Devere Anthony Weaver
COSC670 – Cryptocurrencies & Blockchain
Assignment 0 – Part I

The first cryptocurrency that I found interesting is Monero. Currently Monero (XMR) has a market cap of about $2,678,358,091. Upon initially reading the white paper, I was confused as the paper was describing something called CryptoNote, there is no mention of Monero. After doing some further reading, I found that CryptoNote is simply the name of an application layer protocol that attempts to address perceived issues with Bitcoin, mainly by specifying untraceability and unlinkability properties. This is the protocol Monero implements.

Thus, Monero was first created to give users the ability to execute transactions with cryptographic privacy, this is its derived value. This contrasts with Bitcoin, where typically user's wallet address is tied to a personal identity. Even if the personal identity is unknown, their transactions are still able to be traced 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 paper thus, to keep the 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 that by default, each destination address is a public key, but it is derived from the recipient's address and random data which is itself 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 user. The only downside to this algorithm is that Monero addresses are twice as large as a Bitcoin address, 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. So, 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 a very large pool of private keys. With quite a bit of work, you 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, we now have untraceability.

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

Having a mathematics background and some interest in applied cryptography, hence why I knew about Matthew Green's work, 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 basically a form of elliptic curve cryptography

which was somewhat straightforward and makes sense after sitting with if 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, there are multiple blockchain systems that don't communicate easily with each other due to the different protocol implementations. Since these are typically distinct, developers building an application may need one blockchain to build on but may desire some features of another, meaning they most likely 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.

The reason I found this cryptocurrency interesting is that being a complete novice to the world of cryptos and blockchains, I would have never thought that being able to communicate across a network of different blockchain ecosystems was a problem that people would have in the first place and of course I would have never thought that there needed to be a solution.

The paper was also interesting because they did go into a bit of depth on how they specified the network structure. 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 wouldn't have thought were even a problem in the first place.

While I did enjoy reading the paper, I think the more appealing part is that since it's 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. I believe 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 ultimately it isn't 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 really 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 seems 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.