Devere Anthony Weaver
COSC670 – Cryptocurrencies and Blockchain
Assignment A0 – Part I

The first cryptocurrency I found interesting is Monero. Currently, Monero (XMR) has a market cap of about $2,678,358,091. I was confused reading the white paper as it was describing something called CryptoNote, not Monero. After further reading, I found that CryptoNote is the name of an application layer protocol that addresses perceived issues with Bitcoin by specifying untraceability and unlinkability properties. Monero is an implementation of CryptoNote.

Monero was first created to give users the ability to execute transactions with cryptographic privacy, this is the value of Monero. This contrasts with Bitcoin where typically a user's wallet is tied to a personal identity. Even if the personal identity is unknown, their transactions are still able to be tracked and correlated by analyzing data from the underlying blockchain. With Monero, it is almost impossible to correlate any transactions with a specific wallet and thus any specific user. There is a fair amount of cryptographic material in the white paper, so to keep this paper short, I'll simply just give a high-level view of how Monero implements the properties of untraceability and unlinkability.

In typical cryptocurrency transactions, the destination address of a transaction is a user's public key. However, CryptoNote specifies by default, each destination address is a public key, but it is derived from the recipient's address and random data that is derived from the sender's payload. This ensures each transaction has a unique one-time public key that can't be linked to any specific address and its user. The only downside to this algorithm is that Monero addresses are twice as large as Bitcoin addresses, but it does cryptographically guarantee unlinkable transactions.

To implement untraceability, the CryptoNote protocol specifies the use of what's known as a one-time ring signature. Normally, one signature is linked to exactly one user's private key. The general idea behind the use of a one-time ring signature is that when a user generates a signature for a transaction, the signature is generated in a manner that, mathematically, it could have been generated from an exceptionally large pool of private keys. With quite a bit of work, one can narrow down the pool of private keys; however, this pool will still be large and it's equiprobable that each private key could have generated the signature. Hence, untraceability.

Seeing that privacy is a persistent issue, I would project that Monero will still be in heavy use for the foreseeable future. Being a public ledger is considered a huge design flaw in blockchain technology by some and this implementation addresses the flaw. Regarding how this affects the greater ecosystem, I've now seen other existing coins that are attempting to implement some form of privacy-preserving protocol to provide an optional layer of privacy.

Having a mathematics background and some interest in applied cryptography, I found the material in the paper to be a fascinating use of applied cryptography and it introduced several new concepts that are well outside of my wheelhouse. The portion of the paper on unlinkable payments is a form of elliptic curve cryptography which was somewhat straightforward and makes sense after sitting with it for a few days; however, the portion on the one-time ring

signature algorithm is still a bit of a mystery to me so I'll assume that it's just magic until I can confirm otherwise.

The second cryptocurrency that piqued my interest is the AXL token by the Axelar network. In the world of blockchain technology, multiple blockchain systems don't communicate easily with each other due to the different protocol implementations. Since these are typically distinct features, developers building an application may need one blockchain to build on but may desire some features of another, meaning they must implement it themselves or just sacrifice the feature altogether. This is where the Axelar network comes into play. According to the white paper, it was created to enable applications to communicate across different blockchains by providing developers protocols, APIs, and other tooling which simplifies the communication process, this would be its perceived value. The Axelar network utilizes the AXL token as a proof-of-stake token that supports smart contracts. Currently, AXL's market cap sits at about $1,457,537,436 as of the time of writing.

This coin was interesting to me because this isn't a problem that I would have even thought of having to address. The paper is interesting because they went into a bit of depth on how they specified the decentralized network structure and how the protocols can link blockchains. Specifically, the most relevant sections of the paper to me are found in sections 5, 6, and 7 where they specify, at least at a high level, the engineering decisions made to design an open cross-chain network that met their technical requirements. Later in the same section, they discuss what security concerns go into designing a network such as this one and then specifically how Axelar addresses them. Sections 6 and 7 were the crux of the paper where they describe the actual protocols responsible for synchronizing the state between blockchains and how they can transfer assets between them. Again, for me, these are compelling problems that I would not have thought were even a problem in the first place.

While I did enjoy reading the paper, the more appealing part is that since it is an open-source project, I decided to poke around in their GitHub repo to see what an actual web3 project looks like along with running examples. This is important because as someone on the outside looking in, the thought of using or developing a web3 application feels intimidating and would require some level of expertise but it is not really any different than using any other web application.

Regarding the future of this project and how it affects the greater ecosystem, I would have to take the cop-out answer and say, it depends. Since I don't know much about development with these tools, I can only really speculate that if cross-chain communication is a problem that developers and users care about, then this feels like it has a bright future considering its current progress and contributions from open-source. It seems like they already have the lead on this one. Again, if this is the case, then AXL would have a large positive impact on the ecosystem in that it allows for easier development. Whenever the barrier to entry for development is lowered, there always seem to be amazing and unique projects that take shape due to the creativity of the developers and the larger pool of people willing to build upon it.