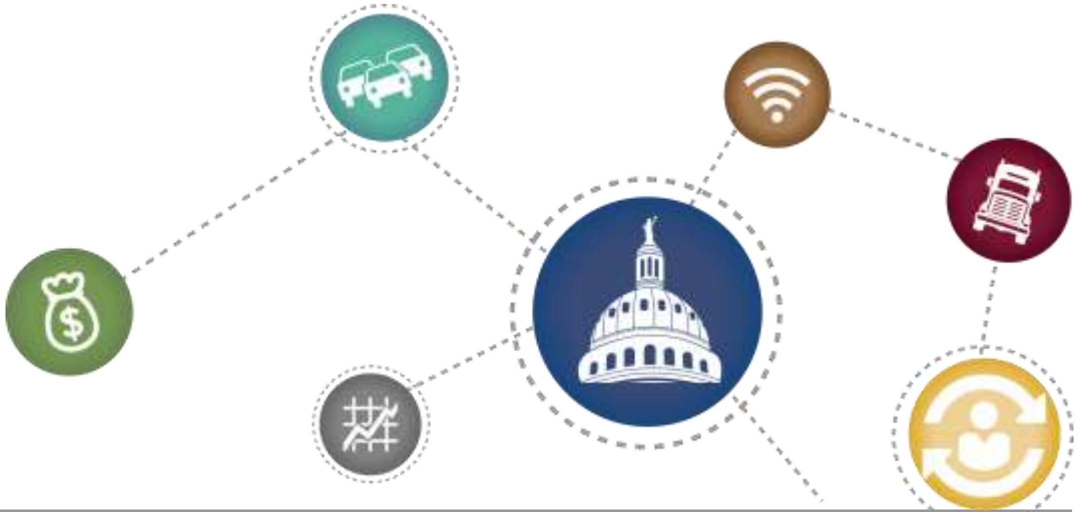
Texas A&M Transportation Institute

Exploring Blockchain – Technology behind Bitcoin and Implications for Transforming Transportation

Final report

PRC 17-13 F



TRANSPORTATION
Policy Research CENTER

Exploring Blockchain – Technology behind Bitcoin and Implications for Transforming Transportation

Texas A&M Transportation Institute

PRC 17-13 F

January 2018

Author

Rajat Rajbhandari, PhD

Acknowledgments

Adi Ben Ari, CEO, Applied Blockchain, London, UK

Chris Ballinger, Toyota Research Institute, Los Altos, California, US

Peter Bidewell, CMO, Applied Blockchain, London, UK

Ginger Goodin, Research Engineer, Texas A&M Transportation Institute, Austin, Texas, US

Gregg Hansen, General Motors, Austin, Texas, US

Hudson Jameson, Cofounder, Oaken Innovations, Dallas, Texas, US

Sudha Jamthe, Stanford University, Palo Alto, California, US

Jane Lappin, Toyota Research Institute, Cambridge, Massachusetts, US

Ahmed Mahmoud, CIO, General Motors, Austin, Texas, US

Matt Milligan, CEO, Milligan and Partners, New York, New York, US

Bryant Nielson, Executive Director, Blockchain Academy, New York, New York, US

Steve Polunsky, Research Scientist, Texas A&M Transportation Institute, Austin, Texas, US

Sweeni Ponoth, General Manager, Bristlecone Labs, San Jose, California, US

Julian Smith, Founder, BlockFreight Inc., Melbourne, Australia,

Daniel Spuller, Chamber of Digital Commerce, Washington DC, US

Louis Stone, Co-founder, Symbiont.io, New York, New York, US

Michael Yeung, CEO, Saftonhouse Consulting Group, Vancouver, Canada

Transforming Transportation through Blockchain Technology

Blockchain is a distributed ledger of transactions, developed originally as the accounting platform for the virtual currency, Bitcoin. The technology is used to verify transactions, creating records that cannot be changed or deleted. Verification is accomplished in a decentralized manner through a network of participants, or distributed nodes, rather than through a third party, such as a bank or credit card company. One of the promises of blockchain is that it can reduce the administrative costs of that third-party validation, or potentially eliminate them altogether. This report examines various blockchain applications in transportation. Potential benefits of those applications include the following.

- Increasing transparency and efficiency in supply chain routes, particularly with documents that change hands numerous times between shippers, carriers, customs agents, banks, and ports.
- Preventing cyberattacks on connected vehicles, since their presence in the Internet of Things exposes them to such attacks on multiple surfaces, including Wi-Fi, cellular networks, and toll transactions. Gaining unauthorized access to a single vehicle may be of little value, but access to the uploading of information from vehicles to broader networks likely would be of value.
- Reducing tolling costs by eliminating the fees that tolling agencies pay on credit card transactions, estimated at more than $300 million annually nationwide. Blockchain could also facilitate the adoption of a nationwide interoperable system in which customers could use a single account to pay tolls on any toll road in the nation.
- Facilitating automated payments from vehicles for things other than toll transactions, including fuel purchases, vehicle registration renewals, routine maintenance, etc.
- Introducing the possibility of true peer-to-peer ride sharing and fractional ownership of vehicles, which could reduce the role of, or eliminate the need for, third-party providers currently operating as companies such as Uber and Lyft.
- Improving the architecture of the Internet of Things devices deployed at transportation facilities, by providing a decentralized alternative to the server-client model; the decentralized blockchain alternative could eliminate bottlenecks which are unsecured and subject to single points of failure which could result in entire system failures.

Researchers have also identified three barriers to widespread application of blockchain technology in transportation:

- Scalability issues – One strength of blockchain lies in the robustness of its validation capability, which depends upon the continued accumulation of blocks in a ledger. This accumulation then requires ever growing computing resources.

- Business challenges – The novel nature of blockchain will likely limit its implementation to innovative idea projects and demonstration projects, delaying its use in government-funded transportation applications.

- Perception issues – The assumption that validation of transactions will fall to a network of computers rather than a traditional third party is a foreign one, and may prompt many people to simply disregard it.

Table of Contents

List of Figures

Executive Summary

With the release of the Bitcoin concept into the public domain in late 2008, the world of cryptocurrency (electronic currency such as Bitcoin, Ethereum, and hundreds of others) and distributed computing gained a new kind of trust protocol called "blockchain." Blockchain is a distributed immutable (cannot be deleted) ledger of electronic transactions. It uses a point to point protocol with financial incentives for computer nodes to validate and secure transactions.

In addition to featuring an immutable ledger of transactions, Blockchain also provides security by having no single point of failure, pseudo anonymity, and traceability. Public blockchain implementations such as Bitcoin operate in an open source environment. That means anybody can join the network as a mining node (user), see the code base, and contribute. On the other hand, private and permissioned blockchain operates in a controlled environment in which an operator controls who can join as nodes and users, and as such, do not need crypto currency as economic incentives to secure the underlying blockchain. Public blockchain needs economic incentives in the form of crypto currency to validate and secure transaction blocks.

Because of the open source environment where crypto currencies and public blockchain operate, companies involved in this technology have proliferated. Hundreds of startups have created their own versions of blockchain built for specific applications such as internet of things, identification, land transfer, etc., along with crypto currencies or tokens to provide economic incentives to secure blockchain. These startups are financially supported by big banks, venture capitalists, technology companies, and even crowd sale of tokens. In 2016, over $1 billion (US) has been invested in blockchain-related startups all over the globe.

Numerous startups are working to develop proofs of concept and deployments using blockchain in transportation because of the following perceived benefits:

- Create frictionless systems - in supply chain to increase efficiency.
- Create a trusted audit trail and transparency – in provenance of products, vendors, public services.
- Use machine-to-machine payments – automated vehicles and assets to pay for services.
- Outsource trust – use blockchain network as a trust instead of individuals or companies, especially in shared mobility and asset sharing applications.
- Secure internet of things – use blockchain's immutable design to ensure secured hardware updates.

In addition to startups and big enterprises, many domestic and foreign government agencies are beginning to experiment with blockchain in a variety of services. General Service Administration recently invited all federal agencies for a summit in identifying use cases in public service. Department of Homeland Security has funded several startups providing blockchain technology.

Blockchain’s key value proposition is in its decentralized verification of transactions or transfer of value and assets. It is a “decentralized” platform. Hence, a trusted third party is not needed to verify transactions, which instead is accomplished by distributed nodes. Because of its append-only design, transactions are for all practical purposes immutable and tamper proof. As a blockchain becomes longer over time, transactions become more computationally difficult to corrupt. This ensures that transactions persist into the future with the assurance that they have not been tampered with. Immutability also engraves trust in the sense that transactions and assets encoded in them are difficult to tamper with or be corrupted.

Blockchain’s value propositions are attractive in use cases where high confidence in immutability is required and when economic risk is high in the event of information corruption. Blockchain will certainly reduce administrative cost for third party verifiers and intermediators. .

Transportation Applications

Researchers envision that implementation of blockchain in transportation will mostly focus on applying technology to reduce or remove third party costs (i.e., supply chain, shared mobility, tolling, asset transfer), reduce single point of failure (i.e., internet of things including connected and automated vehicles), and increase transparency (i.e., supply chain, asset transfer). Researchers believe based on interviews conducted during this research that it is conceivable, over time, that blockchain will touch many transportation applications and become a ubiquitous technology.

Blockchain, as a new technology has introduced a paradigm shift. That is, a trusted network of computers is acceptable as opposed to an organization or individual as a source of trust. Blockchain is also a foundational technology, meaning applications have to be built on it, and by itself has no real-world use.

Barriers and Policy Considerations

Researchers believe there are three key barriers to entry and deployment challenges in short and medium term – scalability issues, business challenges, and perception barriers.

To understand and quantify these barriers, companies are using proof of concept and proof of value projects where specific use cases are tested with blockchain. Proof of concept tries to answer “will it work?” Proof of value tries to answer “will it work and will it benefit my business?” This is a safe way for companies and even government to be familiarized with new technology without expending a significant amount of funds for full implementation. Government agencies in United States and around the world are performing proofs of concept and proofs of value to understand the benefits of blockchain technology to improve public services.

Governments may also regulate legal acceptance of information in blockchain, such as smart contracts. One thing is clear—that the government and regulatory bodies are accustomed to regulating legal entities that provide third party trust services (e.g., trading platforms, notaries, ride-hailing services), but certainly not a network of computers owned by no one and spread across multiple countries and jurisdictions. In order for the government not to stifle blockchain development, it is also important that government does not hastily pursue legislation and regulations without a full understanding of blockchain.

Instead, researchers and blockchain experts suggest that government agencies pursue proof of value projects to analyze benefits and provide platform for standardization and interoperability of blockchain as they begin to be used in transportation infrastructure, security of cyber physical systems, and public services.

Bitcoin: Peer-to-peer Electronic Cash System

An exploration of blockchain cannot begin without understanding Bitcoin because for all practical purposes Bitcoin is the first application built on blockchain. It is somewhat odd that Bitcoin became mainstream before the underlying technology did.

In October 2008, a paper circulated in crypto currency mailing lists describing a peer-to-peer electronic cash system termed “Bitcoin” was followed by open source code in 2009. The paper and source code was authored under the name Satoshi Nakamoto, whose real identity is still unknown. The individual or group created Bitcoin’s original reference implementation called Bitcoin Core. As a part of this implementation, he (or she or they) also devised the first blockchain database [1].

Until 2009, cryptographic currencies were not able to solve a problem called “double spend” or “double spend attack.” Double-spending is a result of spending the same money more than once. In traditional money transfer, a trusted third party such as a bank or clearing house prevents such a double spending problem. Bitcoin elegantly solved the double spending problem without a need for a trusted third party by storing each verified transaction in a decentralized distributed ledger. These transactions are verified by nodes operating in a peer-to-peer network [2]. Blockchain will be discussed further in the next chapter.

Transactions are verified by using consensus of nodes. The transaction—and thus the transfer of ownership of the Bitcoins—is recorded, time-stamped, and displayed in one “block” of the blockchain. Public-key cryptography ensures that all computer nodes in the peer-to-peer network have a constantly updated and verified record of all transactions within the Bitcoin network, which prevents double-spending and fraud [3]. Figure 1 shows how users transfer Bitcoin using the peer-to-peer network without a need for a third party.

Bitcoins are created by a process called “mining.” The Bitcoin network depends on globally distributed computer nodes, which provide computing power to verify transactions and include them in a distributed ledger. These nodes are called “mining nodes,” and they are awarded with mathematically created Bitcoin and transaction fees for their efforts. This is an important concept because the Bitcoin system has incentivized “mining nodes” to validate transactions and thereby maintain the Bitcoin blockchain [4] .

