Tezos-based Vehicular Ad Hoc Blockchains

-

Research Paper - Version 0.1
September 6, 2018

Benjamin Leiding and William V. Vorobev

Chorus Mobility
Email: hello@chorus.mobi

Abstract. The next generation of tightly interconnected vehicles offers a variety of new technologies as well as business opportunities. Vehicles form so-called vehicular ad hoc networks (VANETs). Sophisticated systems of interconnected cars in the context of VANETs assume a full coverage of 5G networks to unfold their full potential. However, nowadays network infrastructure is neither 5G-ready nor does it provide reliable and full coverage of all areas that might be relevant for VANET-based networks. Hence, the conventional mode of operations of all nodes being connected to one blockchain at all times is not feasible. In addition, traditional blockchains also require every node to process each transaction and smart contract commands which are highly inefficient. Therefore, we present a solution based on so-called mobile ad hoc blockchains that enable groups of nodes involved in any kind of collaboration to effectively form temporary networks and coordinate themselves.
Another critical requirement of VANETs and interconnected vehicles is security. The safety of network participants does not only depend on the vehicle's hardware, but also on the correctness of the software that controls the interaction and transaction within the network. Formal verification is a common way to address the issue proving the correctness of software. The self-amending blockchain Tezos supports Turing-complete smart contracts and also offers built-in formal verification of their programming languages, thereby fostering the security of our solution.
This whitepaper fills the gap by introducing Vehicular Ad Hoc Tezos Blockchains based on mobile ad hoc blockchains that allow groups of nodes to be temporarily disconnected from the overall network but still being able to enact and transact on a local network level for the duration of their interaction. We present the advantages of the system, outline the requirements and goals, as well as the architecture of the system.

Keywords: VANET, Formal Verification, Tezos, Mobile Ad Hoc Blockchains, Blockchain, Smart Contracts, Interoperability, Vehicle Networks, V2X

1 Introduction

Despite steadily growing public transport networks and systems, especially in most first world countries, cars are still the default standard for urban trans-

portation. In the US, "about 86 percent of all workers commuted to work by private vehicle, either driving alone or carpooling" [22], even though in recent years the numbers remained relatively stable after decades of consistent increase. Similar applies to other industrial countries [23][13] though the overall percentage of vehicle commuters in Europe is lower than in the US [9]. While it was normal for the last few decades to own a vehicle and commute on a day-by-day basis, the future will be radically different due to the progressing evolution of self-driving cars and autonomous vehicles. The car-sharing economy that developed in recent years in combination with autonomous cars results in a so called *passenger economy* [16]. Users no longer own cars, instead just hop on an autonomous car, pick a destination and get delivered without any human interaction. An Intel report estimates the size of this economy to be around US$ seven trillion in 2050 [16].

A key technology for the next generation of tightly interconnected vehicles are so-called vehicular ad-hoc networks (VANETs) [**?**]. Vehicles form VANETs enable vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-human (V2H), or in general vehicle-to-everything (V2X) communication and interaction. In our previous research paper [**?**][**?**][**?**], we presented a blockchain-based system that enables a manufacturer agnostic platform solution that allows VANET participants to enact and transact any kind of services and goods. Sophisticated networks of interconnected cars require full coverage of 5G networks to unfold their full potential [**?**]. However, nowadays network infrastructure is neither 5G-ready nor does it provide reliable and full coverage of all areas that might be relevant for VANET-based networks. Hence, the conventional mode of operations of all nodes being connected to one blockchain at all times is not feasible [**?**]. In addition, traditional blockchains such as Bitcoin [25] and Ethereum [31] also require every node to process each transaction and smart contract commands which are highly inefficient. Therefore, we present a solution based on so-called mobile ad hoc blockchains that enable groups of nodes involved in any kind of collaboration to effectively form temporary networks and coordinate themselves. They only connect to nodes they need to be connected to, depending on the context, for the duration of their interaction.

Another critical requirement of VANETs and interconnected vehicles is security. The safety of network participants does not only depend on the vehicle's hardware, but also on the correctness of the software that controls the interaction and transaction within the network. Formal verification is a common way to address the issue proving the correctness of software with respect to a certain formal specification or property using formal methods of mathematics [**?**][**?**]. The self-amending blockchain platform Tezos [15] does not only support Turing complete smart contracts, it also offers built-in formal verification of their smart contract programming languages, thereby fostering the security of our solution.

