The Report Committee for Abelardo Arredondo
Certifies that this is the approved version of the following report:

Blockchain and Certificate Authority Cryptography for an Asynchronous On-Line Public Notary System

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: ______________________________
Suzanne Barber

____
Thomas Graser

Blockchain and Certificate Authority Cryptography for an Asynchronous On-Line Public Notary System

by

Abelardo Arredondo

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

December 2017

Dedication

To my wife Cristina for enduring 10 consecutive semesters and
in loving memory of our daughter Roxy.

Abstract

Blockchain and Certificate Authority Cryptography for an Asynchronous On-Line Public Notary System

Abelardo Arredondo M.S.E

The University of Texas at Austin, 2017

Supervisor: Suzanne Barber

The true innovation behind the Bitcoin protocol is blockchain technology. Blockchain is the underlying distributed database and encryption technology that enables trustless transactions that can be verified, monitored, and enforced without a central institution. This master's report presents the core concepts behind blockchain that are concerned with carrying instructions for storage, sharing of non-financial data, including an examination of the byzantine fault tolerant cryptography model.

A literature review describes the types of blockchains, nodes, proof of work, disadvantages, and risks and provides a survey of future applications related to state government records, such as birth certificates, automobile registrations, land deeds, and voting. This review will answer the question: Is it possible for a state government to use blockchain employing trusted nodes given that the nature of blockchain is that of a distributed network of peers accompanied by a public ledger without a central authority?

Finally, the requirements for a specific application case study will be defined and developed. The desired application will be a smart contract to invoke a statutory durable

power of attorney using blockchain technology for oneself in case of incapacitation while still living.

Table of Contents

List of Tables ix

List of Figures x

INTRODUCTION 1

Chapter 1: Bitcoin Financial Blockchain Core Concepts 6

Bitcoin High Level Overview 6

Bitcoin Step-by-Step Example..6

Bitcoin's Blockchain Detailed Example 8

Chapter 2: Byzantine Fault Tolerant Cryptography Model 12

Proof of Work Bitcoin Blockchain Consensus 13

Disadvantages of Bitcoin PoW Consensus 14

Proof of Work Ethereum Blockchain Consensus 16

Ethereum Stage 1: Determine Uncles 16

Ethereum Stage 2: Determine and process transactions 16

Ethereum Stage 3: Apply mining rewards 17

Ethereum Stage 4: Compute mining PoW, EtHash 17

Proof of Stake 18

Proof of Activity 22

Proof of Burn 22

Proof of Capacity, Storage, or Space 23

Proof of Elapsed Time 23

Proof of Luck 23

Private Chain...24

LITERATURE REVIEW -- STATE OF THE ART 27

Chapter 3: Ethereum Process for Non-Currency Transactions.............................31

Smart Contract 33

Ethereum Innovations 37

Ethereum Transaction and Gas 38

Document Verification dApp Implementation Example 41

Chapter 4: Future Applications for the Government using Blockchain 44

Notarized Record Management and Attestation 48

Identity Management 50

Blockchain Identity Use Cases Examples...51

Voting 53

Private Blockchain 54

CASE STUDY **59**

Chapter 5: Blockchain Application Requirements 60

Proposed Blockchain dApp Product Overview Vision.................................60

User Profiles..61

Key User Needs Interview Conclusions 68

Certificate Authority 73

Innovative Proposed Solution using CA and ECC 73

X.509v3 76

Summary of Capabilities and Roadmap 77

Chapter 6: Future Work and Conclusions..79

Main Findings 79

Value and Limitations..80

Future Work...82

Appendices...83

Appendix A 83

Ethereum Block Header Fields 83

Appendix B 87

Requirement questionnaires...87

Appendix C 100

Protocols for Key Distribution Trust Center..100

References...104

Vita 109

List of Tables

Table 1: Summary of Consensus Systems 21

Table 2: Private Blockchain's with Permissioned Validators.........................26

Table 3: Industries and Fields of Blockchain Uses Cases...............................46

Table 4: Government Use Cases of Blockchain Table. 47

Table 5: Requirements of Public Notary Systems 63

Table 6: Blockchain & CA Public Notary System Benefits, & Roadmap......78

List of Figures

Figure 1: Simplified Diagram of a Blockchain. 8

Figure 2: Detailed Diagram of a Blockchain. 9

Figure 3: Blockchain Consensus and Forks 14

Figure 4: Ethereum Blockchain Consensus & Mining Stage Transition 16

Figure 5: Proof of Work vs. Proof of Stake Consensus Mining 19

Figure 6: Ethereum MetaMask Chrome browser extension. 31

Figure 7: Smart Contract Lifecycle 34

Figure 8: Example Ethereum transaction fee calculator 40

Figure 9: Ethereum Solidity document verification code example 42

Figure 10: Blockchain Roadmap 44

Figure 11: Notarized attestation proof of existence blockchain website dApp ..49

Figure 12: Proof of existence certification payment page 49

Figure 13: Blockchain Voting Booth 54

Figure 14: Identity Used Throughout the Year 57

Figure 15: Blockchain & Certificate Authority Public Notary Hybrid System .70

Figure 16: Certificate Authority Cryptographic Scheme 74

Figure 17: Rinkeby Test Network 81

Figure 18: Ethereum Block Header Fields 83

Figure 19: Ethereum Blockchain Example 84

Figure 20: Protocols for Key Distribution Trust Center 101

INTRODUCTION

Blockchain is not just an improvement of the current data exchange on the internet; it is a new organizing paradigm that allows parties to transact at arm's length with total strangers without worry of fraud or third-party intermediaries. Blockchain adaptation is comparable to the change from precious metal coin money to national banknotes fiat currency, or how double-entry bookkeeping gave rise to capitalism during the commercial revolution of 1250 (Bryer 1993) (Tapscott and Tapscott). Fiat currencies are not backed by physical assets; rather, they are backed by the promise of their issuing government. Blockchain establishes trust between two or more parties, a priori, to transact through both a decentralized public ledger and a cryptographic mechanism that ensures secure transactions that cannot be changed after the fact; this is known as triple-entry bookkeeping (Peters and Panayi 2016) (Kiviat 2015). For the first time ever, secure electronic transfers of some value, not necessary currency, can occur without the presence of a trusted third party, such as a bank, a government, brokerages or depository trust, and clearing corporations (Wright and De Filippi 2015) that provide multi-signature escrow services (Peters and Panayi 2016). This new infrastructure is the next generation of Internet interaction, including anonymous online payments, remittance, and transaction of digital assets (Eyal et al. 2016). Swan (Swan 2015b) goes a step further saying that blockchain technology features could be as fundamental for forward progress in society as were Magna Carta or Rosetta Stone. In this case, the blockchain can serve as the public records repository for whole societies, including the registry of all documents, events, identities, and assets.

The current third party intermediaries establish trust and security by preserving a centralized ledger to track account holders' balances and vouch for a transaction's authenticity. Previous to blockchain, without intermediaries, electronic units of value — dollars, for instance, can be counterfeited and spent twice, just as any digital document can be copied over and over again. This double spending problem has riddled programmers for decades (Kiviat 2015). The main problem is the fraudulent act of spending your electronic money, or certificate of value twice. For example, a certificate of value could be your car title or land deed where a deceitful party could sell the valued asset more than once before the first buyer takes possession of the vehicle or item of value. Blockchain solves an elusive networking problem by enabling trustless transactions: value exchanges, other than currency, over computer networks that can be verified, monitored, and enforced without a central bank or government. This is the circulation of confidence.[1] The benefits and importance of blockchain are (Kiviat 2015) as follows.

1. Blockchain is authenticated and verified and can enable more efficient title transfers and ownership verification.
2. Blockchain is programmable and can enable a conditional smart contract. This report examines the requirements for a specific case study of a smart contract, invoking a future advocate service for yourself in the case of aging and incapacitation while still living (Swan 2015a) .
3. Blockchain is decentralized and can perform these functions with minimal trust without using centralized institutions.
4. Blockchain is borderless and frictionless and can provide a cheaper, faster infrastructure for exchanging units of value.
5. Blockchain protects your data, a valuable asset in this new economy (Zyskind and Nathan 2015).

[1] Statement of James Madison at the Virginia Convention (June 20, 1788), in 4 THE DEBATES IN THE SEVERAL STATE CONVENTIONS ON THE ADOPTION OF THE FEDERAL CONSTITUTION 538 (Jonathan Elliot ed., 2d ed. 1836).

6. Blockchain offers innovative models of governance based on transparency and corruption-free voting (Wright and De Filippi 2015).
7. Bits and pieces of your identity can be safeguarded and not be given away with every website profile (Tapscott and Tapscott).
8. Blockchain is important because it is the latest disruptive technology offering people access to alternative self-enforcing smart contracts (Peters and Panayi 2016).

For currency transactions, a characteristic of a blockchain is that the database, or ledger, must be immutable. Immutability is essential to solve the double spending currency problem, and for certificates or registries that are non-reversible such as, a birth, death, or school certificates, a passport, voter registration, patents, copyrights, and inventory systems. Some versions of blockchain frameworks are starting to emerge that alter the perception of immutability, such as the Enigma project (Zyskind, Nathan, and Pentland 2015). This approach only allows access to data in reversible and controllable manners. In particular they also ensure that no one, but the original data owner(s), ever sees the raw data (Peters and Panayi 2016). Excluding currency, a weakness to immutable public ledgers are land registries, where reversibility is a desirable property of the blockchain, as government uncontrolled registries risk not being recognized. A public ledger with a smart contract allowing the government to include the new technology could be a practical adaptation, without undermining the new process. Known certified validators in a private blockchain could eliminate the concept of an anonymous majority attack arising from a collusion of miners, or agents, taking control of a public decentralized network (Pilkington 2015) these topics are discussed at length later in this paper.

In a decentralized trust network, a node, or an agent's reputation is an important factor in whether its transactions are recognized. Similar to volunteers of Wikipedia, blockchain nodes, or agents, are measured by reputation; however, in a blockchain network reputation is a unit of value that can be earned. It is a proxy for status or a type of task that a person, or agent, can do. This is important because agents participating in the system want to assess the contributions they and others have made, and have these contributions tracked and acknowledged for remuneration, reputation, status garnering, and other rewards. It will be possible for social network currencies to become trans actable with web-based cryptocurrency tip jars, such as Reddcoin, (Swan 2015b) and other micropayment mechanisms that were not previously feasible or transnationally scalable with traditional fiat currency (Kiviat 2015). Reputation is important because it builds network consensus.

The decentralized nature of blockchain's makes them an equality technology, one that can be used to expand freedom and liberty (Swan 2015a). As blockchain technology becomes widely adopted, centralized authorities, such as government agencies and large multinational corporations, could lose the ability to control and shape the activities of people through existing means. As a result, opponents believe there will be an increasing need to focus on how to regulate blockchain technology and how to shape the creation and deployment of these emerging decentralized organizations in ways that have not yet been explored under current legal theory (Wright and De Filippi 2015). There are proponents who support inclusion of government regulation and private blockchain's with trusted nodes and there are alternative opponent philosophies supporting never including any regulation and distrusting any central authority. Risks and limitations are discussed later in this report under chapter 4, which outlines government future applications using private blockchains to counter an attack arising from a collusion of a majority of nodes; this pitfall is eliminated with known private and trusted validator nodes (Pilkington 2015). Energy and transaction costs processed by public ledgers are higher, whereas private blockchains enable cost-effective, faster transactions (Pass, Seeman, and Shelat 2016). Timing and scalability limitations are discussed in the prologue of section 2.

This report is divided into 3 main sections. The first section is the introduction and includes an outline of the basic core concepts of bitcoin's blockchain in chapter 1. The Byzantine fault tolerant cryptography model is explained in chapter 2.

The second section investigates the state of the art of blockchain, such as the difference between proof of work vs proof of stake and a side-by-side comparison of the main competing blockchain models used for Bitcoin and Ethereum including risks and disadvantages. Chapter 3 provides a current and deep analysis of the Ethereum processes and methods for non-currency transactions. Chapter 4 includes all the known interpretations of future applications (Pilkington 2015) as they relate to state government and regulation inclusion, such as birth certificates, automobile registrations, land deeds, and voting. This report describes how it is possible for a state government to use blockchain employing trusted nodes.

The final section describes an in-depth case study for a blockchain smart contract (Kosba, Miller et al. 2016) application to invoke a statutory durable power of attorney for oneself in case of incapacitation while still living (Swan 2015) using blockchain technology. Chapter 5 defines the blockchain application requirements including certificate authority protocols. Chapter 6 includes future work direction, main findings, and limitations.

Chapter 1: Bitcoin Financial Blockchain Core Concepts

This chapter will clarify the fundamentals of the established blockchain, specifically for bitcoin.

BITCOIN HIGH LEVEL OVERVIEW

Bitcoin is a digital crypto-currency that uses the original blockchain protocol, also known as the Nakamoto consensus. Satoshi Nakamoto is a pseudonym used by an unknown person or persons who designed bitcoin and created its original reference implementation in 2008. Predecessors for digital currency -- from 1991 to 1998 -- include DigiCash and eCash but these lacked wide public interest (Tapscott and Tapscott). Nakamoto devised the first blockchain database implementation. The original bitcoin blockchain is a method for maintaining a public, immutable and ordered ledger of records, specifically digital financial transactions. Its record of transactions is shared between many parties. Imagine a giant accounting spreadsheet that everyone can access and that you can trust that no one will double spend money because it uses cryptography methods, namely the Byzantine general consensus, explained in chapter 2. Blockchain is the notary for bitcoin transactions. Records can be added to the end of the ledger at any time with a guarantee that records previously added cannot be removed or changed. The Nakamoto consensus mechanism functions in a fully anonymous setting where no username is required, transactions are free peer-to-peer, and no central authority is required (Pass, Seeman, and Shelat 2016).

BITCOIN STEP-BY-STEP EXAMPLE

Let us say that Alice wants to pay Bob for services rendered and both have bitcoin wallet software which accesses the blockchain online, but does not identify the user to the system. The transaction starts with Alice's wallet proposing that the blockchain be changed deducting from her wallet and adding to Bob's. As the proposal propagates over the network, the various nodes check, by inspecting the ledger, whether Alice actually has the bitcoin she now wants to spend. If Alice has funds, specialized nodes called miners will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain (The Economist 2015).

In the Bitcoin blockchain, Alice can be any of the following performers: Alice can accept and trade coins and she can be a miner. Miners collect transactions and put them into a single block. A block contains four pieces of information.

1. A reference to the previous block
2. A summary of included transaction
3. A time stamp
4. A Proof of Work (PoW) that went into creating the secure block

The blocks are strung together into a chain, shown in Figure 1 as 51, 52, and 53. Blocks need numerous independent confirmations (Augur 2015). Confirmation of the blockchain is part of the mining process; miners are generally given bitcoin rewards after successfully adding a block to the chain. Figure 1 shows a simplified block diagram of the bitcoin blockchain.

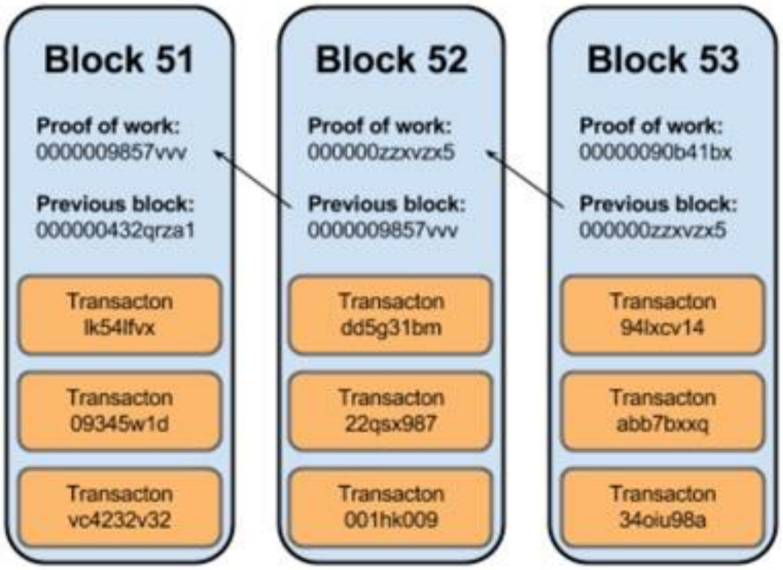


Figure 1: Simplified Diagram of a Blockchain.

BITCOIN'S BLOCKCHAIN DETAILED EXAMPLE

Alice's transaction proposal entails repeatedly feeding the data through a cryptographic hash function which reduces the request down to a string of digits of a fixed length (see input transaction A and Output #A in Figure 2). Specifically, it is an SHA256 Hash. Cryptography makes it is easy to go from the data to their hash, but impossible to go from the hash back to the data. The hash does not contain the data; it is unique to the data. If any change goes into the block, even a single digit, then the hash would be different (The Economist 2015).

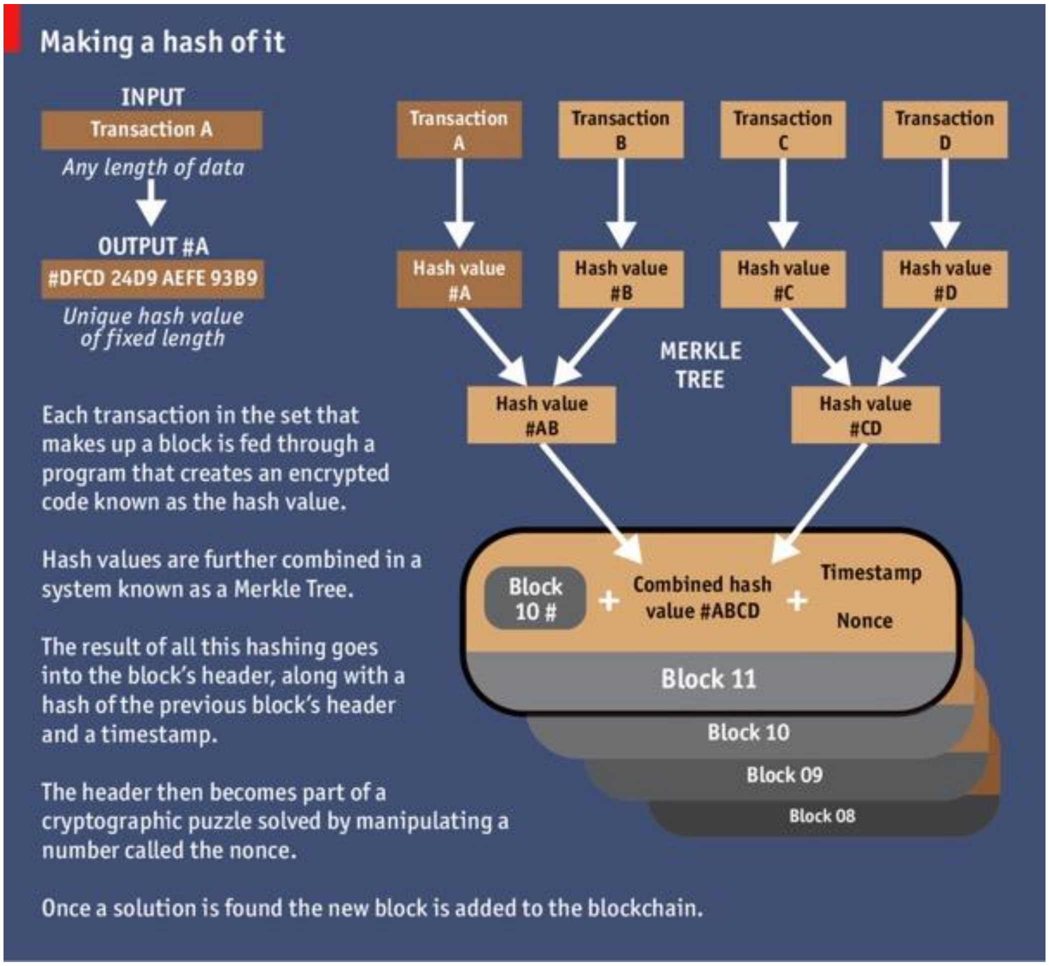

Making a hash of it
INPUT
Transaction A
Any length of data
OUTPUT #A
#DFCD 24D9 AEFE 93B9
Unique hash value of fixed length
Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.
Hash values are further combined in a system known as a Merkle Tree.
The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.
The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.
Once a solution is found the new block is added to the blockchain.
Transaction A
Transaction B
Transaction C
Transaction D
Hash value #A
Hash value #B
Hash value #C
Hash value #D
MERKLE TREE
Hash value #AB
Hash value #CD
Block 10 #
+
Combined hash value #ABCD
+
Timestamp
Nonce
Block 11
Block 10
Block 09
Block 08

Figure 2: Detailed Diagram of a Blockchain.

The hash is put, along with other hash transactions data, into a combined hash header for the proposed block. This header then becomes the basis for finding a number called a nonce, often referred to as the puzzle the miners are in search of. The nonce mathematical puzzle involves using a reverse hash function that proves the miner has invested CPU time and energy; the Proof of Work (PoW) is simplistically shown in Figure 1. This puzzle can only be solved by brute force trial and error; it is difficult to find but not impossible. It is not possible to predict which miner will solve the puzzle. Across the network, miners grind through trillions and trillions of possibilities looking for the answer, similar to buying a lottery ticket. When a miner finally comes up with a solution, other nodes quickly check it. It is a cryptographic attribute in which solving the puzzle is hard, but checking the result is easy. Each node that confirms the solution updates the blockchain accordingly and results in a majority consensus. The hash of the header becomes the new block's identifying string and that block is now part of the ledger. Alice's payment to Bob, and all the other transactions the block contains, are confirmed.

Each new header contains a hash of the previous block's header, which in turn contains a hash of the headers before that all the way back to the beginning. The genesis block has a timestamp of 18:15:05 GMT on January 3, 2009 and was issued by Satoshi Nakamoto (Wikipedia Fdn 2017b). It is this concatenation that makes the blocks into a chain. Starting from all the data in the ledger it is trivial to reproduce the header for the latest block. The miners are paid in bitcoins when solving the puzzle and creating a new block. This effectively inflates the currency, but it winds down over time according to a step-wise schedule (Back et al. 2014). Satoshi capped the supply of bitcoins at 21 million to be issued over time to prevent arbitrary inflation. Given the halving every four years of bitcoins mined in a block and the current rate of mining, six blocks per hour, those 21 million bitcoins (BTC) should be in circulation around the year 2140. No hyperinflation or currency devaluation caused by incompetent or corrupt bureaucracies will occur (Tapscott and Tapscott).

As shown in Figure 1 and Figure 2, a blockchain is a distributed database that consists of data-structure blocks that may contain data or programs, with each block holding batches of individual transactions. Every node in a decentralized system has a copy of the blockchain. No centralized copy exists and no user is trusted. Whenever new transactions occur, such as Alice requesting a transaction, the blockchain is authenticated across this distributed network before the transaction can be included as the next block on the chain. Further, a majority consensus of nodes is required to add the block into the blockchain. The blockchain creates trust because a complete copy of the chain, which shows every transaction, is held by immutability in the entire network (Acronis Intl GmbH 2017). Because the blockchain is copied to all the nodes, there is no single point of failure and it is fault tolerant. Chapter 2 describes the Public Key Infrastructure (PKI) required to reach a consensus in a Peer to Peer (P2P) distributed network.

Chapter 2: Byzantine Fault Tolerant Cryptography Model

The problem is that P2P networks without admission controls are inherently vulnerable to Sybil attacks, in which selfish or malicious processes claim multiple fraudulent identities. This is detrimental to consensus protocols, which typically involve collecting majority votes. Public blockchain's are based on a Byzantine consensus protocol, in which cryptographic puzzles keep a computationally bounded adversary from gaining too much influence (Miller and LaViola Jr 2014).

