Bruce Darcy
CS481 Blockchain
Dr. Gersh

Homework 3

Bruce Schneier makes some really good points about how we don't actually remove all the trusts of society when we use blockchain. The fact the etherium forked is proof of that, there are people on the outside controlling and making decisions about the blockchain system. As a computer scientist, I also know how common bugs and exploits are in anything having to do with technology. A big problem he highlights also, is that most people can't take the time to acquire the technological expertise to understand how blockchain works, and how to be completely safe using it. Intermediary companies are always going to be vulnerable to losing people a lot of money.

Bruce Schneier claims that we don't need blockchain, because the trusts we have in other areas, such as the banking and legal systems, are good enough and don't have issues stemming from technology such as bugs and exploits. One thing I didn't see him consider in the article, is cryptocurrencies use in a lot of countries internationally where things such as inflation and corruption is common. For example, in Zimbabwe, where massive inflation ruined most of the financial system, cryptocurrencies have helped many people survive financial ruin, and continue trading and economic activity. Similar situations have happened in Venezuela, other countries in Africa, and countries in Southeast Asia. Schneier argues that one of the biggest problems with blockchain is that there are many critical points of failure in the technology. What we have seen worldwide, is that often governments can be an even worse point of failure. From a western democracy point of view, our systems are pretty good and trustworthy. That's not the case for most of the population of the world however. Even so, in developed countries with trustworthy systems there's reason enough for people to want to diversify wealth into places that are not controlled by one government or system. Through history, systems bigger than the ones we trust today have failed for people.

I agree with the idea that blockchain is overhyped, and not needed for many things people want to use it for. Bugs and exploits are a problem that take a lot of care to deal with correctly. However, blockchain is simply a tool. Large banks get hacked a few times a year. Anything under the sun has vulnerabilities and ways to exploit a system. Blockchain isn't great for everything, and for some applications it might just be a little big better rather than the change all greatest thing that system has ever seen. But if it can improve something, it's still a good thing and worth using. On another note, about his comment about people losing life savings in cryptocurrencies, that comes to a very basic rule of investing that can be learned in high school business class: diversify your investments. It's not a good idea to have all your money in any one thing, not matter what that thing is.

https://blockonomi.com/cryptocurrencies-developing-countries/