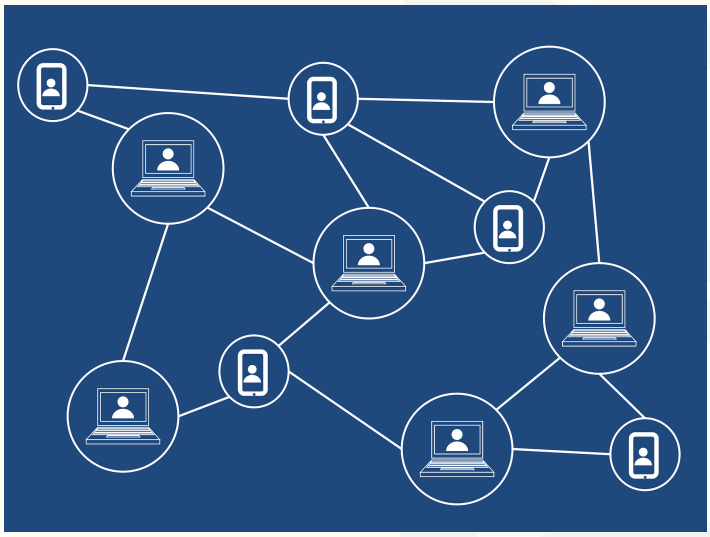
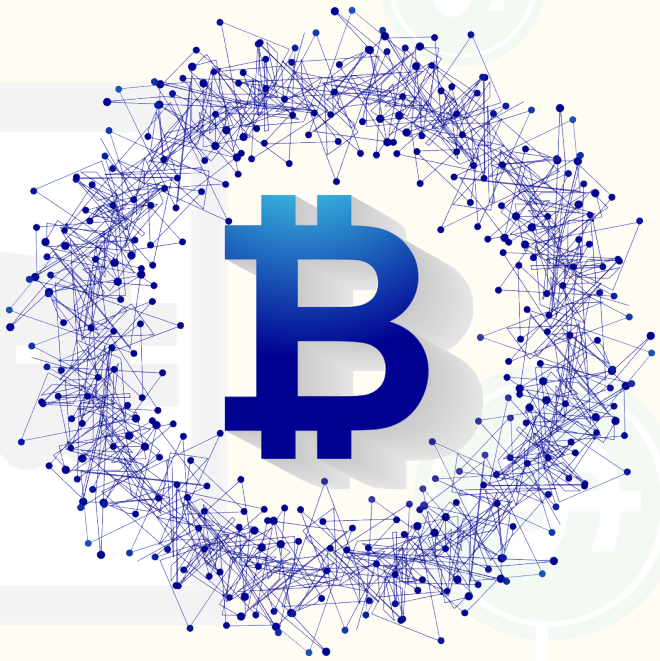
University of Victoria
Faculty of Engineering
ENGR 446: Milestone Report II: Engineering Analysis

Simplification of Transactions by leverage blockchain technologies and smart contracts

David Li Computer Engineering V00818631





June 28, 2018

In partial fulfillment of the academic requirements of this academic course

Table of Contents

List of Figures

List of Tables

1. Proposed approach

Leveraging the largest public blockchains with smart contracts, grants enough computation power for quick transactions, while keeping transparency as a high priority. Reliability of decentralized applications is significant provided users are incentivized to support the shared network.