Coping with failed components that send conflicting information to different parts of a system is expressed as the metaphor of the Byzantine generals problem (Lamport, Shostak, and Pease 1982). The Byzantine agreement problem is one of the fundamental problems in distributed P2P fault-tolerant computing. This riddle pertains to liars and when to trust messages. Imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching an agreement. Furthermore, the messengers might be traitors or be impeded from delivering the messages. The goal is that all the loyal generals must decide on a plan of action, despite the malicious behavior of the corrupted generals (Cachin, Kursawe, and Shoup 2000), and that a small number of traitors could not prevent the loyal generals to adopt a plan. The problem is simplified with the stipulation that the only conclusion to be made is whether to attack or retreat, then the final decision can be based upon a majority consensus vote among the generals. The final conclusion is that the message must be accompanied by a signed written secret, today recognized as the Private Key Infrastructure (PKI). PKI is where asynchronous public and private keys are required. An emerging approach for PKI is to use the blockchain because blockchain technology provides a distributed and immutable ledger of information, it has qualities considered highly suitable for the storage and management of public keys (Wikipedia Fdn 2017a).

Fundamentally blockchains are fault tolerant because by distributing copies of the database, or the keys that legitimize the data, the chain cannot go down or disappear. Blockchain uses the Byzantine fault tolerant cryptography model to solve public P2P network consensus where only a majority needs to agree on a proof about some value, in spite of a minority of faulty processes that deviate arbitrarily from the protocol. The consensus methods of two leading blockchain models are detailed below.

Proof of Work Bitcoin Blockchain Consensus

A consensus algorithm ensures that the next block in a chain is the one and only version of the truth. It keeps adversaries from hacking the system and successfully forking the chain. A fork in the chain is when different nodes may temporarily disagree about the valid chain. This happens when the nodes learn of tied branches at different times normally resulting from propagation or computational delays (Decker and Wattenhofer 2013). Figure 3 shows forks as light colored orphan blocks (Kroll, Davey, and Felten 2013). A fork is resolved when an additional new block is found and is added to the chain making the branch longer.

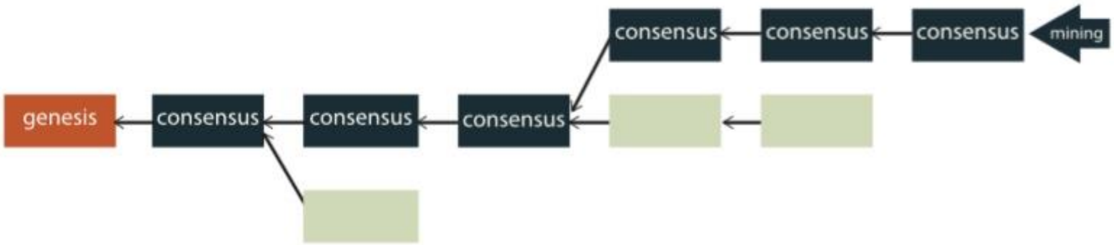


Figure 3: Blockchain Consensus and Forks

In bitcoin PoW, miners compete to add the next block in the chain by racing to find a puzzle, as explained in chapter one. The first miner to solve the puzzle is rewarded with a bitcoin. The difficulty of the PoW puzzle is adjusted periodically by an adaptive algorithm based on the recent block chain history to maintain the long-term invariant such that one new block will be mined every ten minutes on average (Kroll, Davey, and Felten 2013).

Blocks need to be confirmed by a majority of nodes before they are added to the chain. In Bitcoin PoW, it is agreed that every node will consider the longest branch as the valid chain (Rosenfeld 2014). Bitcoin never commits a transaction definitively. Every transaction can be invalidated if a longer chain that started later is created. The reason alternative consensus mechanisms have been created is to solve the main disadvantages of Bitcoin PoW as outlined in the following list.

Disadvantages of Bitcoin PoW Consensus

1. If a single entity could control a majority of the computational power on the network, and thus be able to find blocks faster than the rest of the network combined, it could revert any transaction (Decker and Wattenhofer 2013).

2. If there are 2 branches of the tree, with a separate group of miners growing each branch, the branch whose miners have more computational power will grow more quickly (Kroll, Davey, and Felten 2013).
3. Bitcoin PoW consensus mechanism consumes a great deal of power (Vigano 2016). In 2016 Bitcoin mining consumed 350 Mega Watt hours (MWh). The worst case scenario is that by 2020 Bitcoin mining could consume as much continuous total power as the entire country of Denmark (Deetman 2016). Denmark consumed 33 Tera Watt hours (TWh) in 2014 (Intl Energy Agency 2016). Fortunately, the state of the art ASIC (Application Specific Integrated Circuit) chip, that is designed exclusively for Bitcoin mining, consumes only 1/3 of the energy of legacy graphics processors.
4. Miners have become centralized consortiums operated where electricity is cheap. In 2014 Chinese mining was 40% of all the mining equipment in the world (Vincent 2016). Chinese mining pools control 71% of the bitcoin network's collective hash-rate. AntPool is the largest Chinese mining pool and accounts for 20% of all the blocks successfully mined in 2016 (Tuwiner 2017).
5. Bitcoins do not scale because confirmations take 10 to 60 minutes (Castor 2017).

The search for faster, less centralized and more energy-efficient consensus algorithms is discussed in the next few pages. Because Ethereum is the second most utilized blockchain network that uses PoW, it is necessary to study it separately. Ethereum is noteworthy because it reaches consensus approximately every 15 seconds (ConsenSys 2017). An Ethereum consensus mechanism is listed below and is detailed in Chapter 3.

Proof of Work Ethereum Blockchain Consensus

Ethereum has a distributed and decentralized consensus mechanism in which the nodes assemble the transactions into blocks, similar to bitcoin. Ethereum miners compete with each other to get their blocks added as the next block in the chain. Figure 4 shows the high-level stages that Ethereum mining requires to reach consensus (Arshdeep 2017).

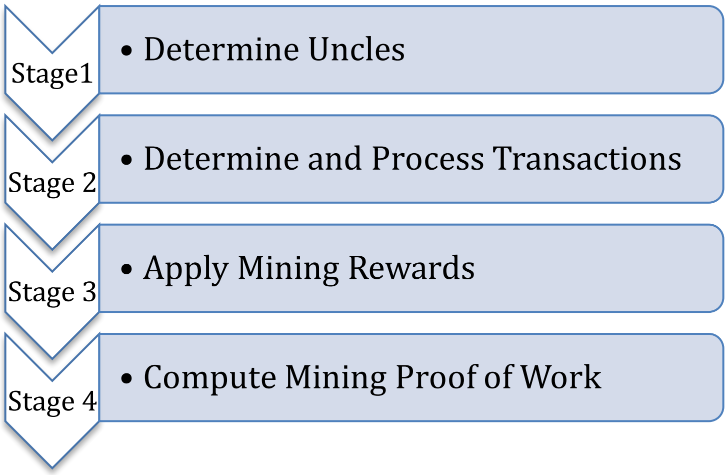


Figure 4: Ethereum Blockchain Consensus & Mining Stage Transition

Ethereum Stage 1: Determine Uncles

Uncles are blocks whose parents are ancestors of the current block. Ethereum allows a maximum of 2 uncles per block. Uncles are included in a block to increase network security, keep mining active, and distribute the mining fee.

Ethereum Stage 2: Determine and process transactions

When the process for mining the next block on the chain is initiated by the Ethereum network, all the transactions received since the last block mined are collected and added to a list of pending transactions for the next block. Next, a new block is initiated based on a parent block. While initializing the block, the block header is created. The Ethereum block header is substantially different from Bitcoin and is listed in Appendix A

Ethereum Stage 3: Apply mining rewards

Miners in the Ethereum network are rewarded for dedicating their computational resources for maintaining the network and mining new blocks. However, the reward is different from Bitcoin reward. A successful miner whose block is selected to be added next on the Ethereum blockchain is rewarded with a fixed reward of 5 Ethers (Ether is an Ethereum coin unit). In addition to the fixed reward, the miner also gets the cost of gas consumed within the block. This can be thought of as a reimbursement for the cost of the transaction. The metaphor of gas is equivalent to a limited resource that is pre-purchased and consumed. For every uncle included in a block, the miner of the block gets an extra reward of 1/32 per uncle, that is, 3.125% of the fixed 5 Ether reward. These mining rewards are the only mechanism by which the wealth is distributed (Arshdeep 2017).

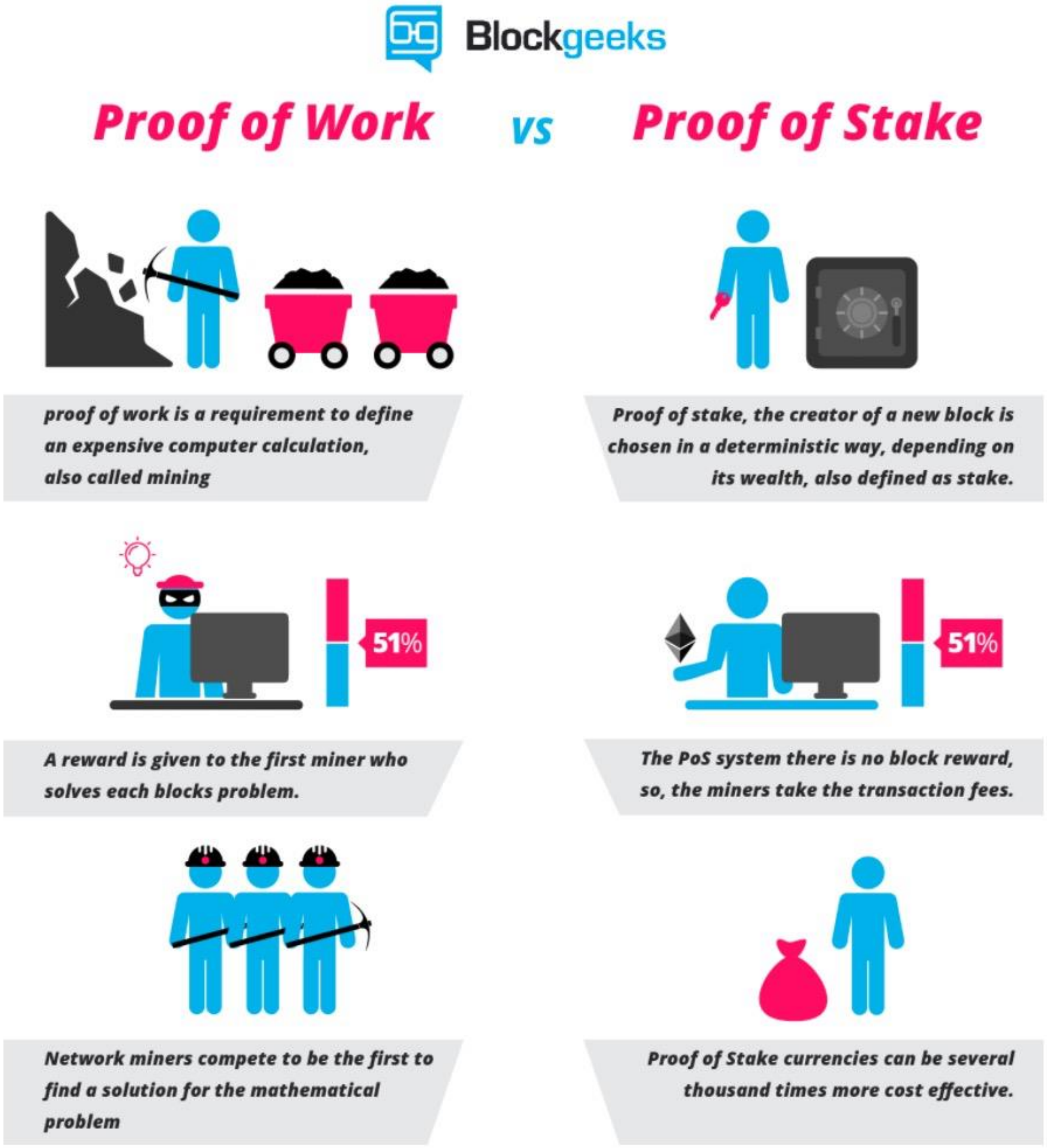
Ethereum Stage 4: Compute mining PoW, EtHash

The PoW algorithm used in Ethereum is called EtHash. The principal objective for constructing a new PoW function, instead of using the existing Bitcoin method, is to mitigate the problem of mining centralization this happens when a group of mining consortiums acquire a disproportionately large amount of power that could manipulate the network. EtHash was designed to prevent the dominance of ASICs and GPU custom mining configuration by using general purpose computations that make the network accessible to as many people as possible. EtHash shifts its dependence to relying on how fast the computer memory can move data. Its sequential memory-hard algorithm consumes nearly the entire available memory access bandwidth, ensuring that it is not possible to use memory in parallel to find multiple nonces simultaneously (Arshdeep 2017). A light client can verify the correctness of EtHash PoW in approximately .01 seconds. The EtHash algorithm involves the following steps (Mukhopadhyay et al. 2016) (Ethereum Wiki 2017).

1. A seed exists that can be computed for each block from the data stored in the block headers.
2. From this seed, a 16MB pseudo-random cache can be computed. EtHash uses its own Pseudo-Random Number Generator.
3. From the cache, a 1GB dataset, a Full Dataset (DAG), can be generated, such that each item in the dataset depends on only a few items from the cache.
4. Mining involves selecting random elements of the dataset and hashing them together. Verification can be done with low memory by using the cache to regenerate the specific pieces of the dataset that is needed, so it is sufficient to store just the cache.

Proof of Stake

The most common alternative to PoW consensus is Proof of Stake (PoS). In this type of consensus algorithm, instead of investing in custom computer ASIC or GPU equipment in a race to mine blocks, a stakeholder validator node invests in the coins of the system. Validator nodes are paid strictly in transaction fees. In PoS, a miner's chance of being picked to create the next block depends on the fraction of coins in the system he or she owns. Once a validator creates a block, it still needs to be validated and committed to the blockchain. It is noteworthy to mention that the Ethereum network is planning to transition to a PoS system in 2018 (Castor 2017). Figure 5 shows a comparison of PoW and PoS (Blockgeeks 2017b).



Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

A reward is given to the first miner who solves each blocks problem.

The PoS system there is no block reward, so, the miners take the transaction fees.

Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

Figure 5: Proof of Work vs. Proof of Stake Consensus Mining

A possible disadvantage in the PoS system is that a validator node might have nothing at stake and may maliciously create and sign 2 blocks claiming two sets of transaction fees. However, this is solved by requiring the validator to lock their currency in a type of virtual vault. Then, if the validator tries to double sign or fork the system, those coins are slashed. Table 1 shows a sample summary representation of enterprises and the type of consensus systems they are using.

Consensus	Crypto Coin Network	Advantage	Disadvantages
Proof of Work Bitcoin PoW	Bitcoin	Longest Chain Most Investment	Too much energy required to mine
Proof of Work Ethereum PoW	Ethereum	Algorithm does not allow ASIC or GPU Hardware	Encryption algorithms are Circa 2013
Proof of Stake PoS	Tendermint	Every node in the sys must sign off on a block for a majority vote	Nothing at stake problem where a node might claim 2 transaction fees
	Peercoin Blackcoin NXT	Random group of signers is chosen	
Proof of Activity PoA	Decred	Hybrid approach PoW & PoS	Too much energy required to mine & nothing at stake
Proof of Burn PoB	SlimCoin	Will burn any Crypto-currency	Too much energy required to mine
Proof of Capacity Storage/Space PoC	Burstcoin	Does not consume excessive Energy	Nothing at stake
Proof of Elapsed Time PoET	Intel	Low power, fixed timing	Trust Intel
Proof of Luck PoL	Not commercially adopted yet	independent algorithm for PoET	Trust Intel
Distributed Proof of Stake DPoS	EOS Block.One	No Fee to Users Fast, Interpreted Cont Voting Sys	Unproven 2018 Roadmap Delegate Trust to Block Producer

Table 1: Summary of Consensus Systems

Proof of Activity

Proof of activity (PoA) is a hybrid approach that combines both proof of work and proof of stake. In PoA, mining kicks off in a traditional PoW fashion, with miners racing to solve a cryptographic puzzle. Depending on the implementation, blocks mined do not contain any transactions. The winning block will only contain a header and the miner's reward address. At this point, the system switches to PoS. Based on information in the header, a random group of validators is chosen to sign the new block. The more coins in the system a validator owns, the more likely he or she is to be chosen. The winning block becomes a full-fledged block as soon as all of the validators sign it.

Proof of Burn

With proof of burn (PoB), instead of pouring money into custom computer equipment, you burn coins by sending them to an address where they are irretrievable. By committing coins to be never retrieved, the miner earns a lifetime privilege to mine on the system based on a random selection process. Miners may burn the native currency or the currency of an alternative chain, such as Bitcoin. The more coins burned, the better chance of being selected to mine the next block. Over time, the miners stake in the system decays, so the Miner will need to burn more coins to increase his odds of being selected. This is similar to Bitcoin's mining process, where miners have to continually invest in more modern custom ASIC computing equipment to maintain hashing power. While PoB is an alternative to PoW, the protocol will use resources needlessly (Castor 2017), and mining power gravitates to those who are willing to burn more money.

Proof of Capacity, Storage, or Space

Variations of Proof of Capacity (PoC) include proof of storage and proof of space. In PoC a miner pays with hard drive space. By investing in terabytes of hard drive space a Miner improves their chances of mining the next block and earning the block reward. Prior to mining in a PoC system, the algorithm generates large data sets known as plots that a miner stores on his hard drive. The more plots a miner has, the better her chance of finding the next block in the chain. Similar to PoS, PoC suffers from a node having nothing at stake and may create and sign 2 blocks claiming two sets of transaction fees.

Proof of Elapsed Time

Chipmaker Intel has come up with its own alternative consensus protocol called Proof of Elapsed Time (PoET). This system works similarly to PoW, but consumes far less electricity. Instead of having miners solve a cryptographic puzzle, the algorithm uses a Trusted Execution Environment (TEE), such as SGX (Software Guard Extension), to ensure blocks get produced in a random lottery fashion, but without the required work. This becomes an Intel customized system that solves the computing problem of random leader election, or selecting who will create the next block of transactions. Intel's approach is based on a guaranteed wait time provided through the TEE. According to Intel, the PoET algorithm scales to thousands of nodes and will run efficiently on any Intel processor that supports SGX. The one problem with this protocol is it requires you to put your trust in Intel (Castor 2017).

Proof of Luck

Proof of Luck (PoL) further extends Intel's PoET by adding a proof of ownership consensus primitives to make mining energy, and time, efficient. Similarly, PoL is based on the use of TEEs using Intel SGX-enabled CPUs. TEEs make PoW mining schemes equitably distributed by preventing the use of ASICs or custom GPU configurations making mining energy, and time, efficient. PoL in combination with the TEE platform provides low-latency transaction validation, deterministic confirmation time, negligible energy consumption, and equitably distributed mining (Milutinovic et al. 2016). Milutinovic recommends waiting for 6 blocks before accepting a transaction, which makes PoL impractical for point of sale applications. Further consensus primitives are needed within the TEE environments to distance the solution from Intel that in turn gains community acceptance. Another capability of TEEs is that they can limit the effect of Sybil attacks.

PRIVATE CHAIN

Private blockchains are also known as permissioned blockchains. Private blockchains have a set of trusted parties, miner nodes, that carry out verification. Additional verifiers can be added with the agreement of the current trusted nodes or a central authority, such as a private corporation, a non-for-profit association, or a government agency. Such a configuration is a traditional finance setting, which operates a Know Your Business (KYB) or Know Your Client (KYC) procedure to whitelist users that are allowed to undertake operations in a particular space (Swanson 2015). Swanson finds that permissionless and permissioned blockchains are fundamentally different in both their operation and the range of activities that they enable (Pilkington 2015).

Permissioned blockchains are intended to be purpose-built, and can thus be created to maintain compatibility with existing financial or database applications. They can be fully private, such as write permissions that are kept within an organization, or consortium blockchains where a pre-selected set of trusted nodes controls the consensus process. Because the trusted nodes on the network are named, the intention is that they are also legally accountable for their activity. In terms of the transactions these private blockchains manage, they will be assets run by the chain, such as, private businesses that provide a secure mechanism for vendors, service providers, supply chain sources, and shareholders.

An advantage of a permissioned blockchain is scalability. In a permissionless blockchain, the data is stored on every computer in the network, and all nodes verify all transactions. In a permissioned blockchain, only a smaller number of preselected trusted participants will need to operate, and if these come from large institutions they will be able to scale their computing power in line with the increase in the number of transactions. For Example, if a state agency, commission, or department wanted to start a private blockchain, it can recruit State Professional Engineers as trusted nodes, because these individuals are trusted and registered with the state.

A disadvantage of private blockchains is that because of the smaller number of trusted participants, it is much easier for a group of users to collaborate and alter the rules, or revert transactions. In addition, it is easy for a collusion to reject transactions and in this sense it is not censorship resistant, as a permissionless public blockchain would be. Examples of permissioned blockchains are included in Table 2 (Peters and Panayi 2016). A private or internal token in this Table 2 context is not a currency, but a crypto receipt internally between permissioned parties and auditing compliance (Swanson 2015).

	Ledgers with an internal private token	**Ledgers without an internal token**
Ledgers based on Ripple	Ripple (XRP)	Tembusu Systems Singapore
Ledgers based on Hyperledger Linux Foundation		Hyperledger (PBFT)
Ledgers based on a Bitcoin like blockchain (Bitcoin fork, colored coin implementation)	CryptoCorp	
Ledgers based on an Ethereum-like blockchain	Eris MONAX	Clearmatics clearmatics
Ledgers based on a Tezos like blockchain		Tezos

Table 2: Private Blockchain’s with Permissioned Validators.

In a fully private ledger, write-permissions are monitored by a central locus of decision-making. Read permissions are either public or restricted. A private blockchain amounts to a permissioned ledger, whereby an organizational process of Know-Your-Business (KYB) and Know-Your-Customer (KYC) enables the white listing (or blacklisting) of user identity. In summary the difference between public and private blockchains is the extent to which they are decentralized or ensure anonymity. (Pilkington 2015).

LITERATURE REVIEW -- STATE OF THE ART

Before this report takes a deep dive into Ethereum smart contracts and private blockchains, it is noteworthy to mention how bitcoin can manage a smart contract by using recent developments in the cryptocurrency industry. Bitcoin offers an alternative to Ethereum smart contracts, with the open assets protocol built on top of the bitcoin blockchain. This allows issuance and transfer of user-created assets, also known as colored coins (Flavien 2016). Although the open assets protocol is used by Nasdaq to expand the equity management capabilities of its Nasdaq private market platform, (Pilkington 2015) it does not have the support and momentum that the Ethereum network possesses.

Currently there are many blockchain networks that provide smart contract blockchains using their own cryptocurrency. However, the noteworthy network by Block.one (block.one 2017) called EOS (Larimer 2017) raised the equivalent of $185 Million USD in the 5 days of the Initial Coin Offering (ICO). An ICO, is an event sometimes referred to as crowd funding sale; this is when a company releases its own cryptocurrency for the purpose of funding the new enterprise. The company gets the capital to fund the product development and the purchasers get their crypto tokens' shares. ICO's are unregulated by the government, and enable startups to forego venture capitalist (VC) investing (Marshall 2017). In 2017, ICO capital events surpassed the private venture capital investments. Any project can launch an ICO at any time with little preparation, and any person can take part in it by contributing their own money, no matter what country they are from (ICObazzar 2017). The Chinese government has recently banned ICOs altogether. There were over 30 ICO events in the month of June 2017 (TokenMarket Ltd 2017) alone. What makes EOS different from Ethereum is the following.

1. There are no fees for Distributed application (dApp) users on EOS to use the network, carry out transactions, or execute smart contracts. Only the creator of the dApp pays the network. Ethereum charges a user transaction fee construed as gas.
2. EOS code is interpreted on the network and is human readable. Ethereum is compiled into machine language and is not human readable.
3. EOS also has not proved the theoretical roadmap that shows the development and testing continuing in 2018 (GitHub 2017).
4. The consensus mechanism is different from PoW Ethereum. EOS plans to achieve commercial retail grade transactions per second performance and a scale capable of supporting trading exchanges, social networks, and payments processors using Delegated Proof of Stake (DPoS) (EOSIO 2017). DPoS allows those who hold tokens on a blockchain adopting the EOS.IO software to select block producers through a continuous approval voting systems. Block producers are delegated major events in the EOS ecosystem. DPoS will reduce transaction processing time, because fewer nodes are involved in the verification process (Jones 2017). The user delegates their trust to the block producer.