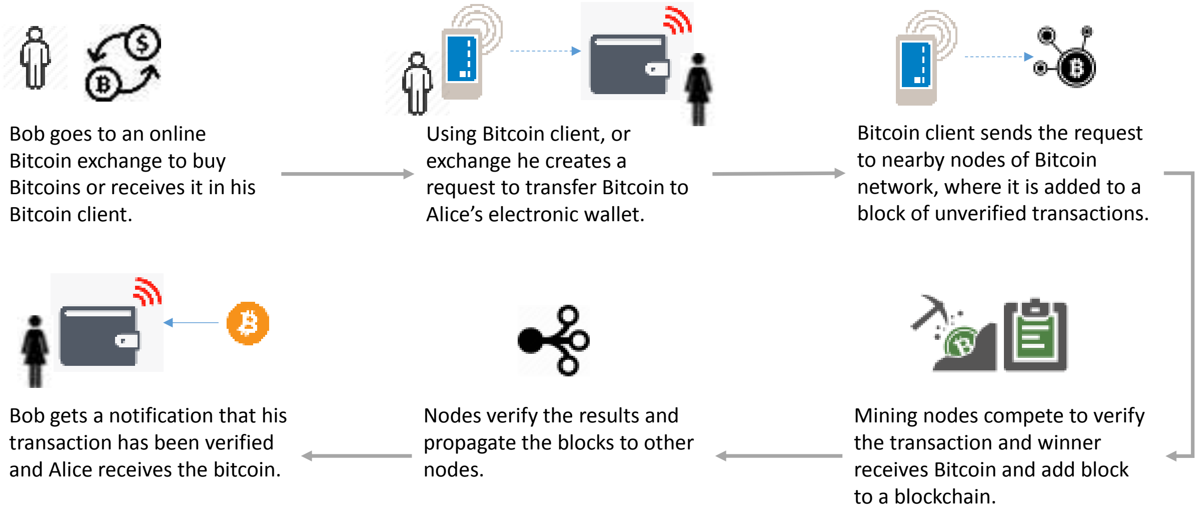
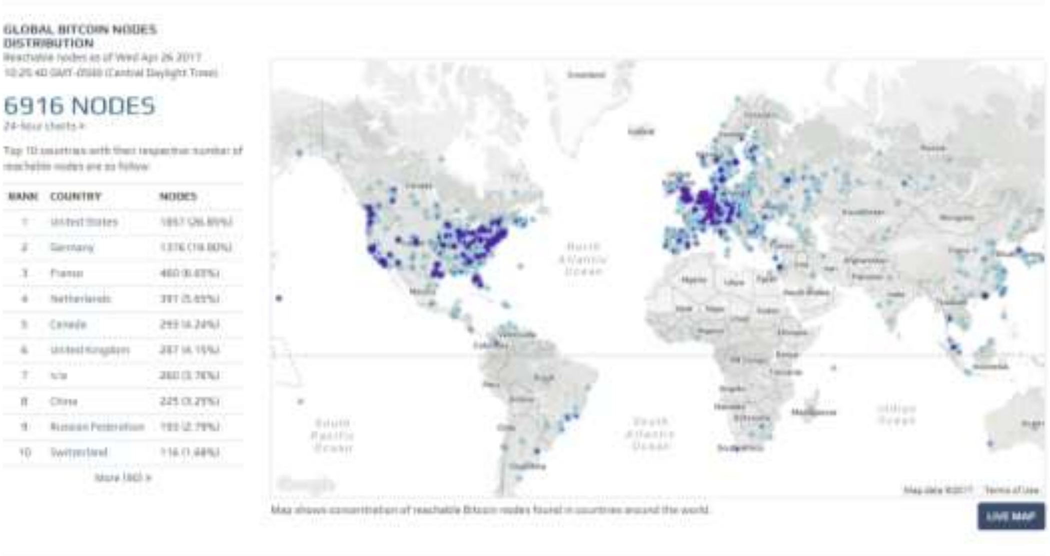

Bob goes to an online Bitcoin exchange to buy Bitcoins or receives it in his Bitcoin client.
Using Bitcoin client, or exchange he creates a request to transfer Bitcoin to Alice's electronic wallet.
Bitcoin client sends the request to nearby nodes of Bitcoin network, where it is added to a block of unverified transactions.
Mining nodes compete to verify the transaction and winner receives Bitcoin and add block to a blockchain.
Nodes verify the results and propagate the blocks to other nodes.
Bob gets a notification that his transaction has been verified and Alice receives the bitcoin.

Figure 1. Overview of Bitcoin Value Transfer.

The Bitcoin network of nodes is not operated or maintained by a single entity in a single country. There are close to 7,000 reachable nodes spread across 90 different countries [5]. Anybody can join the network to become a node given they have sufficient computing resource. Figure 2 shows locations of Bitcoin nodes spread across the globe with heavy concentration in the United States, Germany, and France. Bitcoin's biggest innovations are the absence of central entity or authority, which minimizes single point of failure, and distributed ledger, which provides immutability to reduce fraud and hacking.

The system is essentially "trustless." The blockchain network as it pertains to Bitcoin uses an electronic wallet created by using the user's private and public key, and as such, does not require personally identifiable information to be encoded in transactions. Hence, the Bitcoin blockchain provides pseudo anonymity [6]. Party A simply uses the destination electronic wallet identification of Party B to transmit Bitcoin. There is no reference to Party A or B's physical address, email, or phone number.

Unlike databases maintained by banking and credit card institutions, Bitcoin blockchain does not contain a significant amount of personal data [6]. All the above innovations (by design) contributed to Bitcoin blockchain's record of never having been hacked in its eight years of existence. Bitcoin exchanges and electronic wallets have been hacked many times, but not the underlying blockchain. This does not mean it will never happen. In fact, blockchain can be hacked and compromised, but it would require tremendous computing resource, something no individual or a government entity possesses.



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Apr 26 2017 10:25:40 GMT-0500 (Central Daylight Time)

6916 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow:

RANK	COUNTRY	NODES
1	United States	1857 (26.85%)
2	Germany	1376 (19.90%)
3	France	460 (6.65%)
4	Netherlands	391 (5.65%)
5	Canada	293 (4.24%)
6	United Kingdom	287 (4.15%)
7	n/a	260 (3.76%)
8	China	225 (3.25%)
9	Russian Federation	193 (2.79%)
10	Switzerland	116 (1.68%)

More (90) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

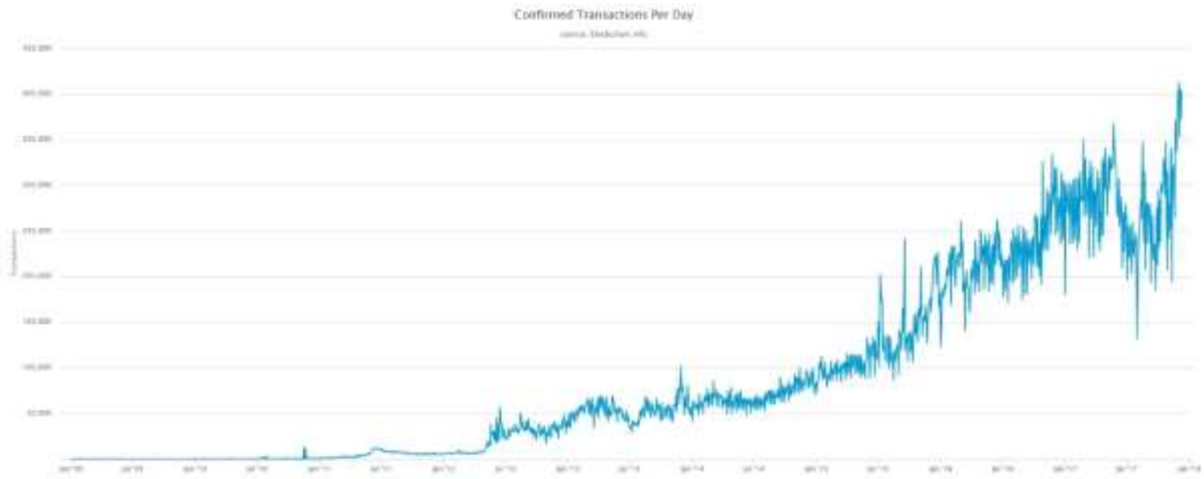
Source: [5]

Figure 2. Image showing Locations of Bitcoin Nodes.

Owners of Bitcoins can transfer them over the peer-to-peer network to do the same things that conventional currencies can do including buying and selling goods and sending money to individuals and organizations. Bitcoins can be purchased, sold, and exchanged for other currencies at Bitcoin exchanges such as Coinbase and Kraken.

Bitcoin's reputation was tarnished by its involvement with Silk Road, an online black market that operated in the dark net (areas usually inaccessible to most Internet users). Silk Road was a platform for anonymously buying and selling illegal drugs, guns, and similar contraband. Bitcoin was the currency of choice to trade in Silk Road. Silk Road was shut down in 2013 by the Federal Bureau of Investigation [7]. The news made headlines around the world, and so in the eyes of the public Bitcoin became associated with the black market.

Nonetheless, Bitcoin has gained traction among the unbanked population, international money transfer, and small businesses due to lower transaction costs because of the absence of third party institutions [3]. It has also given rise to Bitcoin investors, who hold Bitcoin in hopes of increasing value as well as investments in startups, which utilize Bitcoin as a payment mechanism. Bitcoin's market capitalization as of December 2017 stands at over US $100 billion with 20 million Bitcoin wallets creating over 400,000 transactions per day [8]. Figure 3 shows explosive growth of per day Bitcoin transactions since January 2009.



Source: [9]

Figure 3. Growth of Number of Daily Confirmed Bitcoin Transactions Since 2009.

Experts believe that among many external factors causing increased interest in Bitcoin may be that blockchain's use in applications other than Bitcoin has surged, generating positivity around Bitcoin's public blockchain [10].

The blockchain is seen as the main technological innovation of Bitcoin because it stands as a "trustless" proof mechanism of all the transactions on the Bitcoin network. Users can trust the system of the public ledger stored worldwide on many different decentralized nodes as opposed to having to establish and maintain trust with a third party intermediary.

Technology behind Bitcoin and Other Cryptocurrencies

Bitcoin uses a number of underlying technologies: cryptographic hash functions, distributed ledger of transactions, peer-to-peer network, and many more. They all work together to power Bitcoin. These technologies also rely on each other for Bitcoin to work. While it is common to refer to blockchain as a distributed ledger, the process also requires cryptography, a peer-to-peer network, rules to synchronize the ledger, and economic incentives for synchronizing the ledger.

In an abstract sense, blockchain is a combination of a peer-to-peer network of distributed computers working together to synchronize a state (in case of Bitcoin, ledger of transactions) based on mathematical and cryptographic rules supplemented with incentives to maintain the state.

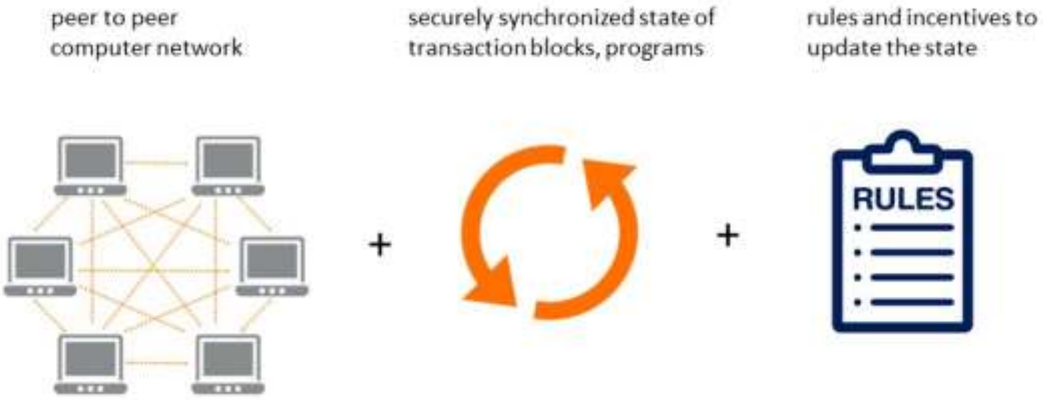
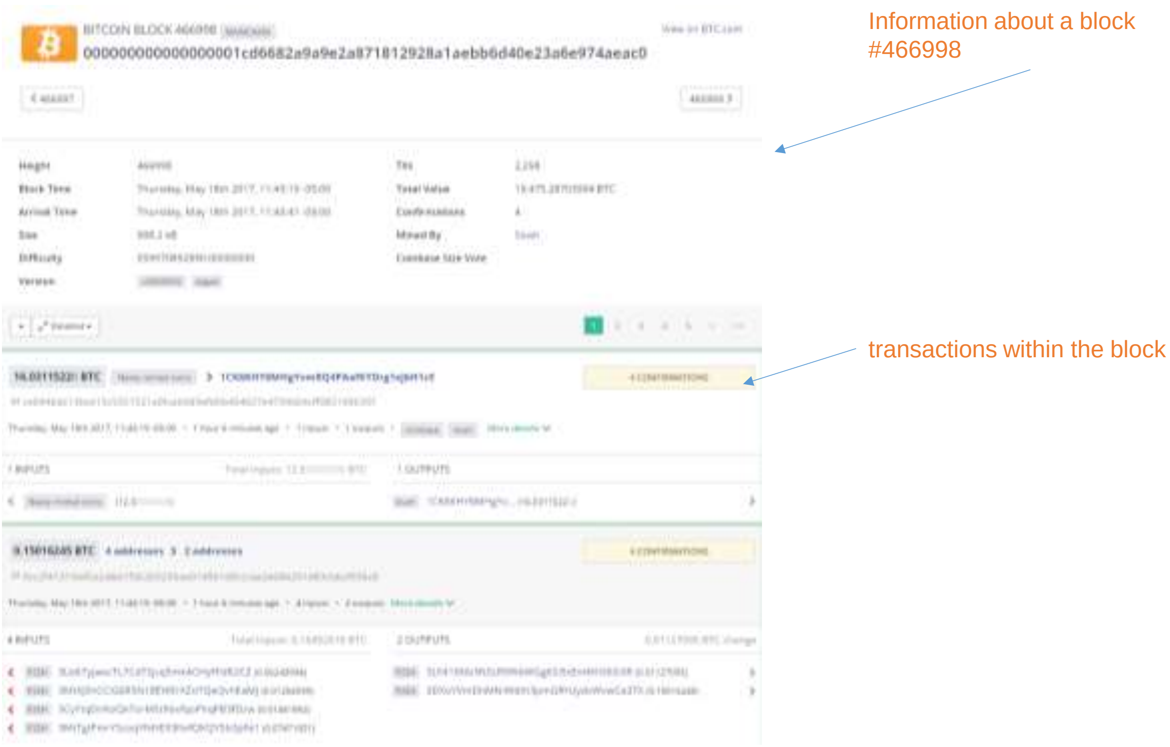

peer to peer computer network
securely synchronized state of transaction blocks, programs
rules and incentives to update the state
+
+
RULES

Figure 4. Abstraction of Blockchain Components.