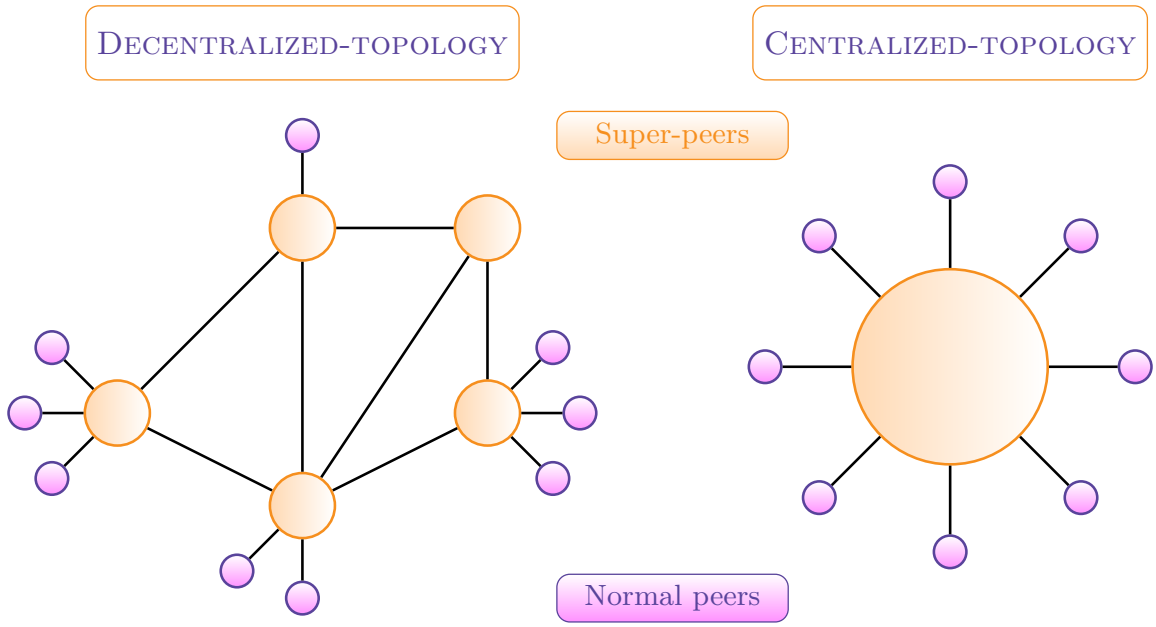


Figure 1.1.: Decentralized and centralized topology

Comparing the process of purchasing a home with and without smart contracts will illustrate its simplicity and efficiency. Since the cost of transactions (gas) on ethereum is relatively low [1] and replicating software costs practically nothing, development is the foremost financial burden. Furthermore, cutting out the middlemen in this process (lawyers and real-estate agents) greatly reduces the financial burden while increasing transaction speed and transparency.

1.1. Project Plan

Creating decentralized applications is challenge because technologies are nascent, undergoing evolution and tools are in infancy.