Ethereum is a platform for building decentralized applications of all kinds. The company's tokens are called Ether, and are used to maintain the operation of dApps that have already been built on the platform. Ethereum comes with the support of the Enterprise Ethereum Alliance (EEA), which includes over 130 corporate members (EEA Fdn 2017). It is primarily interested in reference standards to retain public Ethereum compatibility. It is noteworthy that companies missing from EEA membership are those who are first expected to be disrupted, such as, automobile ride sharing businesses, vacation rentals, and remittance companies. In summary there are 4 types of industries or groups that have purchased subscriptions to the EEA.

1. Large global companies in finance, insurance, and banking, such as JP Morgan Chase, Santander, Wells Fargo, Intuit, ING, Scotiabank, USB, Fubon, BBVA, Credit Suisse, National Bank of Canada, BNP Paribas, and Master Card to name a few.
2. IBM, Microsoft, Samsung, Intel, Accenture, InfoSys, and Cisco are some of the big technology, and consulting members in the so-called Blockchain-as-a-Service (BaaS) space. These companies intend to use their public cloud platforms, and developer tools, to help enterprise organizations build out blockchain infrastructure.
3. Almost half the members of the EEA are cybersecurity and cryptocurrency companies as well as industry associations. A limited list includes ConsenSys, Ripple, bloq, TenderMint, Singapore cryptocurrency and blockchain association, Jiangsu Huaxn blcokchain research institute, Lazarski blockchain technology center, Nordic Ethereum alliance, and the WSBA an advocacy group for Wall Street in the distributed ledger space. There are 8 working groups and initiatives including the state working group, smart contracts alliance, global blockchain forum, digital assets accounting consortium, and the blockchain intellectual property council, et.al.
4. Government agencies, legal committees, and accounting offices including the Illinois department of financial and professional regulation, the government of Andhra Pradesh India, and Deloitte Consulting. Over 10 legal offices include

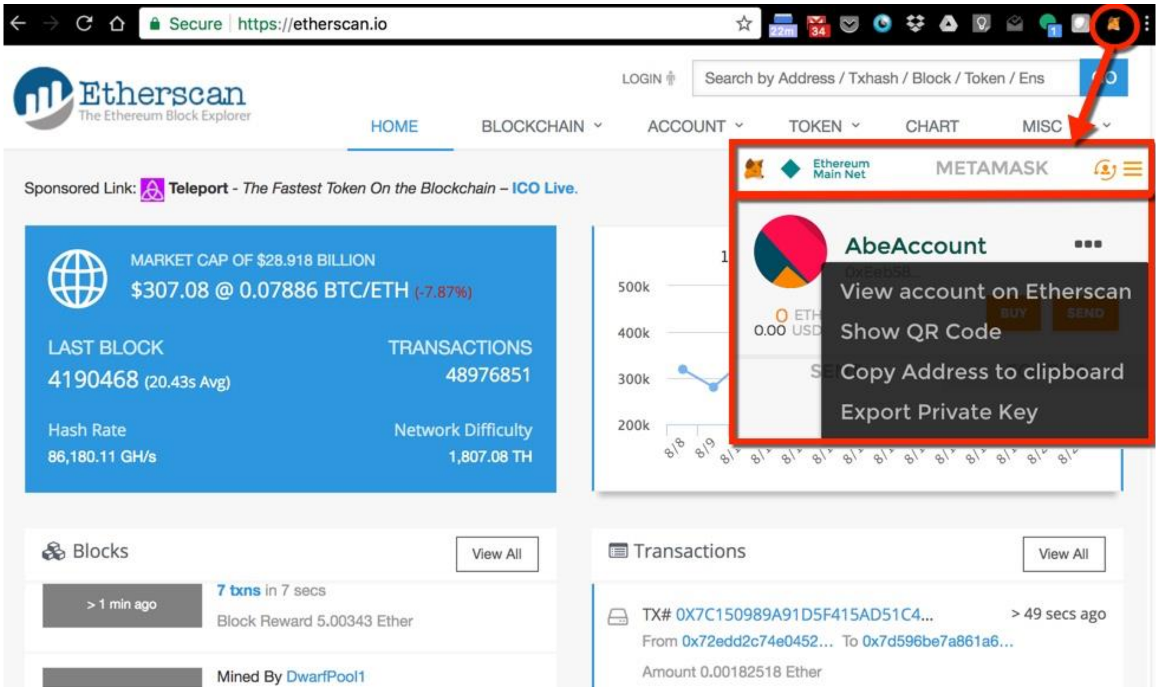
> Blakes of Canada, Buckley Sandler, Cooley, Crowell Moring, DLA Piper, and Steptoe to name a few.

Only the Toyota research institute was listed as an automobile manufacturing member, and British Petroleum was the only energy company.

It is expected that most significant corporate enterprises will run business processes on their own private permissioned corporate blockchain. In simple terms, this is accomplished by putting the chain behind a corporate LAN and enabling trusted nodes. Employees, customers, vendors, and service providers at each company will be able to securely access that company's private blockchain via strong cryptographically authenticated transactions. Private companies will build their ecosystem initially to collaborate on share trusted source-of-truth use cases with supply chains vendors and stakeholders. JP Morgan has launched Quorum (JP Morgan Chase 2017). Quorum is open source and intended for any application requiring high-speed private transactions within a permissioned group of known participants; this is known as a private banking system.

Chapter 3: Ethereum Process for Non-Currency Transactions

Ethereum is primarily an open software platform based on blockchain technology that provides tools to build and run decentralized applications, or dApp's, using a browser wallet called Mist, or the MetaMask browser extension for Google Chrome. This is how a user gets access to a digital wallet to trade and store Ether, as well as write, manage, deploy, and use smart contracts and Decentralized Autonomous Organizations (DAO). All of the topics mentioned are detailed in this chapter. Shown in Figure 6 is the MetaMask Chrome browser extension; the Etherscan website is an example of an Ethereum support web site.



Secure https://etherscan.io
Etherscan
The Ethereum Block Explorer
LOGIN
Search by Address / Txhash / Block / Token / Ens
HOME
BLOCKCHAIN
ACCOUNT
TOKEN
CHART
MISC
Sponsored Link: Teleport - The Fastest Token On the Blockchain – ICO Live.
MARKET CAP OF $28.918 BILLION
$307.08 @ 0.07886 BTC/ETH (-7.87%)
LAST BLOCK
4190468 (20.43s Avg)
TRANSACTIONS
48976851
Hash Rate
86,180.11 GH/s
Network Difficulty
1,807.08 TH
500k
400k
300k
200k
8/8
8/9
Ethereum Main Net
METAMASK
AbeAccount
0 ETH
0.00 USD
BUY
SEND
View account on Etherscan
Show QR Code
Copy Address to clipboard
Export Private Key
Blocks
View All
> 1 min ago
7 txns in 7 secs
Block Reward 5.00343 Ether
Mined By DwarfPool1
Transactions
View All
TX# 0X7C150989A91D5F415AD51C4...
> 49 secs ago
From 0x72edd2c74e0452... To 0x7d596be7a861a6...
Amount 0.00182518 Ether

Figure 6: Ethereum MetaMask Chrome browser extension.

In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, and this native Ethereum token fuels the network. Ether is a tradeable cryptocurrency and is used by dApp users, miners, and developers to pay for transaction fees and services on the Ethereum network (Marvin 2016). Ethereum can provide intermediary services that exist across many of different industries.

Some of the risks and disadvantages of Ethereum are that, similar to Bitcoin, Ethereum presently uses PoW consensus mechanisms and causes miners to consume large amounts of energy. Because of the verification overhead, the number of transactions per second are limited to approximately 30 (Jones 2017). This is relatively small when compared to standard credit card companies, the stock market, Facebook, and Amazon web services. Logic within smart contracts can lead to unintended adverse actions being taken. If a mistake in the code gets exploited, there is no efficient way in which an attack can be stopped once a transaction is committed to the chain. The most successful of these attacks managed to steal $60M from a contract, but its effects were cancelled after an harshly debated revision of the blockchain (Atzei, Bartoletti, and Cimoli 2017). This attack happened on June 18, 2016 to a DAO contract, while implementing a crowd-funding platform, which allowed the attached DAO to raise $150M. A hard-fork in the blockchain nullified the effects of the transactions involved in the attack (Atzei, Bartoletti, and Cimoli 2017) (Bartoletti et al. 2017).

As explained by Atzei, and Bartoletti the risks of smart contracts are the difficulty of detecting mismatches between their intended behavior and the actual one. Although analysis and verification tools may help in this direction, the choice of using the Ethereum Turing-complete language limits the possibility of verification because contract code is compiled and not human readable. However, non-Turing complete human readable languages, such as the EOS proposal, will overcome this issue.

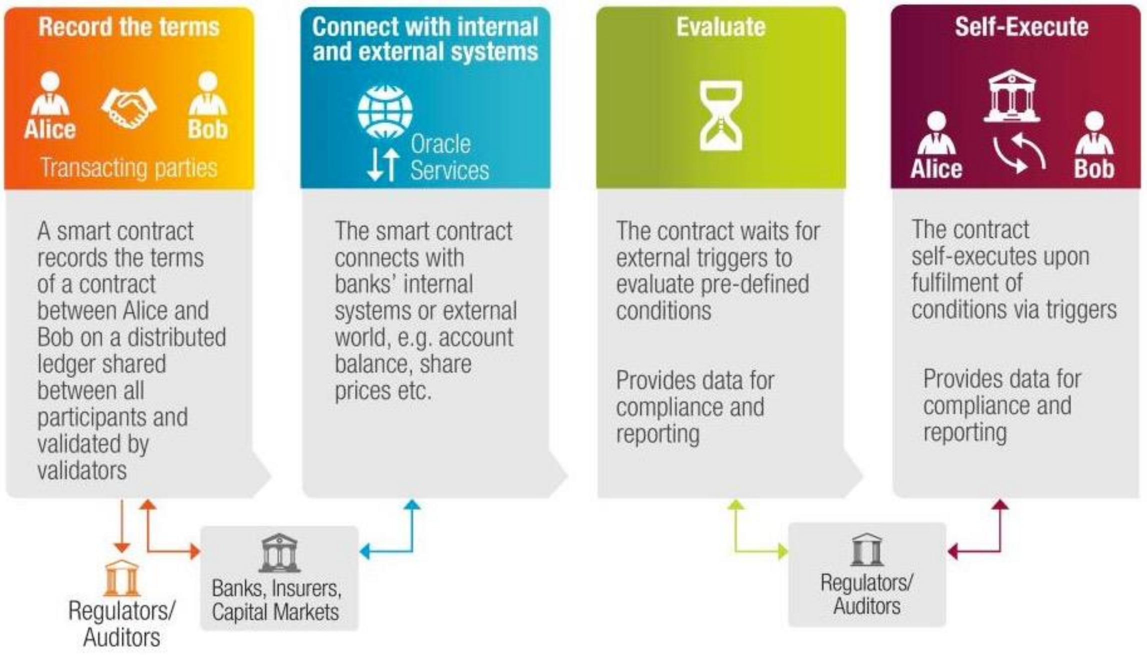
Rubixi is a dApp smart contract that implements a Ponzi scheme, which is a fraudulent high-yield investment program where participants gain money from the investments made by newcomers. Further, the contract owner can collect fees that are paid to the contract upon investments. This attack allows an adversary to steal some ether from the contract, exploiting the immutable bugs' vulnerability. At some point during the development of the contract, its name was changed from Dynamic Pyramid into Rubixi (Bartoletti et al. 2017).

SMART CONTRACT

A smart contract is a set of programmatic rules and penalties automatically evaluated, where a priori does not need to trust each other because the rules will be automatically enforced by the blockchain consensus mechanism (Atzei, Bartoletti, and Cimoli 2017). The Ethereum platform is set up to run decentralized applications and automatically execute smart contracts when certain contract logic is met by handling the enforcement, management, performance, and payment (Tapscott and Tapscott). Smart contracts are a computerized version of an English language paper contract, with a level of automation that essentially provides adjudication-as-a-service. (Marvin 2016). Not only can smart contracts exchange money in the form of Ether, but also anything of value, such as a certificate, a license or registration, content, property, or shares. As shown in figure 7 the smart contract lifecycle includes the following (Marvin 2016).

1. Business rules or a record of the terms of the contract. Details of a smart contract can be made visible to auditors and regulators throughout the process.
2. Internal and external connections to obtain balances, prices, or other asset parameters.
3. Logic to evaluate the contract.

4. The ability to self-execute. When running on the blockchain, a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met.



Record the terms
Alice
Bob
Transacting parties
A smart contract records the terms of a contract between Alice and Bob on a distributed ledger shared between all participants and validated by validators
Connect with internal and external systems
Oracle Services
The smart contract connects with banks' internal systems or external world, e.g. account balance, share prices etc.
Evaluate
The contract waits for external triggers to evaluate pre-defined conditions
Provides data for compliance and reporting
Self-Execute
Alice
Bob
The contract self-executes upon fulfilment of conditions via triggers
Provides data for compliance and reporting
Regulators/ Auditors
Banks, Insurers, Capital Markets
Regulators/ Auditors

Figure 7: Smart Contract Lifecycle

A smart contract's strength is also its weakness because smart contracts run on the blockchain; they run exactly as programmed without any possibility of censorship, downtime, fraud protection, or third party interference. As explained above, once a transaction is committed, verified, and added to the chain it cannot be undone. If a smart contract program leaks money automatically and continuously then the results could be very bad if left untested and unmonitored.

A smart contract includes a set of executable functions and state variables. The functions are executed when transactions are made to these functions. The transactions include input parameters that are required by the functions and the state variables in the contract. Once compiled, the contracts are uploaded into the blockchain network that then assigns a unique address to the contract. Any user on the Ethereum blockchain network can trigger the functions in the contract by sending transactions to the contract. The state transition functions are described in Figure 4. A smart contract includes the following (Arshdeep 2017).

1. State Variables. These are stored in the contracts storage and are used to maintain the contract's state.
2. Functions. Functions in a smart contract include the code, these are executed when transactions are sent to the contract. In Solidity, a contract has a special function called a constructor, that is executed only once when the contract is deployed (Arshdeep 2017).
3. Modifiers. These can be used within a contract to change and check the condition of the function, or to modify the workflow behavior.
4. Events. Events are used to track the execution of the transaction sent to the contract.

Smart contract transactions and calls are the messages that are sent by Externally Owned Accounts (EOA) to other EOAs, or peer contract accounts. Each Ethereum transition includes the following fields.

1. Nonce. This nonce is different from the previously explained Bitcoin PoW. The nonce of an EOA is a scalar value that increases with every transaction. A contract can only make a calls that are triggered by transactions (Bontje 2016).

2. Gas Price. The price per unit of gas, in Wei. The base unit of an Ether is called a Wei, 1 Ether is equal to 10**18 Wei. This is the price that will be paid for all computations involved in the execution of this transaction.
3. Gas Limit or Start Gas. A scalar value equal to the maximum amount of gas that can be used in executing the transaction. In the automobile metaphor, this will be the concept of a full tank of gas that cannot be exceed.
4. To. The 20-Bytes address of the recipient of the transaction. If the transaction is to create a new contract, this field is empty.
5. Value. A scalar value equal to the number of Wei to be transferred with this transaction. If the transaction is to create a new contract, the value acts as an endowment for the newly created account.
6. Data. A byte array containing the input data that is part of the transaction. When the transaction is sent to a contract, the data field is used to provide the input data to the contract.
7. v,r,s. These values correspond to the signature of the transaction and are used to determine the sender of the transaction. In Ethereum, the method of signing transactions is similar to the electrum style signatures, or pretty good privacy protocol (PGP), of private and public key infrastructures. The v,r,s tuple is the raw signature of the transaction, without the signature made with the private key corresponding to the sending account. From these values it is possible to extract the public key, and thus the address of the sender of the transaction (Arshdeep 2017) (Wood 2017).

Refer to appendix A for more details of the Ethereum protocol, and to a graphic made by Lee Thomas on the Ethereum stack exchange for a graphical representation of the Ethereum block architecture (Thomas 2016). These graphs are also found on Reddit

(Reddit 2016). The following sections of this chapter include Ethereum innovations and how a transaction is conducted.

ETHEREUM INNOVATIONS

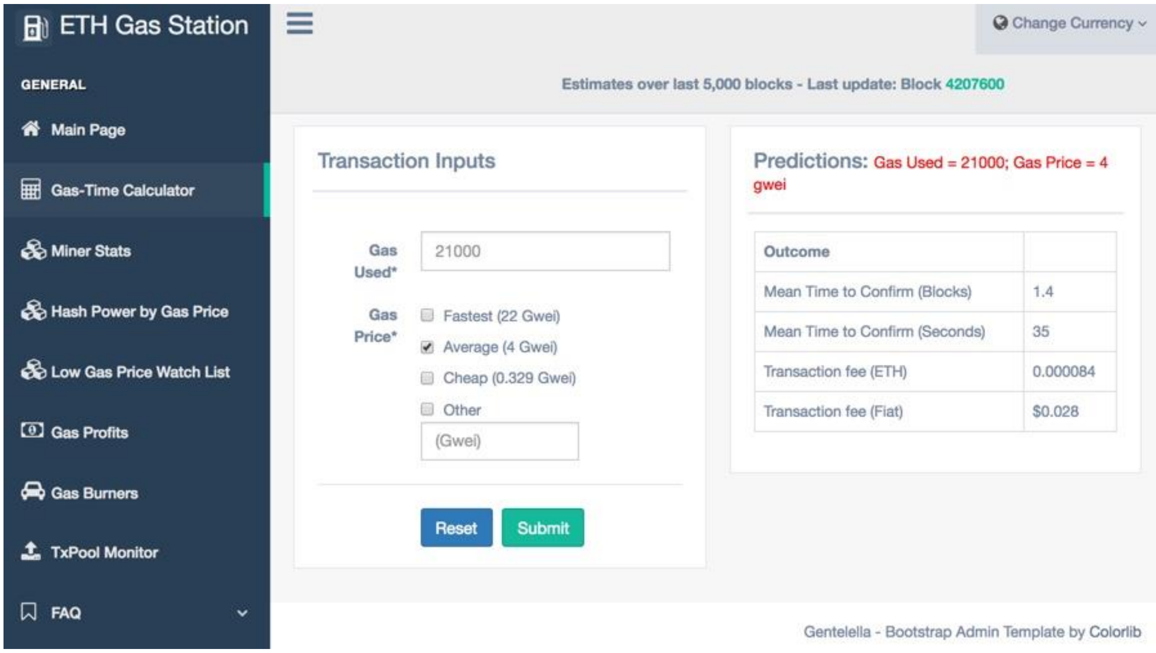
Ethereum's core innovation is the Ethereum Virtual Machine (EVM) that, given enough time and memory, can perform operations and logic making it a Turing-complete system compiling the results into machine language. Vitalik Buterin initiated the development of the Ethereum platform, observing bitcoin's early shortcomings and realizing that blockchain fundamentally could transfer objects of value in addition to cryptocurrency. EVM enables a writer of a smart contract dApp to reuse complicated and time-consuming library constructs, instead of having to build an entirely original blockchain for each new application. Ethereum enables the development of potentially thousands of different applications on the same platform, and can be used to build Decentralized Autonomous Organizations (DAO).

A DAO, also known as a Distributed Autonomous Enterprises (DAE), is a fully autonomous decentralized organization, with no single leader. This is a set of autonomous smart contracts, or agents, that cooperate in a complex blockchain-based ecosystem according to a mission statement and business rules. This is the future of enterprises and organizations. A suite of services could be created to sell to humans or other organizations. DAO's hire people or contract other smart contract programs and could acquire resources. Much of the day-to-day decisions of an organization could be pre-programed. This new form of enterprise can run with minimal traditional management because everything and everyone works according to specific rules and procedures coded into smart contracts. Enterprise founders, or shareholders, would set the software's agenda to execute specific functions. Human employees, or partner organizations, could perform within smart contract rules and when they complete a specified job. They are paid much the way outsourcing is done today, or Freelancing (Freelancer 2017). There are no contract costs, policing and enforcing of terms, or handling of remedies if parties don't deliver as promised. DAO's are run by programming a collection of smart contracts written on the Ethereum blockchain. The code is designed to replace the rules and structure of a traditional organization, eliminating the need for managers and centralized control (Tapscott and Tapscott).

The next generation blockchain enterprises are pioneering new ground of management science by running as much of their company using Ethereum DAO smart contracts. This affects their governance and day-to-day operations from project management, software development and testing, hiring and outsourcing, compensation, and funding. This is done by identifying the work to be done, distributing the load, obtaining agreement on roles and responsibilities and compensation, and then codifying these rights in explicit, detailed, unambiguous, self-enforcing agreements that can serve as the glue to hold all of the business aspects of their relationships together. Some agreements can pay for performance, others meter out annual salary in ether, and still others are more like bounties attached to task completion (ConsenSys 2017).

ETHEREUM TRANSACTION AND GAS

Because of the Turing-completeness of EVM, and the fact that computation is executed on every network node, it could be possible for an adversary attacker to create a denial-of-service infinite loop attack. However, the Ethereum network solution for this type of attack is to require computations to be funded in advance by using fees, termed gas. The sender of the transactions is charged a gas fee that is paid to the Miners, and any balance left over after the transaction is refunded to the sender. The gas fee paid is proportional to the amount of work that is needed to execute the transaction, in terms of the number of individual instructions (Arshdeep 2017). There are website services that help estimate transaction fees in advance. The ETH gas station web site (Gentelella 2017) is shown in Figure 8 and also provides a gas calculator. Transaction or execution fees are the product of gas and gas price in Wei. The transaction which triggers the invocation specifies the gas limit up to which the user is willing to pay, and the price per unit of gas. In this example there are 2100 gas units used -- as a limit -- multiplied by the gas price of 4 GWei; this product is 81000 GWei. Then the calculator divides by 1 billion, that equalizes the units to only Wei, and provides the estimated transaction fee in Ether equal to 0.000084. Finally, this number is multiplied by the number of Ethers per US Dollars, which equates to $307. This final multiplication provides the transaction fiat fee of, $0.028 USD. Gas is consumed by performing operations on the blockchain network. Notice that this final estimated resulting cost of $0.028 USD is the cost of a single transaction within a smart contract. Smart contracts include logic that will cause the price of a complete contract to be increased by 10 times or more depending on the complexity and length of the contract.



