Blockchains from a Distributed Computing Perspective

Maurice Herlihy

Overview

This paper aims to summarize the concepts and mechanisms involved in blockchains from the perspective of distributed computing. It does this by employing a step-by-step method of explanation that gradually becomes more complex, illustrating concepts with intuitive examples. The paper first introduces the concept of a ledger with the help of Alice, who has an online news service, and explains how this abstraction is superior to mutual exclusion-based systems. The paper goes on to explain what consensus protocols are and how they apply to these ledgers. Next, the paper explains private blockchains by using Alice's business' supply chain. In this section, the concept of Byzantine fault-tolerant consensus protocols is explained. The paper then explains public blockchains with a coupon scheme in Alice's frozen yoghurt business. This section also explains the concepts of cryptocurrencies, Sybil attacks and proof of work. The paper then devotes a couple of paragraphs to listing the advantages and disadvantages of private and public blockchains both.

After this, the paper discusses the concept of Smart Contracts, which despite what the name suggests doesn't involve contracts of any kind but adding some functionality to the blockchain. In the example in the paper, the functionality being added is one that prevents an asset from being transferred unless a specific key is provided. The paper then explains how this would play out ideally, and then if something were to go wrong. The paper then discusses the use of smart objects in different scenarios, such as being used as a monitor, and as a read-modify-write operations, with associated examples. The author discusses work involving the pitfalls and bugs in smart contracts and states that following best practices are important for smart contracts. The paper concludes by stating that much work in the area of blockchains has been carried out by those outside the established research community and urges both sides to pay more attention to each other.

Contributions and Positive Aspects

In reading the explanations for the underlying mechanisms of blockchains its positives are easy to identify. The first of these is its distributed and decentralized nature. The fact that blockchains are distributed mean that the associated advantages of distributed systems apply here as well. Specifically, blockchains are more stable and reliable, because it can withstand multiple failures. Additionally, the use of consensus protocols means that there will be no inconsistencies in what the ledger records. In the context of cryptocurrencies, this decentralized nature becomes all the more appealing. Instead of needing a middleman like a bank or some other facilitator like PayPal, which involves a certain degree of trust in that facilitator, the need for the middleman is eliminated

Regarding the consensus algorithm, another strength of blockchains is its employment of Byzantine fault-tolerant consensus protocols in particular. Using these consensus protocols protects the blockchain from the machination of malicious entities and essentially means that the blockchain can be used even if a user does not trust every one else using that blockchain. The proof of work concept in particular helps create a steep barrier of entry from any entity that could otherwise flood the blockchain with cloned nodes that could influence votes.

The paper itself is presented very well. The concepts are all explained in simple, concise terms that gave me a clear picture of the topics in the paper. The paper also has a clearly defined scope which helps define the limits of what the paper covers. The examples were very well-done and consistent in a way that helped me appreciate the increasing complexity of the concepts being discussed.

Limitations

In my opinion, the main drawback of blockchains is that its underlying mechanisms are too complex and inaccessible to people not familiar with distributed computing concepts. When the main selling points of blockchain-based technologies are that they want to shake up the conventional norms of doing business, the level of knowledge required to employ blockchains in a business would mean that a person would either possess a great deal of knowledge regarding blockchains or put their trust in somebody that does. Since the applications of blockchains involve business and thus people's livelihoods and real money, it is understandable that people would be extremely cautious about adopting blockchains for their business.

Tying into this idea of confusion and haziness is cryptocurrencies. While I understand that cryptocurrencies help enable transactions without a middleman, in my opinion, having a middleman in transactions is not really that much of a negative. Banks and major e-Wallet-type apps are reliable, secure and quick ways to transfer money. They are also respected institutions subject to a great deal of Governmental regulations and scrutiny giving it more authority than cryptocurrencies. In fact, given that it is not very easy to obtain cryptocurrency, and the lack of oversight and regulation in transactions involving them, it is easy to see why cryptocurrencies are used in unsavoury and/or illegal transactions. Not helping this image of cryptocurrencies are the dime-a-dozen scams involving cryptocurrencies such as pyramid schemes, fraudulent emails involving Bitcoin, and some websites using JavaScript files to use visitors' CPUs for mining without those visitors' knowledge or consent.

While the intuitive explanation of private and public blockchains helped me to understand those concepts, in my opinion, explanations of how these blockchains are employed in the real world were scares in this paper. For example, I feel that the paper left a lot of details about ledgers vague. Where is the ledger stored? Do people who wish to mine a blockchain have to download this ledger or do they access it online. Considering blockchains for mining Bitcoin, do those ledgers contain every single transaction ever made with Bitcoin? If ledgers cannot be changed, what if an incorrect transaction is added to the ledger; could it be corrected, or would it stay there forever? Would the ledger keep growing forever? The paper has a bit of information about some of these questions, but in my opinion, a few more paragraphs could be added to explain how blockchains work in the real world.

Comments and Points for Discussion

While cryptocurrencies have technical reliability in terms of their distributed infrastructure, do they have similar economic security? The value of Bitcoin has fluctuated wildly since it has been used and I can only assume this is as true for the lesser known cryptocurrencies. While conventional currencies' value are determined by the economies of the countries they are used in as well as the global economy, the methodology for determining the value of cryptocurrencies seems much more vague and not as formalized to me.

Given how much hype surrounds blockchains, and how little of it is actually understood, it begs the question of how prevalent the use of blockchains will be in the future. It seems that every functionality of blockchains has already been implemented in a more efficient way. The main appeal of blockchains are that they bypass powerful institutions like governments and banks, but by their very definition, these institutions are powerful and won't be as easy cast into obsolescence as analogue media was by the Internet. Similar to how media companies, record labels and streaming giants coopted the Internet to ensure their survival, could we see a trend of banks and governments adopting blockchains, bringing it into the fold and legitimizing it? Proponents of blockchains are convinced that this is not a flash in the pan and is the 'next big thing', and make very convincing arguments for this. But there are many ways in which blockchains are different from previous 'next big things' like the internet and television, so in my opinion, it is difficult to make an assessment about the longevity of blockchains.

The paper in its conclusion also brought up the interesting point of how much of the work in blockchains has been done by people outside the established research community and points out that Satoshi Nakamoto's paper on Bitcoin lacks academic rigour. It is interesting to have an area with this kind of distinction, and a lot can be read into this observation. It also raises the question of whether there will ever be a convergence of these two groups in work on blockchains.

Conclusion

This paper was a concise, well-explained primer of the concepts and mechanisms employed in a blockchain from the point of view of distributed computing. The paper acknowledges the hype and hysteria surrounding blockchains and demystifies its workings for a novice audience. It highlights the stark differences in the two distinct groups working on blockchains and calls for them to pay more attention to each other