PRIVATE BLOCKCHAINS IN AUTOMOTIVE SAFETY

Greg Bohl, John F. Dickson, PhD

Abstract

Blockchain has proven to be successful in decision making using the streaming live data in various applications, it is the latest form of Information Technology. There are two broad Blockchain categories, public and private. Public Blockchains are very transparent as the data is distributed and can be accessed by anyone within the distributed system. Private Blockchains are restricted and therefore data transfer can only take place in the constrained environment. Using private Blockchains in maintaining private records for managed history or governing regulations can be very effective due to the data and records, or logs being made with respect to particular user or application. The Blockchain system can also gather data records together and transfer them as secure data records to a third party who can then take further actions. In this paper, an automotive road safety case study is reviewed to demonstrate the feasibility of using private Blockchains in the automotive industry. Within this case study anomalies occur when a driver ignores the traffic rules. The Blockchain system itself monitors and logs the behavior of a driver using map layers, geo data, and external rules obtained from the local governing body. As the information is logged the driver's privacy information is not shared and so it is both accurate and a secure system. Additionally private Blockchains are small systems therefore they are easy to maintain and faster when compared to distributed (public) Blockchains.

1. Introduction

The Blockchain is a computational paradigm which initially emerged with the Bitcoin protocol in 2008 [11]. Blockchains were first used in Bitcoin as an accounting system to verify ledgers and complete transactions made by anyone within a network of nodes. It also solved the problem of double spending, making it the premier method of undisputable records. Private Blockchains became popular in systems that required a controlled network (one company), unlike public Blockchains that are uncontrolled (multiple companies or sources) [12]. Private Blockchains also maintain the data integrity and security within the Blockchain itself. In private Blockchains writing new data is maintained private, which facilitates secure data in one node without overlapping other nodes for validation. Thereby, a network of systems is not required.

2. Literature Review

Blockchains are increasing in popularity in various applications, more specifically private Blockchains verses public Blockchains. Various studies are available in literature with a primary focus on financial and healthcare markets. A few of the studies have been reviewed for this paper. Namely:

A Blockchain system for secured health care data used to improve the quality of a healthcare system is discussed in "Healthcare Data Gateways" [1]. It integrates all healthcare data in a secured environment with sharing capabilities. "Blockchain-Based Architectures for the Internet of Things: A Survey." [2] briefs Blockchain applications in the context of the Internet of Things (IoT). Additionally the paper considers Blockchain for privacy engineering, security, and micro-payments. "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money."[3] reviews all Blockchain technologies including permission Blockchain, permissionless Blockchain, public and private Blockchains. Cutting edge technologies of Blockchains and its working principle is explained in "Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges." [4]. The paper illustrates how applications vary from supply chain, banking and voting industry. A connected vehicle infrastructure is reviewed in "Driving the Blockchain - Why Bitcoin matters in Automotive" [8]. The paper reviews how Blockchains can be used in automotive, however they are public Blockchains connecting all the cars in a given area. The author also addresses how hacking within a car's connected network can also be prevented using Blockchains.

3. Blockchains and Databases

Databases are developed and used for many purposes and industries with features and functions developed for those uses. Some database examples are Relational Database Management Systems (RDBMS), columnar databases, key value storage, document databases, and graph databases. Databases can be distributed or part of a centralized system. A modification made to the data itself may not always reflect across the entire database or database system unless a proper key structure or a master database is used. However, the use of Blockchains can overcome this difficulty by monitoring the data consistency throughout the system before making any decisions. Therefore a Blockchain can be thought of as a database with additional

functionality which adds a row and then validates against the custom rules within the chain so the new block can be added or removed from the chain.

4. What is Blockchain

A Blockchain can be thought of as just another data structure where the data is logically put together and stored, but yet with a very high level of integrity. Examples of other, more common data structures include comma separated values, text files, images, and databases with rows and columns.

The blocks that make up a Blockchain can be referred to as pages in a book, a group of blocks then constitute a Blockchain. However, unlike a book, the set of blocks in a Blockchain can continuously grow thereby maintaining an infinite ordered set of blocks, or records. Each block also contains a timestamp and a link (hash) to the previous block linking the two. The links then form a chain and the iterative process confirms the integrity of the previous block and therefore the entire chain.

Each block in a Blockchain has two components, contents (transactions) and the header (block). The content is the data from a source and the header contains the data about the block itself. The header may also refer to link or reference between two or more blocks. The data can be ordered in number of ways, like block numbers (see figure 1).