Blockchain data structure includes an ordered and back-linked list of blocks that contain verified transactions. Individual blocks contain verified transactions. Transactions include transfer of crypto currency (in case of Bitcoin) between users, timestamp, public key of senders and receivers, etc., as shown in Figure 5. Transactions are then broadcast on the Bitcoin network where each node validates and propagates the transaction until it reaches every node in the network. Transactions are verified by mining nodes and included in a block of transactions that is recorded on the blockchain [2]. Each transaction in the public ledger is verified by mathematical consensus of a majority of participants (nodes) in the blockchain network. Each block is linked to the previous or “parent block.” Figure 6 shows how individual blocks are linked with previous blocks forming a chain. The sequence of each block linked to its parent blocks creates a chain going all the way to the first block created, also known as the “genesis block” [2].



BITCOIN BLOCK 466998

0000000000000000001cd6682a9a9e2a871812928a1aebb6d40e23a6e974aeac0

View on BTC.com

< 466997

466999 >

Height

Block Time Thursday, May 18th 2017, 11:45:19 -05:00

Arrival Time

Size

Difficulty

Version

TXs

Total Value

Confirmations

Mined By

Coinbase Size Vote

16.02115221 BTC

1 INPUTS

1 OUTPUTS

0.15016245 BTC 4 addresses > 2 addresses

4 INPUTS

2 OUTPUTS

Information about a block #466998

transactions within the block

Source: https://www.blocktrail.com/BTC/block/0000000000000000001cd6682a9a9e2a871812928a1aebb6d40e23a6e974aeac0

Figure 5. Construction of a Bitcoin Block in a Blockchain.

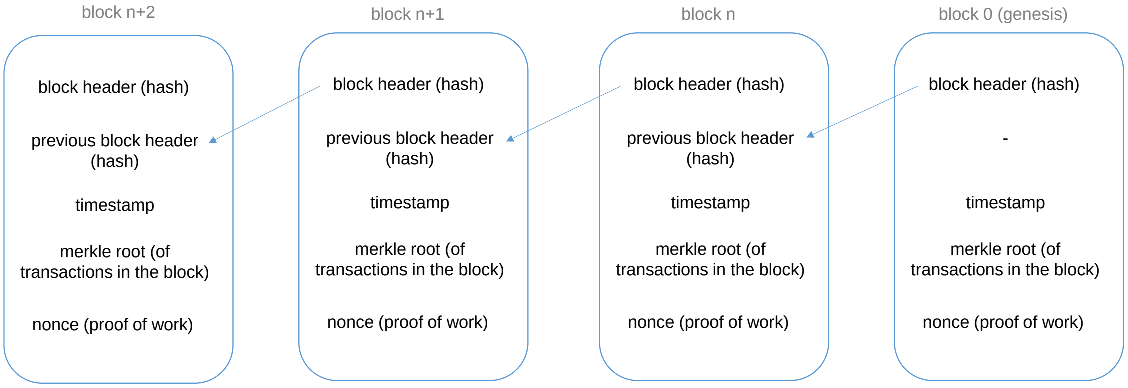
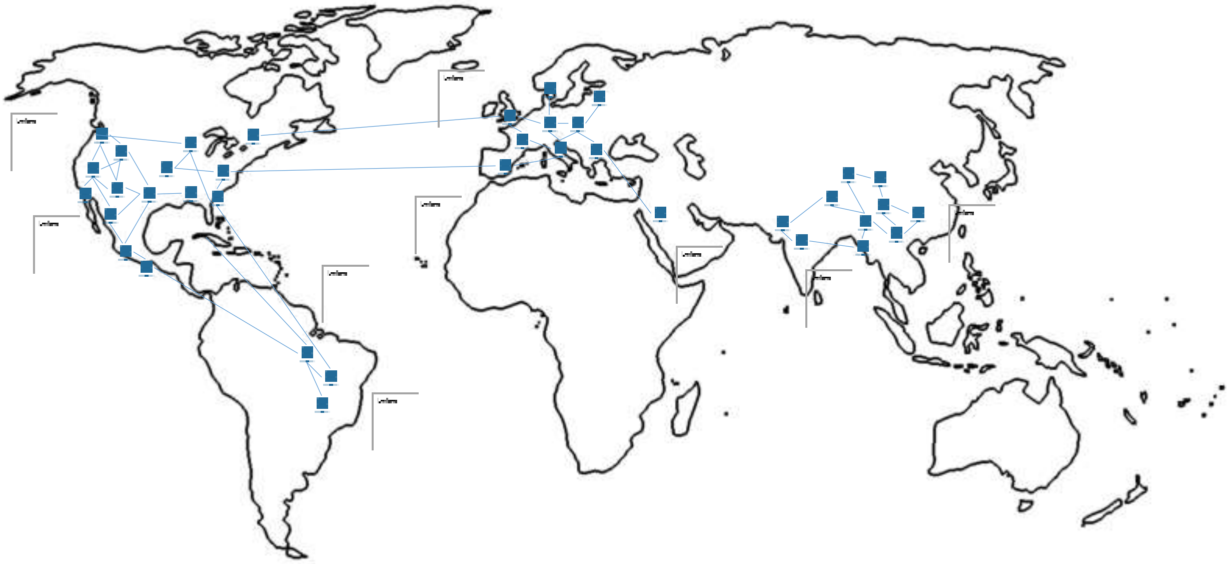

block n+2
block header (hash)
previous block header (hash)
timestamp
merkle root (of transactions in the block)
nonce (proof of work)
block n+1
block header (hash)
previous block header (hash)
timestamp
merkle root (of transactions in the block)
nonce (proof of work)
block n
block header (hash)
previous block header (hash)
timestamp
merkle root (of transactions in the block)
nonce (proof of work)
block 0 (genesis)
block header (hash)
-
timestamp
merkle root (of transactions in the block)
nonce (proof of work)

Figure 6. Arrangement of Blocks in a Blockchain.

Depending on the blockchain, nodes may be globally distributed in a connected peer-to-peer network as shown in Figure 7 or, in the case of permissioned blockchain nodes, may reside within few nodes.



Note: Map does not represent actual location of Bitcoin nodes.

Figure 7. Abstract Representation of Globally Distributed Bitcoin Nodes.

Once confirmed and added to blockchain, it is practically infeasible for anyone to modify or delete transactions, since it would require modification of all previous blocks that are connected in a chain and maintained in hundreds of nodes. This cascading effect ensures that once a block has many generations following it, it cannot be changed without forcing a recalculation of all subsequent blocks [2].

More on this later, but the immutable property of blockchain allows the disintermediation and decentralization of transactions between parties [11]. Blockchain can also be framed as a protocol with an established set of rules in the form of distributed computations to ensure the integrity of data without a trusted third party. Blockchain has been called a “trust protocol [6].”

Blockchain vs. Traditional Databases

If blockchain is just a ledger of transactions, how is it different from databases that are widely in use? Or can’t existing database systems be modified to do the same thing as blockchain? These are questions most people ask when they are first introduced to the concept of blockchain – how are the two different?

The core difference lies not in how data are stored, but how they are managed and controlled. Blockchain enables transactions to be shared across boundaries of trust, without requiring a central administrator [12]. Transactions are verified and processed independently by multiple “nodes” in a peer-to-peer network with the blockchain protocol as a consensus mechanism to ensure those nodes sync the data.

Enterprise businesses design their database systems in such a way that data, permissions, and access are consolidated among a few individuals and firewalled from the public. A database administrator’s main responsibility is to keep the database “obscure” and hidden from those without permission to use it. Bitcoin blockchain on the other hand is open for anybody to download and explore transactions related to wallet addresses all the way back to the first transaction in 2009 [2].

In a traditional database, a central authority manages transactions even though the database may use redundant nodes to create a “shared” database. Hence, in a traditional database the central authority is potentially a single point of failure and is required to always act in good faith to maintain the database.

If decentralization, immutability, single point of failure, and cryptography are not desired or not an issue, then a traditional database with centralized management is adequate. Traditional database technology has evolved through at least thirty years of development and refinement. Both technologies have upsides and downsides that makes them appropriate or inappropriate for specific implementations.

Permissioned vs. Permissionless Blockchain

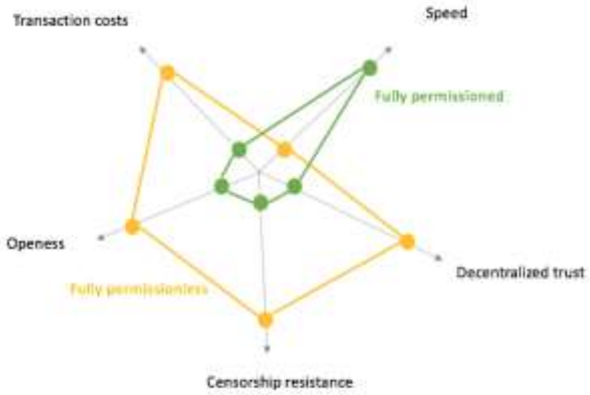
Blockchain that runs underneath Bitcoin is public and permissionless. Public in the sense that there are no restrictions on reading blockchain data and submitting transactions to the blockchain [13]. Anybody can read transaction information pertaining to Bitcoin wallet addresses and exchange Bitcoin. Permissionless in the sense that anybody with a computing resource can process transactions (Bitcoin nodes.) Bitcoin's popularity is attributed to public and permissionless design in which nodes are incentivized to avoid hacking and disruptions by removing the single point of failure. Bitcoin nodes are spread all over the world – mostly concentrated in the United States, Germany, and China (14).

However, permissionless and public blockchain may not be ideal for institutions that need to restrict individuals/entities in terms of processing and validating transactions. From a security perspective, it is difficult to imagine government institutions in the US adding land titles, vehicle ownership, financial transactions, etc., in a blockchain that is accessible to nodes based outside of the country, even though data itself may be encrypted.

For this reason, there is growing interest among financial and government institutions for permissioned (can be public or private) blockchain implementations. In permissioned blockchain, transactions processing is performed by a pre-defined list of entities with known identities [13]. Permissioned blockchain could form a more controlled and predictable platform than permissionless, especially for proprietary applications that are subject to regulatory oversight and audits [13]. Figure 8 illustrates differences between the two concepts with respect to speed, transaction cost, trust, and related issues.

Private permissioned blockchains are also heavily contested among blockchain enthusiasts because "opaque" blockchains that are limited to few known transaction processors (nodes) and limited access to users undermines the very concept of decentralization.

Decentralization and openness can be extremely desirable for specific use cases (e.g. Bitcoin), but they come at a cost because reaching consensus in a distributed network of thousands of nodes takes time. For example, transactions in Bitcoin take an average of seven minutes to confirm [15]. On the other hand, permissioned blockchains can achieve faster speed when deployed in a controlled environment among a handful of pre-approved nodes.



Source: [16]

Figure 8. Comparison of Permissioned and Permissionless Blockchain.

Arguments against permissioned and private blockchains are also based on the fact that they could be subject to vulnerabilities because they may remain undiscovered for a long time. Permissioned blockchains have a small number of “trusted” transaction nodes or processors. This makes the system susceptible to corruption and tampering by a handful of bad actors. In permissionless blockchain such vulnerabilities can be avoided and quickly audited since a large number of transaction nodes would need an incentive to jointly attack the system while the rest of the nodes try to prevent them.

It is still unclear at present how implementation of blockchain in transportation use cases mentioned in Chapter 9 would utilize permissioned vs permissionless blockchains. However, permissioned blockchains have garnered a lot of attention for enterprise solutions in order to allow the solution owner to manage visibility of users under the mutually agreed upon terms and conditions. Also, permissioned blockchains are a lot faster in terms of transaction processing since consensus is not mandatory and neither is underlying crypto currency or token. It is most likely that blockchains deployed for private enterprise or government will be permissioned. Other deployment challenges are discussed in Chapter 11.

Smart Contracts for Machine-to-Machine Payments

Smart contracts are computer codes that reside and operate in blockchain, are triggered by blockchain transactions, and read and write data in the blockchain [17]. In the context of agreements or contracts, it refers to the use of computer code to articulate, verify, and execute an agreement between parties [18]. Typical contracts are drafted using natural language in paper or electronic documents. Instead, smart contracts allow parties to encode contractual clauses in a computer code, attach metadata of digital assets, and exchange them based exactly on the computer code in blockchain as illustrated in Figure 9.

Once deployed in a blockchain, contracts are triggered by events or user inputs and in return perform pre-defined tasks such as pay recipients or transfer shares. Ethereum, a decentralized platform, runs smart contracts on a public blockchain, which is separate from Bitcoin's [19], Ethereum blockchain is a global infrastructure much like Bitcoin's is. The network of nodes running Ethereum blockchain validate contracts independently (consensus). And according to the data used in triggering the transactions, they result in the same output, which makes it unnecessary for a third party to validate the scope or output of a contract.