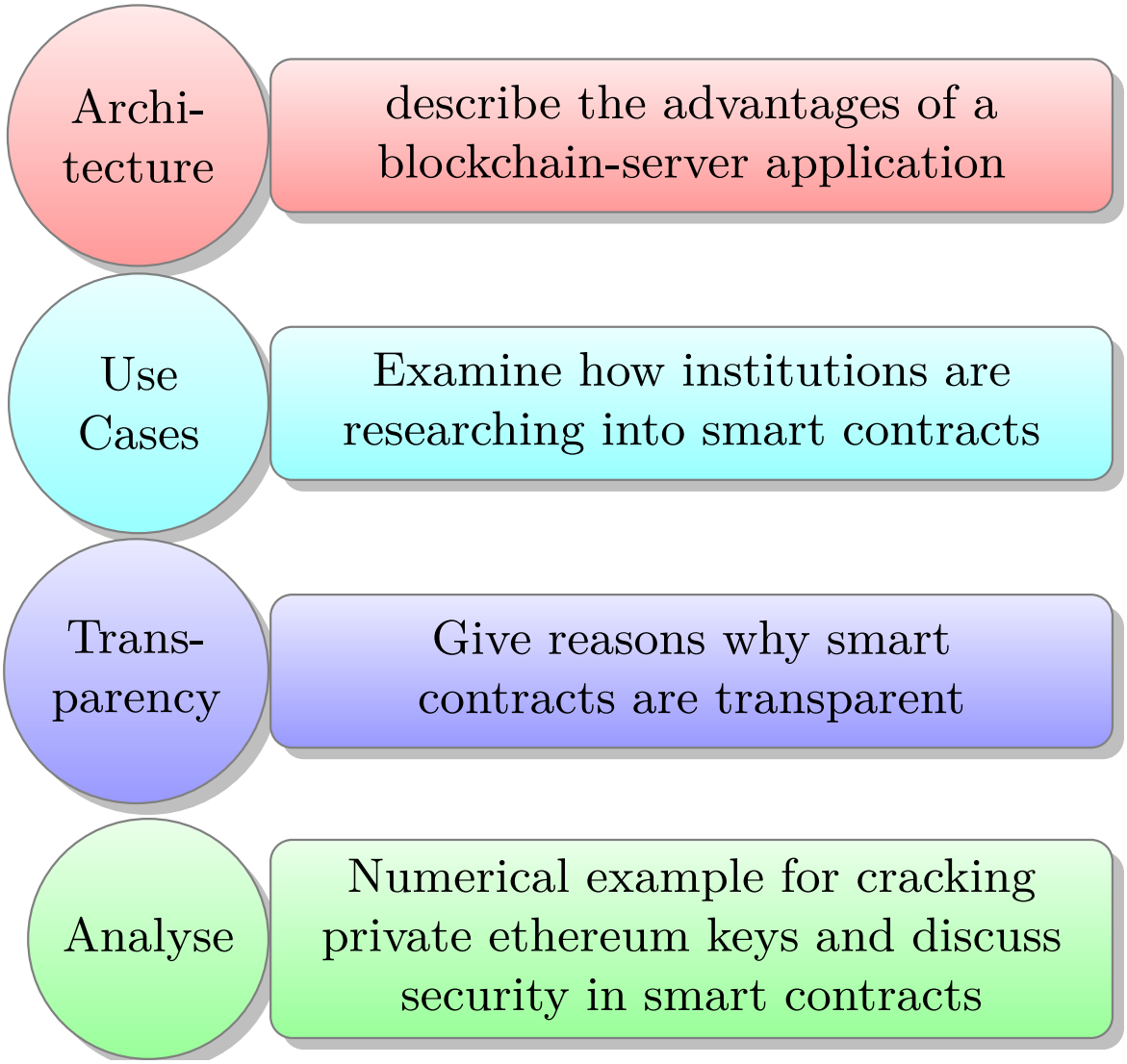


Figure 1.2.: Smart Diagram for proposed approach

2. Engineering Analysis

2.1. Advantages and Disadvantages of Decentralization

Currently, centralized IT systems are vulnerable to "malicious attacks, software and hardware faults, human mistakes (e.g., software and hardware misconfigurations") [2]. Decentralized systems have no single point of failure, improved security and are more transparent, however, efficient code is more important in smart contracts. As illustrated in 2.1 a blockchain-server architecture model allows for developers to implement decentralized applications with smart contracts while maintaining the flexibility and simplicity of retrieving and sending information.

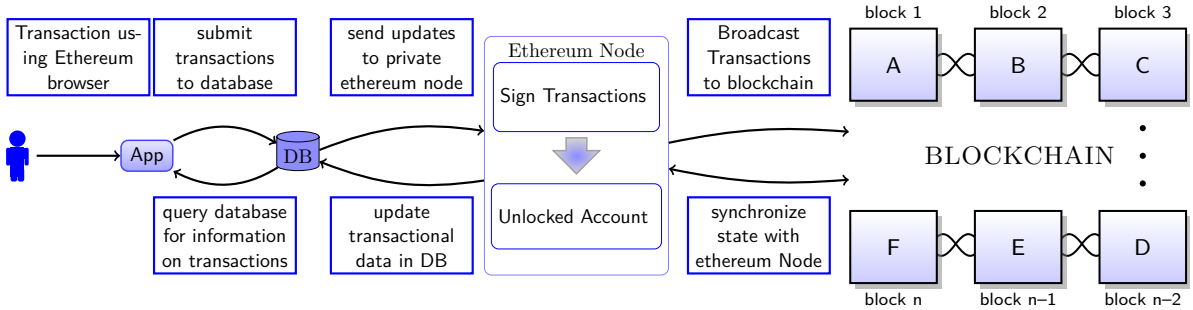


Figure 2.1.: An example of server-blockchain architecture in a DAPP.

