ITESM Software Development

Submit Date: **February 13th, 2017**	**Requestor Info:** **Fernando Lobato Meeser** +52 1 442 467 43 23 lobato.meeser.fernando@hotmail.com **Sponsoring Organization:** **ITESM campus Qro.**

Project Title:

IndieCoin

Project Description:

I sincerely believe that banking institutions are more dangerous to our liberties than standing armies. The issuing power should be taken from the banks and restored to the people to whom it properly belongs.

- Thomas Jefferson

IndieCoin is a light weight implementation of a decentralized cryptocurrency. A cryptocurrency is a digital asset that can work as a medium of exchange using cryptographic principles to ensure security.

A decentralized cryptocurrency allows to parties to transact over an electronic medium without a trusted third party. In today's world if Alice want to send some form of value to Bob, she either must be physically in the same room with Bob to give him some form of cash or asset; or she must trust a third party to send money to Bob (Credit card, bank, western union, friend who will meet Bob). Not all people in the world have access to financial services. Decentralized cryptocurrencies allow any two parties to transact over an electronic medium without the need to trust a third party. Since there is no third party, there is a great deal of anonymity that does not exist in any other electronic medium. Currently carrying transactions over electronic mediums results in very high fees for the parties transacting because of the need to mediate disputes for the third party. This prevents a lot of markets from being accessible outside of their physical realm. Decentralized currencies present an economic scheme that brings these fees to a minimum.

While the field of digital currency and money is not new; the idea of having a decentralized system while keeping consensus could not be achieved until 2009 with Bitcoin. Bitcoin implements a concept called a blockchain. A blockchain is a distributed database where everybody keeps a copy of the records so anybody can verify the consistency of new transactions. In this case, it works as a p2p network. Every specific amount of time a new block is created (*mined* in cryptocurrency slang) by putting together several transactions. Then each node in the network must solve a proof of work, the first node to solve the proof of work broadcasts the block containing the newly validated transactions and the solution to the proof of work to all other nodes on the network. As nodes receive blocks they validate all transactions inside them to the previous copy of the block chain, incorporate the new block into their copy of the blockchain and begin looking a new block. Since the proof of work in the network is automatically adjusted to the computational power of the network and if someone in the network does not have the majority of the computing power, the network is safe from double spending. This is just an overview of how consensus is kept in a blockchain, in further documents there will be a detailed explanation of all aspects involved in the architecture of such a system.

Cryptocurrencies have sparked a great deal of innovation in the Fintech community because of its technological breakthroughs. Since the release of Bitcoin there have been a great of different cryptocurrencies (alt coins). Most of this coins are simply a fork from the original bitcoin source code (which is open source). Being a relatively new field there is still a lot of innovation and research to be done. Nevertheless, being such a young field it lacks a great deal of experts and developers working in ways to bring better payment systems to our digital world. The technology briefly described earlier (blockchain) can be a starting point for creating a lot more things that just currencies. It is the first time in history we can have trust without the need of a central authority.

Another important aspect is the generation of coins. Each node is racing all other nodes for a period of time to have their block included into the blockchain. This happens because this is how the coin is generated. Each node includes a transaction at the beginning of every node sending a specific amount of non-existing coins to themselves. The miner who get his block published into the blockchain first get everybody to agree that he now owns a specific amount of coins that did not exist before. This adds an incentive to miners to keep the network honest. The more people that trust the network the more valuable their asset becomes.

The last important high level aspect is how is value transferred and accounted for in transactions. The blockchain is just a reference of attributing value to this abstract coins. When a coin is generated through the process described earlier called mining, this coin is tied up to the identity of the miner (person who owns the computer who found the new block). The network is anonymous and the way we bind identities is with the use of Asymmetric Cryptography. Every user has a public key and a private key. When they are going to receive money from someone else they send the other party their public key. That who will be sending payment takes some of his previous coins and creates a transaction. A transaction can be seen as an announcement where a party references previously owns coins and says that now the person who presents a digital signature to a specific public key will be able to spend those coins. At the same time, the person spending those coins must present a signature to the public key that was referenced in the previous transaction of those coins. This way the system is kept secure. Only the person who holds a private key referencing certain coins can actually spend them.