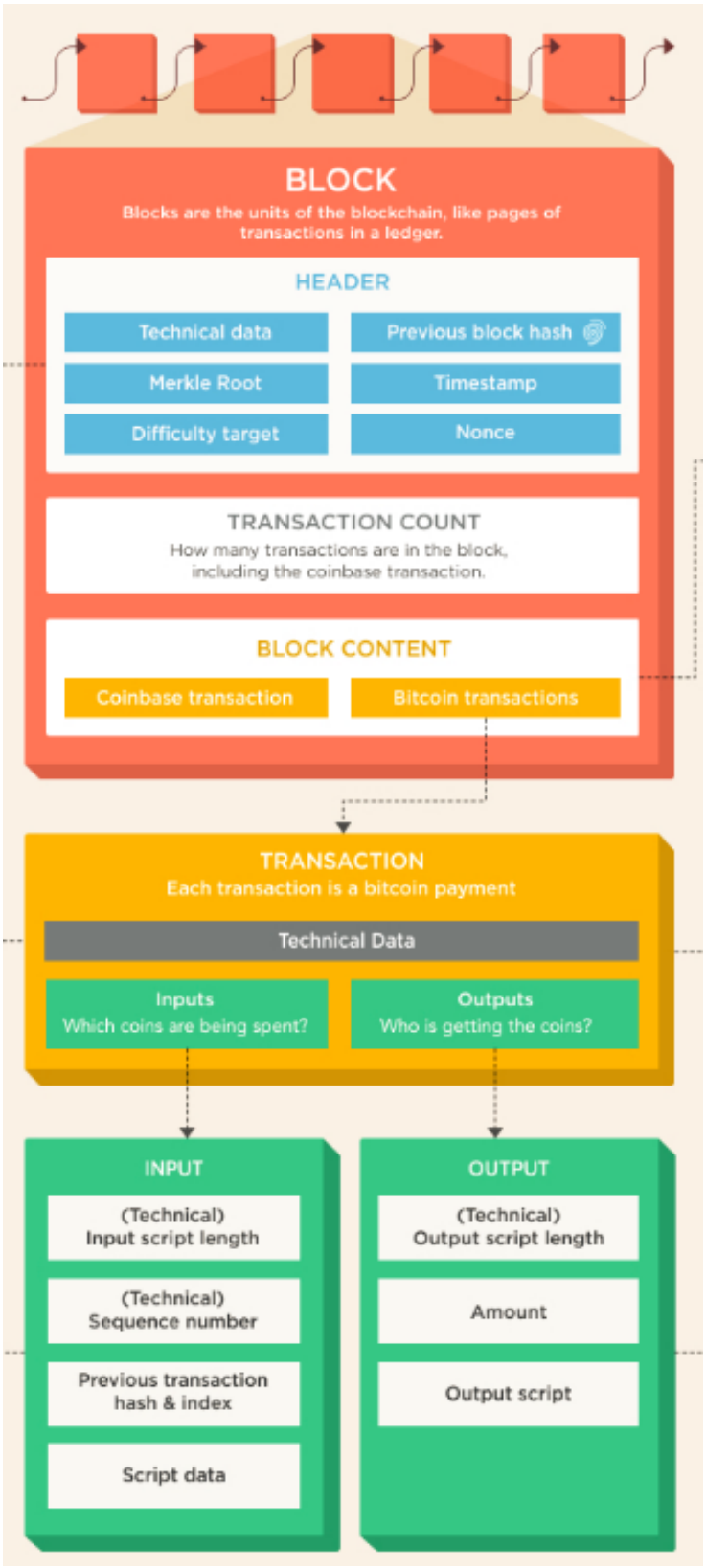

Figure 1: General BitCoin Blockchain Architecture [10]

4.1 Public Blockchains

A public Blockchain is a Blockchain operating on a distributed network of nodes with data that anyone in the world can read, validate, or remove from the system. The public Blockchains are secured by using cryptographic verification mechanisms such as the data source, data registry time and location. Consortium Blockchains are a classification of private Blockchains in which a group of users participate in data transactions. The nodes within the network are preselected and assigned to a selected group. Users belonging to one group can approve the transaction instead of the whole population as in the traditional public Blockchains.

4.1.1 Disadvantages of Public Blockchains

A key disadvantage with public Blockchains are the rules defined in the system as they cannot be changed since the Blockchain has to comply with all the nodes in the system. Therefore, initializing a new public Blockchain requires a significant level of effort. In public Blockchains the data validators are totally unknown, anyone in the system can view and validate the data. The transaction cost is high since it has to be verified by each and every node; public Blockchains use a peer-to-peer validation system. There's also opportunity for security breaches since each node in the Blockchain system has copy of all the data. Due to the high level of overhead public Blockchains do not lend themselves to private enterprises such as automotive manufactures who rely on their private integrated systems to maintain records. Most private enterprises also have no compelling business reason to distribute data beyond their private network.