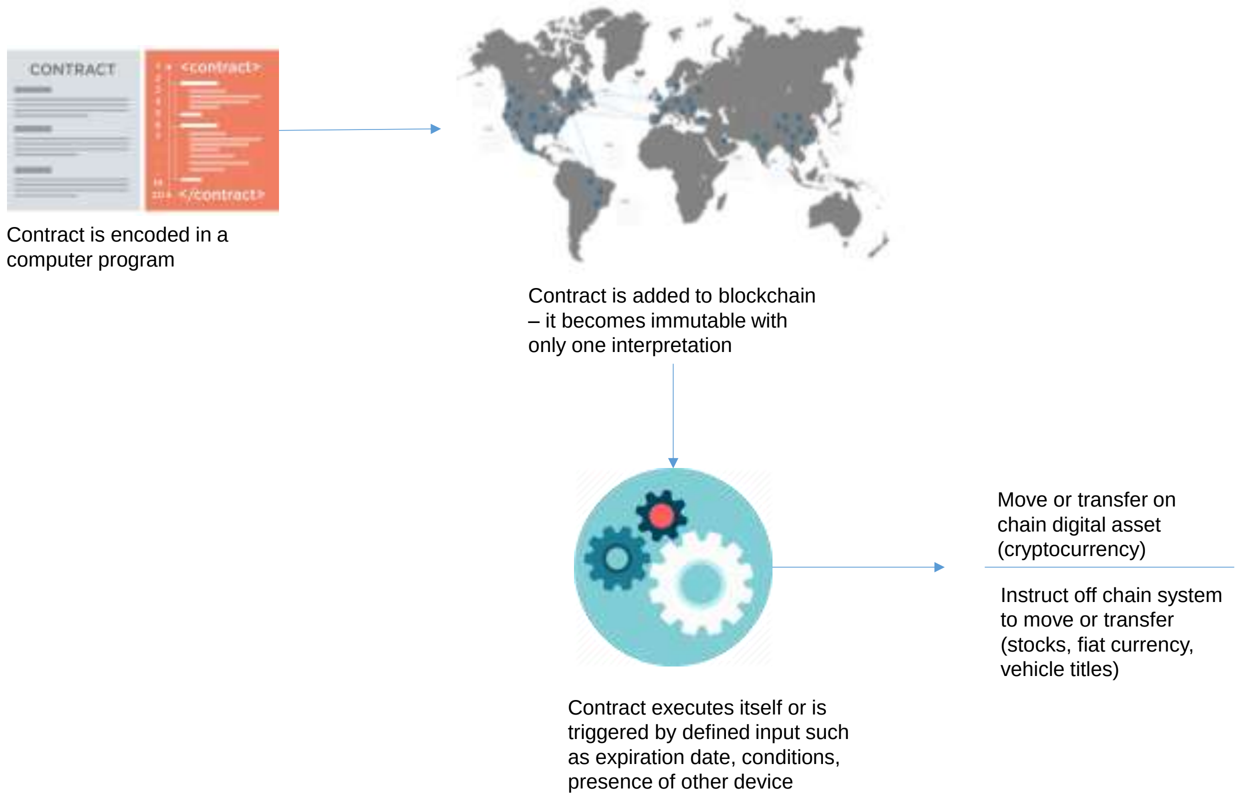

CONTRACT
<contract>
</contract>
Contract is encoded in a computer program
Contract is added to blockchain – it becomes immutable with only one interpretation
Contract executes itself or is triggered by defined input such as expiration date, conditions, presence of other device
Move or transfer on chain digital asset (cryptocurrency)
Instruct off chain system to move or transfer (stocks, fiat currency, vehicle titles)

Figure 9. Abstract Representation of How Smart Contracts Work.

Smart contracts are computer programs and hence are unambiguous by design. Computer programs are predictable and deterministic: the output is always the same for a given input. This also means users exchanging digital assets over smart contracts cannot disagree over the outcome of the contract [20]. Such a deterministic nature of the smart contract and its immutability makes it powerful and at the same time raises questions about its widespread applicability. Smart contracts may never fully replace contracts written in natural language because many contracts can never be fully expressed in code or executed by a computer [18].

If smart contracts are just a “fancy” phrase for a computer code, then why is it any different from stored procedures that are well known in traditional database realm? Stored procedures also take inputs from a database or user, have business logic built in, and create a predictable output. The difference lies in the fact that stored procedures can be tampered with by a centralized authority or whoever manages the database. On the other hand, smart contracts are practically tamper proof once they are added to a blockchain.

Another contested point about smart contracts is whether they are really smart, and are they really contracts in a legal sense? If they are simply computer codes with specific instructions to automatically execute terms and conditions, what is so smart about it [21]? As of now, smart contracts do not have any legal status in any known legal jurisdiction. Should a smart contract do something the parties had not intended, who is responsible?

Discussion of smart contract is interesting in the context that transportation uses cases such as supply chain, shared mobility, vehicle registration, and includes exchange/sharing of digital assets between users resulting in payments. For example, bill of lading is a document that is used to hand over shipment from shipper to carrier to receiver. It is also a document that is easy to tamper with, mainly because the shipper creates a bill of lading, and there is no third party to verify the actual content of the shipment.

Imagine a situation where a bill of lading is encoded in a smart contract (and blockchain). It becomes almost impossible to tamper with the bill of lading. This is good news for insurance underwriters who then have assurance that a shipper or a carrier has not tampered with the bill of lading to falsely claim payments during theft or damages.

Shared mobility is another transportation vertical that might be disrupted by smart contracts [6]. More on this in Chapter 9. However, the basic tenet is that a smart contract allows two parties (and two machines) who do not know or trust each other to contract and pay each other using an immutable program running in decentralized network over blockchain without a trusted intermediator.

Misconceptions about Blockchain

As with any new and promising technology, blockchain has been subject to much hype and misconceptions. A few key misconceptions about blockchain are listed below:

- Blockchain is a database – In fact, it is more of a ledger than a database added with cryptography, and consensus based mining. As such, it is not useful for applications that include high frequency transactions because it takes a few seconds to even several minutes to verify transactions (10 minutes in the case of Bitcoin) and a database that needs frequent modifications at user level [2].

- Public and permissionless blockchain is suitable for all foreseeable use cases – Open and permissionless blockchain will have a hard time finding use cases in government and public sector, especially to store public asset and identification information. It is very difficult to fathom that federal, state, and local government entities will use open and global blockchain to transact digital assets. However, they might employ permissioned +private blockchain. In which case, the system will still be subject to single points of failure.

- There is only one blockchain – There is no such thing as “the blockchain.” Blockchains come in many shapes, sizes, and colors. If they all share a roughly similar architecture, they are very different in how they work and what they are good at [22].

- Blockchain can be used to store documents – Blockchain is neither a database nor a cloud. It doesn’t allow users to store any type of physical information such as image files or document files. However, blockchain can provide a proof-of-existence.

- Everyone can see private information on the blockchain – Because transactions between Bitcoin wallet addresses are accessible to public via blockchain explorers, people assume that private information about users is also accessible. This is absolutely false. What is stored on the ledger is nothing more than the amount of the transaction and a hash. The hash is a code obtained by running the actual transaction details through a one-way cryptographic function [2].

Use Cases in Transportation

Blockchain’s key value proposition is decentralized trust to verify transactions or transfer of value and assets. Hence, a trusted third party is not needed to verify transactions, which is accomplished by distributed nodes.

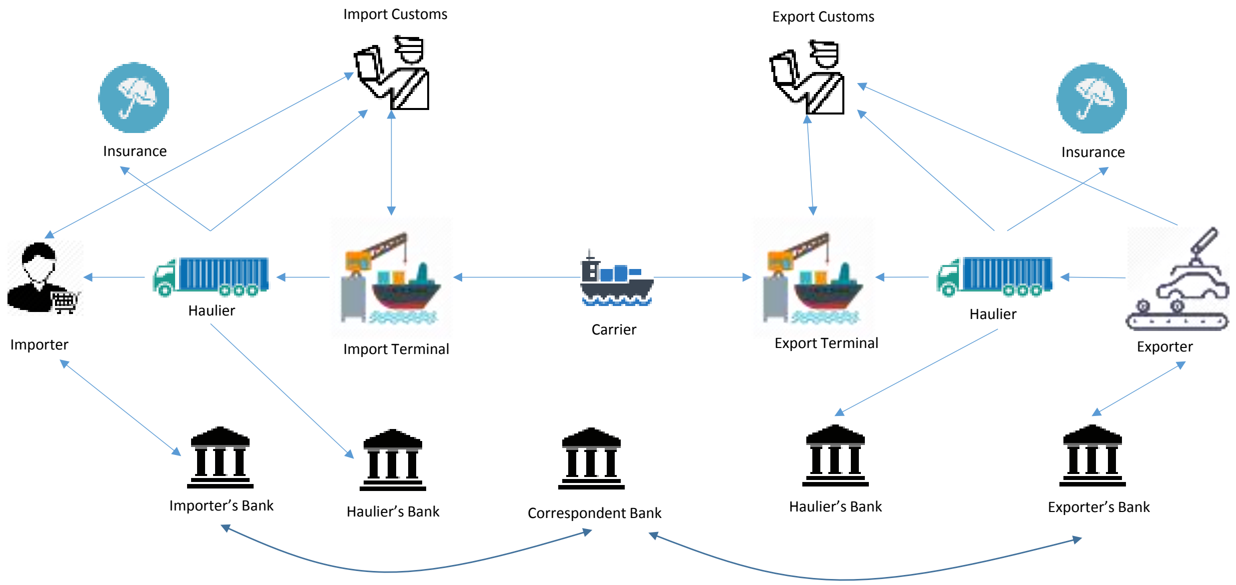
Because of its append only design, transactions are for all practical purposes immutable and tamper proof. As blockchain becomes longer and longer over time, difficulty to corrupt transactions becomes more and more computationally difficult. This ensures that transactions persist into the future knowing that they have not been tampered with. Immutability also engraves trust in the sense that transactions and assets encoded in them are difficult to tamper with or be corrupted.

Blockchain’s value propositions are attractive in use cases where high confidence in immutability is required or when economic risk is high in the event of information corruption. Because blockchain is a “trustless” platform, it will certainly reduce administrative fees provided to third parties for transaction verifications or even remove them entirely.

Implementation of blockchain technology in transportation will mostly focus on applying the above mentioned value propositions in order to reduce or remove third party costs (i.e., supply chain, shared mobility, tolling, asset transfer), reduce single point of failure (i.e., internet of things, automated vehicles), and increase transparency (i.e., supply chain, asset transfer).

Increasing Transparency and Efficiency in Supply Chain

In supply chain, along with physical movement of goods information about of the goods moves between shipper, freight forwarders, banks, carriers, insurance [23]. Some documents are deeds of title (asset transfer) moving the goods to a consignee. A bill of lading describes the condition of goods as described by a shipper. An electronic manifest is a list of all the cargo carried on an airplane, ship, rail, and trucks and is made from bills of lading. These documents change hands numerous times between shipper, carriers, customs, insurance, banks, and ports. Figure 10 illustrates flow of documents (shown by blue line) between multiple entities in the supply chain network.



Note: Modified from Original Image from Boston Consulting Group

Figure 10. Flow of Documents in Supply Chain Network [24].

Supply chain relies on trust between parties involved with moving goods [25]. Trust is built around assumptions that information passed between entities is untampered. In regions where trust between entities, including companies and governments, is low, lack of trust often leads to relying only on known and reputable entities for trading relationships. It also prevents exploration of new partnerships with other suppliers as well as creation of new synergies.

On top of that, there is ample evidence that suggests fraud in supply chain amounting to enormous proportions [23]. Fraudulent documents create risks to letters of credit, customs agencies, carriers, and many more. Hence, there is a need for documents moving from beginning to the end of supply chain to remain untampered. Adding documents as they are created to a public blockchain may reduce the possibility of double-spending and tampering, as illustrated in Figure 11. This would remove the need for a trusted third party to verify documents and reduce time required to settle payments from banks and insurance companies. It could lower the costs of tracking goods and services by expediting the validation of transactions between multiple parties along supply chain routes [26]. This would have tremendous impact on trade finance.

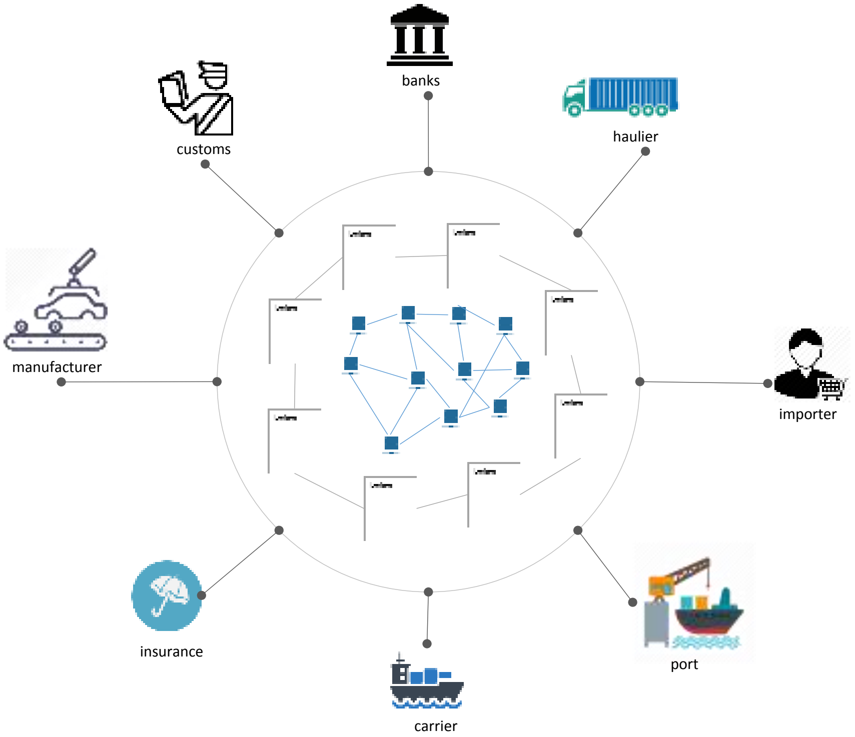


Figure 11. Blockchain Enabled Supply Chain Network.

Blockchains and supply chains are already becoming a busy crossover, with startups, banks, and major retailers working on proof of concepts to deploy blockchain in order to streamline supply chain processes.

Bank of America Merrill Lynch is reportedly developing a blockchain-based experiment for trade finance transactions [24]. Generally, trade finance concerns both domestic and international transactions, where typical activities include lending, issuing letters of credit, factoring, export credit, and insurance. When commonly used, the term “trade finance” is generally reserved for bank products that are specifically linked to underlying national and international trade transactions.

Tokio Marine and Nippon Telegraph and Telephone Data recently completed testing a blockchain-based insurance policy for marine cargo. These policies are forwarded by and shared among parties concerned with shipping [27]. Tokio Marine’s proof of concept created data bill of lading, letter of credit, and commercial invoice on a blockchain. Tokio Marine claims that the blockchain-based system will cut 85 percent of the shipper's time of data inputting work in order to receive an insurance certificate. It also successfully tested accessibility from the parties concerned, such as consignee and banks.

BlockFreight, an Australian startup, is working to create a frictionless logistics in which hash of documents such as bill of lading is added to blockchain as agreed upon a common state attained by network consensus, and thereby serves as an incontrovertible record. This unlocks the opportunity for value added applications, such as performance-based smart contracts and chain-of-custody record management and compliance systems to be built [28]. Symbiont is a startup with a blockchain-based product that allows a frictionless process with deduplication of loan and trade documents [29].