This work fills the gap by introducing Tezos-based platform solution, thereby answering the question of how to enable vehicular ad hoc blockchains that allow groups of nodes to be temporarily disconnected from the overall network but still being able to enact and transact on a local network level for the duration of

their interaction? In order to answer this question with a separation of concerns, we pose the following sub-questions: What is the corresponding architecture of the Vehicular Ad Hoc Tezos Blockchain? What are the detailed network and communication processes? What kind of use cases and application scenarios exist?

The remainder of this paper is structured as follows: Section 2 introduces supplementary literature and related work. Section 3 outlines the system architecture our solution. Afterwards, Section **??** expands on the network communication processes, followed by Section 4 that introduces example use cases and application scenarios. Finally, Section 5 concludes this work and provides an outlook on future work.

2 Technical Background and Supplementary Literature

The following section provides background information and describes related works regarding previous ideas and concepts that focus on a blockchain-based VANET platforms. First, Section 2.1 introduces the general concepts of blockchain technology, terms and frameworks. Afterwards, Section 2.2 and Section 2.3 focus on the fundamentals of vehicular ad-hoc networks as well as formal verification. Finally, Section 2.4 introduces related work.

2.1 Blockchain Technology

As the name suggests, a blockchain consists of a chronologically ordered chain of blocks. Every block consists of a certain number of validated transactions and each of those block links to its predecessor by a hash reference. As a result, changing the content of one block also changes all succeeding blocks and hence breaks the chain. All blocks are stored on and verified by all participating nodes. While the initial Bitcoin blockchain only supported a very limited set of scripting instructions, the next generation of blockchain platforms, e.g., Ethereum [31], Qtum [10], or Tezos [15], provide Turing-complete programming languages on the protocol-layer level in order to enable smart contract capabilities. Smart contracts are "orchestration- and choreography protocols that facilitate, verify and enact with computing means a negotiated agreement between consenting parties" [10]. Hence, the entities participating in the enactment of a smart contract establish binding agreements and deploy applications using such smart contracts in order to provide blockchain-based applications. Those application are as versatile as smart contracts itself and enable services including the finance sector [26][28], academic and business authentication and identity solutions [5][8][18][21][29], reputation systems [6] as well as platforms for Internet-of-Things (IoT) applications [7][27].

The blockchain concept is particularly interesting for the V2X economy for three reasons. First, it removes the need for trusted third parties and instead enables trust-less transaction enactment. Second, transactions that were agreed up on cannot be changed later on since the underlying blockchain is tamperproof.

Third, no human interaction is required for any kind of transaction between vehicles or machines in general.

2.2 Vehicular Ad-Hoc Networks - VANETs

Communication between vehicles, road infrastructure and Internet-based services is a key enabler for the upcoming generation of vehicles. So called vehicular ad-hoc networks provide an abstract concept that models the different components that are required for V2V, V2I, or V2X communication. Figure 1 illustrates the main components of VANETs: Vehicles, on-board-units (OBUs), application-units (AUs) and road-side-units (RSUs).
RSUs are placed along the road side or in dedicated locations such as at crossroads. Typically, RSUs provide short range communication based on IEEE 802.11p radio technology but can also be equipped with other network devices in order to provide communication within the infrastructural network [1]. OBUs are mounted onto a vehicle and used for data exchange. To do so, short range wireless- or radio communication is used to exchange these information [4]. Closely linked to the OBU is the AU, they might even reside in the same physical unit or as a mobile until that is regularly removed from the vehicle (e.g smartphones). The AU provides an execution environment for applications that utilize the OBU's communication capabilities [1][4].
Communication in VANETs occurs either inside a vehicle between AUs and

