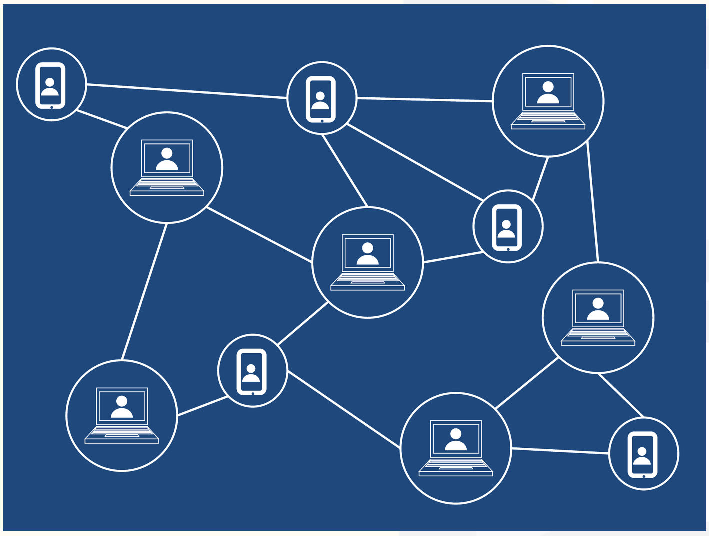
University of Victoria

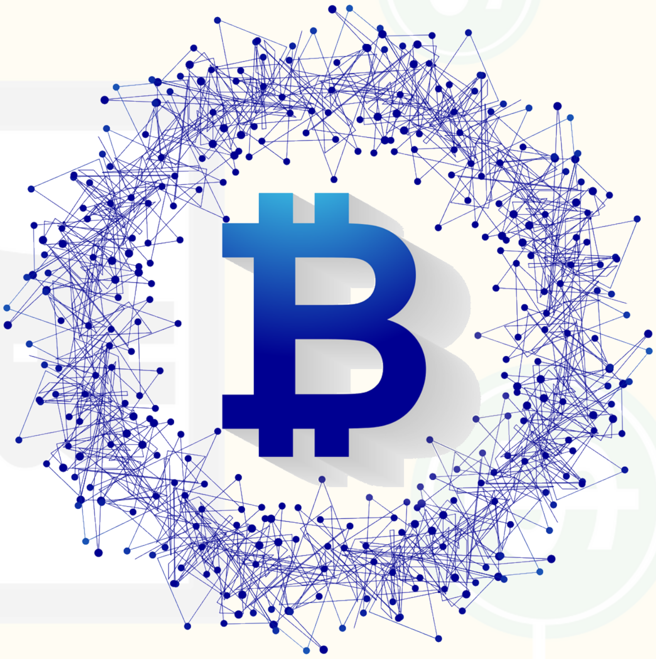
Faculty of Engineering

ENGR 446: Milestone Report II: Engineering Analysis

Simplification of Transactions by leverage blockchain technologies and smart contracts

David Li Computer Engineering V00818631





June 9, 2018

In partial fulfillment of the academic requirements of this academic course

Table of Contents

List of Figures

List of Tables

1. Proposed approach

2. Engineering Analysis

2.1. Security of private keys

A ethereum key, which is randomly selected 256 digits [1], is very difficult to hack. The calculation below illustrate the impracticalities of brute force hacking for a 256 bit ethereum key.

Assuming that a 1 exaflop (10^{18} calculations per second) 15 megawatts supercomputer [3] is used, electricity costs are 0.1326 per kWH [2]. In order to hack a 256 bit key by brute force 2^{256} decryptions are required. Powering the machine costs $ 1.989 million excluding maintenance and hardware costs. It can perform

$$10^{18} calc/s \times \frac{3.154 \times 10^7 s}{1 year} = 3.154 \times 10^{25} calc/year$$

$$2^{256} = 1.1569 \times 10^{77} calculations$$

So in order to brute force hack a private key in a year

$$Numberofmachines = \frac{1.1569 \times 10^{77}}{3.154 \times 10^25} = 3.66804 \times 10^{51}$$

or 3.66804×10^{51} years for a single supercomputer.