Estimates over last 5,000 blocks - Last update: Block 4207600

Transaction Inputs

Gas Used* 21000

Gas Price*

☐ Fastest (22 Gwei)

☑ Average (4 Gwei)

☐ Cheap (0.329 Gwei)

☐ Other

(Gwei)

Predictions: Gas Used = 21000; Gas Price = 4 gwei

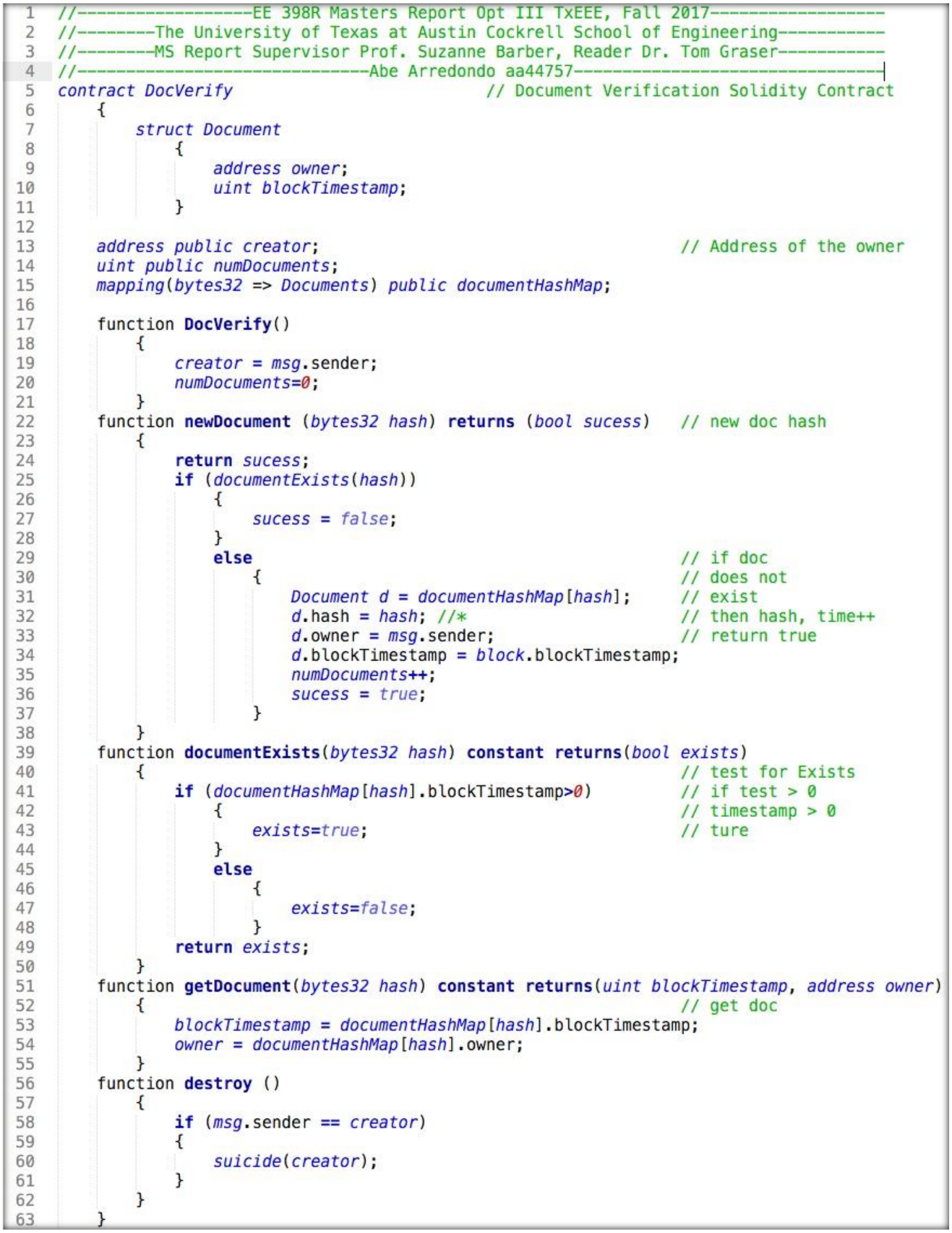
Outcome	
Mean Time to Confirm (Blocks)	1.4
Mean Time to Confirm (Seconds)	35
Transaction fee (ETH)	0.000084
Transaction fee (Fiat)	$0.028

Figure 8: Example Ethereum transaction fee calculator

Miners execute a transaction until its normal termination, unless an exception is thrown. A transaction fee is lost if it does not terminate successfully. A transaction is considered invalid if a user’s gas balance is insufficient to perform the associated computation (Peters and Panayi 2016). If a transaction consumes all the allocated gas without completing the required operation or transaction, then it terminates with an out-of-gas exception and the user loses the entire gas fee. An adversary wishing to attempt a denial-of-service attack would need to allocate a large amount of gas, and pay the corresponding ether, thus making the attack very expensive (Atzei, Bartoletti, and Cimoli 2017).

DOCUMENT VERIFICATION dAPP IMPLEMENTATION EXAMPLE

Chapter 5 of this report specifies the requirements for the document verification dApp that acts as an authentic proof of the existence for a power of attorney document. The same can be used for a will or other legal documents, where the recipient or executors are holding the original document. The document verification dApp is used to store a cryptographic hash, or a unique signature of these legal documents on the Ethereum blockchain. The dApp does not store the document itself, just its signature hash. The cryptographic hash code is computed on the client side. The Solidity document verification code shown in Figure 9 demonstrates the document hash, along with a timestamp and the address of the owner of the document or the person who submitted the document (Arshdeep 2017).



```
//------------------EE 398R Masters Report Opt III TxEEE, Fall 2017------------------
//--------The University of Texas at Austin Cockrell School of Engineering-----------
//--------MS Report Supervisor Prof. Suzanne Barber, Reader Dr. Tom Graser-----------
//------------------------------Abe Arredondo aa44757--------------------------------
contract DocVerify                          // Document Verification Solidity Contract
    {
        struct Document
            {
                address owner;
                uint blockTimestamp;
            }

    address public creator;                                     // Address of the owner
    uint public numDocuments;
    mapping(bytes32 => Documents) public documentHashMap;

    function DocVerify()
        {
            creator = msg.sender;
            numDocuments=0;
        }
    function newDocument (bytes32 hash) returns (bool sucess)   // new doc hash
        {
            return sucess;
            if (documentExists(hash))
                {
                    sucess = false;
                }
                else                                            // if doc
                    {                                           // does not
                        Document d = documentHashMap[hash];     // exist
                        d.hash = hash; //*                      // then hash, time++
                        d.owner = msg.sender;                   // return true
                        d.blockTimestamp = block.blockTimestamp;
                        numDocuments++;
                        sucess = true;
                    }
        }
    function documentExists(bytes32 hash) constant returns(bool exists)
        {                                                       // test for Exists
            if (documentHashMap[hash].blockTimestamp>0)         // if test > 0
                {                                               // timestamp > 0
                    exists=true;                                // ture
                }
                else
                    {
                        exists=false;
                    }
            return exists;
        }
    function getDocument(bytes32 hash) constant returns(uint blockTimestamp, address owner)
        {                                                       // get doc
            blockTimestamp = documentHashMap[hash].blockTimestamp;
            owner = documentHashMap[hash].owner;
        }
    function destroy ()
        {
            if (msg.sender == creator)
            {
                suicide(creator);
            }
        }
    }
```

Figure 9: Ethereum Solidity document verification code example

After the information outlined in Figure 9 is added to the smart contract, any Ethereum user can later verify if the document existed at that time. The cryptographic hash of the document depends on the document's content. Any changes in the document will change its hash. Any Ethereum user can securely verify the existence of a document and be assured that the exact same document existed at a particular moment in time (Arshdeep 2017). Notice in Figure 9 that Solidity is like JavaScript. Atzei et.al., states that the implementation of a smart contract is prone to errors, due to the JavaScript programming language similarities. Many unintended adverse actions of a smart contract are caused by misunderstandings between the semantics of Solidity and legacy programming conventions. The problem is that Solidity looks like the JavaScript language with ordinary exceptions and functions. However, in Solidity when an exception is thrown, it cannot be caught; the execution stops and the fee is lost. Deploying a smart dApp contract that is not thoroughly tested can be costly and frustrating. Solidity does not introduce constructs to deal with domain-specific aspects, such as, explicitly stating that computation steps are recorded on a live or test blockchain, where they can be delayed, and if the fees are permanent (Atzei, Bartoletti, and Cimoli 2017).

Chapter 4: Future Applications for the Government using Blockchain

Blockchain technology can be used in a number of ways for non-financial intangible assets to facilitate identity verification, digital document attestation, or peer-to-peer transfers (Swan 2015a). It can also be used for voting, health data, and intellectual property (Swan 2015b). One conclusion from the IBM 2017 blockchain trend report, a survey conducted with 200 governments leaders from 16 countries on the topic of blockchain, is that mass adoption of the technology is expected to peak in 2019 (Chamberlin 2017) because government regulation would be slow to adopt blockchain any sooner. IBM and Chamberlin's opinions seem to be optimistic as compared to Marvin, illustrated in Figure 9, where mass adoption is anticipated to start in 2020 (Marvin 2016).

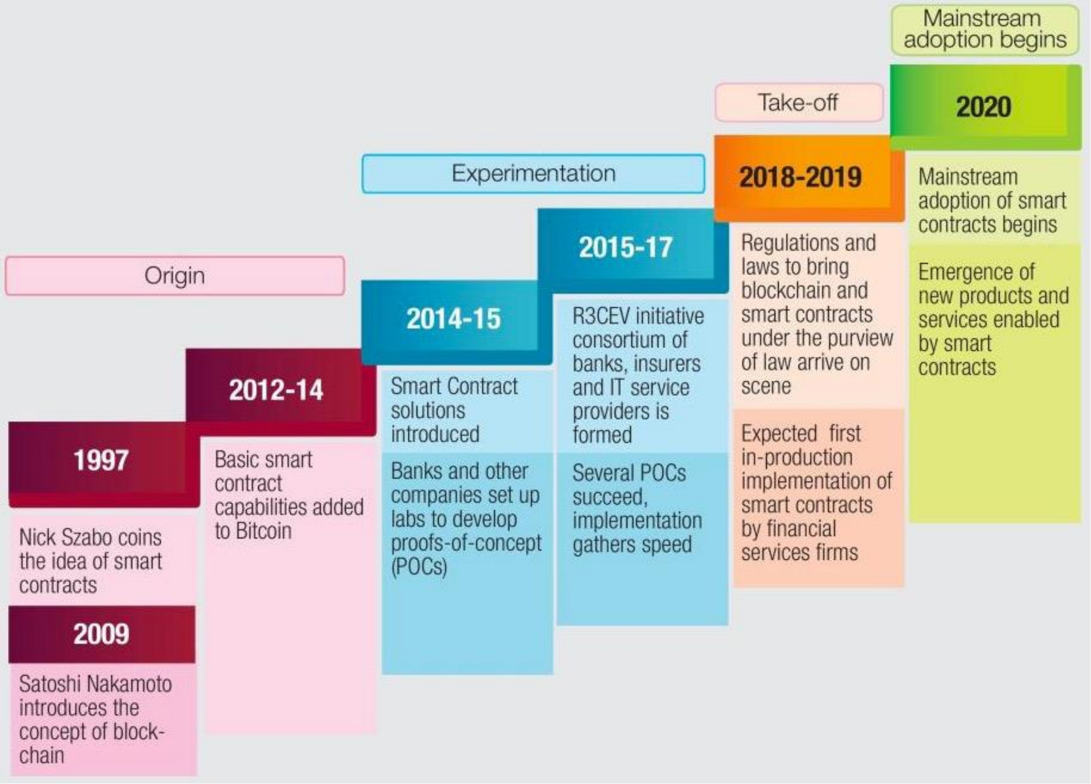

Origin
1997
Nick Szabo coins the idea of smart contracts
2009
Satoshi Nakamoto introduces the concept of block-chain
2012-14
Basic smart contract capabilities added to Bitcoin
Experimentation
2014-15
Smart Contract solutions introduced
Banks and other companies set up labs to develop proofs-of-concept (POCs)
2015-17
R3CEV initiative consortium of banks, insurers and IT service providers is formed
Several POCs succeed, implementation gathers speed
Take-off
2018-2019
Regulations and laws to bring blockchain and smart contracts under the purview of law arrive on scene
Expected first in-production implementation of smart contracts by financial services firms
Mainstream adoption begins
2020
Mainstream adoption of smart contracts begins
Emergence of new products and services enabled by smart contracts

Figure 10: Blockchain Roadmap

Website blogs and Tweeter sourced lists (Ledra Capital 2015) have discontinued updating an exhaustive list of all the possible applications blockchain could have outside of the financial technology realms, because the list expands to include most anything that could be tracked in any form of ledger, record, or database. Pilkington's list of future applications (Pilkington 2015), as they relate to state government and regulation inclusion, also leaves much to be desired because the listing only includes birth certificates, automobile registrations, land deeds, and voting with no in-depth analysis of the potential applications. Table 3 features an expanded list of different industries and examples of blockchain use cases by category, originally provided by Moody's investor service and reported in Brave New Coin News (Parker 2016) (Swan 2015b).

Financial Institutions	Private Corp	GOVERNMENT	Cross Industry
Remittances, international transfer and payments	Supply chain management	Notarized record management and attestation	Cyber security
Capital markets	Healthcare	Identity management	Internet of things
Financial trades	Real estate	Voting	Data storage
Insurance	Energy	Transportation	Big data reporting
Anti-money Laundering and know your customer	Accounting and financial management	Legislation, compliance, regulatory audit and oversight	
Peer to peer transaction	Media	Environmental, energy and utility services	
		Education	
		Taxes	

Table 3: Industries and Fields of Blockchain Uses Cases.

Expanding the government industry column listed above, Table 4 below provides detailed insight example use cases of where a government – a state government for the purposes of this report -- can implement blockchain technology. The use cases originated from bloggers, forums, Tweeter tags, and technology journalists (Parker 2016).

Government Service Category	Examples where blockchain can be used
Notarized record management and attestation	Land management, property titles, marriage certificates, birth certificates, death certificates, wills, trusts, escrows, power of attorney, proof of insurance, proof of ownership, notarized legal documents and contract agreements
Identity management	Identity cards, voter registrations, business licenses, business incorporation, passports from a federal perspective, professional licensing, such as; Attorneys, Pharmacists, Chiropractors, Engineers and others.
Voting	Voting
Transportation	Roads and public transportation, highway patrol, motor vehicles registration, driver's licenses, vehicle license plates
Legislation, compliance, regulatory audit and oversight	Law creation, congress, senate, constitution, audit non-profits for transparency, housing, agriculture, railroad, lottery, and insurance, state parks
Environmental, energy and utilities	Environmental protection, oil, sewage treatment, energy credits and subsidiaries for wind, gas, coal, and solar power, fresh water, hydro power
Education	University System, education agency, public schools, financial aid and loans, teachers, child development,
Taxes	Tax records, public employee pensions, unemployment, workers compensation
Food and safety	Occupational safety and health, food safety, food management, food aid and special need assistance, public health, medical safety, consumer protection, product safety, foster care, mental health, substance abuse and treatment
Law enforcement and judicial	State police, courthouses, corrections and parole, prisons, civil service, national guard, veterans affairs, border protection,

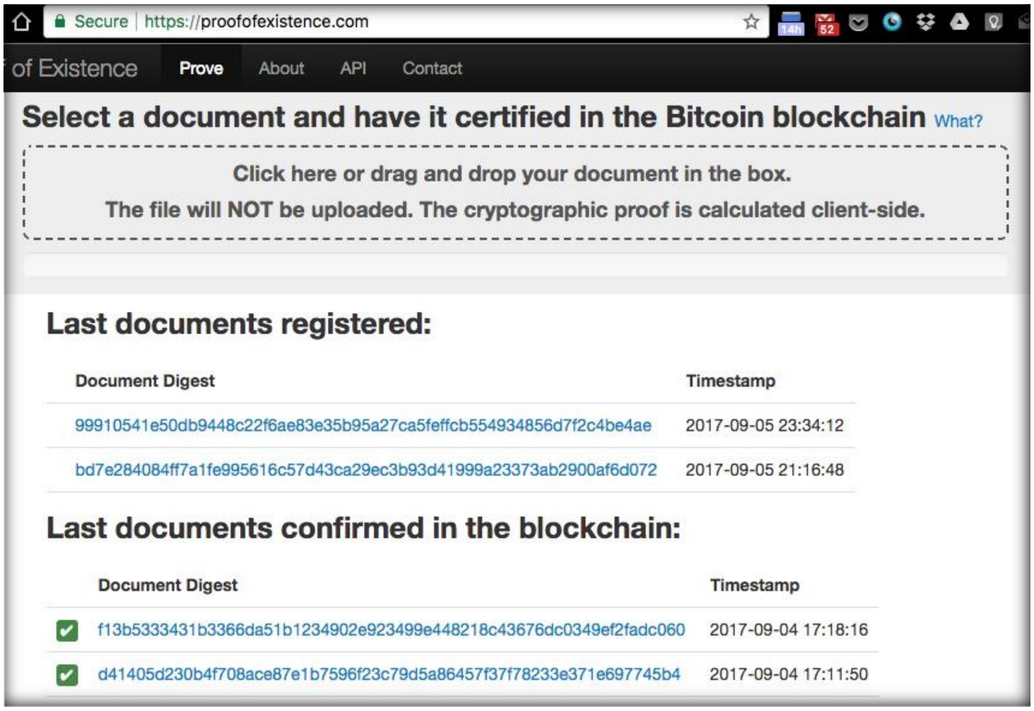
Table 4: Government Use Cases of Blockchain Table.

Next, three examples will be detailed: (1) Notarized Record Management and Attestation, (2) Identity Management, and (3) Voting.

NOTARIZED RECORD MANAGEMENT AND ATTESTATION

For attestation services, blockchain technology brings together two key functions: cryptographic hashing and secure time stamping. Instead of notarizing a document, it can be encoded on the blockchain and offer proof of a specific cargo being registered (Swan 2015b). As a trustless decentralized network, blockchain essentially confirms the existence of a document at a stated time that is potential evidence in a court of law. Until now, only centralized notary services could serve this purpose (Rosic 2016). One of the first dApps that has continually provided this service is Manuel Araoz's Proof of Existence shown in Figure 11 and Figure 12 (Araoz 2017). The dApp shown allows users to upload a file and pay a transaction fee of 2 mBTC, approximately $8 USD at the time of this writing. After the payment, the cryptographic proof of the document will be included on the bitcoin blockchain. The actual data is not stored online and therefore does not risk unwanted publication of the user's material; the process is completely anonymous. This process, in effect, uses the public and ledger-like nature of the blockchain to store proof of your file which can later be verified should an issue of authorship or dating arise. The limitations of the Proof of Existence dApp are as follows (Swan 2015b).

1. Time stamping does not prove ownership.
2. A blockchain is not required for time stamping because other third-party services provide this for free.
3. Transaction confirmations are not immediate; the time the document was submitted to the dApp is not the same precise time as the digital asset creation.



Select a document and have it certified in the Bitcoin blockchain What?

Click here or drag and drop your document in the box.
The file will NOT be uploaded. The cryptographic proof is calculated client-side.

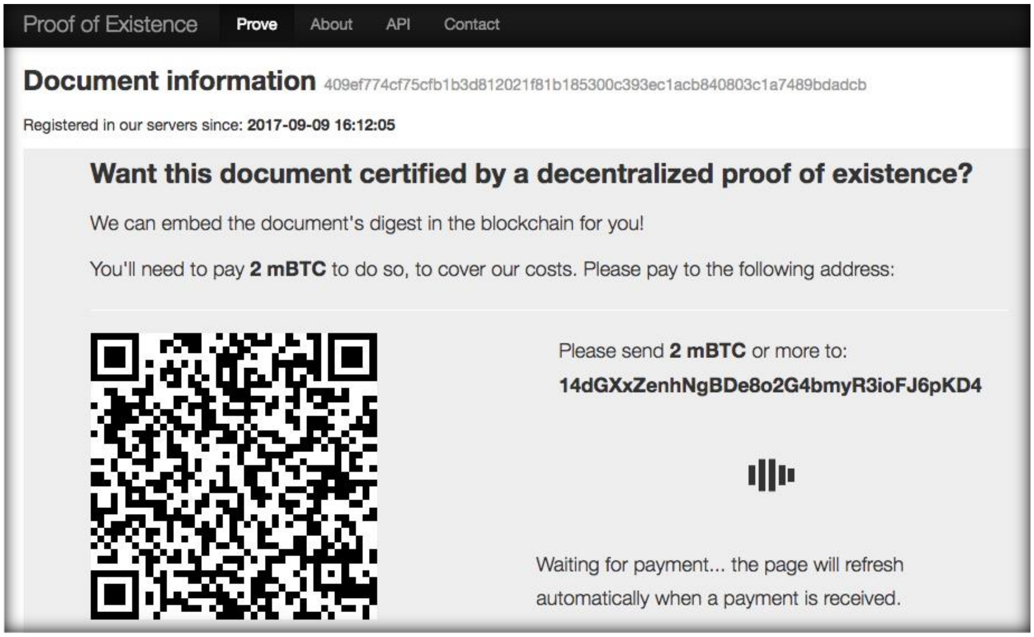
Last documents registered:

Document Digest	Timestamp
99910541e50db9448c22f6ae83e35b95a27ca5feffcb554934856d7f2c4be4ae	2017-09-05 23:34:12
bd7e284084ff7a1fe995616c57d43ca29ec3b93d41999a23373ab2900af6d072	2017-09-05 21:16:48

Last documents confirmed in the blockchain:

	Document Digest	Timestamp
✓	f13b5333431b3366da51b1234902e923499e448218c43676dc0349ef2fadc060	2017-09-04 17:18:16
✓	d41405d230b4f708ace87e1b7596f23c79d5a86457f37f78233e371e697745b4	2017-09-04 17:11:50

Figure 11: Notarized attestation proof of existence blockchain website dApp



Document information 409ef774cf75cfb1b3d812021f81b185300c393ec1acb840803c1a7489bdadcb

Registered in our servers since: **2017-09-09 16:12:05**

Want this document certified by a decentralized proof of existence?

We can embed the document's digest in the blockchain for you!

You'll need to pay **2 mBTC** to do so, to cover our costs. Please pay to the following address:

Please send **2 mBTC** or more to:
14dGXxZenhNgBDe8o2G4bmyR3ioFJ6pKD4

Waiting for payment... the page will refresh automatically when a payment is received.

Figure 12: Proof of existence certification payment page

Providing timestamped data in an unalterable state while maintaining confidentiality is perfect for a wide range of legal and civic applications. Attorneys, clients, and public administrators could use the Proof of Existence blockchain functionality to prove the existence of many documents including wills, deeds, powers of attorney, health care directives, promissory notes, the satisfaction of a promissory note, and other legal government documents without disclosing the contents of the document (Swan 2015b). Most will-related litigation involves challenges to the authenticity of a will. While blockchain would not completely remove these challenges, its distributed ledger system would make it easier to identify factual information and dismiss meritless claims. Linking documents related to a person's estate through a verifiable blockchain system would give executors access to a more trusted pool of data than current systems to determine their veracity (Howard 2015). Blockchain technology could automatically check state death registries, allocate assets from a testator's estate, and send applicable taxes to governmental agencies without administering the will through probate (Wright and De Filippi 2015).

IDENTITY MANAGEMENT

Current identity methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain-based authentication systems are designed through irrefutable identity verification using digital signatures and public key infrastructure cryptography. In blockchain identity authentication, the only check performed is whether or not the transaction was signed by the correct private key. It is inferred that whomever has access to the private key is the owner; the exact identity of the owner is deemed irrelevant (Rosic 2016). Imagine never having to worry about your digital security every again. Blockchains provide an opportunity to establish a strong system for digital identity because it is not based on accounts and permissions associated with account ownership. Instead, private keys are a secure way to manage identity in the digital world and avoids exposing users to sharing too much vulnerable personal information (Bauerle 2017). Blockchain technology offers a solution to many digital identity issues where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner.

Blockchain Identity Use Cases Examples

Blockchain technology can be applied to identity applications in the following areas.

1. Digital Identities.

   Blockchain prevents online companies from selling identities to advertisers by creating a protected data point where you encrypt only the information that you want relevant people to know at certain times. For example, if you're going to a bar, the bartender simply needs the information that tells him you are over 21 (Blockgeeks 2017a). Two companies, uPort (uPort 2017) and personal black box (PBB 2017), have created blockchain privacy tools to keep personal information private and allow users to know what personal data is collected about them and by whom. They also give the user the ability to use personal data as a financial asset.

2. Passports.

   The dipass.io Digital-Passport launched on GitHub helps owners identify themselves online and off. The process is similar to the voting dApp listed below from FollowMyVote; you take a picture of yourself then stamp it with a public and private key, both of which are encoded to prove it is legitimate. The passport is stored on the ledger, given a Bitcoin address with a public IP, and confirmed by Blockchain (Blockgeeks 2017a).

3. E-Residency.

In February 2016, Nasdaq and the Republic of Estonia announced that Estonia's e-Residency platform would be facilitating a blockchain-based e-voting service to allow shareholders of companies listed on Nasdaq's Tallinn Stock Exchange, Estonia's only regulated securities market, to vote in shareholder meetings. The country's e-Residency platform is an electronic identity system used by both Estonian residents and those with business interests in the country to access government services through e-Residency's digital authentication (Mesropyan 2016).