Skuchain, a United States (US) based startup is working to streamline a process to receive line of credit for carriers and others to receive advanced payments based on bill of lading and other documents [30]. Provenance, a United Kingdom (UK) based startup is using blockchain to share the product's journey and its impact on environment and society. Walmart is working with IBM and Tsinghua University, in Beijing, to follow the movement of pork in China with a blockchain [31]. Mining giant BHP Billiton is using the technology to track mineral analysis done by outside vendors. Everledger is another startup working to upload unique identifying data on a million individual diamonds to a blockchain ledger system to build quality assurances and help jewelers comply with regulations barring "blood diamond" products [31].

Bristolcone, a subsidiary of Mahindra and Mahindra and a supply chain firm, is working on proof of concepts to track and trace components coming from different vendors, supplier registry, item mapping, and version control using blockchain [32]. They see opportunities to reduce the cost of due diligence in selecting suppliers, certifications of supplier documents, and provenance of parts as key value propositions.

There are three main challenges to widespread use of blockchain in supply chain, in addition to the scaling challenges of blockchain technology itself:

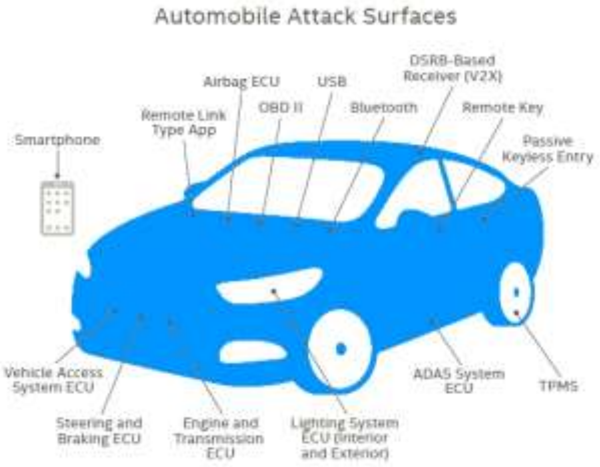
- First is the realization that supply chain is hugely complex and massive in scope. Hence, it is not surprising that supply chain industry is slow in adopting new technology – especially one that might disrupt the incumbent business model. Pushback from internal forces against decentralization is to be expected.
- The second challenge is that in order to realize sustainable benefits from an open decentralized system, where a number of parties from multiple countries/languages interact, some kind of common data and operating standards are necessary.
- The third challenge is the deployment itself. Supply chain involves dozens of parties to complete a transaction (moving goods from A to B.) So, somebody has to huddle all these parties together to participate and move the information flow in blockchain.

Supply chain and especially logistics across regions and international borders require working with unknown individuals and companies. There are rules, and regulations in place, but parties still have to assume that other parties will adhere to them. Hence, application of blockchain may be a low-hanging fruit since it allows parties to work together in a trustless environment. Supply chain also does not have much government touch points (except at the ports), individual's privacy issues, etc., which may be obstacles in proof of concept and pilot development.

Securing Automated and Connected Vehicles

Ever since the Internet of Things discovered blockchain as a viable concept to prevent multiple attack vectors from taking place, using blockchain to prevent cyberattack or hacking of automobiles has become a subject of discussion; after all, automobiles will be part of the Internet of Things [33]. It is safe to say tomorrow's automobiles will be computers on wheels connected to the internet or at least to each other.

With automobiles continuously connected to outside networks, the attack surface for hackers is broad, touching most in-vehicle systems via a wide range of external networks such as Wi-Fi, cellular network, service garages, toll roads, fuel stations, traffic lights, and aftermarket devices [34]. Figure 12 illustrates attack surfaces in automated and connected cars. Attack on an individual vehicle may not be profitable, but gaining unauthorized access to an organization's system by hacking vehicles that are uploading information to those organizations via wireless connections can be.


Automobile Attack Surfaces
Smartphone
Remote Link Type App
Airbag ECU
OBD II
USB
Bluetooth
DSRB-Based Receiver (V2X)
Remote Key
Passive Keyless Entry
Vehicle Access System ECU
Steering and Braking ECU
Engine and Transmission ECU
Lighting System ECU (Interior and Exterior)
ADAS System ECU
TPMS

Source: [34]

Figure 12. Attack Surfaces in Today's Automobiles.

Gaining unauthorized access to a batch of in-vehicle computers and using them to organize a distributed denial of service attack on organizations is also possible. In reality, this is the kind of attack that occurred in October 2016 when thousands of home devices (including baby monitors) were used to attack the servers of Dyn, resulting in outages of major content providers such as Netflix and Paypal. [35].

Vehicles are produced with more and more computer nodes or electronic control units – from 30 to 100 in automated vehicles [33]. Over the air updates of electronic control unit firmware in vehicles and the very fact that they may be connected to potentially unsafe Wi-Fi networks at fuel stations, homes, dealers, etc., also increases risk of attack. Each unit embeds dedicated operating system and thousands of lines of code. Although over the air updates make a lot of sense for auto manufacturers and owners, they need to guarantee safety, security, reliability, and flexibility.

Another aspect of automobile security is its supply chain. Original equipment manufacturers are typically the final integrator of hundreds of components they receive from multiple suppliers from around the globe [33]. They may not be aware of security flaws in components they received. Hence, cyber security of components and the end product has to flow down to the end of supply chain, making the security even more challenging.

Blockchain technology's immutable ledger of transactions, decentralized consensus through transparent nodes, and trustless platform may have a role to play in some aspects of securing automobiles from cyberattacks. As of this writing, no literature was found that described proof of concepts or real-world deployments of blockchain in cyber security of automobiles. However, there is consensus that blockchain has potential in automobile cyber security [33] [36] [37] [38]. Various literature sources indicate blockchain's inherent strength of immutability of transactions, and decentralized consensus can be used to mitigate the following automobile cyber-attacks:

- Tamper proofing over-the-air updates of firmware in electronic control units by timestamping, cryptographic signature, and hash of authorized updates in a decentralized network [38]. Figure 13 and Figure 14 illustrate the concept of using blockchain to ensure firmware has not been tampered with during delivery to vehicles.
- Validating over-the-air sharing of critical information with roadside infrastructure (and vice versa) using blockchain as a verification source.
- Trusted ledger of maintenance activities performed on a vehicle throughout its life cycle.
- Provide continuous monitoring of in-vehicle firmware, software, and configuration parameters triggering alerts in the event of malicious or out-of-policy updates [39].
- Peer-to-peer critical software update, instead of solely relying on a central server by an automobile or component manufacturer and use of blockchain to validate authenticity of update.

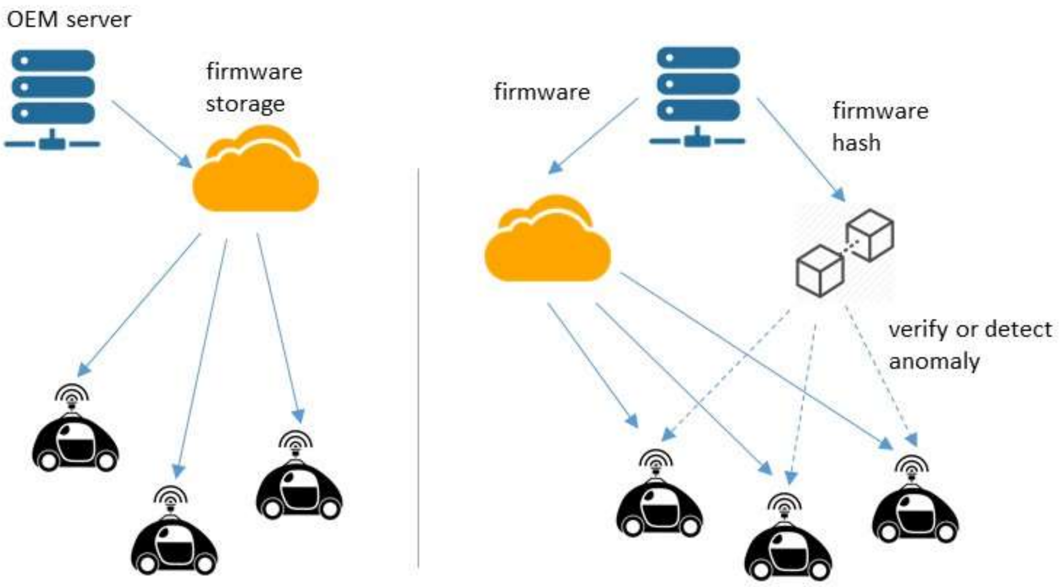


Figure 13. Using Blockchain to Verify Firmware Update over the Air.

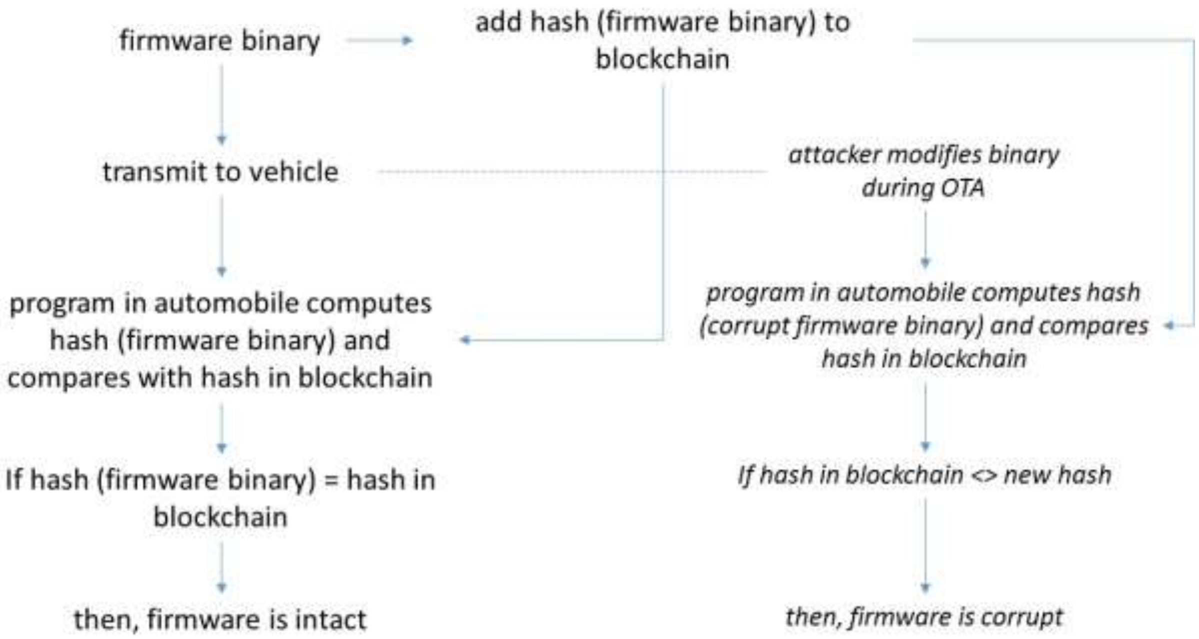

firmware binary
add hash (firmware binary) to blockchain
transmit to vehicle
attacker modifies binary during OTA
program in automobile computes hash (firmware binary) and compares with hash in blockchain
program in automobile computes hash (corrupt firmware binary) and compares hash in blockchain
If hash (firmware binary) = hash in blockchain
If hash in blockchain <> new hash
then, firmware is intact
then, firmware is corrupt

Figure 14. Using Firmware Hash in Blockchain to Verify Updates.

At present it is unclear from the literature search if any automobile manufacturers are pursuing blockchain based security implementations. One of the limitations of using public blockchain-based implementation is that the time required for participating mining nodes to come into consensus of transaction blocks is several minutes. This might not be suitable for critical updates that need to happen in few seconds. On the other hand, use of public blockchain for overnight updates would be appropriate.

For faster and critical updates, private or permissioned blockchains may be more suitable since time to consensus can be much quicker than public blockchain. However, it may become susceptive to attacks to the blockchain infrastructure itself due to a small number of mining nodes, if any. The other option is to form a consortium of auto and parts manufacturers and create a permissioned blockchain where invitation only participants operate mining nodes with financial incentives to keep the blockchain secured.

The question still remains as to what kind of firmware updates are suitable – local/direct updates at dealer, cloud based with encryption, or using blockchain technology. Also, auto manufacturers can learn a lot from how companies are planning to use blockchain or not to update firmware of Internet of Things devices, since over-the-air updates and the type of attacks are similar in both cases.

Reduce Tolling Cost and Increase Interoperability

Tolling agencies in the United States collect over $13 billion in annual revenue from 6,000 miles of roadway in 35 states and territories. Tolling in the United States is primarily collected from vehicles using transponders or toll tags – 37 million of them [40]. The transponder in a vehicle is activated by overhead antennas when it passes under a toll gantry, thereby reading its unique identification. A back office system receives identification data and it credits fees from a credit or debit card account associated with the identification number. Hence, tolling agencies have to pay credit card transaction fees to vendors such as Visa and MasterCard.

In 2016, North Texas Tollway Authority in Dallas Fort Worth region paid approximately $17 million in credit card transaction fees, which is 2.6 percent of the total revenue [41]. Assuming the rest of toll agencies in the United States pay credit card fees at the same rate as the tolling agency from the Dallas region, total credit card fees nationwide amount to approximately $340 million.

If tolling agencies allowed users to pay in Bitcoin or other cryptocurrencies, they would pay nearly zero transaction fees to a third party. Users would pay a miniscule amount of fees to miners to verify transactions. Figure 15 shows a comparison of traditional tolling vs. tolling using digital or cryptocurrency. Tolling agencies may have to pay some small percentage to convert the cryptocurrency to dollars. For example, Coinbase.com, a major cryptocurrency exchange and e-wallet charges approximately 1 percent to convert Bitcoin to dollars and vice versa [42]. Otherwise, savings to tolling agencies over time will be significant.

