9/22/20

**Computing Innovation Final Project**

BLOCKCHAIN

Though often used as a fancy technology buzzword, blockchain is in fact a well-defined protocol, that allows for some very cool new developments. In essence, blockchain allows for a removal of centralization online. This has far reaching implications, from its typical use in cryptocurrencies to more esoteric functions in medical, political, and person fields.

SO WHAT ACTUALLY IS THIS THING?

Blockchain is, for all intents and purposes, a community ledger. Anyone can add to the ledger and use it to keep track of all sorts of things. The key with blockchain is that it incorporates two cryptographic technologies to turn a typical ledger into something much more powerful. The first is a cryptographic signature. A cryptographic signature is essentially just a number, but through complex math it is able to verify the identity of the person who uses it, without being copiable. This prevents people from stealing the identity of others. The second is more complicated, but in essence, it’s a mechanism that allows anyone to be sure that their copy of the ledger is the same one that everyone else has, by linking every message together. These both seem like small additions, but they allow for some very big developments.

IMPACTS

By combining the two aforementioned elements, a blockchain ledger can be distributed, held, and broadcasted by anyone who’s part of the ledger. This gives the ledger decentralized properties: there’s no need for a large, trusted middleman. This feature is why blockchain is the foundation for cryptocurrencies. They allow banks to be hacked out of the equation, by letting users safely do all of that functionality themselves. However, the ability to create a safe, decentralized ledger with user authentication has the potential for use in nearly every field of cryptography.

DATA USES

Blockchains can be used for almost any kind of data. Any user can add something to the chain, which will then become visible to all other users. And thanks to the prior techniques, this process is assured to be safe and reliable.

DATA CONCERNS

Blockchain is widely known for its ability to prevent data issues. However, it’s not perfect. Thanks to the nature of its safety features, it can be compromised. If any agent gets more than 50% of all contributing computing power, they can fully control the chain, making users see items that other users can’t. This would naturally wreak havoc on any critical technology that was depending on it. Though no one person could practically do this, a massive corporation like Google or a country like China might. This poses a real risk if blockchain was to be incorporated into something like an election.

CONCLUSION

Blockchain is fairly wonky