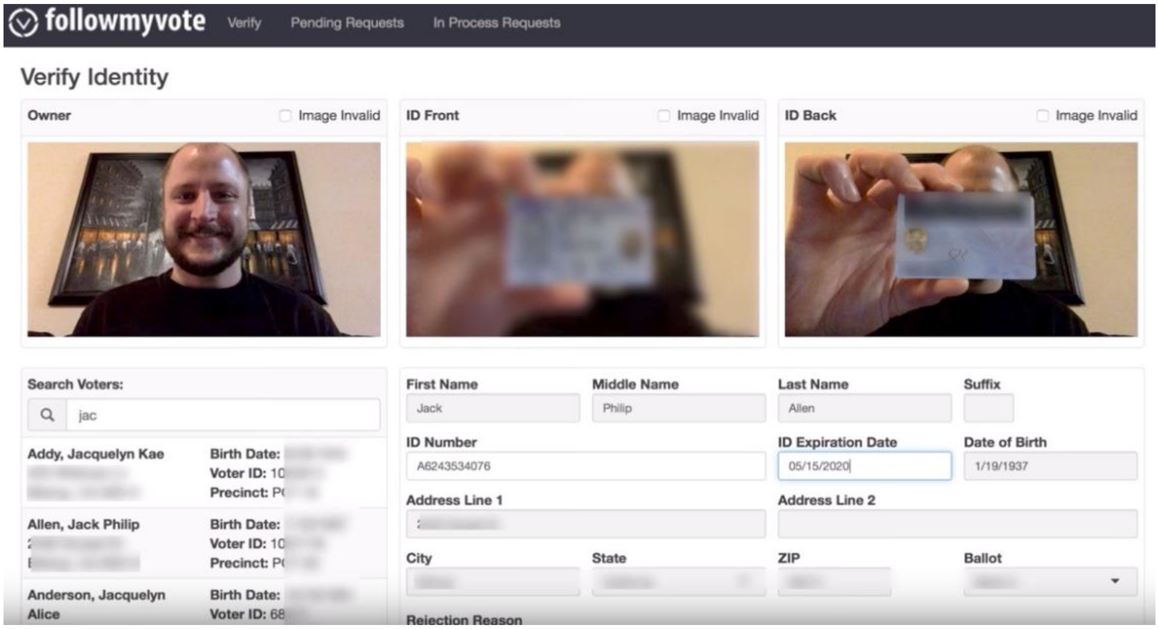
4. Birth Certificates.

Blockchain ID is a digital form of ID that is engineered to replace drivers' licenses, computer passwords, identity cards, social security IDs, and other forms of ID. People rely on birth and marriage documents for certain rights and privileges, such as voting, working, and proof of citizenship. According to a UNICEF report in 2013, up to a third of children under age 5 have not been issued a birth certificate. The blockchain could make record-keeping more reliable by encrypting birth and death certificates and empowering citizens access to this crucial information (Blockgeeks 2017a).

VOTING

Many states in the U.S. use voting machines over 10 years old that are often antiquated and failing. These dated machines are becoming increasingly expensive to maintain as parts are no longer manufactured. A team tasked to observe the 2013 municipal elections in Estonia, the only country to run Internet voting on a wide scale, revealed that they observed election officials downloading key software over insecure Internet connections, typing PINs and passwords, using cameras, and preparing election software on insecure PCs. These actions result in election fraud which undermines democracy. The greatest barrier to getting electoral processes online, according to detractors, is security. Using blockchain a voter could check that her or his vote was successfully transmitted while remaining private to the rest of the world. Norway canceled trials of e-voting systems in local and national elections, concluding that voters' fears about their votes becoming public could undermine democratic processes. In 2014, Liberal Alliance, a political party in Denmark, became the first organization to use blockchain to vote. Blockchain allows a secure voting process that is free of corruption and transparent (Due 2016) (Rosic 2016).

The FollowMyVote website (Follow My Vote 2017) offers a secure and transparent online voting solution that uses blockchain technology and elliptic curve cryptography to ensure that election results are honest and accurate. The company is developing an online open source voting platform that provides transparency into election results by allowing voters to independently audit the ballot box (Mesropyan 2016). As shown in Figure 12, to start the voting process, a voter needs a government issued ID card, takes a picture of himself, then shows the front and back of the government issued ID card. In this case an election official is the identity verifier and looks up the voter name in the list of registered voters. If approved, the voter is provided with a voter ID key and ballot, and proceeds to vote. This process was used in the Inyo County California, U.S.



Verify Identity

Owner □ Image Invalid

ID Front □ Image Invalid

ID Back □ Image Invalid

Search Voters: jac

Addy, Jacquelyn Kae [redacted] Birth Date: [redacted] Voter ID: 10[redacted] Precinct: P[redacted]

Allen, Jack Philip [redacted] Birth Date: [redacted] Voter ID: 10[redacted] Precinct: P[redacted]

Anderson, Jacquelyn Alice Birth Date: [redacted] Voter ID: 68[redacted]

First Name: Jack

Middle Name: Philip

Last Name: Allen

Suffix:

ID Number: A6243534076

ID Expiration Date: 05/15/2020

Date of Birth: 1/19/1937

Address Line 1: [redacted]

Address Line 2:

City: [redacted]

State: [redacted]

ZIP: [redacted]

Ballot: [redacted]

Rejection Reason

Figure 13: Blockchain Voting Booth

Private Blockchain

The nature of blockchain is that of a distributed network of peers accompanied by a public ledger with the purpose of distrusting central authorities (Zyskind and Nathan 2015) such as governments. This report asserts that a government can use a hybrid blockchain approach by employing trusted nodes, such as state certified engineers or other state registered professionals to implement and mine a government private blockchain. The benefits of this approach beyond efficiency and cost is that citizens can be assured that the government is being more transparent putting the ledger of government activities into an immutable, distributed process that is authentic and trustworthy (Swan 2015b). It is possible to create a blockchain system where access permissions are more tightly controlled, with rights to modify or even read the blockchain restricted to a few users, while still maintaining guarantees of authenticity and decentralization that the blockchains provide (Buterin 2015). The first type of private blockchain is a consortium hybrid arrangement blockchain that will be of interest to institutions. A consortium blockchain is a blockchain where the consensus process is controlled by a preselected set of trusted registered or certified nodes. For example, there could be a consortium of 30 state board of professional engineers who operate a node such that 20 must sign every block in order for the block to be valid. The right to read the blockchain may be public or restricted to the participants.

The metaphor for a private blockchain is a secure and encrypted Wikipedia for Ledgers. This type of blockchain partially returns the centralized role into transactions. The private institution who handles the blockchain can write and verify all the transactions. This type of blockchain is more suitable for traditional businesses and governance models. This also ensures greater speeds and connectivity (Srivastava 2017). A fully private blockchain keeps write permissions centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. A private blockchain is housed behind a firewall on a private LAN. Applications for a fully private blockchain include database management and auditing internal to a single institution, where public readability features may not be necessary. However; public auditability is desired. Governments have an interest in blockchain because of the following advantages and factors.

1. There are ownership rights surrounding cryptographic key possession, revocation, generation, replacement, or loss of a key. A government may wish to expel or punish an intentional bad member, or reset a lost key.
2. The government is interested in who can act as part of a blockchain network to prevent access from foreign enemy states, or terrorist organizations, from taking a majority control of the chain. If only known node validators are

accepted, such as state certified engineers or other state registered professionals, then risk of a 51% attack arising from some miner collusion in China is unwarranted.

3. The government has an interest in blockchain protocols that authorize transactions because governments often regulate transaction authorization through compliance regimes. For this reason, regulatory compliance is seen as a business opportunity by many blockchain developers (Bauerle 2017).
4. The consortium or institution running a private blockchain can change the rules of a blockchain or revert transactions. This functionality may be a necessity because a government would not allow a known criminal to have legal ownership rights over a plainly visible valuable asset such as land. An attempt to create a government uncontrollable land registry would in practice quickly devolve into one that is not recognized by the government itself.
5. Transactions are cheaper, since they only need to be verified by a few known validator nodes that can be trusted to have very high processing power, and not by ten thousand laptops.
6. If read permissions are restricted, private blockchains can provide a greater level of privacy.

Blockchain is being researched by many governments throughout the world, China, Vietnam, Denmark, the United Kingdom, Japan, and state governments within India to name a few. In the U.S., the State of Illinois has created a blockchain initiative to explore blockchain’s impact on government to create a self-sovereign identity for citizens during the birth registration process. Self-sovereign identity is a digital identity that remains entirely under the individual's control. Illinois State government agencies will verify birth registration information and then cryptographically sign identity attributes such as legal name, date of birth, sex or blood type, creating what are called verifiable claims or attributes. The identifier guarantees each attribute is cryptographically sealed and only accessible with explicit consent by the identity holder or, in the case of a newborn child, a legal guardian (Allison 2017). The Australian Post has published a graph of identities used throughout the year organized by different sectors as shown in Figure 14 (Australia Post 2016).

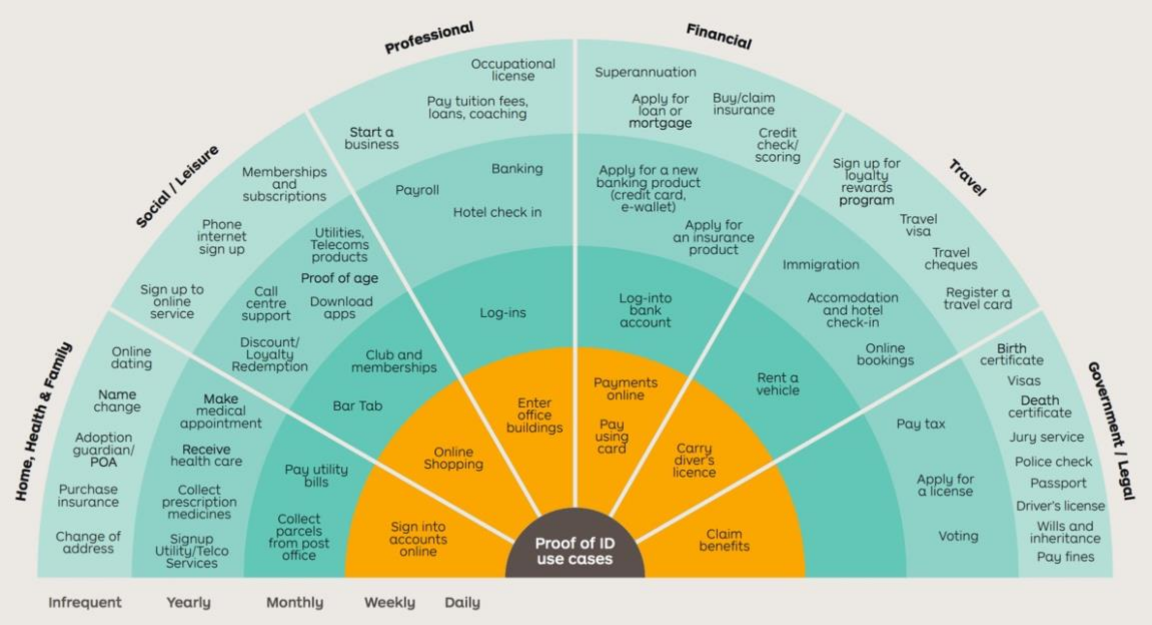


Figure 14: Identity Used Throughout the Year

In New York State, bit licensing is required by cryptocurrency companies that operate in, or serve customers who are based in, New York. Established in 2015 by the New York State department of financial services, bit licensing is a regulatory framework for bitcoin and digital currency businesses (Santori 2015). The State of Delaware allows corporations to maintain shareholder lists along with other corporate records using blockchain. Companies incorporated in Delaware may now keep a list of shareholder names, which they must do by law, on a blockchain of registered agent nodes instead of conventional methods like an Excel spreadsheet or a database (Roberts 2017). In Nevada, lawmakers (Cuen 2017) signed a cryptocurrency bill into law, Senate Bill 398, that blocks local governments from taxing blockchain transactions or requiring a permit for them. The following section describes a blockchain case study highlighting how governments could authorize notaries to use blockchain technology.

CASE STUDY

The final section describes an in-depth case study for a blockchain smart contract (Kosba, Miller et al. 2016) to invoke a statutory durable Power of Attorney (PoA) using blockchain technology for oneself in case of incapacitation while still living (Swan 2015). This is achieved by adding logic to the smart contract where the grantor of the PoA must reply to a health check email message or text message acknowledging he is okay, in much the same way that police, public utility, or healthcare workers verify their okay status to their employers during a disaster or disaster readiness exercise. The health check message could include a memory test or game quiz that the grantor must answer correctly, with the result going to the agent or recipient of the PoA. The frequency of the health check is variable and can be preprogrammed by the grantor when the PoA is defined.

Chapter 5 outlines the vision of a hybrid website that describes both blockchain proof of ownership or proof of existence attestations and an innovative asynchronous Certificate Authority (CA) public notary method using photographs, personal and live video conferencing, or short video recordings of a grantor, providing video proof that an oath was taken to open a trusted certificate on a specific date.   Because of the CA private key infrastructure (PKI) security features, the grantor of the PoA, or other documents that require notarization, will not need to resubmit a second live video conference, or video recording attestation on any subsequent document requests because the certificate will only be known to the issuing authority and grantor. Furthermore, the method proposed in this report also requires second factor authentication and the answering of security questions. The CA should be a trusted professional recognized by the state government such as a notary, state board registered professional engineer, or any other professional in good standing with the local government.

Chapter 5: Blockchain Application Requirements

This chapter defines the blockchain application requirements and proposed Certificate Authority cryptographic methods. The blockchain dApp hybrid website overall vision is described, followed by high-level requirements for notarizing a power of attorney by legacy and blockchain means. These requirements were collected, analyzed, and merged from interviews with three stakeholder viewpoints: the notary, the grantor of the PoA, and an IT Administrator. The names and identities of the people interviewed are withheld from this report, and user profile pseudo names are used instead. An example of the interview process and forms are shown in Appendix B.

PROPOSED BLOCKCHAIN DAPP PRODUCT OVERVIEW VISION

The proposed solution is a hybrid website that implements a blockchain proof of existence on the Ethereum network and is backward compatible with existing notarization rules and regulations. The hybrid website is compliant with government procedures in that it provides a mechanism for the user, the grantor of the power of attorney in this case, the ability to provide an electronic signature using DocuSign or Adobe Acrobat Pro. The user also must provide a video recording affirming that he wishes to sign the document, and photographs of a government issued ID. Within the same calendar day, the notary verifies the users ID and video recording, then signs and stamps the document also using DocuSign or Adobe Acrobat Pro and a custom seal. If the user fails to provide a verifiable video recording, then the notary initiates a video conference by facetime or any other live video chat mechanism. A certificate authority key distribution center will distribute private key certificates for users, such as grantors, agents, witnesses, and beneficiaries. After two-factor authentication, users will not need to re-submit a new video recording or live video conference for subsequent documents to be notarized. The website accepts payments by anonymous Bitcoin or Ether cryptocurrency as well as legacy credit card, or PayPal.

This new Power of Attorney document attestation service provides an entry point into the other common notary services, such as application for vital records, an affidavit for one parent traveling with a minor without the other parent, mobile notary services for nursing homes, and assisted living or homebound individuals who cannot travel to a notary's office. Following are the distinguishing main features of this service.

1. Blockchain Poof of Existence
2. Certificate Authority providing certificates after live or video notary validations
3. Second-level role authentication for returning users with a valid certificate
4. Documenting electronic signatures for grantor and notary, appending notary electronic seal to original document
5. Anonymous Bitcoin and Ethereum payment
6. Legacy secure internet PayPal and credit card payment processing

USER PROFILES

The requirements for notarizing a power of attorney by legacy and blockchain means are collected from 3 interviews an example of which is shown in Appendix B. The users of the system are as follows.

1. The grantor of the Power of Attorney. The grantor is the person seeking to provide his agent the powers over his estate and is the initiator of the document to be notarized.

2. The notary. A person who is commissioned by the state as a notary and who signs and stamps a document (Notaries Ogr 2017).
3. IT Administrator. An information technology operations and security professional.

The names and identities of the people interviewed are withheld from this report; instead generic user profile names are used. Appendix B shows artifacts from the interview with the notary (AWARE Software 2009) (Barber and Graser 1999) (the grantor and IT administrator interviews are not included in this report), and Table 5 lists the combined high-level needs and features after analyzing and merging the requirements gathered from the three stakeholders. The resulting requirements are divided into functional, business data, business timing, and non-functional requirements. Following the Systems Engineering Process Activities methodology (Graser et al.), the annotation following each requirement in Table 5 traces back to the corresponding stakeholder: NP for Notary, GR for Grantor, and IT for IT administrator.

Combined Requirements Resulting from all Interviews:

This table contains the combined requirements that resulted from the interview with (1) the Notary (NP), (2) the IT Administrator (IT), and (3) the User or Grantor (GR) of a Power of Attorney document. The numbers following each entry represent the traceability to the interview questionnaire.

Requirements:

1. Following are the combined Business Functionality Requirements that resulted from all the interviews categorized by major feature requirement heading.

   a. Roles/users

      i. There should be Grantor, Notary, IT Admin, and an Auditor users- NP0, NP16, NP18, NP61, IT1, IT16.

      ii. There should be grantor users -

      iii. There should be new users - NP20

      iv. There should be other administrative users such as a government regulator user. – NP16

   b. Automated Notifications

      i. Blockchain Global Public Notary System automatically sends users an email when Notary is done - NP19, NP26

      ii. Notary, IT Admin, & Grantor would like system to send user an email if they need to complete an action – NP27, NP40, IT26, GR12, GR28

   c. Notary Process

      i. Notary requires choice for automated video recording - NP14

      ii. IT Admin is concerned about bandwidth speeds video recordings, and face to face live videoconferencing – IT9

         1. Exceptions mentioned are when: user is determined to cause fraud or intentionally misuse the system- NP37, IT29, IT37

      iii. Notary needs to access Notary button to approve the document after the user is verified, this should be automated as much as possible. - NP25

      iv. Notary needs to be served the next user record that needs to be notarized NP15, NP26

      v. Grantor, IT Admin and Notary should be able to search for documents and users – GR3, GR5, GR9, GR26, IT5, IT12, IT23, IT30, IT34, IT38, IT49, NP1, NP2, NP4, NP12, NP22, NP30, NP37, NP41, NP52

      vi. IT Admin wants to see info on required authentication for a Document - IT17, IT45

      vii. IT Admin & Notary would like automatic user ID checking – IT47, NP47

Table 5: Requirements of Public Notary Systems

        viii. Grantor and Notary would like the system to calculate the remaining documents needed to complete a batch – GR29, NP4
        ix. Notary wants mechanism to prioritize & distribute the users & their documents – NP4, NP52
    d. user - System interactions
        i. All users should be able to complete the process themselves – GR3, GR4, GR5, GR7, GR8, GR9, GR12, GR13, GR19, GR20, GR26, GR30, IT13, NP8, NP13, NP24
        ii. A method should be investigated with the secretary of state to know if there is a way to witness a signature without having to upload a video. NP43
        iii. System shows Document status – GR26, GR27, NP52, IT52
    e. Other Functionality
        i. Notary can waive authentication failure – IT7, IT47
        ii. Documents cannot be cancelled - NP47

2. Business Data Requirements
    a. The Blockchain Global Public Notary System should show the following information in completing a power of attorney document- NP1, NP22, NP37, GR19.
        i. The name of the person, and address, granting the power of attorney NP1, NP22, NP37, GR19
        ii. The name of the person, and address, appointed as the agent, attorney in fact NP1, NP22, NP37, GR19
        iii. Image of the grantor, video, photos of ID – IT7, IT8, IT14, IT23, IT25, IT37, IT45, NP1, NP,2, NP3, NP7, NP8, NP17, NP22, NP23, NP37, NP41, NP51, GR8, GR11, GR22

        The following powers need to be checked off by the Grantor specifically for a Power of Attorney document

        1. Real Property transactions -
        2. Tangible personal property transactions-
        3. Stocks and bonds transactions -
        4. Commodity and option transactions -
        5. Banking and other financial institution transactions-
        6. Business operating transactions-
        7. Insurance and annuity transactions-
        8. Estate, trust, and other beneficiary transactions-
        9. Claims and litigation-
        10. Personal and family maintenance -
        11. Benefits from social security, Medicare, Medicaid, or other governmental programs of civil or military service
        12. Retirement plan transactions
        13. Tax matters
        14. All of the above powers listed above

Table 5: Requirements of Public Notary Systems (Continued)

b. The Blockchain Global Public Notary System should obtain the following information from the database

i. Document inventory – NP4, NP12, NP21, NP26, NP30, NP34, NP35, NP36, NP37, NP41, GR18, GR26, GR28, IT5, IT12, IT23

ii. Grantor, Agent, and Notary information, NP1, NP22, NP37, GR19

iii. Notifications, Payment information IT13, IT23, IT39, GR15, GR29, NP39

iv. X.500 certificate information. This is a technical question about the Certificate Authority database not asked during the interviews.

v. Videos, Photos, Video Conferences IT7, IT8, IT14, IT23, IT25, IT37, IT45, NP1, NP,2, NP3, NP7, NP8, NP17, NP22, NP23, NP37, NP41, NP51, GR8, GR11, GR22

c. The Blockchain Global Public Notary System should maintain the following information

i. Information per Document

1. Grantors name - NP1, NP22, NP37, GR19

2. Grantors Address - NP1, NP22, NP37, GR19

3. The name of the person appointed as agent - NP1, NP22, NP37, GR19

4. The address of the person appointed as agent NP1, NP22, NP37, GR19

5. Special instructions open text -

6. Is the power of attorney affected by subsequent disability or incapacitation –included as logic in the smart contract explained in case study above. GR19

7. This power of attorney becomes effective upon my disability or incapacitation –included as logic in the smart contract explained in case study above. GR19

ii. Information per User

1. Grantors name – GR12

2. Grantors Address – GR12

3. Grantors contact information – GR12

d. The Blockchain Global Public Notary System must obtain data on document size - NP53, IT53

i. IT Administrator can set document size - IT53

Table 5: Requirements of Public Notary Systems (Continued)

e. Other business data that exists outside of Blockchain Global Public Notary System

1. Document history, accessible online that is not part of Blockchain Global Public Notary System – NP21, IT51

2. The public blockchain hashes must be searchable. This question was not asked during the interviews but is deemed necessary for the blockchain anonymous solution.

3. Business Timing Requirements

a. User Attestation Notification NP1, NP22, NP37, GR19.

i. Pre-conditions

1. Notary contact information GR3, GR12, GR16

2. Preconfigure databases - NP4, NP12, NP21, NP26, NP30, NP34, NP35, NP36, NP37, NP41, GR18, GR26, GR28, IT5, IT12, IT23

3. Document inventory is retained for 4 years and sent to IT administrator who maintains Document database – NP22

ii. Frequency

1. Notify users about attestation and documents quarterly, is variable by the grantor- This question was not asked during the interview

b. Preventing known unlawful users from using the system

i. Pre-conditions

1. User must be verified not to be on government black lists before they can have a document notarized – IT29, IT37, NP29

2. It should be possible for the IT administrator to manually override the blacklist feature based on a legitimate error. Not asked during the interview.

c. Notary Attestation

i. Pre-conditions

1. Users may request notarization – GR1, GR2, GR5

a. Notary batches are ordered by largest to smallest- GR29, NP4

b. Previous users with established accounts can notarize first - NP18

c. New users notarize after all other users – IT8, IT25, GR4, GR7, GR8, GR29

2. Users may request notarization during the normal attestation timeline on the same calendar day – NP15, NP19, NP26, NP41, IT8

Table 5: Requirements of Public Notary Systems (Continued)

        i. Frequency
            1. Notary must notarize documents on same calendar day. – NP15, NP19, NP26, NP41, IT8
            2. Documents are stored for 4 years then deleted as notaries license must be renewed every 4 years. - NP22

2. Non-Functional Requirements
    a. Cost
        i. What is the Blockchain Global Public Notary System development budget? None of the stakeholders interviewed could answer the question. Some of the development work can be outsourced and it is anticipated that the development cost may be approximately $10,000. Over 2 years
        ii. What is the yearly operating budget? Again, none of the stakeholders interviewed could answer the question. The operating budget on Amazon Web Services, Ethereum, and using low volume PayPal invoicing is expected to be a minimum of $300 per year
    b. Schedule
        i. Phase 1 of the Blockchain Global Public Notary System should be available by March 2018. - The stakeholders interviewed are not aware of the schedule.
    c. Usability
        i. The Blockchain Global Public Notary System should easily allow Notary to notarize user documents. – NP25
        ii. The Blockchain Global Public Notary System should easily allow Notary to find whether the users have completed the Identification requirements, such as, a photo, a picture of a government license, a video, an acknowledgement. IT7, IT8, IT14, IT23, IT25, IT37, IT45, NP1, NP,2, NP3, NP7, NP8, NP17, NP22, NP23, NP37, NP41, NP51, GR8, GR11, GR22
        iii. The Blockchain Global Public Notary System should make the system quick and easy to operate from a mobile phone. – GR20
    d. Security
        i. The Blockchain Global Public Notary System should require returning users who have already received a certificate and been verified to authenticate using 2 levels of authentication. - IT7
        ii. The Blockchain Global Public Notary System should contain and controls permissions to do specific actions on user documents. – IT16

Table 5: Requirements of Public Notary Systems (Continued)

3. Installation Requirements
    a. The proposed website will be developed on Amazon web services elastic cloud computing platform to allow for scalable computing capacity.