Usage on blockchain technologies is actively being explored in medical research [3] more transparency, real-estate and supply chains. Despite, the obvious advantages of decentralized and blockchain technologies, a lack of resources for unpopular materials may result in prolonged downloads. An equivalent anecdote is a inadequately seeded torrent results in intolerable download speeds. Whereas a traditional database only checks, writes and stores data once, a decentralized blockchain system require thousands of operations to write and store data, therefore the costs of maintaining a blockchain are substantial higher and only justifiable with increased utility/security [4].

2.2. Security of Smart Contracts

Blockchain transactions are secure because that are immutable and decentralized. However, exploiting bugs in smart contracts are financially devastating [5] as fraudulent transactions cannot be reverted. Disconnects between software developers and security experts has resulted in 3 out of 4 "applications produced by software vendors fail to meet

OWASP Top 10 standards" [6]. Although blockchain technologies increase underlying security and reliability, exploiting poorly coded and insecure smart contracts remains a major risk, and releasing open-source code allows hackers exploit flaws in the codebase before corrective processes are applied.

2.2.1. Brute force cracking of private keys

A ethereum key, which is randomly selected 256 digits [1], is very difficult to hack. A simple calculation illustrates the impracticalities of brute forcing for a 256 bit key. Assuming that a 1 exaflop (10^{18} calculations per second) 15 megawatts supercomputer [7] is used, electricity costs are 0.1326 per kWH [8].

$$2^{256} = 1.1569 \times 10^{77} \text{decryptions} \tag{2.1}$$

$$10^{18} \frac{\text{decryptions}}{\text{second}} \times \frac{3.154 \times 10^{7} second}{1 year} = 3.154 \times 10^{25} \frac{\text{decryptions}}{year} \tag{2.2}$$

$$\text{Number of machines} = \frac{1.1569 \times 10^{77}}{3.154 \times 10^{25}} \text{years} = 3.66804 \times 10^{51} years \tag{2.3}$$

