MSDS 7349 – Term Project Proposal

Blockchain Technology – A Survey and Tutorial

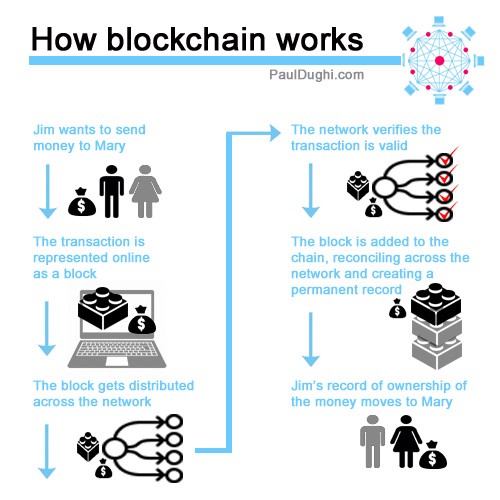
Steven Cocke (cockes@mail.smu.edu), Daniel Davieau (ddavieau@mail.smu.edu), Alex Salamah (ysalamah@mail.smu.edu), Lakeitra Webb (lwebb@mail.smu.edu), Randall Hendrickson (rhendrickson@mail.smu.edu)

## Abstract

Blockchain, the foundation of Bitcoin, has received extensive media attention recently. Blockchain serves as a distributed, immutable ledger which allows transactions to take place in a decentralized manner. There are many challenges facing blockchain technology such as security, scalability, and legal implications. We will attempt to provide a broad overview on blockchain technology and its fundamental architecture and algorithms and mathematical background. We will provide an evaluation of an experimental blockchain database and implementation.

## Introduction

Blockchain technology is increasingly being used in various industries such as healthcare, banking, supply-chain, finance, social media and is the heart of Bitcoin. The goal of this project is to provide a survey of the current research and a tutorial on blockchain technology.

The blockchain idea was conceived back in 2008 to support bitcoin cryptocurrency exchanges. It is a very special decentralized transaction and data management technology that is critical for ensuring enhanced security and (in some implementations, non-traceable) privacy, security and data integrity of transactions between participating parties without going thru a 3rd party and without the third party being in control of the transactions. Even though cryptocurrency such as Bitcoin, Litecoin, Ethereum, and the like, is highly controversial, the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and nonfinancial world. Furthermore, BC uses a changeable Public Key (PK) to record the users’ identity, which provides an extra layer of privacy. Not only in cryptocurrency has the successful adoption of BC been implemented but also in multifaceted non-monetary systems such as in: distributed storage systems, proof-of-location, healthcare, decentralized voting and so forth. Recent research articles and projects/applications were surveyed to assess the implementation of BC for enhanced security, to identify associated challenges and to propose solutions for BC enabled enhanced security systems.