Galaxis: Scalable Privacy within a Smart Contracts Protocol

***Tao Minoru, Ashton Linker, Carter Hilliard**

Abstract: A p2p network built on the basis of enabling various users to both run and store private data, while simultaneously providing instant, feeless transactions, and a smart contracts platform for decentralized applications. The Galaxis model is an optimized version of verifiable, but anonymous contract sharing. The network will run as its own chain, while having an off-chain solution in order to become a universal blockchain that can handle public and private information.

The Problem

The incredible growth of the internet has, thus far, coincided with an increase in centralization. As fewer and fewer companies begin to maintain control over massive portions of the web, they attain more and more data while providing less and less transparency. This is an example of just one negative side effect of centralization.

Bitcoin and other blockchains have begun to disrupt this space, and allow us to envision a new future. We can now have applications built on a decentralized foundation, where no single entity can maintain control over the network. We can now have transparency of data within applications, and work through an immutable record of activity. In many ways, Bitcoin itself as a currency was the first application built on top of the blockchain, but we now can see the drawbacks of such a model.

Since then we have seen countless attempts at finding a solution for what things like Bitcoin and Ethereum have yet to perfect. A single and limitless blockchain platform

that can easily scale for mass adoption, while still being free to use… just like the current internet is. A service that can offer transparency OR privacy, based on the goals of the user. A smart contracts platform for developers to build upon without having to worry about whether or not their product can actually run efficiently, or will be bottlenecked by the outdated technology on which they are building.

The Solution: Galaxis

Galaxis is many things. It aims to be a one stop solution for blockchain services, that will render all platforms before it obsoleted… Blockchain 4.0, if you will. Our goal is to allow developers to build in their own way, while also allowing users of the chain to participate by using products built on Galaxis and/or simply creating feeless transactions on the network. This may sound simple, but has not yet been done in a way where all entities on the network are equals.

- ***Fast & Free TX's***

  The use of a network currency, the XLS token, for FREE transactions. A DPoS foundation where network fees are scrapped in favor of a 'computational power borrowing' [CPB] method which applies to stakeholders, who receive XLS for helping to secure the network.

- ***Scalability Through Distribution***

  Galaxis will allow scaling unlike any of its predecessors because of its unique design and computational distribution. A small amount of PoW is performed by all users on the network, regardless of their status [developer, user, stakeholder, etc.]. This allows the platform to easily scale without having any noticeable bottlenecks.

- ***Optional Privacy – The First of Its Kind***

  A simple design of transparency versus anonymity will allow users to specify whether or not the action they will perform on the Galaxis network will be private or transparent. Galaxis accomplishes this by using a simple block status for transparency and sMPC [secure Multi-Party Computation] for private actions on off-chain mini platforms. No single entity ever has access to any set of data in the anonymous pool of activities on the network.

The Galaxis Protocol

The core design of Galaxis works by utilizing off-chain connections in order to off-load any private data and heavy computational requirements. Currently in our space, we have projects like Enigma which handle these intensive workloads as service to an existing blockchain platform. Developers must still construct smart contracts on something like Ethereum, while the Enigma protocol helps with storage and scaling. While clever, this is far from ideal. Why?

Because what if these issues that hinder blockchain technology so severely, actually only require one solution as opposed to multiple parties trying to simultaneously 'band-aid fix' a fundamentally flawed protocol? Early adopters of the internet admit that if time could be reversed, the web would have been built in an entirely different way… so why continue adding top layer improvements onto poor existing technology, especially when the space is so young that a new network from scratch is the best solution?

This is what Galaxis is offering. With the Galaxis protocol, coding is done on both the main blockchain and the Galaxis off-chain networks, or 'side-chains'. These side-chains

ensure privacy while freeing up the main network - the main chain will host all transparent and public activity, same as a traditional blockchain platform. The scripting language is also turing-complete for designers looking to work on decentralized apps.