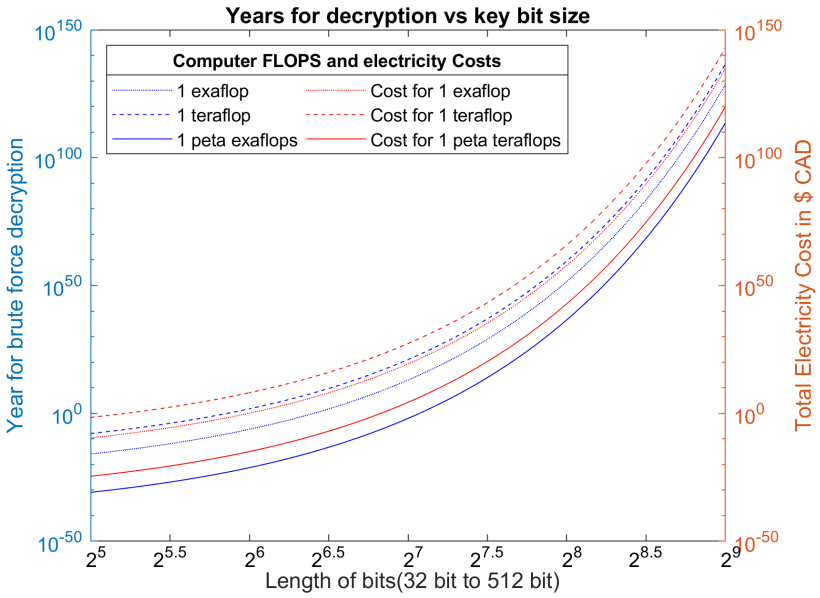


Figure 2.2.: Difficulty of brute forcing a 256-bit key

2.2.2. Considerations for Quantum computing

As shown in 2.2, if powerful quantum (1 peta teraflops) computers become commonplace existing 128 bit (2^7) are easily hacked and 256 bit (2^8) are insecure. According to the the Margolus–Levitin theorem processing power of computer can reach 6×10^{33} operations per second per joule. This indicates that existing 128 bit keys and even 256 bit keys are unsecure in a quantum computing age.

2.2.3. Cheaper and Faster Transactions

Typically, transactional costs are be categorized broadly as: [9]

- Search and information costs (determining what is the suitable goods that is available on the market)
- Bargaining costs (costs to come to acceptable agreement)
- policing and enforcement costs (making sure other party sticks to term of contract)

Usage of smart contracts practically eliminate policing and enforcements costs as transactions are dictated by code, bargaining costs are reduced since the middlemen are removed, and reliable, immutable information on current and previous transactions are publicly displayed on the blockchain. Deploying a smart contract is inexpensive, however any changes in source code require the contract redeployment.

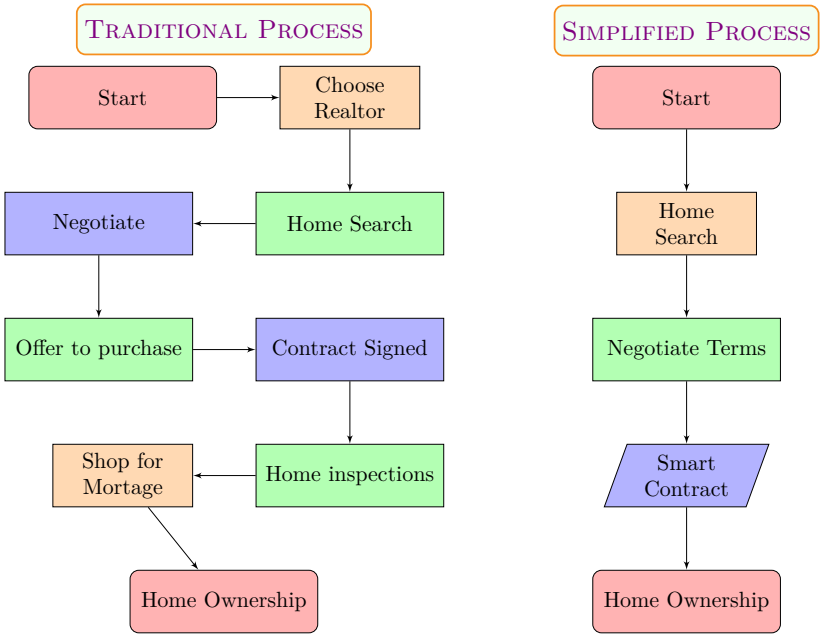


Figure 2.3.: Flow Chart illustrating how smart contracts can simplify buying a home

As specified in [10], the process of purchasing a home can take up to a month, however by using smart contracts, friction between parties will be reduced, the transactions are more transparent and occur much quicker. Writing data to the blockchain is slower than a traditional database, however usage of side-chains (separate blockchain that enables fast transactions without clogging up the main network) can greatly reduce transaction completion time [11]. For instance, inserting information info a database is an order of magnitude in milliseconds, but writing to the blockchain requires a order of magnitude in seconds.

3. Discussion

Decentralized systems are inherently more reliable, resilient against brute force attacks, and are more transparent. Even though immutable and irreversible transactions are advantageous, criminals leverage cryptocurrencies for illegal transfer of funds. This implies the ability to undo fraudulent or criminal activity is extremely important, but reversible transactions is an anti-pattern. For example EOS, a centralized blockchain platform, was criticized for freezing accounts without due process and community backing. [12]. In addition, centralized systems require users to trust vendors and oftentimes personal data usage lacks transparency. Currently, research into blockchain technologies are actively researched that can disrupt existing industries including finance, real-estate and supply chains.

