Willis Allstead
11/29/18
CS 491

Review of: Towards Dependable, Scalable, and Pervasive
Distributed Ledgers with Blockchains

The presentation of this paper is very clear, they explain many aspects of blockchains and how different parts of blockchains interact. They also pose interesting uses for these aspects of blockchains in the industry throughout the paper. Connecting the ideas to actual use cases in the industry is important for any fledgling technology, especially one associated with massive economic bubbles, such as the Internet back when it was new. The problems this paper tries to address are making ledgers more dependable, scalable and pervasive. This paper also generally acts as an educational tool for learning why certain parts of distributed ledgers were created and how they interact. Due to this field being relatively speaking very new, there are a lot of pieces of the distributed ledger puzzle that need extensive research before wide adoption in the general business world. This paper is structured as an exposition of blockchains, rather than one that focuses on specific ways of making them better.

Currently the most talked about application of blockchain technology is Bitcoin and a number of other alt-coins as they are called. One such alt-coin is Ethereum, which is focused on provided a Turing-complete language to developers that is able to execute arbitrary code (called Smart Contracts) to support the adoption of decentralized apps. They cover the concept of a Smart Contract, giving a specific example of the types of functions that you might want to include in that contract. I think it would have been nice to include a section in this paper regarding the vulnerabilities of blockchains. Specifically on the topic of Smart Contracts I have read many posts online about the different vulnerabilities that have been discovered, and how some ways of fixing these are simply to make changes to the compiler for a smart contract language, but that some vulnerabilities currently are things you just have to keep in mind when you create the contract. If a smart contract is written without taking these vulnerabilities into account, it could result in a lot of people losing a lot of money. And people losing money to something they have no understanding of is the *opposite* of the sort of thing you want happening to further adoption.

The paper also touches on different ways of providing consensus within a network, the most popular being proof-of-work. This one is used in Bitcoin and many others. They also touch on the idea of proof-of-stake in the paper, which I think they should have expounded on. When the Cryptocurrency bubble was at its most recent peak I remember stories being written about how the amount of energy being used in the proof-of-work system for Bitcoin was larger than the energy use of some countries. In an age where I believe most people at least acknowledge that

climate change is happening, it seems weird to the public for such a forward thinking technology to use so much energy. And in the case of bitcoin, where you use it as currency only, why would we switch to using that instead of just using our debit cards that use existing technologies like databases that take far less energy to run? Questions like this are not answered in this paper.

Another topic mentioned is the Lightning network, a solution to a couple issues happening in Bitcoin, including the cost of a transaction. But again, this paper doesn't talk about what I immediately think of here, regarding the high cost of a transaction. I don't believe people will switch currencies if it costs them more money or time to go about their day making transactions. These issues, while they seem small, add up to be the main force stopping the wide adoption of cryptocurrencies in the public. They need to be addressed, and I am surprised that the writers didn't acknowledge any of them properly.

With the hype of Cryptocurrencies that happened near the end of last year, and the pop in the bubble that occurred soon after, there is definitely a lot of skepticism from the public when it comes to the term "blockchain". Maybe once enough research goes into the area and different applications of blockchain technology becomes used more in public-facing products or platforms, people will realize that blockchains != cryptocurrency necessarily. Some aspects of blockchains are simply too perfect to toss they baby out with the bathwater, per se. For example the ability to have public ledgers that are verifiable by anyone, with the power of the group is amazing in itself. Things like supply-chain management are perfectly suited for blockchain technologies. Imagine if the medical industry started using distributed ledgers to track the exact costs of medicine and other expensive materials. A lot of the over-inflated prices in certain industries like medicine could come down to a lack of transparency in actual costs of materials, services, etc.