3. Discussion

A. Project Background

A.1. Background

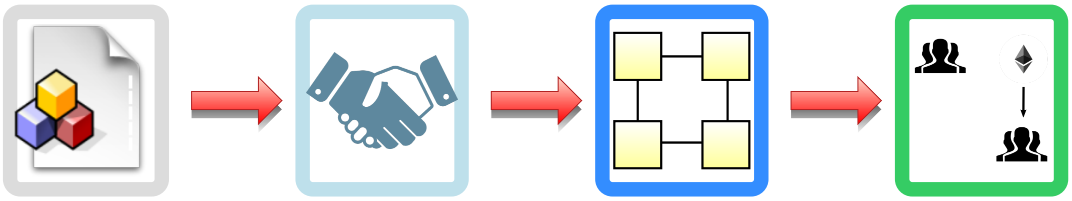
In 2008 bitcoin white paper [1] described a way to solve the double spending problem without a centralized body using blockchain. Although, the value of bitcoin (BTC) has grown exponentially, high computational and energy consumption in mining and slow performance [2]. Released in July 30, 2015, Ethereum, an open-source platform based on blockchain technology, distinguishes itself from bitcoin through faster transactions, unlimited processing capability for smart contract, and its network is optimized to support Decentralized Applications [3].

Table A.1. Timeline of Cryptocurrency

2008	Bitcoin White Paper
2009	Bitcoin Genesis Block
2013	1 BTC = $ 31 USD
2013	Ethereum White Paper
2015	Ethereum Genesis Block
2015	HyperLedger starts
2017	Over 1000 different cryptocurrencies
2018	AWS Blockchain Templates

Blockchain technology is revolutionizing the internet by establishing trust in shared data. [3]. Additionally, transactions recorded on the blockchain are practically impossible to remove or change. A decentralized application, or DApp are deployed on peer to peer networks such as Ethereum or on the cloud.

Traditional legal contracts are written to represent the contracting parties. In a smart contract, self-executing source code is used to automatic transactions that are publicly available on the blockchain [3].



SOURCE CODE	TRANSPARENT	BLOCKCHAIN	PAYMENT
self-executing code that faciliates agreement between parties	terms of contract are available on the public ledger	event triggers the execution of the contract (redeeming a ticket)	accounts are updated, parties recieve amounts based on contracts

Figure A.1.: Illustrating how a smart contract works

A.2. Objective

The prominence of cryptocurrency and decentralized applications suggests usage of smart contracts will experience explosive growth.

A.2.1. Problem

Currently commonplace transactions require days to process and for parties verify correctness. For example to purchase houses, a plethora of steps are required, one must interactive with lawyers, real-estate agents, home inspector, buy insurance and shop for a mortgage.

A.2.2. Purpose

Leveraging existing blockchain technologies can automatic the majority of steps and cut out the middlemen, resulting in buyers conversing directing with sellers.

A.2.3. Aims

The aims of this project are to develop a decentralized blockchain system that:

1. Reduce cost of transactions by at least 50% from removing middlemen.
2. Improve transparency in software systems through augmented accessibility and understandability.
3. Has increased reliability and more secure than traditional systems.

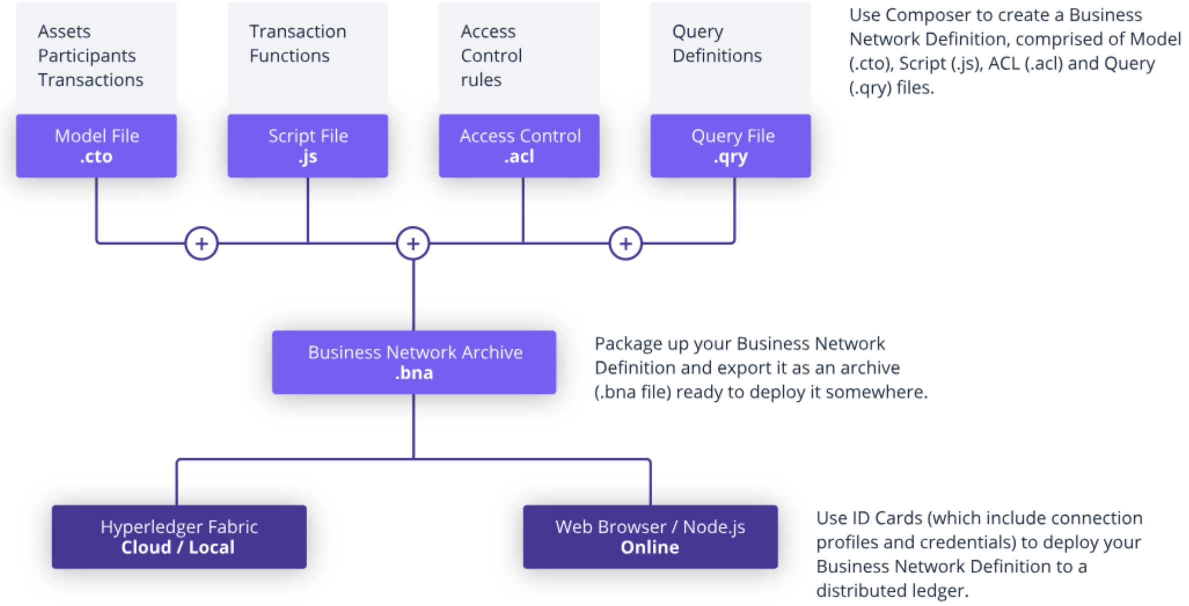
A.2.4. Limitations

The regulatory uncertainty and impact of future regulations on blockchain technologies such as smart contracts will not be investigated. In addition, criminal usage of cryptocurrencies to avoid taxation and legal repercussions are beyond the scope of this report.