List of Additional Stakeholders to Interview:

1. Attorney
2. Secretary of State office
3. Other International users
4. Person or persons advocating a new system

Table 5: Requirements of Public Notary Systems (Continued)

KEY USER NEEDS INTERVIEW CONCLUSIONS

After all the interviews it became apparent that only the IT administrator was aware of blockchain technology, since cryptocurrency techniques are not widely understood or used by the general population. To have an immediate benefit, the proposed website must comply with current government rules and regulations. To meet short-term practicality, the proposed website implements certificate authority private key infrastructure as an additional intermediate step, giving authority to current notaries and central government control. The solution will still provide the SHA blockchain hash signature and still load the hash onto the Ethereum blockchain. Altogether, the proposed hybrid website is an innovative solution that does not exist. This proposed website could be used as an example of what can be done to facilitate future legislative ideas for notarizing a document and have them recognized by all the parties who need them. All the users interviewed need a solution that provides low-cost, fast, and convenient Power of Attorney notarization. Following are some key requirements from the stakeholder interviews.

1. A need to notarize a document without going to the notary, in a way that is recognized by the government, bank, or TSA airport inspectors.
2. A need for a documents repository because my agent will not find the document when needed or will lose the document.
3. The dApp must interface with the Ethereum network and provide Certificate Authority services, a notary stamp, and an electronic signature.
4. Even in times of peak use, all certificates, stamps, and signatures must occur on the same calendar day.

The combination of needing the notarized document to be valid with local government regulations and keeping a trusted central authority in control motivates implementing a Certificate Authority (CA) model, and adding the CA layer to the hybrid website meets those needs. The CA should be a trusted professional recognized by the state government, such as a notary, state board registered professional engineer, or any other registered professional in good standing with the local government. The CA can verify the user’s identity, provide electronic signature authority, and apply a government seal presently recognized by other authorities. Figure 15 shows a high-level overview of the functions and actions a user can perform on the website.

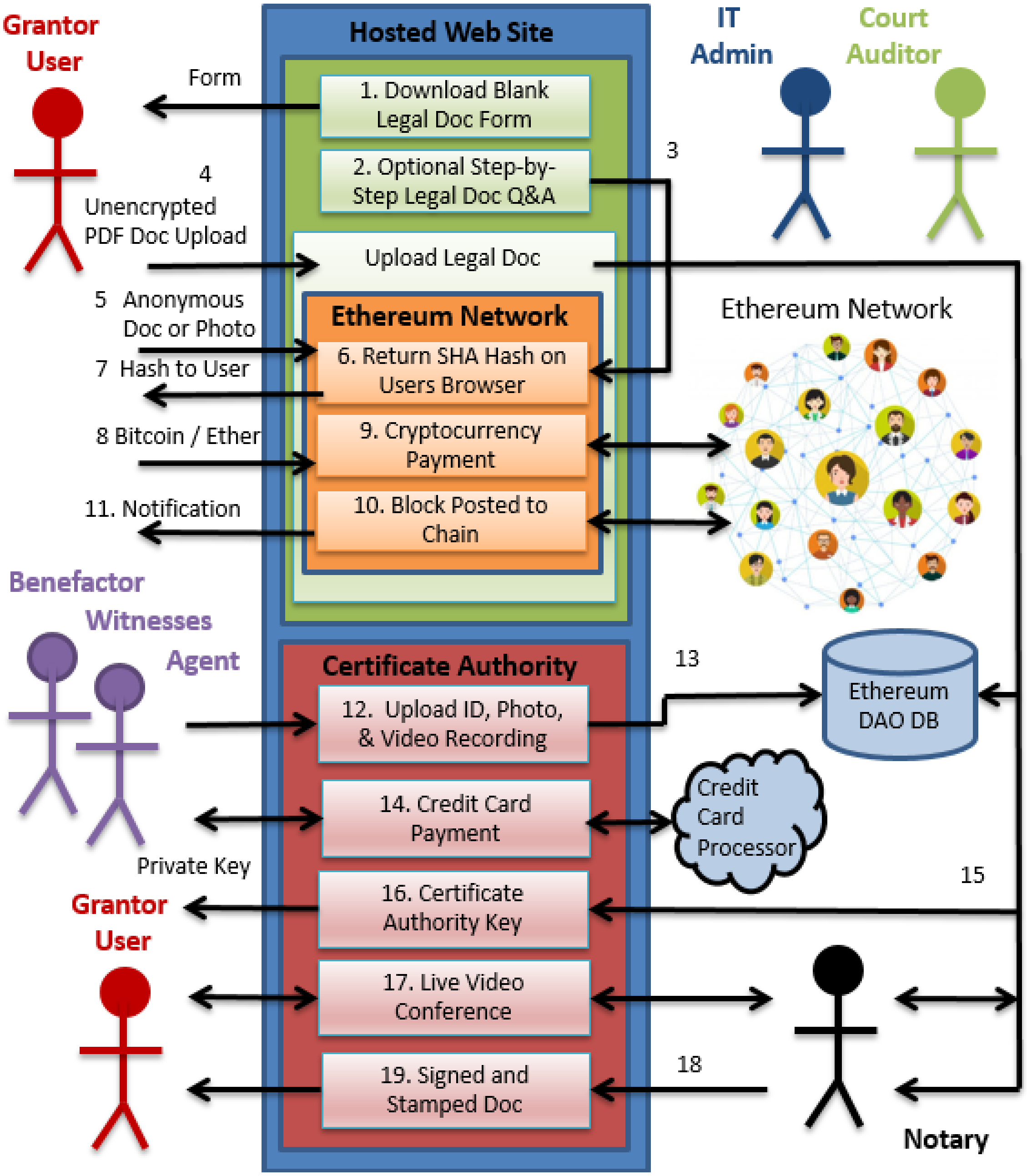


Figure 15: Blockchain & Certificate Authority Public Notary Hybrid System

Following is a description of the steps detailed in Figure 15.

1. The grantor user is a person who wishes to grant an agent a power of attorney in the event he is not able to make decisions for himself. He comes to the website and is presented with the following choices:
   a. Download a blank form to fill out independently later.
   b. Chose the web site step-by-step guide as shown in the business data requirements of Table 5, number 2.
   c. Upload a completed legal document, that is a Power of Attorney in this example.
   d. Anonymously create a hash on his own browser of any photo or document to be used as a proof of existence of such information, similar to the example shown in figure 11 of chapter 4.
2. All the above paths converge again when a hash of the document is provided to the user, steps in 6 and 7 of Figure 15.
3. If the user chooses only the anonymous route and is in possession of Bitcoin or Ether, then the user can pay to have the Website add the hash onto the current block and added to the next chain of Ethereum blockchain, steps 8 and 9, similar to the process followed in Figure 12 of Chapter 4.
4. In steps 10 and 11, the block that contains the hash is posted to the chain and a notification is sent to the public key address of the user. The Ethereum network process is completely anonymous. The Website never has, or knows, the contents of the document being hashed and does not know the identity of the user.
5. If the user does not care for blockchains, and does not have any cryptocurrency, but instead prefers a more traditional notarization, then the

grantor needs to establish his identity with the verifying notary. In step 12 the user or grantor of the power of attorney takes a picture of himself and a picture of the front and back of his government issued ID. This process is outlined by the on-line voting procedures of Figure 13 in Chapter 4.

6. The user makes a short video recording of himself testifying that he wishes to sign the document previously uploaded and is given a mechanism to sign the document electronically. The user states his name, date, and any other information the notary might need.
7. The user is required to commit his credit card, or PayPal, information before the next steps. The payment information is verified before proceeding.
8. The CA saves the user's ID and issues the user a private key that is used as the certificate, encrypted by the methods shown in the following section and Appendix C. If desired, the user and CA notary website have a secure means of communication. The certificate will be the first method used when authorizing the user upon returning to the website in subsequent sessions.
9. The notary, acting as the identity verifier, checks the photos and video recording. If the notary is not satisfied with the photos or video recording then the notary may request a live video conference by phone to witness the intention of the grantor.
10. Finally, if the notary is satisfied with the photos, video recording, or video conference, then the notary affixes his notary stamp and electronic signature to the document and sends it back to the user, encrypted or unencrypted as requested by the user.

CERTIFICATE AUTHORITY

Cryptographic algorithms play a highly important role in certificate authority network security proposed in this report. This report proposes Elliptic Curve Cryptography (ECC) as the proposed algorithm to generate public keys. One of the advantages of the elliptic curve implementation is that it relies on the hard-elliptic curve logarithms. Another advantage is that ECC can use much smaller key sizes than RSA, something that is ideal for mobile applications that rely on small data space. ECC adds longer key sequences ensuring certificate authority network security. Appendix C provides network security background information for key distribution center (KDC) methods and algorithms for a Document Notarization Network (DNN).

Innovative Proposed Solution using CA and ECC

The proposal is to use a hybrid of cryptographic methods, algorithms, blockchain, and security policies to form a combined innovative solution, creating a new Document Notarization Network (DNN). The goal is to design the most secure, fast, and scalable network possible. This report's contributions include policies and ECC key distribution methods specifically for new users entering and re-entering the certificate authority network after the initial video validation. The proposal is based on a hierarchical Certificate Authority (CA) notary website that can calculate, store, and distribute private keys, the directory of ID name identifiers, and digitally signed certificates (Stallings and Tahiliani 2014). This local notary CA is responsible for only its domain or local government jurisdiction. If two entities wish to communicate from different domains, then the notary CA can exchange keys by a global CA government agency. This innovative solution uses an Elliptic Curve Cryptographic algorithm to generate the initial asymmetric key only when a new user first enters the certificate authority network. The first-time entry is important because the notary validator will attest to the user's ID by video recording or video conference. The method followed is Certificate-based Key Establishment (CBKE) using the ECC algorithm. Figure 16 shows a representation of the CA cryptographic method outlined in the following paragraphs.

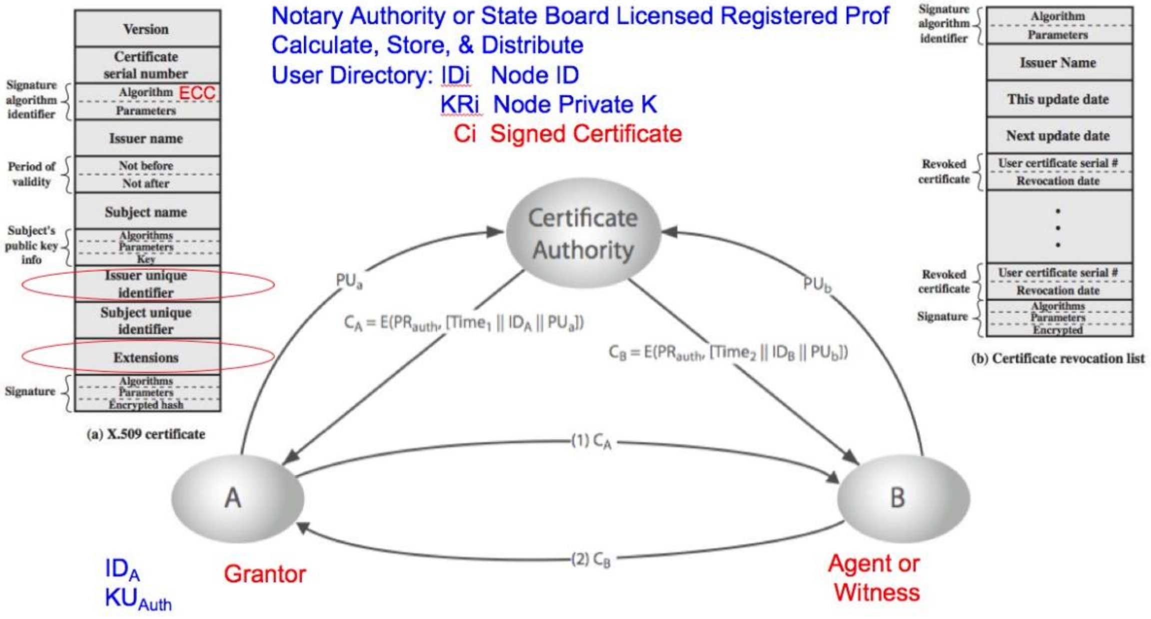


Figure 16:   Certificate Authority Cryptographic Scheme

To make the proposed solution fast, an approach is taken that was first suggested by Kohnfelder (Kohnfelder 1978) that allows certificates that to be used by participants to exchange keys without contacting a public-key authority, in a way that is as reliable as if the keys were obtained directly from a public-key authority. In this specific use case, a grantor of a power of attorney, witness, or benefactor may wish to securely communicate with his agent. Anyone on this new Document Notarization Network (DNN) can communicate with another user through well-known and established certificates.

As shown in Figure 16, a certificate consists of a public key and an identifier of the key owner, and the whole block is signed by a trusted third party. In this case, the certificate authority is the hierarchical notary website trusted by the DNN community. A user can present its public key to the authority in a secure manner and obtain a certificate. The user can then publish the certificate. Anyone needing this user's public key can obtain the certificate and verify that it is valid by way of the attached trusted signature. A user can also convey its key information to another by transmitting its certificate. Other users can verify that the certificate was created by the authority.

Each user applies to the Certificate Authority, supplying a public key PU_A and requesting a certificate. Application must be made when the user is originally verified by video conference or video recording. As shown for user A in Figure 16, the authority provides an encrypted certificate of the form where the private key PR_{AUTH} used by the authority is combined with a timestamp $Time_1$, the user's ID_A, and the returned public key PU_A. User A, the grantor, may then pass this certificate on to any other user such as a witness or an agent, who reads and verifies the certificate. The recipient then uses the authority's public key to decrypt the certificate. Because the certificate is readable only using the notary website certificate authority's public key, this verifies that the certificate came from the certificate authority.

The user's ID and Public Key provide the recipient with the name and public key of the certificate's holder. The timestamp validates the currency of the certificate and serves as an expiration date. If a certificate is sufficiently old, it is assumed to be expired (Stallings and Tahiliani 2014). One of the policies of the notary website is to check if the user is a returning user with a current certificate who is requesting a subsequent document to be notarized, and if so, then additional second-authentication rules will be applied. The X.509 standard has become universally accepted for formatting public-key certificates, are more common than blockchain, and are more likely to be accepted by a government agency. X.509 certificates are used in most network security applications, including IP security and transport layer security (TLS), which are discussed in detail in the next section.

X.509v3

The standard calls for compatibility with X.509 Version 3. As explained by Stallings (Stallings and Tahiliani 2014), X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory serves as a repository of public-key certificates and is located on the certificate authority website. Each certificate

1. Contains the public key of a user and
2. Is signed with the private key of a trusted certification authority.

X.509 is based on the use of public-key cryptography and digital signatures. The standard does not dictate the use of a specific algorithm but recommends RSA. The unique identifier fields, as shown in Figure 15, in the X.509 standard are intended to handle the possible reuse of subject and/or issuer names over time; this can be used in the case of a document notarization network user who enters and re-enterers the network multiple times. The CA signs the certificate with its private key. If the corresponding public key is known to a user, then that user can verify that a certificate signed by the CA is valid. All user certificates can be placed in the key distribution center notarization certificate authority directory website for access by all users. Key Distribution trust centers are further explained in Appendix C. A user can transmit its certificate directly to other users. In either case, once B is in possession of A's certificate, B has confidence that messages it encrypts with A's public key will be secure from eavesdropping.

SUMMARY OF CAPABILITIES AND ROADMAP

The key innovations offered by the solution presented are (i) adding the Certificate Authority layer to form a combined blockchain, (ii) video recording verification, and (iii) the notary electronic stamp and signature so that the resulting notarized document is immediately recognized by the government, banks, hospitals, or airport TSA screeners when needed. The solution gives the entire system backwards compatibility with existing legacy notary systems, is on-line, and is asynchronous in that the notary can verify the user's ID and video recording hours later yet on the same calendar day. Such a combined system does not yet exist.

The development and delivery of the global blockchain public notary system will be divided into the four main project phases outlined in the roadmap in Table 6. The following are notable implementation details:

1. The Ethereum code will be developed as explained in Chapter 3, Figure 8.
2. A shortcut to developing a custom Certificate Authority is to use Pretty Good Privacy (PGP) readily available tools.
3. The proposed website will be developed on Amazon web services elastic cloud computing platform to allow for scalable computing capacity.

Customer Benefit	Roadmap Target Phase	Supporting Features
Anonymous proof of existence blockchain functionality. Hash, crypto payment Bitcoin and Ether, and post the block to the production Ethereum chain.	Phase 1 Ethereum proof of existence Timeline is 2 months after project start. Available in Ethereum network externally immediately.	Ethereum network compatibility. Accept Bitcoin and Ether payments.
Amazon web services cloud computing platform, Basic Website. Download, Upload doc, step-by-step PoA doc.	Phase 2 2 Months	All webpages must be responsive to be viewed on a mobile device. JavaScript Website. API or WSDL interface to Amazon Web Services. Supporting Terms and conditions
Accept secure credit card and PayPal payments over the internet using Amazon available services. Sign and Stamp a Doc using Adobe or DocuSign	Phase 3 2 Months	Establish DB X-500 infrastructure in advance of the Certificate Authority functions
Add Certificate Authority capability and storage	Phase 4 4 Months	JavaScript Website original development or partner with PGP exiting tool
Production Rollout	2 Months	YouTube Training, Social Media Marketing on Facebook & Google. Sustaining and Operations. Plan next iteration of improvements.

Table 6: Blockchain & CA Public Notary System Benefits, & Roadmap.

Chapter 6: Future Work and Conclusions

This master's report discussed the core concepts behind blockchain concerned with the storage, and sharing of non-financial data, and presented an innovative web-based solution using blockchain for invoking a statutory durable power of attorney. Blockchain is a foundation technology poised to disrupt current methods of recordkeeping, and as with all foundation technologies, it is not a fad or a bubble, but something that will be developed for decades (Srivastava 2017). The following subsections conclude the report with main findings, values, limitations, and future work direction.

MAIN FINDINGS

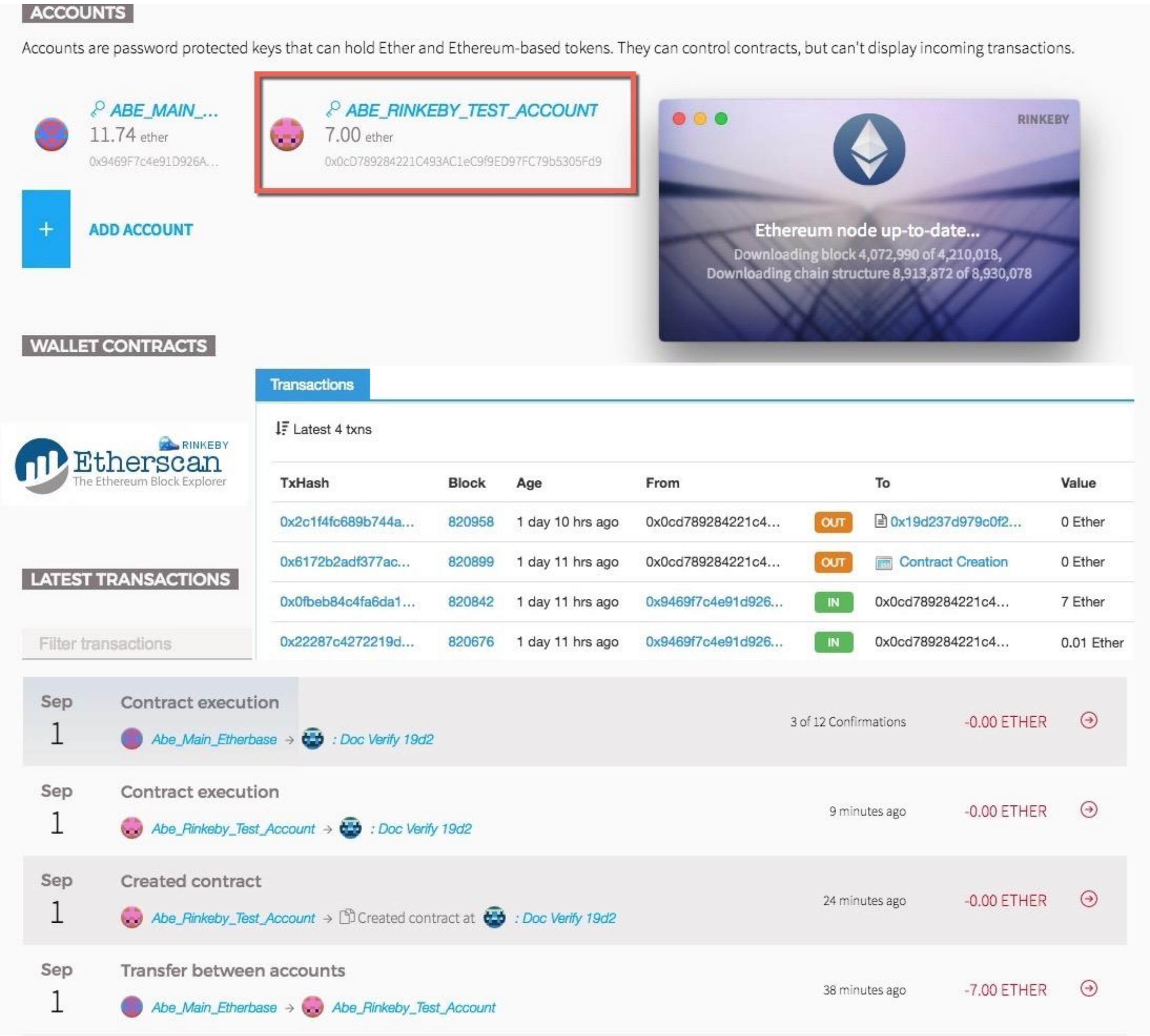
Beyond the fundamental blockchain findings, what was not anticipated when interviewing users for this master's report is that not only are users unaware of blockchain and any cryptocurrency matters, but they lose interest quickly. There must be a driving motivator, such as, stopping corruption, protecting privacy, or preventing theft. The requirements interviews also led to proposing a more common security approach using a Certificate Authority (CA), providing a better solution for on-line notaries.

The proposed website service uses cryptographic methods, blockchain, and security policies to form a combined innovative solution valuable today and into the future. Elliptic Curve Cryptographic (ECC) algorithms will further improve CA security, generating the initial key only when a new user first enters the notary certificate network. The first-time entry is important because the notary validator will attest to the user's ID by video recording or video conference. ECC key distribution methods are specifically for new users entering and re-entering the network, allowing users to communicate securely with one another and the notary (see Figure 16).

VALUE AND LIMITATIONS

Blockchain offers innovative models of governance based on transparency. This report described how to use the Ethereum model for the transfer of assets that are non-financial, and how it is possible for a state government to use blockchain employing trusted nodes. The key innovations presented are adding the Certificate Authority (CA) layer to form a combined blockchain proof of existence, live video conferencing or video recording verification, and the notary electronic stamp and signature so that the resulting notarized document is immediately recognized by the government, banks, hospitals, or airport TSA screeners when needed (see Figure 15). This innovation gives the entire system backwards compatibility with existing legacy notary methods. Identity verification can be done by the notary asynchronously, and securely, without the witnesses or stakeholders being in the same place at the same time, an ability that is currently not available. The concepts and services proposed here will benefit notary services by rendering them more trustworthy, and making them part of a publicly accessible record.