Smart contracts are useful because that cannot be changed by the parties involved in the transactions, yet, in some cases such as criminal activity, the ability to reverse transactions or freeze accounts is extremely desirable. Deployment of a smart contract is inexpensive, however, development and maintenance costs for blockchain applications can be costly. This implies that transaction expenses decrease significantly, but running a blockchain node, ensuring high quality code for smart contracts is challenging and expensive. Decentralized applications are transparent because information is available in the publicly ledger and parties participating in a transaction cannot alter it. Overcomplicated code and bugs in smart contracts are severely detrimental because of malicious transactions by scammers or hackers.

As shown in Figure 2.3, smart contract reduce complexity of transactions allowing buyers to directly interact with sellers. This illustrates how useful smart contracts are, but lack of legislation for blockchain technologies, consortiums unwilling to adopt decentralized applications (may prefer private blockchains), and ability for hackers to exploit bugs suggest transactions governed by code is decades away. Solutions to existing problems in blockchain technologies such as latency, immutable transactions and widespread acceptance by consortiums are addressed through innovations such as sidechains, centralized blockchain platforms like EOS and private blockchains infrastructure.

Overall, blockchain technologies allow for users to have a unique digital presence, securely transfer ownership of assets and avoid key shortcomings of centralized IT systems.

Bibliography

[1] Ethereum White Paper. [Online] Available: https://github.com/ethereum/wiki/wiki/White-Paper. Accessed April 25, 2018.

[2] P. Smith et al. "Network resilience: a systematic approach". In: IEEE Communications Magazine 49.7 (2011), pp. 88–97. ISSN: 0163-6804. DOI: 10.1109/MCOM.2011.5936160.

[3] T. Nugent, D. Upton, and M. Cimpoesu. "Improving data transparency in clinical trials using blockchain smart contracts". In: F1000Res 5 (2016), p. 2541.

[4] Vitalik Buterin. Ethereum scalability research and development subsidy programs. [Online] Available: https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/. Accessed June 28, 2018.

[5] Thijs Maas. Yes, this kid really just deleted 300 MILLION by messing around with Ethereum's smart contracts. [Online] Available: https://hackernoon.com/yes-this-kid-really-just-deleted-150-million-dollar-by-messing-around-with-ethereums-smart-2d6bb6750bb9. Accessed May 29, 2018.

[6] How Do Vulnerabilities Get Into Software? Tech. rep.

[7] Robert F. Service. "Design for U.S. exascale computer takes shape". In: Science 359.6376 (2018), pp. 617–618. ISSN: 0036-8075. DOI: 10.1126/science.359.6376.617. eprint: http://science.sciencemag.org/content/359/6376/617.full.pdf. URL: http://science.sciencemag.org/content/359/6376/617.

[8] Residential Rates. [Online] Available: https://app.bchydro.com/accounts-billing/rates-energy-use/electricity-rates/residential-rates.html. Accessed June 06, 2018.

[9] Carl J Dahlman. "The Problem of Externality". In: Journal of Law and Economics 22.1 (1979), pp. 141–62. URL: https://EconPapers.repec.org/RePEc:ucp:jlawec:v:22:y:1979:i:1:p:141-62.

[10] How long does home buying process take. [Online] Available: http://www.homes.com/blog/2016/03/how-long-does-the-home-buying-process-take/. Accessed June 26, 2018.

[11] Adam Back Matt Corallo. Enabling Blockchain Innovations with Pegged Sidechains. [Online] Available: https://blockstream.com/sidechains.pdf. Accessed May 31, 2018.

[12] EOS Emergency Actions. [Online] Available: https://bitcoinexchangeguide.com/eos-undergoes-emergency-actions-after-block-producers-freeze-accounts-without-community-input/. Accessed June 26, 2018.