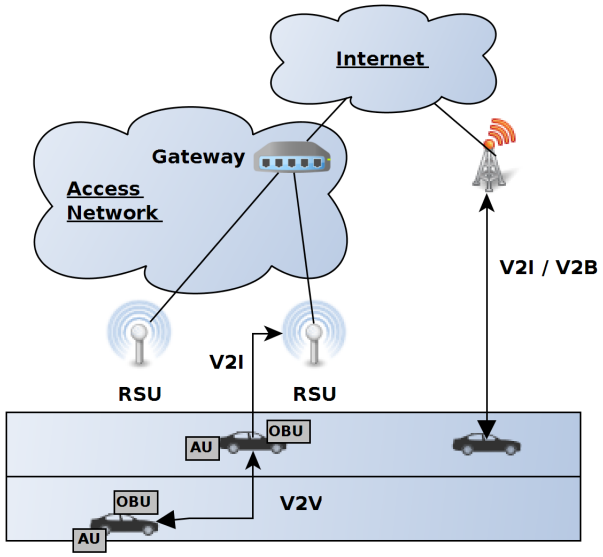

Fig. 1. General VANET architecture (Based on [4] and [19])

OBU, wirelessly between different vehicles (V2V), vehicles and infrastructure

(V2I) or vehicles and the infrastructure via broadband (V2B) [12]. For authentication purposes, each network participant is equipped with a unique public/private key pair that resides in a tamper-proof-device (TPD). In blockchain terms, the TPD is similar to an external hardware wallet.

2.3 Formal Verification

basic introduction with motivation, advantages and disadvantages A380 example?

connect formal verification and blockchain Tezos[1] [15] Cardano[2] [**?**] others?

"A formal method is a mathematically-based technique used in computer science to describe properties of hardware and/or software systems. It provides a framework within which large complex systems may be specified, developed, and verified in a systematic rather than ad-hoc manner. A method is formal if it has a sound mathematical basis, typically given by a formal specification language" [**?**]. Over many decades, several approaches and concepts for formal methods have been introduced. Among them, without claiming completeness: Statecharts [**?**], abstract state machines (ASMs) [**?**], Petri nets [**?**], the Calculus of Communicating Systems [**?**] and π-calculus [**?**], as well as timed automata [**?**] and communicating sequential processes [**?**].
In this thesis, the Authcoin protocol is modeled using formal methods based on Coloured Petri Nets (CPNs) [**?**], a special type of Petri nets. "A CPN is a graphical oriented language for the design, specification, simulation and verification of systems. It is in particular well-suited for systems that comprise a number of processes that communicate and synchronize. Typical examples of application areas are communication protocols, distributed systems, automated production systems, or work flow analysis" [**?**]. A further advantage of CPNs is, that it "allows for the semantically deterministic design of system structures and also behavior that is verifiable for correctness and performance tests with tool support" [**?**]. CPN models are regularly used for the modeling and verification of security protocols as well as authentication protocols (e.g. [**?**][**?**][**?**][**?**][**?**][**?**][**?**]).

2.4 Related Work

MONET [2] invented mobile ad hoc blockchains downside -¿ hashgraph [3] requires license they do not explain how they ensure 1:1 mapping between pub/priv key identity and network participant in their permissioned chain. Right now I could run a sybil node attack

Cosmos exists [14]

[1] `https://tezos.com/`
[2] `https://www.cardano.org`

3 System Design and Architecture

As previously mentioned in Section 2.4 the concept of mobile ad hoc blockchains is not new and has been recently applied to mobile ad hoc networks (MANETs) in the form of the MONET project [2]. The following sections now outline the process of adapting the general concept of mobile ad hoc blockchains to VANETs. VANETs are a sub-category of MANETs. There are two main differences between the two types of networks. First, not all entities in VANETs are mobile and only sparsely connected to the Internet, e.g., RSU and infrastructure components. They are stationary and hence it easy to establish permanent Internet access for them, making them the perfect relay stations. Second, in VANETs the communication nodes are moving on predefined roads in contrast to nodes in MANETs that are not bound to any restrictions. Note that this definition excludes flying vehicles such as drones from VANETs in the context of this work.

Section 3.1 presents the high-level architecture of the VANET blockchain, followed by Section 3.3 that discusses the topics of identities within our system. Finally, Section 3.4 outlines the consensus strategies for vehicular ad hoc blockchains.

3.1 System Architecture

The system architecture illustrated in Figure 2 extends the commonly used VANET concept of Figure 1 that we introduced earlier. RSUs, vehicles equipped with OBUs and AUs as well as the infrastructure backend remain the same. However, similar to the concept of MONET, mobile nodes, i.e., vehicles, can form so called mobile ad hoc blockchains. Only vehicles within a certain range of each other form such networks. To do so, they agree up on an initial list of participants, while new nodes may join later or current nodes leave - depending on the context.