Current on-line notary services use video conferencing but do not use CA or blockchain protocols. Some of the risks and disadvantages of Ethereum are that it presently uses proof of work consensus mechanisms and causes miners to consume large amounts of energy. Because of the verification overhead, the number of transactions per second are limited to approximately 30, as discussed in Chapter 3. Software development quality is key because on some blockchain networks, such as Ethereum, logical transactions have financial consequence and detecting mismatches between intended behavior and the actual one is critical. Because an error cannot be stopped once a transaction is committed to the chain, functional correctness must be verified in an Ethereum test network before a new dApp is released into a live environment. Figure 17 shows an example of a Rinkeby test network account, made on Ethereum, with temporary cryptocurrency valid for 3 days. Additional test dApps should be developed to exercises the key functions.



ACCOUNTS

Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

ABE_MAIN_...
11.74 ether
0x9469F7c4e91D926A...

ABE_RINKEBY_TEST_ACCOUNT
7.00 ether
0x0cD789284221C493AC1eC9f9ED97FC79b5305Fd9

Ethereum node up-to-date...
Downloading block 4,072,990 of 4,210,018,
Downloading chain structure 8,913,872 of 8,930,078

WALLET CONTRACTS

Latest 4 txns

TxHash	Block	Age	From		To	Value
0x2c1f4fc689b744a...	820958	1 day 10 hrs ago	0x0cd789284221c4...	OUT	0x19d237d979c0f2...	0 Ether
0x6172b2adf377ac...	820899	1 day 11 hrs ago	0x0cd789284221c4...	OUT	Contract Creation	0 Ether
0x0fbeb84c4fa6da1...	820842	1 day 11 hrs ago	0x9469f7c4e91d926...	IN	0x0cd789284221c4...	7 Ether
0x22287c4272219d...	820676	1 day 11 hrs ago	0x9469f7c4e91d926...	IN	0x0cd789284221c4...	0.01 Ether

LATEST TRANSACTIONS

Sep 1 Contract execution
Abe_Main_Etherbase → : Doc Verify 19d2
3 of 12 Confirmations -0.00 ETHER

Sep 1 Contract execution
Abe_Rinkeby_Test_Account → : Doc Verify 19d2
9 minutes ago -0.00 ETHER

Sep 1 Created contract
Abe_Rinkeby_Test_Account → Created contract at : Doc Verify 19d2
24 minutes ago -0.00 ETHER

Sep 1 Transfer between accounts
Abe_Main_Etherbase → Abe_Rinkeby_Test_Account
38 minutes ago -7.00 ETHER

Figure 17: Rinkeby Test Network

FUTURE WORK

Document notary networks, as explained in Chapter 5, will be a new class of notary chains that will form part of an evolving blockchain infrastructure. Each certificate notary authority website using blockchain can be a Decentralized Autonomous Organization (DAO). With its own set of autonomous smart contracts, all these cooperate in a complex blockchain-based ecosystem according to business rules. An improvement to the hybrid website is to replace the notary with multiple DAO smart contracts. The improved services will employ sector-specific functionality, for example using biometrics of a person requesting a notary service to verify their identity. Additional smart contracts can read a government issued ID and perform document storage. The next generation DAO notary services will require less human intervention. If signing and stamping a document is a thing of the past, then the time for private enterprises providing this service is also limited because local governments have the opportunity to take back the notary service and generate new revenue.

Appendices

Appendix A

Ethereum Block Header Fields

The Block in Ethereum is the collection of relevant pieces of information (known as the block header), H, together with information corresponding to the comprised transactions, T, and a set of other block headers U that are known to have a parent equal to the present block's parent's parent. Such blocks are known as ommers. Following is an explanation of the Ethereum block header fields (Wood 2017).

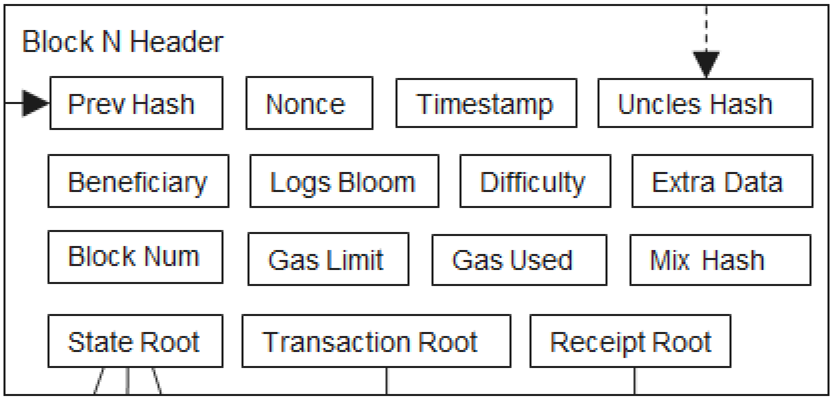


Figure 18: Ethereum Block Header Fields

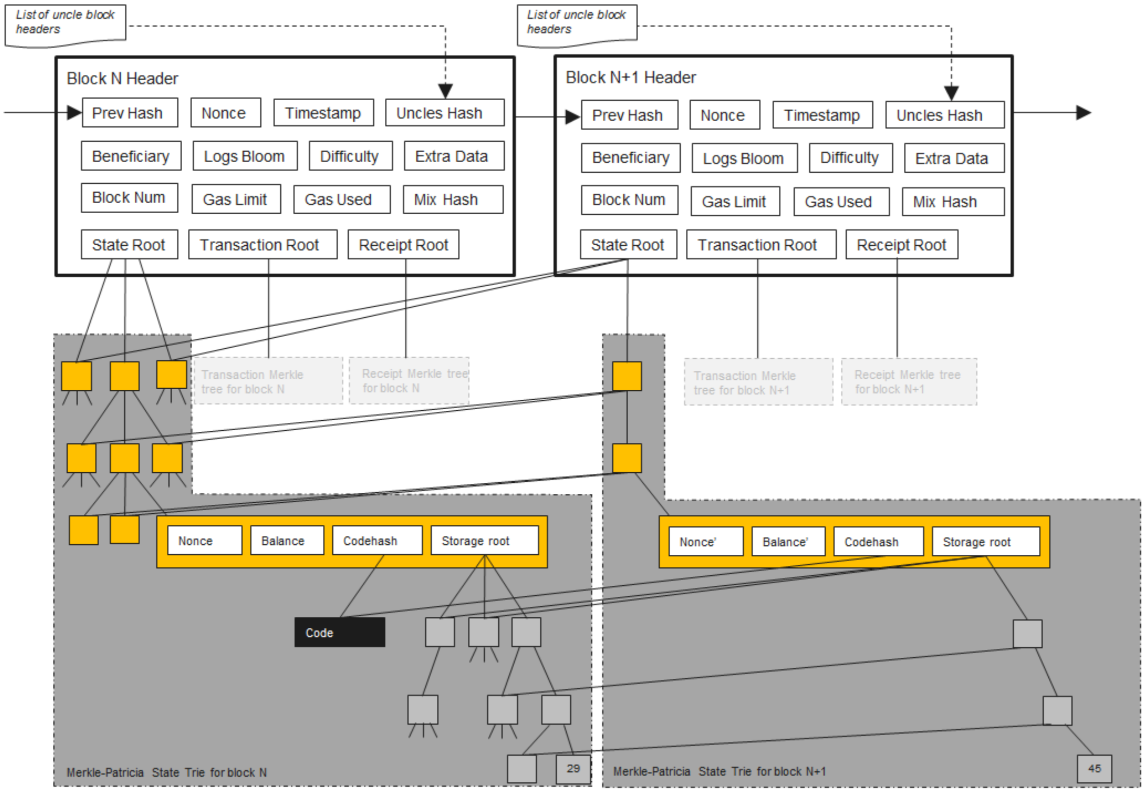


Figure 19: Ethereum Blockchain Example

The block header contains the following pieces of information.

1. ParentHash: The Keccak 256-bit hash of the parent block's header, in its entirety; formally Hp.
2. OmmersHash: The Keccak 256-bit hash of the ommers list portion of this block; formally Ho.
3. Beneficiary: The 160-bit address, to which all fees are collected, is from the successful mining of this block be transferred, formally Hc.
4. StateRoot: The Keccak 256-bit hash of the root node of the state trie, after all transactions are executed and finalisations applied, formally Hr.

5. TransactionsRoot: The Keccak 256-bit hash of the root node of the trie structure populated with each transaction in the transactions list portion of the block, formally Ht.
6. ReceiptsRoot: The Keccak 256-bit hash of the root node of the trie structure, populated with the receipts of each transaction in the transactions list portion of the block, formally He.
7. LogsBloom: The Bloom filter composed from indexable information, logger address and log topics, contained in each log entry from the receipt of each transaction in the transactions list, formally Hb.
8. Difficulty: A scalar value corresponding to the difficulty level of this block. This can be calculated from the previous block's difficulty level and the timestamp, formally Hd.
9. Number: A scalar value equal to the number of ancestor blocks. The genesis block has a number of zero, formally Hi.
10. GasLimit: A scalar value equal to the current limit of gas expenditure per block, formally Hl.
11. GasUsed: A scalar value equal to the total gas used in transactions in this block, formally Hg.
12. Timestamp: A scalar value equal to the reasonable output of Unix's time() at the created block's inception, formally Hs.
13. ExtraData: An arbitrary byte array containing data relevant to this block. This must be 32 bytes or fewer, formally Hx.
14. MixHash: A 256-bit hash which proves, combined with the nonce, that a sufficient amount of computation has been carried out on this block, formally Hm.

15. Nonce: A 64-bit hash which proves, combined with the mix-hash, that a sufficient amount of computation has been carried out on this block, formally Hn.

Appendix B

REQUIREMENT QUESTIONNAIRES

Appendix B shows an example interview requirements acquisition template from AWARE Software (AWARE Software 2009) (Barber and Graser 1999) in this case specifically for the notary stakeholder. The grantor and IT administrator interviews are not included in this report. The requirements gathering is divided into the following categories.

1. Functional requirements
2. Business data requirements
3. Business timing requirements
4. Non-functional requirements.

Project Name: Blockchain Global Public Notary System

Notary Requirements		**10/10/2017** **12:00** **1 hours** **Public Restaurant**
Unique ID:	*NotaryUsage_NotaryUser_06102017_1000*	
Stakeholder:	*Name: Notary Public* *Title: Independent Notary Public* *Employer: Independent Notary ID* *Email:* *Phone:* *Viewpoint: Notary Verifier User*	
Requirements Engineer:	*Name: Abe Arredondo* *Email abe_arredondo@utexas.edu* *Phone: 512-468-xxxx*	**Scribe:**

Session Goals and Desired Outcomes

Goal	Description
Topics for goals may include:	• *Gathering Requirements for Use Cases from Notary* • *Gathering Requirements improvement to current manual system* • *Gathering Requirements on attestation process surrounding use cases* • *Type of Requirements to be acquired: user Record, Document Information, Notary Timing*

Outcomes and Products	Description
Outcomes and Products may include:	• *Notary Public requirements list* • *System data list* • *Notary Process Diagrams* • *List of other stakeholders to interview*

Input to Guide Requirements Acquisition Session

Portion of System under Discussion	Blockchain Global Public Notary System Overall, Notary Interface
Guiding Scenario (if used)	This session is an introductory session to get an overview of the Notary process and key needs that Notary users have for the system.
Reference Documents	None

Action Items or Outstanding Issues/Requirements from Previous Sessions (if necessary)

Previous Session Date:	*Not applicable, first session.*	**Previous Meeting Purpose**	*Not Applicable*
Number	**Description**	**Assigned To**	**Status**
None.			

Planned Questions

Question #	Description
	Business Functionality required for the system
1	High Level: What key functions should the Blockchain Global Public Notary Systems provide and who are the users of each of these functions? What are the user types?
2	With the first use case being a power of attorney document, what are the minimum functional deliverables for the first release?
3	For an on-line system should users log into the system or just use it anonymously, what information is requested at log in?
4	Should users have the ability to view current and past attestation documents? Should users be able to view the notary log? Is the notary log book public or private?
	What information should be displayed?
	Should they be allowed to perform any actions from this page?
5	What information about the user record may be displayed?
6	How should users be required to add a request for a document to be notarized?
	What data is requested from the User?
	What information should be displayed to the User?
	Should authentication be verified by the system, if so which?
	Should there be a limit to the number of documents a user may notarize as a batch?
	What user eligibility requirements should be validated to allow a user to notarize a document?
	What errors should be able to be reported to the user?
	What attestation types are supported; Affidavit, Jurat, Notary Signing Agent? Do all documents support all attestation options?
	How should users be required to validate documents?
	What data is requested from the User?
	What information should be displayed to the User?
	Should authentication be verified by the system, if so which?
	What user eligibility requirements should be validated to allow a user to notarize for a document?
	What errors/warnings should be able to be reported to the User?
8	Should a history of transactions be required to be presented to the user? Does the Notary ever keep a document?
9	Should any sort of email notification be required by the system?
10	What billing/accounting information must the system have?

11	Should a Document history be presented on the Notary site? Should it be searchable, if so, by what Document data record fields? What information should be presented about the documents in the history?
12	Should any help systems be required directly on the Notary site pages? What type of help?
13	Should users be allowed to save attestation selections without committing them?
14	Should users be allowed to preview Document information for future attestation?
15	Should users receive notification of canceled attestations (loss of eligibility, Document failure due to inability to verity the grantor's identity etc.)?
16	What happens if the document is too large?
17	What are the best features of the existing manual process? What are the worst features of the existing manual process?
18	Are there any user types besides users that should access the Blockchain Global Public Notary System, or are adjacent functions (downstream processing, Notary/IT Administrator preview of attestation information, etc.) performed in other systems, such as Auditing?
19	What other parts of the notarization process should be accessible from the Blockchain Global Public Notary System?
20	Should the users be allowed to update their profile (contact info etc.?)
	Business data to be managed by the system?
21	What is the list of data inputs?
22	What is the list of data outputs?
23	What are the data and records that the system must store/manage? How do you convert the manual Journal to an online journal?
24	What is the list of data presented to the user?
25	What is the list of data the system must calculate?
26	What information is contained in a user record? Is it read write? Where and how is it obtained from?
27	What data is required to represent a Document – ID, Name, video, photograph, category etc.? Where and how is this information obtained?
28	What other data for Document validation should be required? Video, photograph, ID, counter check an online database?
29	Should correspondence or contact information be maintained by the system?
30	Is there any other data that must be displayed or maintained by the system?

	Business timing of functionality presented (i.e., a process flow)
31	What key process flows are involved in the system and what are the timing requirements of each of these flows?
32	What is the Notary process today?
33	When is a user allowed to view attestations?
34	When is a user allowed to perform attestations functions?
	How long is the attestation timeline by function?
	Who administrates the attestation timeline
	What should determine when a user can attest to a document
	Non-functional requirements
35	What are the key non-functional requirements for the system? Certification, Auditability, Compliance, Accessibility, Availability, Escrow, Price, Scalability, Operability, Reliability.
36	What are the minimum deliverables for the first release? Consider that the initial use case is only for a power of attorney document.
37	What should be the budget for the project?
38	After delivery, what is the budget & resources for support and maintenance of the system
39	What should be the deadline for the project?
40	How long should the system or documents should, be sustained?
41	Are there any system/transactional performance requirements? Speed, timeline to Notarize.
42	How many total users must the system be able to support?
	Should this requirement change over time? (scalability)
43	How many concurrent users must the system be able to support?
	Should this requirement change overtime?
44	What method of UI should be used – web interface, another client, mobile, etc.?
	What type and version of user clients should be supported – skype support?
45	Are there any branding or look/feel requirements for the Notary site pages?
46	What security requirements are there?
47	What accessibility requirements does the system have?
48	What localization requirements are there, if any? State of Texas Only, National, International?
	What languages?
49	What administrative and user documentation is required?
50	What regulations or specifications is the system required to comply with?
51	Are there any interface or usability guidelines that apply to this system?

52 What re-usable code/requirements/testing assets exist to support this system?

53 How do you prioritize the non-functional requirements?

Installation requirements

54 What are the installation requirements for the system?

55 What other systems must the Blockchain Global Public Notary System interface to? (Document databases, Document databases, government

What information must be read from a system interfaced?

What information must be written to a system interfaced?

56 Are there any existing online Public Notary Systems already implemented?

57 What software platform requirements are there?

58 What database requirements are there?

59 Where should the server be located?

60 What hardware should be required by the system – are there any server, storage, networking, cloud, etc. requirements?

Are there any high availability or fault tolerance requirements for the installation environment, how much down-time can be tolerated between a request and an acknowledgement?

Business Functionality required for the system

61 High Level: What key functions should the Blockchain Global Public Notary Systems provide and who are the users of each of these functions? -Or- What are the user types?

62 What are the minimum functional deliverables for the first release?

63 How should users log into the system, what information is requested at log in?

64 Should users have the ability to view current attestations?

What information should be displayed?

Should they be allowed to perform any actions from this page?

65 What information about the user record may be displayed?

66 How should users be required to add documents

What data is requested from the User?

What information should be displayed to the User?

Should authentication be verified by the system, if so which?

Notes:

Questions for Notary – example interview questions and answers for Appendix B:

Q-NP0 Is a new online system a good idea? If so Why?

Notary Public Answer: Yes, it is because it is easier
Imagine when people just don't have the time

Q-NP1: Can you describe the function of the existing manual process.
Notary Public Answer:

1) Identify the person
2) They must have the correct ID
3) And I put it in the Logbook
   a) Name
   b) Date
   c) Kind of doc
   d) Address
   e) How I identified them, thumbprint or normal ID

There are different ways to ID a person. Self-knowledge is valid without an ID and every state is different.

Q-NP2: What is the system you have – what are the limitations?
Notary Public Answer: If they have no ID then I cannot notarize their documentation. They might bring school records this is valid if I don't know the person. I am not looking for fake documents

Q-NP3: Do you notarize any person how do you check the person's ID? Is there anyone you would not notarize?
Notary Public Answer: I could not notarize someone who did not have their valid ID, even an expired ID is okay.
ID in Spanish are acceptable, State issued ID cards are acceptable, Not debit cards not credit cards as ID's

Q-NP4: on an on-line system how do you want to generate or manage the available Document by a batch list? Import, generate?
Notary Public Answer: Import it because they are providing the list of documents

Q-NP5: What is your favorite thing about the current manual system? What would you change?
Notary Public Answer: Putting it on line. I have no time and I don't carry the stamp with me all the time

Q-NP6: What would you change about the current manual system?
Notary Public Answer: Enter the information on-line instead of a book

Q-NP7: For an online system would it be helpful if the system pre-checking a user's ID and it were automated?
Notary Public Answer: Yes,

Q-NP8: Should you be enhancing the current manual system or going with a new one? What do you think of the anonymity of blockchain technology? Do you think the government would agree to a proof of existence process?

Notary Public Answer: I think blockchain is a great new concept. I think the government would agree as long as long as there is a picture ID, a short video and a physical signature

Q-NP9: What are the cost, quality, and timeline constraints?
Notary Public Answer: I don't know

Q-NP10: Is there a budget?
Notary Public Answer: I don't know

Q-NP11: What is the schedule?
Notary Public Answer: I don't know

Q-NP12: Are there offline components – documents etc. which need to be integrated into the system? How do you stamp a document electronically?
Notary Public Answer: I don't know

Q-NP13: As the users go through the Notary process, is there a point where the user says they are ready for Notary?
Notary Public Answer: Online yes

Q-NP14: Is it desirable to keep face to face aspect of notarization, can it be done online by video or video recording?
Notary Public Answer: No I prefer the video recording and by advance appointment would be better

Q-NP15: Do you want to open the attestation timeline wider beyond the same calendar day? Is it possible to notarize a document the next calendar day?
Notary Public Answer: That cannot be done to my knowledge, the person signing and the notary must be the same calendar day. Most people come to the independent notary after work after 7 PM because the bank is closed and they cannot find a notary.

Q-NP16: Using an On-Line system should an IT Administrators give/take permission from the users? Should there be an auditor or government regulator who occasionally looks at the system?
Notary Public Answer: A user would need IT person, or a help desk person if they need help. The only reason the government would need the logbook is for a court issue. There are no Auditors now for the manual system.

Q-NP17: For the Notary, when you use online functions do you use any automation, what web sites are available to use? Should you ever check a person's ID on line?
Notary Public Answer: I have never checked a person's ID online, I am not an investigator

Q-NP18: Can you describe more about the attestation timeline for multiple witnesses?
Notary Public Answer: While it is rare, the notary can be a witness. A will requires 2 witnesses

Q-NP19: Is an email is sent to tell users their calendar day timeline expiring?
Notary Public Answer: No

Q-NP20: What other groups or staff should have access to the Blockchain Global Public Notary System?
Notary Public Answer: IT person, Notary, The User

Q-NP21: Do you need to see other personal information such as if the person is disabled, a veteran? His race? Is the person an International User? Can you stamp a document anywhere in your state? Can you stamp a document in another state? Have you ever stamped a document in Spanish or another language that is not English?
Notary Public Answer: No other personal information is not asked or needed. No, I have never stamped a document in another language. My stamp is valid anywhere in Texas not just in the county where I am registered. Yes, my stamp is valid in another US states court system; however, I have never stamped outside of Texas. I do need to know if a user is an international user because I9’s are common because of the foreign temporary workers

Q-NP22: What data elements do you see that you don't need? What potentially sensitive information do you need? What do you record in your notary journal? How long do you have to keep your notary journal?
Notary Public Answer: I keep my journal for 4 years, then I discard it.

1) The Logbook contains
    a) Name
    b) Date
    c) Kind of doc
    d) Address
    e) How I identified them, thumbprint or normal ID

Q-NP23: In your notary journal do you keep user history and user validation methods, such as, a driver’s license number? Do you know about know your customer, that is, if you personally know your customer is it legitimate to waive checking their ID?
Notary Public Answer: No I do not keep user history or validation methods. I do however need to verify their ID’s. If I know the person online (or in person) then I do not need to verify their ID

Q-NP24: Would it help if the system could take the history of a user who previously logged on to show them what is missing or where they left off?
Notary Public Answer: Yes, the example is to start the process and finish it later

Q-NP25: What would be the ideal world?
Notary Public Answer: It would be easy, profitable, and convenient 24/7

Q-NP26: For Notary – would you like email or SMS text messages from the system to notify you that you need to take an action, such as, take a video call? How much lead time do you need? Would you prefer an appointment? How could you legitimately notarize a document the next day?
Notary Public Answer: Yes, I would like an SMS message, and an appointment would be preferred. I just need a 1-hour lead time. I cannot legitimately notarize a document the next day it needs to be done the same calendar day.

Q-NP27: Apart from personal email, is there another forum you would like to interact with Users? Would you like discussion board or online forum to discuss with Users, SMS text messages, video calls? Online chat, Facebook social media? Have you ever heard of a Notary using Facebook?
Notary Public Answer: I don't want to talk to anyone after I notarized their documents

Q-NP28: Are there certain circumstances where online attestation could not be allowed?
Notary Public Answer: if there is an obvious fake document

Q-NP29: Would you like to disallow some users from using the system?
Notary Public Answer: Only if it is a hacker, or someone who intentionally misuses the system

Q-NP30: Do you want the system to monitor each document and their rules?
Notary Public Answer: Yes

Q-NP31: Should you be the executive sponsor for this program? As requirements change in the future?
Notary Public Answer: I don't know

Q-NP32: Who is the principal stakeholder?
Notary Public Answer: The person who creates the system

Q-NP33: Does the user have to declare what type of attestation he is interested in? ; Affidavit, Jurat?
Notary Public Answer: Usually the people already have their forms, I record this in the journal logbook

Q-NP34: Is it useful for the notarized document to be stored or uploaded in the Blockchain Global Public Notary System?
Notary Public Answer: YES,

Q-NP35: Are there separate government systems that there must be compatibility with?
Notary Public Answer: Not that I know of unless the document is from another country, such as, Mexico, China, India

Q-NP36: Is there a way to link Texas Notary documents to other states?
Notary Public Answer: There is no known why to link Documents. A document notarized in one state is generally recognized by another state.

