Contents

Since the end of 2020, the cryptocurrency market has gained, once again, mainstream attention. All-time high prices for Bitcoin and Ethereum, recognition of Decentralized Finance systems (DeFi), rise of Non-Fungible Tokens (NFTs), and more institutional investors jumping in the cryptocurrency market are some of the traits of the new cryptomania wave.

In this post, I will try to adopt some of the applications of these technologies, with the eyes of a researcher and (when I have time :cry:) a blogger.

1 Blogpost Timestamping

A known application of blockchain-based Distributed Ledger Technologies is *trusted digital timestamping* (Haber and Stornetta 1991) (Haber and Stornetta 1991). Previously, there were several timestamping schemes and standards (Adams et al. 2001; ANSI 2016; "Information Technology — Security Techniques — Time-Stamping Services — Part 1: Framework" 2008; Massias, Avila, and Quisquater 1999), but they had to rely on a trusted third party Timestamping Authority (TSA) for the issuing of the timestamp. With the advent of the Bitcoin system, it is possible to use it as a decentralized timestamping mechanism not only for transactions but also for arbitrary data, as if it acted as a *notary* (Gipp, Meuschke, and Gernandt 2015).

OpenTimestamps is an open-source project that implements this idea. In particular, it uses Bitcoin block headers as time attestations: proof that a notary that we trust attested to the fact that some data existed at some point in time.

For bloggers, a timestamp of their blogposts would be useful to prove that the post was not created after the date that the timestamper certifies. For example, this post is timestamped using OpenTimestamps. The timestamp is produced against the PDF version of the post. The links to the PDF version and the timestamp file are reported in the header of the post. Anyone can verify the correctness of the timestamp either by using the CLI tool `ots verify`, or by relying on a third-party service like this. I will try to keep this habit in the next posts.

As a reseracher, one could also timestamp PDF versions of his publications; however, it is less necessary as the published papers are already disseminated on the web by trustworthy (but centralized) aggregators, publishers, and search engines, e.g. Google Scholar, DBLP, ArXiv etc.

2 IPFS

The InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files (Benet 2014). It is arguably one of the most interesting project of the decentralized web.

An entire website could be easily hosted on the IPFS network, like Juan Benet's website, the creator of IPFS. All is needed is to either run a local IPFS node on your machine, or to rely on remote pinning services, like Pinata, to improve the availability of your files. At the moment, I have only uploaded some of my documents (see the IPFS links in publications page), but eventually I will run the entire website on IPFS, so to not rely on any third-party services.

3 Unstoppable Domains

Unstoppable Domains is a company building blockchain-based domains to replace cryptocurrency addresses with human-readable names. Being decentralized, such domains are inherently unstoppable (as long as the Ethereum blockchain and the transport layer it builds on are operational), and the sole owner is the owner of the private key associated with the domain. The system works thanks to the Crypto Name Service (CNS) built on Ethereum, and consists of a bundle of smart contracts. See the architecture documentation page for more details.

I set up my Unstoppable Domain marcofavorito.crypto that currently redirects to marcofavorito.me (see transaction here), hosted on GitHub Pages. I also have associated to it my email address, and my BTC and ETH addresses.

An easy way to navigate in the decentralized web is by means of this browser extension. If I had deployed the website on IPFS, I could have set up a redirection from my crypto-domain to the IPFS address of the website.

4 Blogposts as NFTs

Non-Fungible Tokens (NFT), proposed in ERC-721 (Entriken et al. 2018) are tokens minted on blockchain that are unique. An NFT is not like any other one, differently from ERC-20 tokens, which are fungible. This makes them particularily apt to represent ownership of digital assets. NFTs are now used by crypto artists (e.g. see artist Beeple's *Everydays: the First 5000 Days* sold as NFT for $69m), blockchain games, and several other uses to ensure digital scarcity and ownership. The Unstoppable Domain above is indeed an NFT. Usually, an NFT is minted on-chain and the data linked to it is stored off-chain in a content-addressed data storage such as IPFS.

This post is associated to this NFT, that represents the ownership of this post. Who knows, it could be the next Beeple's *Everydays*!

5 Conclusions

As a technology at its early stages, when it comes to applications of blockchain systems, the sky's the limit. In this post, I wanted to play with several crypto-based services and see how they could be used for blogging.

Among other ideas not explored in this post, there are:

- Tokenize yourself as a professional/researcher/blogger. That is, make the token to represent something, material or immaterial, that you have or you can provide. For example, your working hours can be tokenized and then sold to people who'd like you to work for them, or to write the next blogpost :slightly_smiling_face:. The token can be provided on DeFi exchanges like Uniswap.

- NFTs can be a way to post anonymously and still receive compensation for the work.
- NFTs allow for crowfunding writing in which an author can be supported in advance by contributors that in turn receive equity ownership from the writer's work; everything coordinated by a smart contract in a trustless setting.

References

Adams, Carlisle, Pat Cain, Denis Pinkas, and Robert Zuccherato. 2001. "Internet X. 509 Public Key Infrastructure Time-Stamp Protocol (Tsp)." *RFC3161* 8.

ANSI, ASC. 2016. "X9. 95 Standard for Trusted Time Stamps (2012) Accredited Standards Committee X9 Inc."

Benet, Juan. 2014. "IPFS-Content Addressed, Versioned, P2p File System (Draft 3)." *arXiv Preprint arXiv:1407.3561*.

Entriken, William, Dieter Shirley, Jacob Evans, and Nastassia Sachs. 2018. "EIP 721: ERC-721 Non-Fungible Token Standard." *Ethereum Improvement Proposals*.

Gipp, Bela, Norman Meuschke, and André Gernandt. 2015. "Decentralized Trusted Timestamping Using the Crypto Currency Bitcoin." *arXiv Preprint arXiv:1502.04015*.

Haber, Stuart, and W. Scott Stornetta. 1991. "How to Time-Stamp a Digital Document." Article. *Journal of Cryptology* 3: 99–111.

"Information Technology — Security Techniques — Time-Stamping Services — Part 1: Framework." 2008. Standard. Vol. 2000. Geneva, CH: International Organization for Standardization.

Massias, H., X. Serret Avila, and J.-J. Quisquater. 1999. "Design of a Secure Timestamping Service with Minimal Trust Requirement." In *The 20th Symposium on Information Theory in the Benelux*.