A. Project Background

A.1. Background

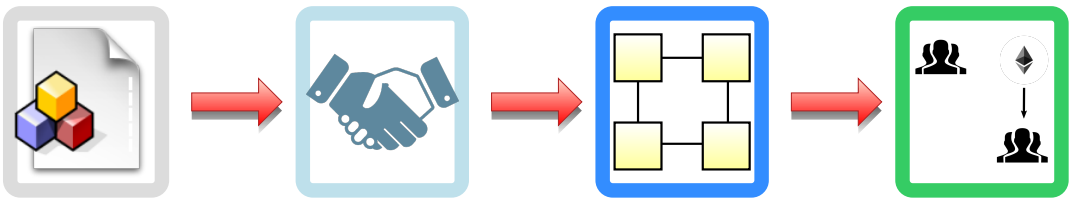
In 2008 bitcoin white paper [1] described a way to solve the double spending problem without a centralized body using blockchain. Although, the value of bitcoin (BTC) has grown exponentially, high computational and energy consumption in mining and slow performance [2]. Released in July 30, 2015, Ethereum,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

Table A.1.: Timeline of Cryptocurrency

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

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

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



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

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

A.2. Objective

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

A.2.1. Problem

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

A.2.2. Purpose

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

A.2.3. Aims

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

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

A.2.4. Limitations

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

A.3. Potential Solutions

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

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

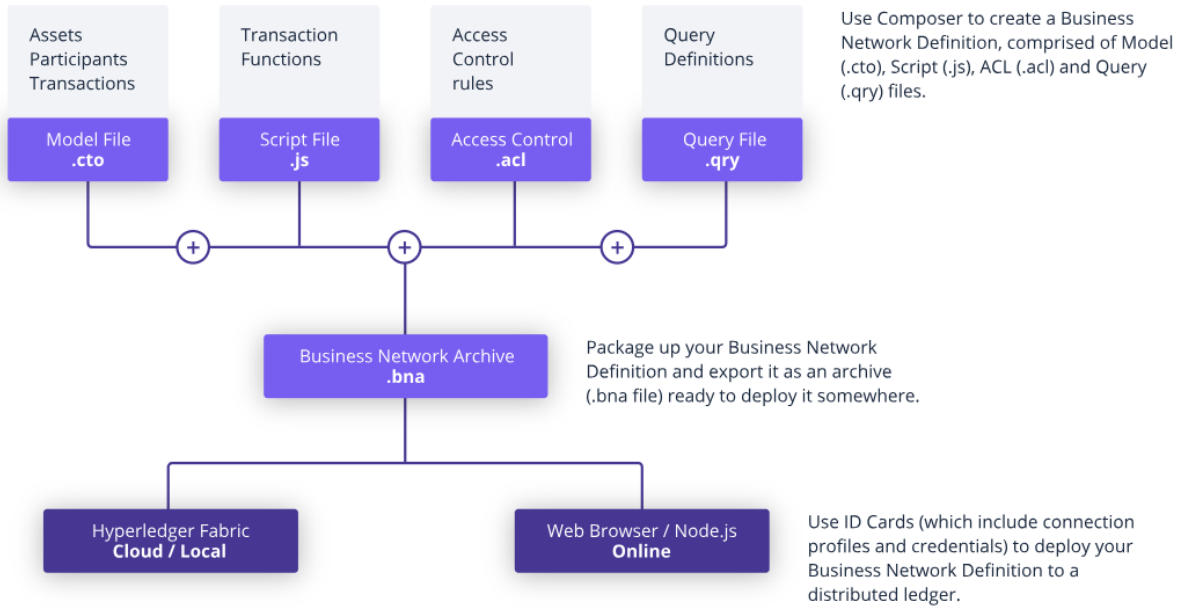


Figure A.2.: Architecture of Hyperledger composer

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

A.4. Initial Assessment

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

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

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

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

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

References for Appendix

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

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

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

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

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

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