A.3. Potential Solutions

- Public blockchains are large distributed networks that are run through a native token such as bitcoin or ether. Anyone can participate and the community maintains its open-source code. The two largest public blockchains are Ethereum and Bitcoin. They are open for anyone to participate at any level and have open-source code that their community maintains.

- Permissioned blockchains define role based access control for individuals in the network and uses native tokens. HyperLedger Composer, an open-source framework for permissioned blockchains, is used for smart contracts and for blockchain application development [4]. One use case is an accounting system that calculates payment, while hiding that information from unrelated organizations.



Use Composer to create a Business Network Definition, comprised of Model (.cto), Script (.js), ACL (.acl) and Query (.qry) files.

Package up your Business Network Definition and export it as an archive (.bna file) ready to deploy it somewhere.

Use ID Cards (which include connection profiles and credentials) to deploy your Business Network Definition to a distributed ledger.

Figure A.2.: Architecture of Hyperledger composer

- Private blockchains membership is tightly controlled and lacks a native token. Useful for consortiums with trusted associates and exchanging confidential information, however, less powerful because it is supported by limited private resources. Large organizations such as governments will likely use these extensively.

A.4. Initial Assessment

Determining which platform is best for smart contracts should be done using a weighted decision matrix, based on the particular application. For internal processes such as supply chains, a private blockchain makes sense (data cannot be changed) and cryptographic auditing with known identities (public keys). For a trustless system that verifies every transaction, using a public blockchain is essential. In comparison, role-based access control is feasible by using a permissioned blockchain.

Despite the slow speed of the public blockchain, innovations such as side chains enable quick transactions and are used in decentralized game development [5]. A permissioned blockchain allows role based access control which is essential in business applications. One example is to prevent unrelated parties from viewing other's data. Furthermore, smart contracts allow buyers and sellers exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman. This allows validation of complex transactions swiftly while maintaining transparency.

Table A.2.: Sample Decision Matrix for designing a blockchain system

	Existing Systems	BlockChain Systems		
Criteria	Centralized	Public	Permissioned	Private
speed and latency	5	7	7	6
scalability	5	9 8	7	4
security and immutablity	3	7	8.5	9
storage capacity	4	9	9	6
transparency	3	9	7	5
Total	21	41.6	38.5	30

A decentralized system (peer to peer) has many advantages over a conventional centralized network including no single points of failure, cheaper distribution (servers are expensive), faster upload speeds and improved security. In addition, irreversible and immutable transactions are both an advantage and disadvantage. For example, an amateur coder killed the contract that allowed users to transfer Ether for the Parity Ethereum Wallet, rendering 150 to 300 million dollars completely useless [6]. Overall, the public blockchain with access to substantial collective resources is most viable in terms of scalability and transparency, however, institutes may prefer implementing permissioned or private blockchains internally for extended security and privacy.

References for Appendix

[1] ”Bitcoin white paper.” https://bitcoin.org/bitcoin.pdf.

[2] S. Elnaj, ”The problems with bitcoin and the future of blockchain.” https://www.forbes.com/sites/forbestechcouncil/2018/03/29/the-problems-with-bitcoin-and-the-future-of-blockchain.

[3] ”Ethereum white paper.” https://github.com/ethereum/wiki/wiki/White-Paper.

[4] ”Hyperledger composer overview.” https://www.hyperledger.org/wp-content/uploads/2017/05/Hyperledger-Composer-Overview.pdf.

[5] A. B. M. Corallo, ”Loom network sdk for developers.” https://medium.com/loom-network/loom-sdk-for-developers-using-an-indexing-layer-for-lightning-fast-dapp-performance-b17f8ba25a3c.

[6] T. Maas, ”Yes, this kid really just deleted 300 million by messing around with ethereum’s smart contracts.” https://hackernoon.com/yes-this-kid-really-just-deleted-150-million-dollar-by-messing-around-with-ethereums-smart-2d6bb6750bb9