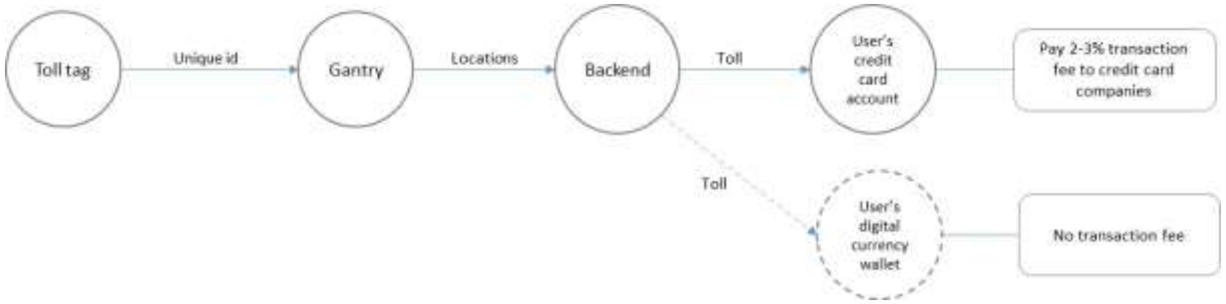

Toll tag
Unique id
Gantry
Locations
Backend
Toll
User's credit card account
Pay 2-3% transaction fee to credit card companies
Toll
User's digital currency wallet
No transaction fee

Figure 15. Comparison of Traditional Tolling vs. Digital Currency Based Tolling.

There is a lot of buzz about electronic wallets to store vehicle and owner identity, as well as to hold cryptocurrency for automated vehicles, and even regular vehicles to not only pay for tolling, but also for parking, shared ride, registration, etc. [43] [44]. Electronic wallets interact with blockchain-based systems (e.g., tolling, services, parts) to submit transactions to blockchain, initiate smart contracts, and other external applications. Project Oaken, a Dallas-based startup is developing a device that connects a car's controller area network bus with Ethereum blockchain to pay tolls with Ether (cryptocurrency) using a smart contract [45]. Project Oaken demonstrated that smart contracts running on blockchain can remove intermediaries (i.e., credit card companies) from toll collection systems. Obviously, the catch is that users have to have electronic wallets with some form of cryptocurrency. When more and more users have cryptocurrencies, this sort of electronic payment will be attractive for tolling agencies to implement.

Another blockchain application in tolling is interoperability in terms of payment processing. Many tolling agencies have adopted electronic toll collection systems, which are cashless solutions using radio frequency transponders connected to a customer's credit card account. Tolling agencies have been discussing a nationwide interoperable system in which customers have the ability to pay tolls on any participating toll facility in the country using a single account [46].

In that effort, tolling agencies have been consolidating back office payment processing support so that the customer's single account is in the system for multiple agencies to charge tolls. In blockchain and cryptocurrency enabled solutions, a customer's electronic wallet pays directly to the tolling agency's electronic wallet [47]. Hence, back office processing can eliminate payment processing.

Another solution is based on the customer's mobile device with a global positioning system. As a customer reaches certain locations on a tollway, the mobile device can pay from its electronic wallet cryptocurrency to the tolling agency's smart contract. Obviously, it requires the phone's global positioning system to have high accuracy so that the payment is triggered on time and at the desired locations. Figure 16 shows a high level illustration of the concept. The same digital currency wallet in a car can pay at multiple tolling jurisdictions without a need for interoperable transponders.

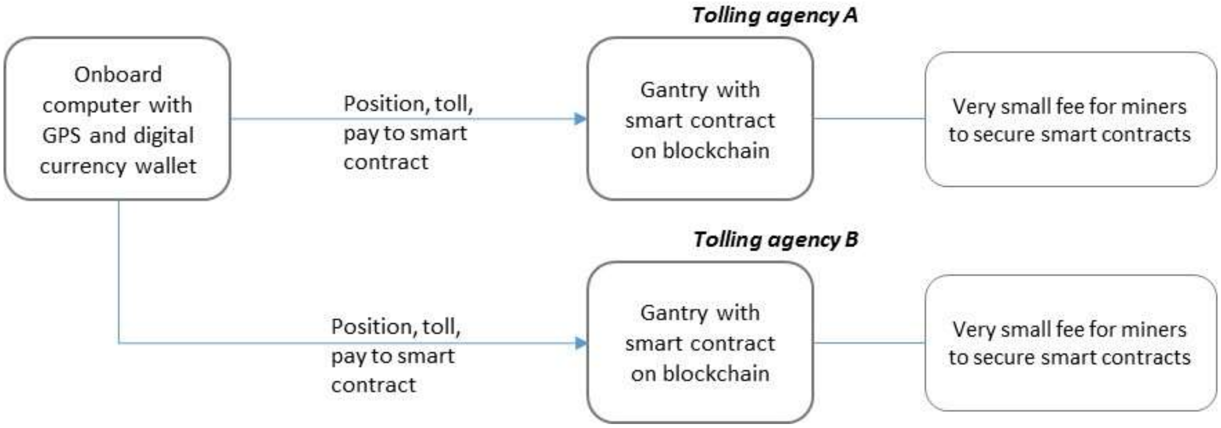

Tolling agency A
Onboard computer with GPS and digital currency wallet
Position, toll, pay to smart contract
Gantry with smart contract on blockchain
Very small fee for miners to secure smart contracts
Tolling agency B
Position, toll, pay to smart contract
Gantry with smart contract on blockchain
Very small fee for miners to secure smart contracts

Figure 16. Using Smart Contracts and Onboard Computer to Pay Tolls.

A similar concept of an onboard computer or electronic wallet in vehicles interacting with public blockchain to send transactions (i.e., payments) can be extended to store mileage information for mileage-based user fees and pay directly to smart contracts without a third party.

Electronic Wallets for Vehicles and Machines

Until now, much of the debates and discussions about automated vehicles have been related to mobility and safety. That is where testing and development is taking place. With so much technology being added to automated vehicles, they should be able to perform menial functions on their own without the vehicle owner’s input. For example, automated vehicles should be able to pay at electric charging stations, buy fuel, pay tolls, renew registration, get routine maintenance, pay for software updates, or get paid for ride-sharing, and much more.

For this to happen, there should be two critical components inside vehicles – the electronic wallet and the identification of vehicle and owner. Both pieces of information can be added by owners in the form of credit cards (for payment) and an electronic copy of vehicle registration, license plate, and perhaps, the owner’s driver license (for identification).

Instead of storing credit card information in vehicles as electronic wallets, cryptocurrency electronic wallets are much more secure, since public addresses of these wallets are not associated with the vehicle owner’s personal identification. Hence, public addresses can be encoded inside an in-vehicle app or even into a firmware.

Another problem that electronic wallets may solve is interoperability at tolling and electric charging stations. However, with the myriad cryptocurrencies available in the market, a true interoperable charging station is a big question mark unless vehicles store multiple electronic wallets with multiple currencies. On the vendor side, they should be willing to accept multiple cryptocurrencies, which may be a hassle to set up.

At the same time, the blockchain can be used to verify identity, age, level of insurance coverage, and the ability of the vehicle user to pay for the ride, while keeping all of this information anonymous and inaccessible to third parties. How comfortable owners will be about storing electronic copies of their identification and credit cards in their automated vehicles is a huge question mark.

Once electronic wallets with appropriate currencies are encoded in vehicles, they can autonomously pay for services mentioned earlier in this section. For example, the United States Postal Service explored a possibility of using smart contracts for its fleet to automatically order vehicle parts and pay manufacturers to install replacement parts and services based on the warranty written in smart contracts [48]. Expanding that concept, adding maintenance transactions (log) of vehicles in a blockchain could help consumers, insurance companies, and manufacturers to know true information about a vehicle's conditions throughout its lifecycle.

Auto insurance companies provide discounts to vehicle owners if they allow an onboard device to be installed in motorists' vehicles. Current onboard devices are black boxes. Vehicle owners do not know how they work and what kind of data is transmitting to their insurance companies. Even if the insurance company tells them what the transactions entail, owners do not see those transactions. This creates a trust issue.

On the other hand, if vehicles transmit mileage-related transactions directly to a public blockchain such as Ethereum, then the vehicle owner will know exactly what is being reported to the blockchain. Insurance companies and government also see the same transaction by virtue of the vehicle owner sharing its public key with them at his/her own will. Essentially, both motorists and insurance/government agencies can see the exact same transactions. This creates a level of trust between both parties. That is a huge value proposition with regard to privacy concerns.

Opportunities to use machine-to-machine payments without a third party is tremendous. Figure 17 illustrates vehicle-to-machine payments using smart contracts. They are triggered based on a change in location, service, and internal attributes such as parts failure. Besides paying tolls and mileage-based insurance and user fees, vehicles can pay for parking, as well as roadside transportation assets such as traffic signals. A new business model is feasible whereby the public can contribute without friction directly to installation and maintenance of other roadside assets.

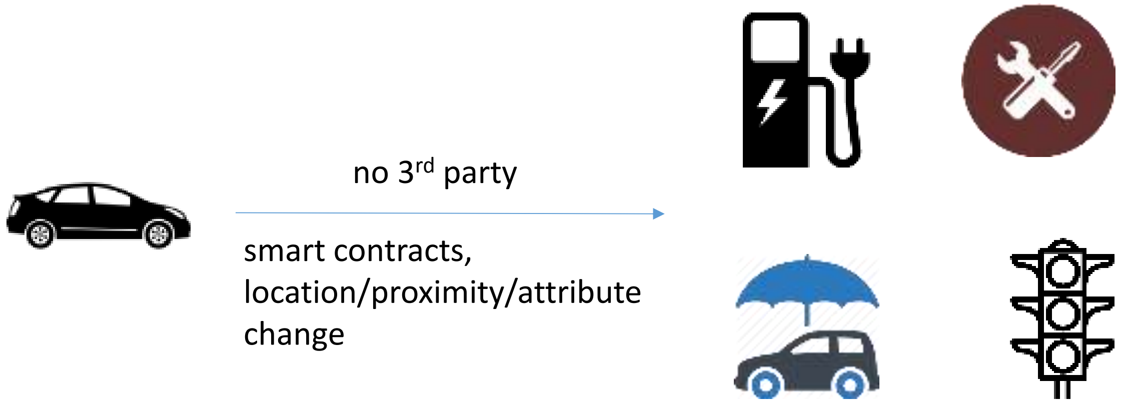


Figure 17. Vehicle to Machine Payments Using Smart Contracts.

Peer-to-Peer Shared Mobility in the Age of Automated Vehicles

Companies such as Uber, Lyft, and Didi provide riders with convenient and cost efficient access to mobility without the burdens of vehicle ownership. In return, they profit from vehicle owners who “share” their assets based on the value that they are able to bring riders into a single platform and aggregate resources. In essence, Uber and the likes operate as a central authority in aggregating vehicle information so that they can be presented to riders. Their other value proposition is ensuring vehicle and vehicle owners are legit and functionally capable, in a legal sense. These companies also manage payment between owner and riders for transparency and ease. And as with any central authority, they generate revenue by taking commissions from vehicle owners.

Some experts believe blockchain may turn the ride-sharing industry on its head because they argue that blockchain will remove a need for central authority [6] [49]. Hence, they argue that in the future, ride sharing companies that act as third party trusted sources will not be required, and instead peer-to-peer ride sharing companies will emerge. Drivers or vehicle owners will benefit by smaller commission fees paid to the third party. In the future with automated vehicles, can these vehicles and riders connect with each other directly without using a third party such as Uber or Lyft?

Another aspect of shared mobility is a new kind of ownership in which multiple users rent vehicles from a fleet owner or own or lease from auto companies. This might be beneficial for a population that cannot afford to solely lease cars for several years, but only need to use vehicles to commute back and forth from work. Appropriate names of this concept are “fractional ownership” or “time share of cars” or “sharing machines.” The concept of fractional ownership built over blockchain is illustrated in Figure 18.

In this scenario, users may utilize smart contracts to define ownership conditions, use blockchain to keep track of accurate mileage and even track vehicles without location being spoofed or tampered with. Vehicles would be able to upload mileage directly to a blockchain, where transactions will be timestamped and recorded in immutable blocks for auditing in case of fraud and insurance claims. Public or consortium blockchain can be used where mining nodes provide “proof of movement” instead of “proof of work” in Bitcoin, or “proof of stake” in Ethereum as verification of mileage by individual owners or drivers. While public blockchain will work as a decentralized trust system, service providers will help users find peers, find vehicle sellers, help define and deploy smart contracts, etc.

In this model, “trust” is out-sourced to a public blockchain. Trust will be maintained by a network and will even allow riders to pay directly to drivers using smart contracts through payment gateways, instead of holding payment on behalf of drivers like current ride-sharing companies do. Hopefully, this new model will increase payments to drivers since service providers do not have the burden of “trust.”

General Motors is working on a proof of concept of fractional ownership in its Maven platform [50]. Toyota through a blockchain-mobility.org alliance is partnering with several startups for a proof of concept, which includes an open ecosystem not dominated by a single platform but an auto manufacturer agnostic system [51]. In this open ecosystem, any asset owners as well as auto manufacturers, can put their cars for rental or fractional ownership. Using blockchain and immutability of transactions consisting of mileage/usage, the system and users have a confident usage information of vehicles, which is key in building a network of trust among users.