Q-NP37: Does the current manual system allow you to identify a person who is trying to notarize wrong type of document or a person intentionally causing fraud? Can a user miss use a notary's services?
Notary Public Answer: We don't know if it is fraud we cannot check the content of the document. There was an example of a wife signing her ex-husband's name on a land sale this was recognized as fraud and was not notarized.

Q-NP38: Are there cases where the user can't notarize a document?

Marissa. Generally, as stated earlier as long as the user has a valid ID he can get a document notarized.

Q-NP39: Should this system maintain payment?
Notary Public Answer: yes

Q-NP40: Should the user receive an email confirming documents?
Notary Public Answer: yes

Q-NP41: Can they print from the system? What does a person do with the notarized document? Can an electronic signature be proven on a print out? For an online system should a certificate be issued on security paper and be mailed out later?
Notary Public Answer: Users need a document to walk away with, this is very important. A certificate means nothing only the notary stamp is the certification. Users need their original documents notarized in writing for their school, IRS, or airport TSA proofs, or to give to their consulates if they have international matters. Just a certified form is not needed, the original document must be notarized and stamped. Furthermore, different states require different color ink to see that it is an original immediately, others require only black ink, an embossed seal is required in Alabama, the District of Columbia, and the U.S. Virgin Islands.

The steps that should be followed for an online notarization that would be recognized by the government are

1. Create or follow the rules for a notary stamp on line, if they already exist.
2. Input the document, perhaps the only format acceptable should be pdf.
3. Take the information from the user ID and record it in the journal
4. The person signs the document on-line in the presence of the notary, this must be done on the same calendar day.
5. If this is done by facetime then they can sign on their phone. Or by video recording but it must be on the same calendar day.
6. Add this information to the document, a pdf editor will be necessary
7. Return the modified document to the requester electronically
8. Then add it to the blockchain
9. Save the document if the user requests this service

Q-NP42: Should the system handle rejected Users?
Notary Public Answer: Yes, as explained above such as malicious users should not be allowed to use the system.

Q-NP43: Is there anyone else we should be talking to about the system?
Notary Public Answer: YES, a lawyer, and most importantly someone from the secretary of state.

Q-NP44: Is there a preference for previous Users?
Notary Public Answer: yes

Q-NP45: What is the biggest pain point for Users?
Notary Public Answer: presently the idea of the grantor making a video of himself taking an oath seems difficult

Q-NP46: Can the system solve this?
Notary Public Answer: No.

Q-NP47: Does the system automatically cancel a document? Can you cancel a notarized document?
Notary Public Answer: no

Q-NP48: Who decides on the type of the documents that can be notarized, such as, wills, power of attorney, etc.?
Notary Public Answer: The user

Q-NP49: Are there cases in which the users want a document, but they already did that previously?
Notary Public Answer: Would not know that

Q-NP50: How early do you inform users when their documents are notarized?
Notary Public Answer: Immediately

Q-NP51: Are user records ever kept in an external system?
Notary Public Answer: We should keep their ID so when they come back -- -unless it is expired
If their ID was still current, then they would just need to do a video for a secondary document

Q-NP52: Should the system do reporting?
Notary Public Answer: Yes, especially if there is a batch of documents coming together

Q-NP53: Who determines document sizes?
Notary Public Answer: The IT person

Q-NP54: Based on the questions so far, what is the most painful part of the current manual system?
Notary Public Answer: You must see the person in person validating their identification and writing down all the information in the book

Q-NP55: What do the users like least?
Notary Public Answer: The video

Q-NP56: What do you find requires the most of your attention?
Notary Public Answer: The document

The Requirements resulting from this interview are listed in Chapter 5:

Action Items

Action Number	Description	Assigned To	Due when
1.			
2.			
3.			
4.			

Agreements and Approvals

On the delivery date listed, I agree to deliver notes documenting this requirements session to the Stakeholder's listed below.

Requirements Engineer Name	Requirements Engineer Signature	Delivery Date
Abe Arredondo		

The above requirements session report accurately reflects the session for which I served as an expert on the dates indicated above.

Stakeholder Name	Stakeholder Signature	Approval Dates
Notary Name		

Appendix C

PROTOCOLS FOR KEY DISTRIBUTION TRUST CENTER

Appendix C provides network security background information for key distribution center (KDC) methods and algorithms for a Document Notarization Network (DNN).

Three entities are involved as explained by Razouk (Razouk, Crosby, and Sekkaki 2014): (1) the Trust Center or Key Distribution Center, (2) the grantor or initiator user A, and (3) the agent, witness, or responder user B. Each user i stores its identifier IDi and its secret key Ki. The Key Distribution Center has access to a database where information related to the network is stored (in this case we are interested in the IDs and secret keys related to the users). No keys are shared permanently among the users, considerably reducing the ability to compromise the network upon the exposure of one single user. Finally, the temporary session key Ks is a one-time-use key shared between both the grantor or initiator and agent, witness, or responder users during a given communication. In this approach, Razouk proposes using random numbers as nonces to ensure the freshness of the messages containing the session keys. The nonce Ni is updated after each communication to prevent replay attacks. An improvement could be to use a timestamp as the nonce. In the figure below Figure 19, the term Trust Center is interchangeable with Key Distribution Center.

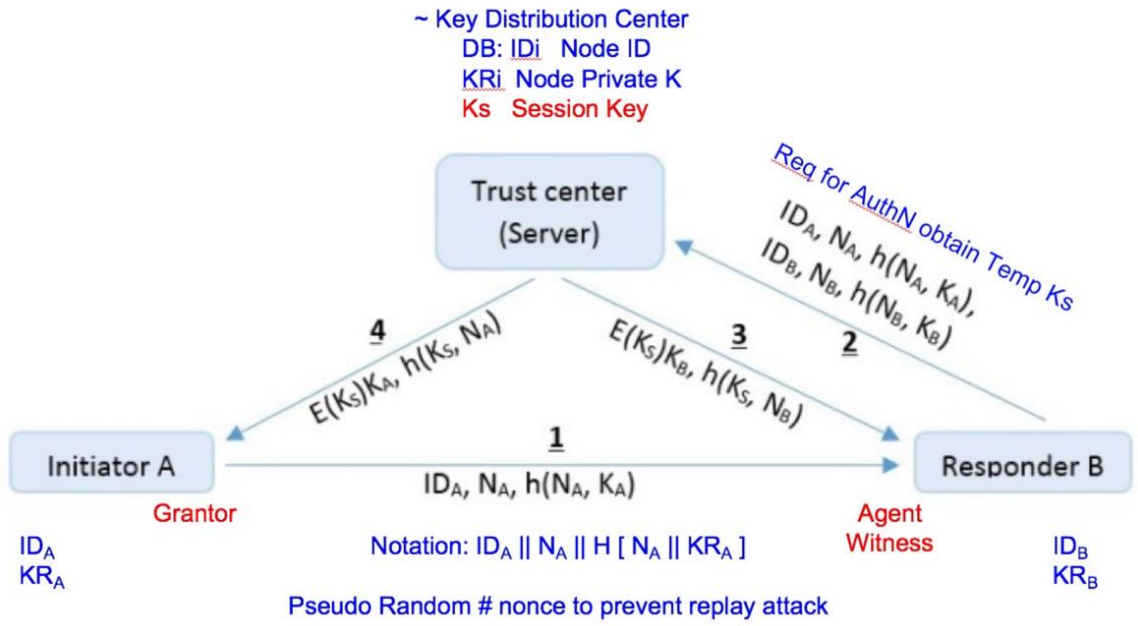


Figure 20: Protocols for Key Distribution Trust Center

The following steps outline the algorithmic solution described by Razouk (Razouk, Crosby, and Sekkaki 2014) that map to a key distribution center model.

1. As shown in the figure 19 above, the grantor or initiator A sends a request to establish communication with the user B. The message (1) contains the user's identifier ID_A, a nonce N_A generated by A and H_A which is a hash of N_A along with the private key K_A. Razouk adds the nonce to this step to provide freshness and ensure that when receiving the next message, A will be sure that the communication has not been replayed as N_A is random and different for each session. This report offers a time stamp as a better choice

than a nonce. Only the Key Distribution Center has access to K_A and can rebuild H_A to determine whether A is a legitimate user. Note that H_A is a one-way function, as hash functions are required to be irreversible. Therefore, even if this message is disclosed, the attack cannot be successful, as only legitimate parties possess the secret key K_A to recover the plain message of the next step (Razouk, Crosby, and Sekkaki 2014).

2. The agent, witness, or responder B build its own message in the same way, and sends the received information related to A along with its information to the Key Distribution Center as a request for authentication and also to obtain a new temporary session key.
3. The Key Distribution Center receives the message (2) from B, and verifies whether the forwarded message is valid or not by rebuilding H'_A and H'_B using K_A and K_B for the stored ID_A and ID_B respectively. To clarify the example diagram of Figure 19, H_A is the hash of N_a and K_A. Comparing H'_A with H_A and H'_B with H_B proves the message is legitimate as only A and B possess the secret keys K_A and K_B and are able to build a valid message. Steps 3 and 4 are almost simultaneous each with its own user's private key.
4. The Key Distribution Center generates the session key K_S, and sends it in an encrypted form using K_A and K_B to both A and B respectively. The nonces N_A and N_B provide protection against replay attacks. Note that in this solution, both user's A and B authenticate as legitimate users, and can verify the freshness of the received messages from the Key Distribution Center.
5. Finally, the user's A and B receive the encrypted information, and retrieve the secret session key using their private keys K_A and K_B respectively. A

and B are sure that the received message is fresh as it contains the nonces N_A and N_B. At this point, both the grantor or initiator A and the agent, witness, or responder B can communicate in a secure way using the session key K_S.

The Key Distribution Center can make a periodic verification and verify whether all users are still in the document notarization network. If not, the KDC can revoke the access from a specific user simply by deleting or disabling its related information in the database. This technique prevents the exploitations of secret information by an adversary. While the Razouk solution is secure, it is also slow, the proposed innovative solution provided in this report extends the Key Distribution Center using faster Certificate Authorities as explained in chapter 5.

References

Acronis Intl GmbH. 2017. "Acronis Notary: a new way to prove data authenticity via Blockchain." accessed July 8, 2017. https://www.acronis.com/en-us/resource-center/resource/data-protection/.

Allison, Ian. 2017. "The Illinois Blockchain Initiative creates self-sovereign identity at birth." http://www.ibtimes.co.uk/illinois-blockchain-initiative-creates-self-sovereign-identity-birth-1637530.

Araoz, Manuel. 2017. "Proof of Existance (Blockchain dApp)." https://proofofexistence.com/.

Arshdeep, Bahga; Madisetti, Vijay. 2017. *Blockchain Applications A Hands-On Approach*: Bahga, Arshdeep; Madisetti, Vijay.

Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. 2017. "A Survey of Attacks on Ethereum Smart Contracts (SoK)." International Conference on Principles of Security and Trust.

Augur, Hannah. 2015. "WTF Is The Blockchain? A Guide for Total Beginners." accessed July 5, 2017. http://dataconomy.com/2015/10/wtf-is-the-blockchain-a-guide-for-total-beginners/.

Australia Post. 2016. "Developing the right identity solution for Australia." https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf.

AWARE Software, Inc. . 2009. "Requirements Acquisition Template." http://www.awaresoftwareinc.com/index.html.

Back, Adam, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. 2014. "Enabling blockchain innovations with pegged sidechains." *URL:* http://www/. *opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*.

Barber, K Suzanne, and Thomas J Graser. 1999. "Requirements evolution and reuse using the systems engineering process activities (sepa)." *Australasian Journal of Information Systems* 6 (2).

Bartoletti, Massimo, Salvatore Carta, Tiziana Cimoli, and Roberto Saia. 2017. "Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact." *arXiv preprint arXiv:1703.03779*.

Bauerle, Nolan. 2017. "What Are the Applications and Use Cases of Blockchains?". https://www.coindesk.com/information/applications-use-cases-blockchains/.

block.one. 2017. "Block.one." http://block.one/.

Blockgeeks. 2017a. "17 Blockchain Applications That Are Transforming Society." https://blockgeeks.com/guides/blockchain-applications/.

Blockgeeks. 2017b. "Proof of Work vs Proof of Stake: Basic Mining Guide." https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

Bontje, Joris 2016. "Do contracts also have a nonce?". https://ethereum.stackexchange.com/questions/764/do-contracts-also-have-a-nonce.

Bryer, Rob A. 1993. "Double-entry bookkeeping and the birth of capitalism: accounting for the commercial revolution in medieval northern Italy." *Critical perspectives on Accounting* 4 (2):113-140.

Buterin, Vitalik. 2015. "On Public and Private Blockchains." https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

Cachin, Christian, Klaus Kursawe, and Victor Shoup. 2000. "Random oracles in constantipole: practical asynchronous Byzantine agreement using cryptography." Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing.

Castor, Amy. 2017. "A (Short) Guide to Blockchain Consensus Protocols." [Web]. https://www.coindesk.com/short-guide-blockchain-consensus-protocols/.

Chamberlin, Bill. 2017. "Blockchain Trend Report." https://www.slideshare.net/HorizonWatching/blockchain-trend-report-2017.

ConsenSys, Media. 2017. "Ethereum is how the Internet was supposed to work." https://consensys.net/ethereum/.

Cuen, Leigh 2017. "Nevada Just Became The First State To Squash Blockchain Taxes." http://www.ibtimes.com/nevada-just-became-first-state-squash-blockchain-taxes-2548475.

Decker, Christian, and Roger Wattenhofer. 2013. "Information propagation in the bitcoin network." Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on.

Deetman, Sebastiaan 2016. "Bitcoin Could Consume as Much Electricity as Denmark by 2020." https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.

Due, Inc. 2016. "6 Blockchain Applications That Go Beyond Bitcoin." http://www.nasdaq.com/article/6-blockchain-applications-that-go-beyond-bitcoin-cm716269.

EEA Fdn. 2017. "Enterprise Ethereum Alliance." https://entethalliance.org/.

EOSIO. 2017. "EOS.IO Technical White Paper." GitHub. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md - conclusion.

Ethereum Wiki. 2017. "EtHash." GitHub Ethereum Wiki. https://github.com/ethereum/wiki/wiki/Ethash.

Eyal, Ittay, Adem Efe Gencer, Emin Gun Sirer, and Robbert Van Renesse. 2016. "Bitcoin-ng: A scalable blockchain protocol." 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16).

Flavien, Charlon. 2016. "Open Assets Protocol." GitHub. https://github.com/OpenAssets/open-assets-protocol.

Follow My Vote, Inc. 2017. "Blockchain Technology in On Line Voting ". https://followmyvote.com/.

Freelancer, Tech Pty Ltd. 2017. "Hire expert freelancers for your job, online." https://www.freelancer.com/?t=o&utm_expid=294858-547.6N2hr5HUQT6elKFflMTyfg.1&utm_referrer=https%3A%2F%2Fwww.freelancer.com%2Ffind%2Fprogramming%3Fgclid%3DCjwKCAjwuITNBRBFEiwA9N9YEFKAFI2TwrUy91ESwf5KmsiOa6S_rQH53IgO9Oz_IYs8Nc8UrEmTBxoCC04QAvD_BwE%26ft_prog%3DANU%26ft_prog_id%3D197618382888.

Gentelella, Bootstrap Admin Template by Colorlib. 2017. "Gas Time Calculator ". http://ethgasstation.info/calculator.php.

GitHub. 2017. "EOS.IO Software Roadmap." https://github.com/EOSIO/Documentation/blob/master/Roadmap.md.

Graser, Thomas Jeffrey, K Suzanne Barber, James C Browne, ECE Craig Chase, ECE Margarida Jacome, and ECE Aleta Ricciardi. "Dissertation Proposal."

Howard, Gary. 2015. "Code Named As Executor, a First in Legal History." http://www.prweb.com/releases/2015/05/prweb12714046.htm. https://globenewswire.com/news-release/2015/05/11/734632/10133782/en/Code-Named-As-Executor-a-First-in-Legal-History.html.

ICObazzar. 2017. "ICO participation made simple." https://icobazaar.com/.

Intl Energy Agency. 2016. "Key world energy statistics." http://www.iea.org/publications/freepublications/publication/KeyWorld2016.pdf

Jones, Jason. 2017. "Could EOS be the Google of the Blockchain?". Lend Academy http://www.lendacademy.com/eos-google-of-blockchain/.

JP Morgan Chase. 2017. "Quorum advancing blockchain technnology ". https://www.jpmorgan.com/country/US/EN/Quorum.

Kiviat, Trevor I. 2015. "Beyond Bitcoin: Issues in Regulating Blockchain Tranactions." *Duke LJ* 65:569.

Kohnfelder, Loren M. 1978. "Towards a practical public-key cryptosystem." Massachusetts Institute of Technology.

Kroll, Joshua A, Ian C Davey, and Edward W Felten. 2013. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries." Proceedings of WEIS.

Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982. "The Byzantine generals problem." *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4 (3):382-401.

Larimer, Dan. 2017. "EOS.IO explained at Consensus 2017." https://eos.io/.

Ledra Capital, LLC. 2015. "The Mega-Master Blockchain List." http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list.

Marshall, Andrew 2017. "ICO Explained." https://cointelegraph.com/explained/ico-explained.

Marvin, Rob 2016. "Blockchain in 2017: The Year of Smart Contracts." https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts.

Mesropyan, Elena 2016. "21 Areas of Blockchain Application Beyond Financial Services." https://letstalkpayments.com/21-areas-of-blockchain-application-beyond-financial-services/.

Miller, Andrew, and Joseph J LaViola Jr. 2014. "Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin." *Available on line:* http://nakamotoinstitute/. *org/research/anonymous-byzantine-consensus*.

Milutinovic, Mitar, Warren He, Howard Wu, and Maxinder Kanwal. 2016. "Proof of Luck: An efficient Blockchain consensus protocol." Proceedings of the 1st Workshop on System Software for Trusted Execution.

Mukhopadhyay, Ujan, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, and Richard Brooks. 2016. "A brief survey of Cryptocurrency systems." Privacy, Security and Trust (PST), 2016 14th Annual Conference on.

Notaries Ogr. 2017. "E-Notarization." American Society of Notaries. https://www.asnnotary.org/?form=enotary.

Parker, Luke 2016. "Moody's new report identifies 25 top blockchain use cases, from a list of 120." https://bravenewcoin.com/news/moodys-new-report-identifies-25-top-blockchain-use-cases-from-a-list-of-120/.

Pass, Rafael, Lior Seeman, and Abhi Shelat. 2016. "Analysis of the Blockchain Protocol in Asynchronous Networks." *IACR Cryptology ePrint Archive* 2016:454.

PBB, LLC. 2017. "Consumers receive insights and rewards based upon the data they share – anonymously." http://pbb.me/trust.html.

Peters, Gareth W, and Efstathios Panayi. 2016. "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money." In *Banking Beyond Banks and Money*, 239-278. Springer.

Pilkington, Marc. 2015. "Blockchain technology: principles and applications." *Browser Download This Paper*.

Razouk, Wissam, Garth V Crosby, and Abderrahim Sekkaki. 2014. "New security approach for ZigBee weaknesses." *Procedia Computer Science* 37:376-381.

Reddit, inc. 2016. "If you find the Yellow paper hard to read, this will help you ". https://www.reddit.com/r/ethereum/comments/560h6s/if_you_find_the_yellow_paper_hard_to_read_this/.

Roberts, Jeff John. 2017. "Companies can put shareholders on a blockchain." http://fortune.com/2017/08/01/blockchain-shareholders-law/.

Rosenfeld, Meni. 2014. "Analysis of hashrate-based double spending." *arXiv preprint arXiv:1402.2009*.

Rosic, Ameer 2016. "5 Blockchain Applications That Are Shaping Your Future." http://www.huffingtonpost.com/ameer-rosic-/5-blockchain-applications_b_13279010.html.

Santori, Marco 2015. "BitLicense: Who Has Applied and Who Has Left New York." https://www.coindesk.com/bitlicense-2-0-latest-revisions-mean-bitcoin-businesses/.

Srivastava, Ashwin 2017. "Why is This Global PE Firm Interested in Blockchain Technology?". Growthword Digital Private Limited. http://www.iamwire.com/2017/07/why-is-this-global-pe-firm-interested-in-blockchain-technology/155900.

Stallings, William, and Mohit P Tahiliani. 2014. *Cryptography and network security: principles and practice*. Vol. 6: Pearson London.

Swan, Melanie. 2015a. "Blockchain thinking: The brain as a dac (decentralized autonomous organization)." Texas Bitcoin Conference.

Swan, Melanie. 2015b. *Blockchain: Blueprint for a new economy*: " O'Reilly Media, Inc.".

Swanson, Tim. 2015. "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger
systems." http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

Tapscott, Don, and Alex Tapscott. *Blockchain revolution : how the technology behind bitcoin is changing money, business, and the world*: Penguin Publishing Group Kindle Edition.

The Economist. 2015. "The great chain of being sure about things."

Thomas, Lee. 2016. "Ethereum Block Architecture ". https://ethereum.stackexchange.com/questions/268/ethereum-block-architecture.

TokenMarket Ltd. 2017. "Ongoing ICOs." https://tokenmarket.net/ico-calendar.

Tuwiner, Jordan 2017. "Bitcoin Mining in China." buy bitcoin worldwide. https://www.buybitcoinworldwide.com/mining/china/.

uPort, Inc. 2017. "Self-sovereign ID." https://www.uport.me/.

Vigano, Laura. 2016. "The Colour of Bitcoin? Certainly not green." http://steamgreen.unibo.it/2016/09/20/the-colour-of-bitcoin-certainly-not-green/.

Vincent, Danny 2016. "We looked inside a secret Chinese Bitcoin mine." Last Modified 2016, accessed July 29, 2017. http://www.bbc.com/future/story/20160504-we-looked-inside-a-secret-chinese-bitcoin-mine.

Wikipedia Fdn. 2017a. "Public key infrastructure."

Wikipedia Fdn. 2017b. "Satoshi Nakamoto." accessed July 8, 2017. https://en.wikipedia.org/wiki/Satoshi_Nakamoto.

Wood, Gavin. 2017. "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER." GitHub Ethereum. https://ethereum.github.io/yellowpaper/paper.pdf.

Wright, Aaron, and Primavera De Filippi. 2015. "Decentralized blockchain technology and the rise of lex cryptographia."

Zyskind, Guy, and Oz Nathan. 2015. "Decentralizing privacy: Using blockchain to protect personal data." Security and Privacy Workshops (SPW), 2015 IEEE.

Zyskind, Guy, Oz Nathan, and Alex Pentland. 2015. "Enigma: Decentralized computation platform with guaranteed privacy." *arXiv preprint arXiv:1506.03471*.

Vita

In addition to blockchain and cryptography, Abelardo (Abe) Arredondo is interested in the internet of things (IoT) and the development of mobile applications. Currently he is a Kanban scrum master at AT&T WiFi services working with Linux and networking IT Operations teams. From 2007 to 2017 Abe was a principal program manager, technical product owner, and scrum master for multiple software development teams with diverse technology domains developing a customer B2B web portal, from inception throughout its lifecycle. The web page has over 5500 external customer logins per day and 600 employee logins per day as reported by Bing Maps and Webtrends over a 3-year period. From 1995 to 2007 Abe worked at 3 small companies and startups, as an engineering manager. For more details please view his LinkedIn profile at: www.linkedin.com/in/AbeArredondoPublicProfile

Abe holds a BSEE from the University of Illinois at Chicago, and a graduate of business MSTM degree from Embry Riddle Aeronautical University. His 1994 previous thesis topic was software productivity and process quality assessments SEI-CMM vs. ISO-9001, 9000-3. Abe has held a special access top secret DoD security clearance while working with the aerospace industry. He is currently listed as an active State of Texas Registered Professional Engineer, license 72631.

Address arredondo.abe@gmail.com

This report was typed by the author