4.2 Private Blockchains

Private Blockchains offer the same level of data integrity as a public Blockchains, but don't require the same level of effort to initialize or maintain as they don't rely on a distributed public network of nodes. Data in private Blockchains are added and removed only by trusted people within a network or a system. The write permissions are completely private and is given only to the user to which the node belongs to. Some private Blockchains have read permissions made public but write permissions are always private. However, regardless of the write permission or add/removal control, validation of the data's integrity can easily be checked with automated audits.

4.2.1 Benefits of Private Blockchains

Data in private Blockchains is simple to maintain and still offers a high degree of security. Data can be read from any node in the network if the node is accessible. The Blockchain mechanism itself doesn't host a log system to keep track of activities per se, but features can be added so that every activity is logged. In private Blockchains there are several different ways to write data using username, password, and digital signatures. In public Blockchains there's only one security layer to grant access to the entire system for writing data. Comparatively, in private Blockchains writing data in a private node you would have to pass two levels of security, which gives more privacy and security for each user. Additionally, multiple layers of security can be added for improved security within the system. Adding an extra node to the system is quick and easy in a Blockchain system when compared to adding a client to a server. Private Blockchains do not allow all the data to be duplicated, which can be customized at each node thereby maintaining confidentiality. Data can be read at high speed between and within the nodes.

4.3 Data Communication

The most common way of data communication in the majority of data related systems is peer-to-peer network and client to server network. Peer-to-peer is transferring data between users and the latter is sharing data between user and a centralized data storage system. Peer-to-peer is less efficient as every data instance has to be stored in every node (user), which also gives an advantage of customizing data independently. On the other hand, client to server is focused on data storage at one location and can be read by anyone with proper access to the server. A Blockchain reflects more of a peer-to-peer system but with additional security.

4.4 Current Blockchains Applications

Today, Blockchains are widely used in the finance industry where sensitive payment data is stored and validated. A subset of the financial industry, market trading uses public Blockchains where the transactions are visible to all data consumers within the system. Blockchains are also widely used in digital identity verification systems which tracks and manages digital identification. This is both a secure and efficient method for a niche industry relying on undisputable records. Digital identification is used in a multitude of industries and services such as banking, health care, national security, citizenship documentation, and online retailing.

4.4.1 Future Blockchain Applications

Future Blockchains use could be found in various applications and industries where data sensitivity and undisputed records are an issue. Private Blockchains have a greater opportunity for use and growth due to the lower costs of operations and the greater level of control for a single enterprise. Private Blockchains are gaining greater use in applications that requires a system to maintain personal user information as well as share the records with trusted parties. The automotive case study in the following section explains how a driver's information can be kept confidential but also shared when an action is triggered by an unplanned event.

5. Private Blockchains in Automotive

A typical publicly distributed Blockchain system as seen in the Bitcoin operation has data flowing across many nodes; data of all users are available to every other user and the rules cannot be customized. There is one standard set of rules that is used across all the units or users. However, using a distributed Blockchain such as Bitcoins is not possible in tracking automotive use such as a driver's actions while operating a vehicle due to the high number of factors that differ among individuals and regions. Private Blockchains are a controlled system in which permissions are kept centralized to one organization unlike distributed Blockchains. Private Blockchains therefore ensure data such as the driver's usage history is not shared beyond a trusted party or counterfeited by internal or external efforts.

5.1 Automotive Safety Case Study

Today, private Blockchains are used in several industries such as health care and finance, generally wherever there is sensitive data or undisputable records required. The automotive industry could also benefit from the implementation of private Blockchains within the vehicle itself as the data is sensitive, and in some cases requires undisputable records. In this paper we apply private Blockchain methodology to a road safety system in which each driver's data records are closely monitored and flagged during an anomalous activity. Data records are collected from the driving activity, driver's historical data, external data such as GPS, and regulatory body such as a local government agency. Private Blockchain assures the confidentiality of drivers records due to the private network used by the automotive manufacture and the basic building blocks of Blockchain assure the undisputable records.