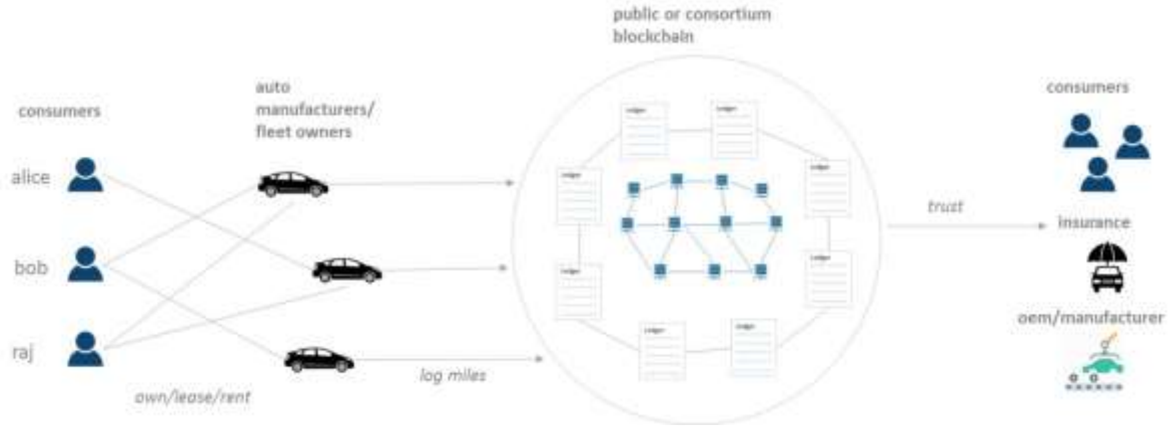


Figure 18. Fractional Vehicle Ownership Built over Public or Consortium Blockchain.

Scaling Internet of Things and Digital Transportation Assets

More and more vehicles are connected to the internet and other wireless networks. In connected transportation, vehicles communicate with a variety of field devices that are connected to wireless networks and the internet for communication with centralized servers and vehicles. With onboard computers and persistent communication with other objects, vehicles and roadside devices will eventually become types of Internet of Things devices. Hence, the definition of Internet of Things devices not only includes home and personal devices such as refrigerators, thermostats, etc., but also connected vehicles, roadside devices, and industrial sensors.

The biggest challenge facing the Internet of Things is coming from the very architecture of the current deployment system, which is based on a centralized model known as the client-server model [52]. The client-server model is used in updating device firmware and managing authenticity and integrity of devices. However, with the growth of the Internet of Things devices reaching billions, the centralized client-server models will soon become bottlenecks, as well as unsecure and subject to single points of failure.

On the contrary, a decentralized and peer-to-peer approach would eliminate single points of failure, creating a more resilient ecosystem for devices to run on [52]. In a peer-to-peer approach, Internet of Things devices, instead of using a centralized server to receive updates or authentication, would use nearby "peer" devices and nodes to update firmware, relieving network bandwidth.

As described in the section “Securing automated and connected vehicles,” firmware updates and transactions can be performed using blockchains. The ledger used in blockchain is tamper-proof and cannot be manipulated by malicious actors because it does not exist in any single location, and man-in-the-middle attacks cannot be staged because there is not any single thread of communication that can be intercepted.

Internet of Things devices can also be empowered to autonomously execute smart contracts such as agreements, payments, and barters with peer devices by searching for their own software updates, verifying trustworthiness with peers, and paying for and exchanging resources and services. This allows them to function as self-maintaining, self-servicing devices. The power to autonomously trade with other devices opens up whole new business models [53].

Internet of Things ecosystems are very diverse in terms of device capabilities, functions, manufacturers, etc. Blockchain storage or transaction is additive, meaning blocks continue to grow as their usage grows and more and more transactions are added. With billions of Internet of Things devices creating trillions of transactions, the size of blockchains and reaching consensus would require a lot of time and very high computing power.

Barriers to Entry and Deployment Challenges

Scalability Issues

In any blockchain, the number of blocks grows over time as usage grows. For example, the size of the entire Bitcoin blockchain has reached 142 gigabytes from a few megabytes in 2009 (blockchain.info), which means reaching consensus requires more and more computing resources. Another public blockchain, Ethereum's size has increased to 32 gigabytes (Fast sync) in less than two years.

Bitcoin takes roughly 10 minutes to confirm transactions and can process less than 10 of them per second, while Visa can confirm 2,000 transactions per second. With the rise in transactions and price of cryptocurrencies, the cost of confirmation is also increasing.

There are discussions about increasing the block size, sharding, different consensus algorithms, and using a faster network (i.e., Lightning network) to move transactions faster between peers in the network. The good news is, because public blockchains are open source, anybody can create a better process/algorithm and fork them (make them available) as improved blockchains. The open source community saw similar phenomena with Linux, and now it is one of the most secure and widely used operating systems.

While immutability and mining provides security, current public blockchains are not fast enough for low latency (microseconds) transactions. Most likely, early deployment of blockchain in mobility use cases will occur where transaction settlements do not require microseconds or several seconds, such as trade finance, document and identity verification in logistics, and even mileage reporting.

Business Challenges

Researchers believe implementation of blockchain in public transportation projects such as connected vehicles and the Internet of Things for critical transportation infrastructure has an uphill battle to climb. This is mostly because public transportation, and even transit projects, are largely budgeted and funded by local, state, and federal agencies. Knowledge about blockchain is limited among transportation planners and policy makers.

For the next few years, implementation of blockchain will be limited to innovative idea projects and perhaps demonstration projects. Researchers think blockchain will see more deployments, beyond demonstrations, in private space before they appear in government-funded projects. Obviously, there will be exceptions.

That is why researchers recommend more research and demonstration projects in order to analyze benefits and technical challenges to implement blockchain technology in public transportation projects.

Perception Barriers

The concept of a network of computers taking over “trust” is so alienating that many will simply disregard it [6]. Perception about blockchain’s association with Bitcoin and later being falsely accused of being the currency of choice for illegal activities simply makes things worse. Stigma from Silk Road fiasco remains. However, recent popularity of cryptocurrency, rise in investment in blockchain startups, and press releases about big corporations joining blockchain alliances have helped reduce the stigma.

Path to Deploy Transportation Applications on Blockchain

In line with recently discovered foundational technologies, startups are in the forefront of developing customer-focused applications utilizing blockchain. They are supported by investments from bigger firms and even crowdsourcing. Some companies are in “let’s wait” mode. Others are already working on proof of concepts and proof of value projects by themselves or with other startups. Individuals who TTI researchers interviewed mentioned that they are not aware of any firms that have fully integrated or implemented blockchain technology in their day-to-day operations. That is because they believe the technology has not matured enough.

Proof of concepts examine if the technology or application works or not and identify what is required to take it for wider adoption. Proof of value examines if an application can create significant value (monetary or otherwise) to the organization and/or its customers.

In the coming years, the industry will hear of success and failure of these proof of concepts and proof of value projects. Irrespective of the industry type, blockchain deployment would occur in three possible forms [54]:

- Entirely new business models and new opportunities that may or may not challenge the incumbents. Examples include fractional ownership of cars and trucks that will challenge current ride-sharing companies. Other applications include electronic wallets for vehicles, document registry, notary, asset transfer, etc.
- Improved processes with fall back mechanisms already in place. Examples include transaction settling in supply chain and trade finance. If a blockchain-based process does not work, they can still do it in old ways without hampering the goods movement.
- Abandon current design and adopt blockchain right away. Examples include over-the-air updates and security of Internet of Things devices. Adoption of blockchain instead of traditional client-server models has dragged security implementation of Internet of Things devices. The cyber-attack in late 2016 in which home devices were turned into zombie computers has hyped interest among Internet of Things service providers, including auto manufacturers, to adopt blockchain and abandon client-server architecture.

Implementation of blockchain by private companies in customer-focused applications is a whole different ball game compared to implementing in public transportation projects. Implementing radically new technology in publicly funded projects is a much steeper climb because of bureaucratic protocols, regulations, funding, and other reasons. However, research and demonstration projects funded by public transportation agencies should begin in the next year onwards.

With regard to the above implementation models, researchers think the second model is a safer bet for transportation agencies. With heightened awareness of the Internet of Things and cybersecurity of transportation infrastructure, government may be interested in the third model as well.

Hype around Blockchain

Global investments in blockchain-related startups exceeded US $2 billion in 2016 and 2017. Major banks such as JP Morgan, Barclays, and Wells Fargo are working on proofs of concept either in-house or through collaboration with startups. Hype around blockchain has also fueled speculation of cryptocurrencies in that they fluctuate irrationally. It has become difficult to find global tech companies, supply chain, finance, retail, and logistics companies that are not working on a proof of concept or thinking about it. Big tech companies such as IBM and Microsoft have introduced blockchain development platforms. Developers can create and deploy their own private blockchain and layer it with web applications and user interface.

Another evidence of hype is that blockchain has managed to suddenly appear at the peak of Gartner's 2016 hype cycle, thought it was not mentioned in 2015 hype cycle [55] [56]. Fall from that peak will certainly mean that many startups working on blockchain applications will fold due to lack of traction. Many proof of concepts will never be implemented. That is normal in the natural course of technology innovation. Because, what will emerge from this "purge" is robust, acceptable applications and use cases of blockchain that will greatly benefit everyday users and companies. This will also lead to technological maturity.

Government's Role and Opportunities

Historically, governments have played a critical role in creating foundational technologies, such as the internet and mobile telecommunication, and in that process became the biggest consumers of these technologies they helped to flourish. Blockchain seems to be an exception to that trend. Government had little or no role in the initial development of Bitcoin and blockchain. However, over the last two years, as discussion about blockchain's potential emerged, governments and public sector entities have begun to show keen interest in deploying it to "upgrade" government services.

Governments in Georgia (the country) and Honduras are working on proofs of concept to use blockchain to register land titles and validate property-related transactions. The United Kingdom is testing welfare payments using blockchain. Estonia has already implemented identity management, e-voting, and electronic health records [57]. Sweden is testing blockchain-based land registry, and Dubai wants all its government services to be powered by blockchain by 2020 [58]. The Chinese government wants to be a leader in blockchain research and development, with investment in a research institute that employs over 100 blockchain developers [59].

The United Kingdom government's Office of Science through its Chief Scientific Advisor wrote extensively about opportunities to apply blockchain in improving government services and recommended that the government's digital platform could include blockchain [60]. A few of these opportunities are as follows:

- Protection of critical infrastructure against cyberattacks.
- Reduced costs of protecting citizens' data.
- Reduced market friction, making it easier for small/medium companies to interact with government services.

Across the Atlantic, several US government institutions are already getting their feet wet with blockchain. Last year, Department of Homeland Security awarded small business grants to four startups working in blockchain-based security products [61]. Austin, Texas-based startup Factom received a grant from the department to prevent spoofing of its cameras at the border used to monitor flow of goods and people [62]. The United States Postal Service released a report outlining blockchain's potentials to improve its operation in remittance, identity management, device management, and supply chain [63].

Government agencies involved with transportation and mobility, such as the National Highway Traffic Safety Administration (NHTSA), the Federal Highway Administration (FHWA), Departments of Motor Vehicles (DMVs), and State Departments of Transportation can also initiate proof of concepts and proof of value to explore benefits of blockchain in providing frictionless public service. NHTSA and FHWA may be interested in cyber security of automated and traditional vehicles and use of decentralized trust protocol for identity management in connected infrastructure space. DMVs may find value in maintaining a vehicle identification, chain of custody of vehicles, driver identification in blockchain, in order to create a frictionless system. Air traffic regulation agencies such as Federal Aviation Administration might be interested in drone registry and airspace management [64] .

Besides creating opportunities and taking part in development of blockchain, government may be called in to regulate blockchain because of its association with cryptocurrency. At the moment, it is unclear how and which entity will do this. However, one thing is clear that the government and regulatory bodies are used to regulating legal entities that provide third party trust services (e.g., trading platforms, notaries, ride-hailing services), but certainly not a network of computers owned by no one and spread across multiple countries and jurisdictions [54].

The complexity of blockchain and cryptocurrency provides a particular challenge for policy makers considering regulation [6]. In that, blockchain advocates see parallels between blockchain and the Internet. Regulations concerning the internet did not happen until it matured [54].

Conclusions

Blockchain technology’s potential in creating frictionless and secured applications is promising because of its decentralized trust principles. It has widespread use in sectors that use intermediaries; mobility and logistics are no different. As blockchain matures, new business models will emerge such as fractional ownership of assets. These new business models have the potential to disrupt existing ones. For example, fractional ownership may seriously challenge current ride sharing models.

Disruption of intermediaries or decentralization of trust and machine-to-machine payments are innovative as well as disruptive concepts. Both concepts have major implications, not only in building customer-facing frictionless mobility and logistics applications, but also governance and leadership for public agencies.

Policy Considerations

Researchers propose four policy considerations for public agencies in order to facilitate innovation in transportation using blockchain technology:

More formal dialogue about blockchain's benefits and challenges – Twelve out of 19, or 63 percent of chief information officers of various state governments said they were investigating blockchain through formal discussions [65]. Set for July 18th 2017, the United States Federal Blockchain Forum is being organized by the General Services Administration and the State Department. The goal, according to an announcement, is to develop a six-month plan for how agencies can collaborate to achieve their goals and support the creation of shared services for blockchain technology [66]. Because blockchain is a relatively new technology, public agencies and technology vendors would greatly benefit from formal dialogues in order to forge synergetic paths forward and debate about blockchain's suitability in improving public service.

Fund proof of value and research projects to reduce friction in public services in transportation – Blockchain technology is in early stages with regard to wider adoption. As with any new foundational technology, it will take several years if not decades to be ubiquitous. However, it provides unique opportunities for public agencies to be early adopters and gradually work around its benefit to improve public services affecting transportation and mobility, instead of re-building the entire service later. Examples include: using blockchain for driver licensing and asset transfers, connected vehicle security, and sharing assets between public agencies.

Provide legal pathways for wider adoption of blockchain in transportation – There are debates about appropriateness of public vs. private and permissionless vs. permissioned blockchains for government services. Most likely, government applications will be built around some form of public or permissioned blockchains. However, the private sector will continue to build applications on permissionless blockchain because of security and open access. Permissionless blockchains need cryptocurrency as financial incentive to secure them. Any legislation that criminalizes cryptocurrencies will stifle innovation for widespread use of permissionless blockchain, which are used to build applications on top of those blockchains – for example building enterprise and public smart contracts on Ethereum. There is also a need to ensure smart contracts are legally enforceable. Smart contracts allow machine-to-machine payments and enforce legal terms and conditions between parties by coding them. Arizona recently passed HB 2417 legalizing smart contracts, as did Vermont [67].