Cryptocurrencies have sparked a great deal of innovation in the Fintech community because of its technological breakthroughs. Since the release of Bitcoin there have been a great of different cryptocurrencies (alt coins). Most of this coins are simply a fork from the original bitcoin source code (which is open source). Being a relatively new field there is still a lot of innovation and research to be done. Nevertheless, being such a young field it lacks a great deal of experts and developers working in ways to bring better payment systems to our digital world. The technology briefly described earlier (blockchain) can be a starting point for creating a lot more things that just currencies. It is the first time in history we can have trust without the need of a central authority.

The actual bitcoin blockchain implementation is a very big and complex project for someone completely new into this are to understand. To understand it one must master c++, and need a lot of theory into GNU build system. While they are the current tools to implement the bitcoin blockchain, they are not needed in

theory to understand and begin to build and test new blockchain applications. The purpose of this project is to create a scaled down version of a cryptocurrency, following the footprints of many existing currencies and implementing a simple blockchain in a p2p network in the python programming language, that allows any newcomer into the blockchain to easily understand the technical concepts and can build and modify simple prototypes.

As of now (2017) there exist a great deal of online resources of how blockchain works. Very few of this online resources cover any technical details that would empower developers to be able to understand the blockchain in a deeper sense.

Requestor's Due Date: 27 March 2017

Business Objective:

The objective of this project is to create a solid starting point for any curious developer or engineer that wants to understand the technical aspects of blockchain implementation in cryptocurrencies. This will give them a bigger insight into blockchain itself and can complement the existing books and articles that already explain the theory without diving much into technical aspects.

Business Requirements: *(Describe from a business perspective what the change will include. Provide the current process and the desired future process within this section.)*

The scaled down version should allow anyone who downloads the application and follows the development guide to run a node that connects to multiple peers in the network. The node should be able to request blocks from the network until it has an updated copy of the blockchain. Once a node has a complete copy, it can begin to listen and relay transactions. Every specific amount of time it will try to put these transactions into blocks and will also be listening to incoming blocks. At the same time a node should cooperate and deliver information requested to its peers.

The blockchain uses digital signatures to verify the authenticity of transactions, a node should be able to listen for transactions and create new transactions if the proper credentials are provided by the user.

Business Impact:

With the current lack of technical didactical materials for understanding the blockchain and cryptocurrencies, the field is restricted to few people who are willing to go through a great deal of research and abstraction to understand the implementation of something that is not that complex. It is just new and needs more people focusing on how to transmit it to others in an understandable way.

Business Value:

Cryptocurrencies have showed us again one very important thing. "Value does not exist outside the consciousness of men.[1]" When Satoshi Nakamoto released the bitcoin white paper into the public domain, very few people could see the actual value of what that abstract idea could become into. While there is no specific way to quantify this project yet, it's value lies in the power that it can give to the next generation of developers so that their abstract ideas of re-shaping the way we interact become billion dollar ideas. Just as bitcoin today (16 billion-dollar market cap.).

Budget Information:

A test server and a developer are needed to develop this project.

Specific Customer Information: *(If change is for a customer please provide the following)*

This project is not for a customer.

Impacted Application / Product: *(Describe which application/product will be impacted by this change.)*

The purpose of this project is to create a scaled down version of a decentralized cryptocurrency. This means that development must be made from zero, without impacting any current technology.

In terms of the impact that this development could bring to other existing tools; There will most likely not be any big impact since more complex and optimized versions of this idea are already implemented.

[1] Carl Menger http://www.incrementum.li/en/austrian-school-of-economics/the-austrian-view-on-value/