5.2 Automotive Safety Blockchain Architecture

The objective of the Blockchain in this case study is to collect data, monitor, and detect any anomalies within the data set which is derived from active driving behavior. Anomalies detected in this example are speeding within a given geo-fenced area, and if detected take necessary actions. The vehicle data itself comes from multiple sources and is stored within the blocks as shown in figure 3. The data considered in this case study are vehicle speed and vehicle location. The speed data is measured using sensors and saved in blocks for every n period time frame and so does the location data. The header identifies the type of data and stores it separately to make it easy for retrieval. There's are also external data, such as the speed limit at any given location or within a goefenced area. The transaction count keeps track of data coming into the blocks. All the historical data can be stored in the Blockchain, transferred to the cloud, or removed within a defined time frame. Each transaction is the combination of vehicle data and the geofencing data at that given location. The inputs are the transactions occurring every defined time frame and then converted into blockhash. The blockhash is nothing but a string that consists of details about every single data collected at an instance. Future data retrieval is made easy by using the hash, which is the most significant advantage of Blockchains. The output is the comparison between actual vehicle data and the recommended data at that instance, which is then compared using a machine learning algorithm to check for anomalies which is an external component to the Blockchain itself.

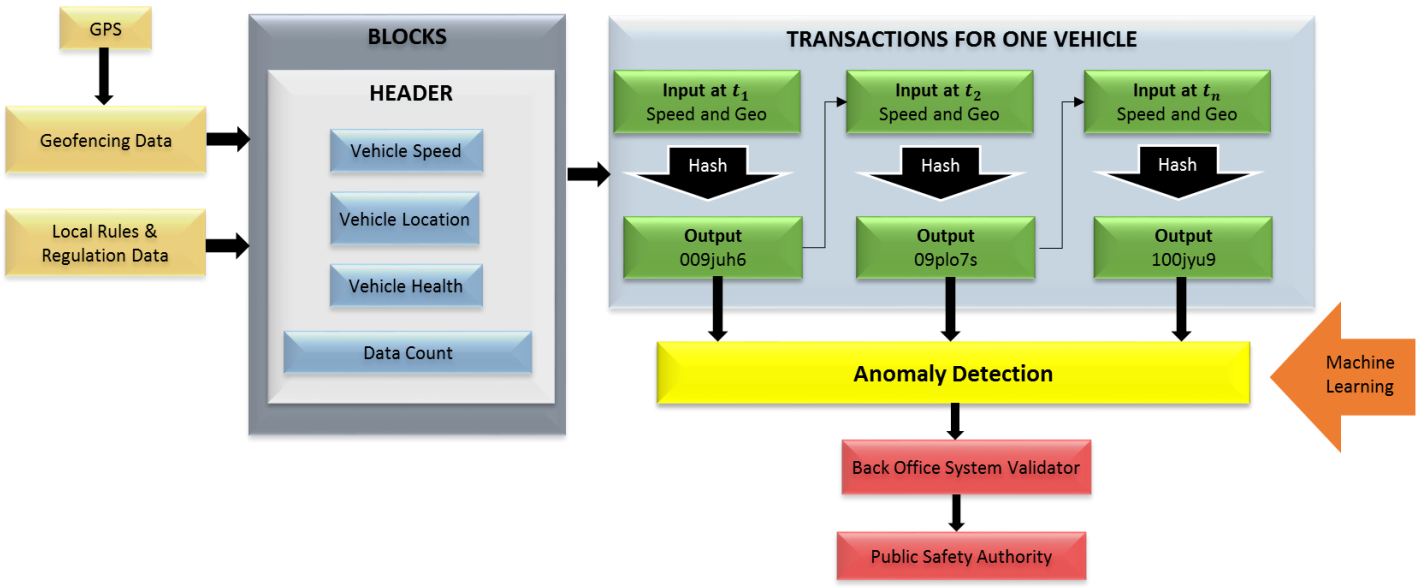

Figure 3: Automotive Private Blockchain Architecture

5.3 Automotive Safety Blockchain Working

The data for detecting anomalies in driver behavior that is used within a Blockchain system is first collected from the vehicle and then compared to the allowable rules such as maximum speed for the given location within a geofence or controlled area. The data collected can include the amount of speed over the given limit, duration, road conditions, and geographical location. If an anomaly activity is detected, the data is sent to a third party and verified against the driver's historical records including identification. Once the driver data is verified the detail will be transferred to respected government authority who can then issue violations directly to the driver at that moment. The whole process occurs as a single transaction within Blockchain in seconds. The validated data is then very well connected between the vehicle, third party and the third party system, which is a unique property of private Blockchains.

5.3.1 Blocks, Data and Transactions

A private Blockchain system starts by collecting the vehicle data and storing it in a database. A time period can be set or controlled dynamically for data collection from the vehicle. There's also another database that collects data from local geo satellites at the same time frequency. Data from each vehicle is referred to as separate node and functions independently within the Blockchain system. The data structure, data type and data collection frequency may or may not be same across all the nodes depending on several factors like vehicle type, geographical location etc. The nodes never communicate between each other and so data are not duplicated across the nodes unlike public Blockchains.