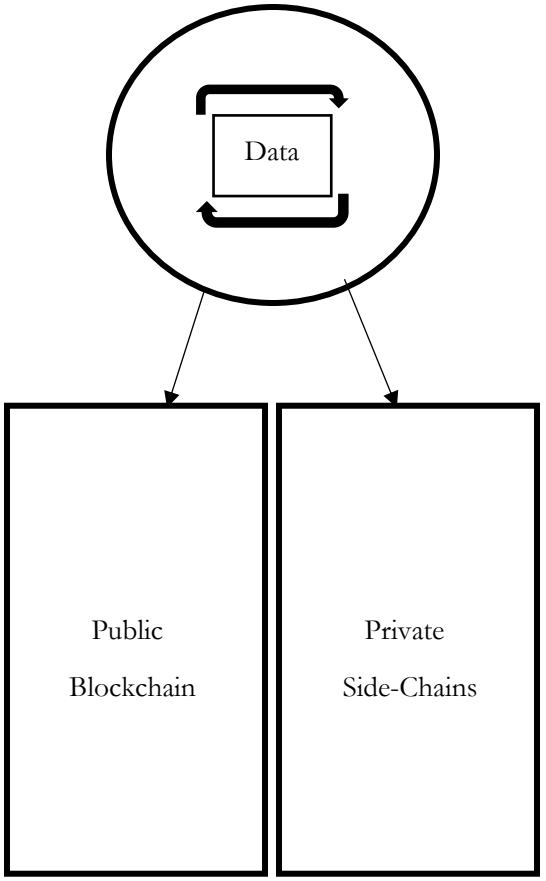

Figure 1. Design of implementation of coding via main and side chains.

Storage is accessible through the main blockchain, even though it is not directly held there. The chain will have 'keys' that are linked to each piece of encrypted data, stored off-chain. Our protocol will also be able to execute code without sacrificing any of the raw data to the nodes securing the network.

Details on the XLS Token

Ticker: XLS, ERC20 at the moment

Token Supply: 5,000,000,000 XLS

Contract Address: 0x308C8644953F7bBe8b4e15528169c2985770FC6C

Network Details

In order to maximize the efficiency of the network, CPB is distributed randomly to a subset of users. These users are selected to lend computational power when they are running a node; the choice is made based on reputation of the node, which is accumulated over time, as well as load balancing. With this method, the network is fully operational at all times regardless of usage.

Coding on Galaxis will not leak any information unless the network falls victim to a majority attack.

The XLS token is the heart of the incentive program on the Galaxis blockchain. Fees are non-existent to users of any DApps and anyone simply making transactions over the network. All fees are paid by developers using the protocol to build upon. Fees are split up as rewards to users who secure the network by running nodes. This setup creates incentive for users to transact over the network, while simultaneously offering rewards for those who are willing to offer up their computational power to help keep the protocol safe.

All fees are a fixed percentage, but since the platform is turing-complete the cost of an activity cannot be pre-calculated accurately in every instance. Once a computational act is complete, the cost of each action is deducted from the account balance of each node.

Works Cited

[1] Diamond, Jared, and Germs Guns. Steel: The fates of human societies. New York: W. W. Norton, 1997.

[2] de Montesquieu, Charles. The spirit of the laws. Digireads. com Publishing, 2004.

[3] Perry, Barlow John. A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation 8, 1996.

[4] Vindu Goel. Facebook tinkers with users emotions in news feed experiment, stirring outcry. The New York Times, 2014.

[5] James Ball. "Nsas prism surveillance program: how it works and what it can do." The Guardian, 2013.

[6] Bill Hardekopf. "The Big Data Breaches of 2014." Forbes, 2015.

[7] Nick Szabo. "The dawn of trustworthy computing." 2014

[8] Nick Szabo. "The God Protocols." 1997

[9] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Consulted 1.2012 (2008): 28.

[10] Clark, Joseph Bonneau Andrew Miller Jeremy, Arvind Narayanan Joshua A. Kroll Edward, and W. Felten. ”SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.”, Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.

[11] Maymounkov, Petar, and David Mazieres. ”Kademlia: A peer-to-peer information system based on the xor metric.” In Peer-to-Peer Systems, pp. 53-65. Springer Berlin Heidelberg, 2002.

[12] Yao, Andrew C. ”Protocols for secure computations.” 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. IEEE, 1982.

[13] Ben-David, Assaf, Noam Nisan, and Benny Pinkas. ”FairplayMP: a system for secure multiparty computation.” Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008.