Provide stewardship for innovation – Provide stewardship, collaboration platforms, and incentives to innovate. Illinois recently passed a bi-partisan House Resolution 120 to create a joint task force to request the government to create an inter-governmental blockchain task force to provide a more efficient and regulatory-friendly ecosystem for blockchain development firms, research organizations and businesses [68].

References

[1] S. Nakamoto, "Bitcoin: Peer-to-peer Electronic Cash System," bitcoin.org, 2008.

[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, 2015.

[3] J. Brito and A. Castillo, "Bitcoin: A Primer for Policymakers," George Mason University, 2013.

[4] BitFury Group, "Incentive Mechanisms for Securing the Bitcoin Blockchain," BitFury Group Limited, 2015.

[5] Bitnodes, "Global Bitcoin Distribution Nodes," Bitnodes, 26 April 2017. [Online]. Available: https://bitnodes.21.co/. [Accessed 26 April 2017].

[6] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, New York: Penguin Random House , 2016.

[7] D. Leger, "How FBI brought down cyber-underworld site Silk Road," USA Today, 21 October 2013. [Online]. Available: https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/. [Accessed 14 April 2017].

[8] M. Jackson, "Bitcoin's Big Challenge in 2016: Reaching 100 Million Users," Coindesk, 01 January 2016 . [Online]. Available: http://www.coindesk.com/2016-bitcoin-challenge-100-million-users/. [Accessed 02 April 2017].

[9] Blockchain.info, "Confirmed Transactions Per Day," Blockchain Luxembourg SARL, 03 April 2017. [Online]. Available: https://blockchain.info/charts/n-transactions?timespan=all. [Accessed 03 April 2017].

[10] C. Bovaird, "5 Factors Experts Say Drove Bitcoin's Rise to $700," Coindesk, 13 June 2016. [Online]. Available: http://www.coindesk.com/five-factors-driving-bitcoin-price-demand/. [Accessed 05 April 2017].

[11] M. Swan, Blockchain, O'Reilly Media, 2015.

[12] G. Greenspan, "Blockchains vs centralized databases," 17 March 2016. [Online]. Available: https://www.linkedin.com/pulse/blockchain-vs-centralized-trade-off-gideon-greenspan. [Accessed 12 April 2017].

[13] Bitfury Group, "Public versus Private Blockchains," Bitfury Group Limited, 2015.

[14] TradeBlock.com, "Mapping Bitcoin Adoption: A Global Perspective In 11 Graphs," 19 May 2013. [Online]. Available: https://tradeblock.com/blog/mapping-bitcoin-adoption-a-global-perspective/. [Accessed 10 April 2017].

[15] Quandl.com, "Bitcoin Median Transaction Confirmation Time," 10 April 2017. [Online]. Available: https://www.quandl.com/data/BCHAIN/ATRCT-Bitcoin-Median-Transaction-Confirmation-Time. [Accessed 11 April 2017].

[16] Y. Ghalim, "Why we should drop the whole “Bitcoin vs blockchain” discussion," Medium Corporation, 7 October 2015. [Online]. Available: https://medium.com/@YacineGhalim/why-we-should-drop-the-whole-bitcoin-vs-blockchain-discussion-e3e38e9a5104. [Accessed 6 April 2017].

[17] G. Greenspan, "Why Many Smart Contract Use Cases Are Simply Impossible," 16 April 2016. [Online]. Available: http://www.coindesk.com/threesmartcontractmisconceptions/. [Accessed 12 April 2017].

[18] J. Stark, "Introduction to Smart (Legal?) Contracts," Medium Corporation, 18 April 2016. [Online]. Available: https://medium.com/@jjmstark/introduction-to-smart-contracts-part-1-8f191a324d0a. [Accessed 12 April 2017].

[19] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," December 2013. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper. [Accessed 14 April 2017].

[20] G. Greenspan, "Smart contracts: The good, the bad and the lazy," 02 November 2015. [Online]. Available: http://www.multichain.com/blog/2015/11/smartcontractsgoodbadlazy/. [Accessed 12 April 2017].

[21] N. Ayton, "Seven Myths About Blockchain," Innovation Enterprise, 28 October 2017. [Online]. Available: https://channels.theinnovationenterprise.com/articles/7-myths-about-blockchain. [Accessed 14 April 2017].

[22] Y. Ghalim, "Why we should drop the whole “Bitcoin vs blockchain” discussion," Medium Corporation, 07 October 2015. [Online]. Available: https://medium.com/@YacineGhalim/why-we-should-drop-the-whole-bitcoin-vs-blockchain-discussion-e3e38e9a5104. [Accessed 10 April 2017].

[23] D. Hesketh, "Weaknesses in the Supply Chain," *World Customs Journal*, vol. 4, no. 2, pp. 40-20, 2010.

[24] L. Parker, "Bank of America Merrill Lynch explores using a blockchain for trade finance," BraveNewCoin, 02 March 2016. [Online]. Available: https://bravenewcoin.com/news/bank-of-america-merrill-lynch-explores-using-a-blockchain-for-trade-finance/. [Accessed 23 April 2017].

[25] B. Sahay, "Understandng Trust in Supply Chain Relationships," *Industrial Management and Data Systems,* vol. 103, no. 8, pp. 553-563, 2003.

[26] A. Earls, "Blockchain not a panacea for supply chain traceability, transparency," TechTarget, December 2016. [Online]. Available: http://searchmanufacturingerp.techtarget.com/feature/Blockchain-not-a-panacea-for-supply-chain-traceability-transparency. [Accessed 24 April 2017].

[27] I. Allison, "Tokio Marine and NTT DATA complete blockchain-based cargo insurance certificates," International Business Times, 24 April 2017. [Online]. Available: http://www.ibtimes.co.uk/tokio-marine-ntt-data-complete-blockchain-based-cargo-insurance-certificates-1618300. [Accessed 25 April 2017].

[28] J. Smith, Interviewee, *Founder, BlockFreight.* [Interview]. 20 June 2017.

[29] L. Stone, Interviewee, *Co-founder, Symbiont.* [Interview]. 13 April 2017.

[30] I. Allison, "Skuchain: Here's how blockchain will save global trade a trillion dollars," International Business Times, 08 February 2016. [Online]. Available: http://www.ibtimes.co.uk/skuchain-heres-how-blockchain-will-save-global-trade-trillion-dollars-1540618. [Accessed 24 April 2017].

[31] M. Casey and P. Wong, "Global Supply Chains Are About to Get Better, Thanks to Blockchain," Harvard Business Review, 13 March 2017. [Online]. Available: https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain. [Accessed 24 April 2017].

[32] S. Ponoth, Interviewee, *General Manager at Bristlecone Labs.* [Interview]. 05 June 2017.

[33] C. Bordonali, S. Ferraresi and W. Richter, "Shifting Gears in Cyber Security for Connected Cars," McKinsey & Company, 2017.

[34] Intel Security, "Automotive Security Best Practices," Intel, 2016.

[35] Wikipedia, "2016 Dyn cyberattack," Wikipedia, 01 May 2017. [Online]. Available: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack. [Accessed 08 May 2017].

[36] A. Dorri, M. Steger, S. Kanhere and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," ARXIV, 2017.

[37] N. Bishop, "Enterprise Intelligence Brief: Three Experts Discuss Blockchain in Cybersecurity," Security Intelligence, 14 March 2017 . [Online]. Available: https://securityintelligence.com/enterprise-intelligence-brief-three-experts-discuss-blockchain-in-cybersecurity/. [Accessed 08 May 2017].

[38] M. Burgess, "Blockchain technology will help protect your autonomous car," Wired UK, 23 June 2016. [Online]. Available: http://www.wired.co.uk/article/mark-walport-chief-scientific-advisor-blockchain. [Accessed 28 April 2017].

[39] M. Ruubel, "AssureNet and Guardtime Implement Blockchain based Connected Car Liability Management," Guardtime.com, 21 September 2016. [Online]. Available: https://guardtime.com/blog/assurenet-and-guardtime-implement-blockchain-based-connected-car-liability-management. [Accessed 10 May 2017].

[40] International Bridge, Tunnel, and Turnpike Association, "2015 Report on Tolling in the United States," IBTTA, Washington DC, 2015.

[41] North Texas Tollway Authority, "Final Budget - 2017," NTTA, Dallas, 2017.

[42] Coinbase.com, "Coinbase Pricing & Fees Disclosures," Coinbase.com, 18 April 2017. [Online]. Available: https://support.coinbase.com/customer/portal/articles/2109597-buy-sell-bank-transfer-fees. [Accessed 24 April 2017].

[43] A. Butler, "Why Your Driverless Vehicle May Use a Blockchain," LinkedIN, 02 March 2017. [Online]. Available: https://www.linkedin.com/pulse/why-your-driverless-vehicle-may-use-blockchain-anthony-butler. [Accessed 27 April 2017].

[44] P. Rizzo, "Blockchain Wallets Are Coming (Maybe Soon) to a Car Near You," CoinDesk, 22 January 2017. [Online]. Available: http://www.coindesk.com/blockchain-wallets-coming-maybe-soon-car-near/. [Accessed 27 April 2017].

[45] L. Silva, "Project Oaken Puts A Tesla On The Blockchain," ETH News, 07 January 2017. [Online]. Available: https://www.ethnews.com/project-oaken-puts-a-tesla-on-the-blockchain. [Accessed 27 April 2017].

[46] International Bridge, Tunnel, and Turnpike Association, "Status of Toll Interoperability – September 2016," 2016. [Online]. Available: http://ibtta.org/sites/default/files/documents/Interoperability/IBTTA%20White%20Paper%20Toll%20Interoperability%20September%202016.pdf. [Accessed 30 April 2017].

[47] M. Milligan, "A Unified Tolling Network," Milligan Partners LLC, 2016.

[48] Office of Inspector General: United States Postal Service, "Blockchain Technology: Possibilities for the U.S. Postal Service," United States Postal Service, 2016.

[49] P. Filippi, "What Blockchain Means for the Sharing Economy," Harvard Business Review, 15 March 2017. [Online]. [Accessed 15 May 2017].

[50] M. G. M. Mahmoud, Interviewee, [Interview]. 26 May 2017.

[51] C. Bellinger and J. Lappin, Interviewees, *Toyota Research Institute.* [Interview]. 31 May 2017.

[52] A. Banafa, "A Secure Model of IoT with Blockchain," Technology Review, 05 January 2017. [Online]. Available: https://www.technologyreview.com/s/603298/a-secure-model-of-iot-with-blockchain/. [Accessed 23 May 2017].

[53] IBM Institute for Business Value, "Device Democracy: Saving the Future of the Internet of Things," IBM, 2015.

[54] W. Mougayar, The Business of Blockchain, New Jersey: John Wiley and Sons, 2016.

[55] Gartner Inc., "Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage," Gartner, 16 August 2016. [Online]. Available: https://www.gartner.com/newsroom/id/3412017. [Accessed 25 November 2017].

[56] Gartner Inc., "Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor," Gartner Inc., 18 August 2015. [Online]. Available: https://www.gartner.com/newsroom/id/3114217. [Accessed 24 November 2017].

[57] T. W. Kwang, "How are Governments Using Blockchain Technology," Enterprise Innovations, 14 March 2017. [Online]. Available: https://www.enterpriseinnovation.net/article/how-are-governments-using-blockchain-technology-1122807855. [Accessed 13 June 2017].

[58] The Economist, "Governments may be big backers of the blockchain," The Economist, 01 June 2016. [Online]. Available: http://www.economist.com/news/business/21722869-anti-establishment-technology-faces-ironic-turn-fortune-governments-may-be-big-backers. [Accessed 13 June 2017].

[59] M. Yeung, Interviewee, *Director of Operations, Jiangsu Huaxin Blockchain Research Institute.* [Interview]. 07 April 2017.

[60] UK Government Chief Scientific Adviser, "Distributed Ledger Technology: Beyond Block Chain," UK Government Office of Science, London, 2016.

[61] L. Parker, "U.S. Department of Homeland Security funds four blockchain companies developing new cyber security technology," Bravenewcoin.com, 17 August 2016. [Online]. Available: https://bravenewcoin.com/news/u-s-department-of-homeland-security-funds-four-blockchain-companies-developing-new-cyber-security-technology/. [Accessed 13 June 2017].

[62] Econotimes, "US DHS tests blockchain to track cross-border activities," Econotimes.com, 11 January 2017. [Online]. Available: http://www.econotimes.com/US-DHS-tests-blockchain-to-track-cross-border-activities-482955. [Accessed 14 June 2017].

[63] United States Postal Service Office of Inspector General, 23 May 2017. [Online]. Available: https://www.uspsoig.gov/sites/default/files/document-library-files/2016/RARC-WP-16-001.pdf. [Accessed 14 June 2017].

[64] B. Ari and P. Bidewell, Interviewees, *Applied Blockchain.* [Interview]. 28 April 2017.

[65] T. Douglas, "Blockchain a 'Next Big Transformational Technology' in Government," Govtech.com, 16 May 2017. [Online]. Available: http://www.govtech.com/security/Blockchain-a-Next-Big-Transformational-Technology-in-Government.html. [Accessed 17 July 2017].

[66] W. Zhao, "US Government Organizes 'Federal Blockchain Forum' for July," Coindesk.com, 29 June 2017. [Online]. Available: http://www.coindesk.com/us-government-organizes-federal-blockchain-forum-july/. [Accessed 16 July 2017].

[67] L. Parker, "US States working on blockchain legislation in 2017," Bravenewcoin.com, 02 April 2017. [Online]. Available: https://bravenewcoin.com/news/us-states-working-on-blockchain-legislation-in-2017/. [Accessed 17 July 2017].

[68] J. Young, "US State of Illinois Prepares to Regulate Blockchain Industry," Cointelegraph.com, 04 July 2017. [Online]. Available: https://cointelegraph.com/news/us-state-of-illinois-prepares-to-regulate-blockchain-industry. [Accessed 17 July 2017].