Every data point collected at each time frame is stored in the blocks and then hashed to make the blockhash. The blockhash is nothing but naming a collection of data put together with a string value. All data collected is appended with the hash from the previous data, which is a new string value. Hence, changing the data at some point of time will be reflected across all the blocks. Blockhash helps to retrieve data at any point of time seamlessly and gives more data security and integrity.

5.3.2 Anomaly Detection

The data from vehicle and geo satellites are compared using a machine learning algorithm which continuously validates the vehicle and if it is following the rules at that location. The custom rules in private Blockchains help to adjust the algorithm to accommodate temporary changes such as construction zone rules in a given location. The algorithm within the Blockchain ensures there is no difference between the actual and the measured value. Algorithms can be machine learning algorithms such as classification models which detects an outlier if the new data does not follow particular distribution. The machine learning model is built using historical data based on users driving pattern and other factors including vehicle use and geography. A flag is triggered if the new data collected at a given point of time does not follow the distribution of historical data. If there is an anomaly detected, the data measured at that instance is then transferred to the third party system that monitors drivers for a given geography or controlled area. The data can be transmitted to the third party in two ways, either by setting a time period or can be transferred only during when an anomaly is created. The third party then sends the vehicle and driver's history to the public safety system or governmental agency.

5.3.3 Decision Making

Decisions for action (notification and/or ticket) can be taken at three primary points: The third party following a rule set within a back office system, by a government agency using rules within their back office system, or a custom rules set within the Blockchain. Whether or not to issue notification to the driver or ignore the violation can be automated using additional rules or by human audit for the given instance. If the decision is to issue notification is generated from the third party, the case is forwarded to the government issuing authority, who then issues a notification directly to the driver. At the end of each violation notification sent within the Blockchain, a label is created denoting whether a notification (or ticket) is being issued or not. This data can be tracked by a larger public road safety department and can also be used for other purposes like insurance or driver's license renewal. It's important to note the data collected is considered tamper proof (undisputable) due to data coming directly from the vehicle and using Blockchain technology. This is far more accurate than camera/radar systems used in the U.S.

5.4 Benefits

The use of private Blockchains in the automotive industry can facilitate data transactions and records anonymously in a controlled environment and some transactions can be overturned if necessary without the overhead or data exposure of distributed public Blockchains. The frequency of data collection and the transmission can vary over any period of time, can vary independently by region, and can operate under customized rules. Thus private Blockchains gives the flexibility and durability required for the automotive industry.

6. Conclusion

Maintaining confidentiality in data while continuously monitoring the activities is a big challenge in today's big data world. Proposed private Blockchain methodology is a way to maintain integrity of data, data security, and data confidentiality. Private Blockchains can assist in tracking the anomalies without exposing the data to all users within a given the system. They also provide an efficient way of collecting and storing data using rules unlike traditional databases. The case study detailed illustrates how seamlessly data can be tracked privately and yet interact with governing agencies who role is to maintain road safety. The methodology can be expanded to other automotive applications which require data security and integrity.

7. Future of Blockchains

Both private and public Blockchains has numerous applications with many under development. Blockchains are here to stay with a very bright future, taking data security to next level. Many Blockchain applications will be experimented within the next few years given the high demand. Additionally the need for data security and systems has increased drastically in the past decade, which gives more mobility for Blockchain systems. Given the exponential growth in automotive data, the need to interact with both IoT and government agencies, Blockchain has a very promising future with all data driven companies within the automotive industry.

7. References:

1. *Yue, Xiao, et al. "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control." Journal of medical systems 40.10 (2016): 218.*
2. *Atzori, Marcella. "Blockchain-Based Architectures for the Internet of Things: A Survey." Browser Download This Paper (2016).*
3. *Peters, Gareth William, and Efstathios Panayi. "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money." Available at SSRN 2692487 (2015).*
4. *Peters, Gareth William, and Guy Vishnia. "Overview of Emerging Blockchain Architectures and Platforms for Electronic Trading Exchanges." (2016).*
5. *Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data." (2016).*
6. *Linn, Laure A., and Martha B. Koo. "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research."*
7. *Pilkington, Marc. "Blockchain technology: principles and applications." Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar (2016).*
8. *Steve, Ratheram, "Driving the Blockchain - Why Bitcoin matters in Automotive", Birmingham City University, Advanced Powertrain Control Symposium.*
9. *http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/*
10. *http://fortune.com/2016/05/18/linkedin-data-breach-email-password/*
11. *https://bitsonblocks.net/*
12. *S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System*
13. *https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains/*