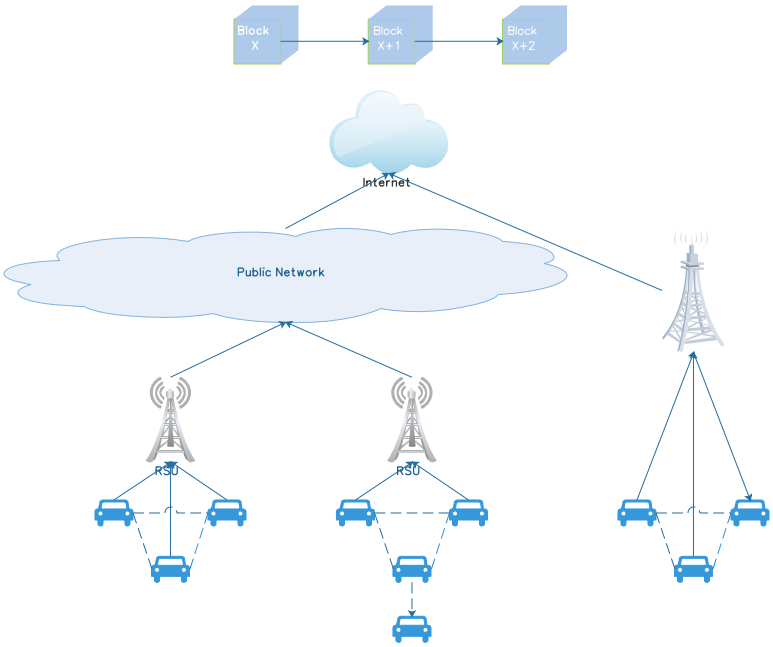

Fig. 2. Caption.

Nodes that form a vehicular ad hoc blockchain agree up on transactions on their own (see Section 3.4 for more details on consensus) and periodically forward state and status information to RSUs or other infrastructure entities. Those permanent and fixed components have a direct connection to the Internet as well as the VANET backend which enables them to relay received information from the specific independent vehicular ad hoc blockchains to the main blockchain (depicted at the top of Figure 2). Vehicular ad hoc blockchains are either directly connected to RSUs or to some other kind of infrastructure that providers access to the Internet. Vehicles that do not have access to a RSU or alternative options can use a mesh-based approach where they connected to an ad hoc network that relays their information to the destination (middle of Figure 2). Due to the missing full network coverage along the existing road infrastructure, there might be periods where a complete set of nodes is only interconnected among each others, but not to the main network. Our system tolerates such temporary disconnects as detailed later.

3.2 Tezos Master Blockchain

some hub stuff here

3.3 Identities

Tamper-proof-devices (TPDs) are a standard component of VANETs. They usually contain a public/private key (similar to wallet addresses) pair that uniquely identifies a vehicle and serves for authentication and signing as well as verification purposes. Usually, TPDs are pre-equipped by the car manufacturer and built into the vehicle's hardware. In the context of blockchains, an identity is further required in most consensus algorithms to uniquely identify participants. Moreover, a mapping between public/private keys (that constitute an identity) and vehicles is also necessary to prevent sybil node attacks. This type of attack is a common issue in large-scale peer-to-peer (P2P) systems, where hostile or faulty computing elements threaten the security of the whole network. Single faulty entities may be able to present multiple identities, thereby controlling a substantial fraction of the system, consequently undermining its functionality and security [11]. Unfortunately, the majority of current cars does not have a such a TPD that could constitute a cars identity. Hence, an alternative solution is required. We are currently evaluating different approaches. First, equipping vehicles on our own with small hardware devices that can easily be attached to vehicles and contain a TPD that ensures an identity binding. Second, utilizing smartphones as identity providers. Third, using blockchain-based validation and authentication protocols such as Authcoin [17][18][20].

3.4 Blockchain Consensus in VANETs

In the context of blockchains, consensus algorithms are usually used to agree on a set of transactions that constitutes the next block that is added to the chain. Proof-of-Work [25] and Proof-of-Stake [**?**] are most common and used for example by Bitcoin and Ethereum. For both major consensus algorithms, different flavors exists as well as a large variety of alternative protocols. However, almost all current state of the art algorithms suffer some kind of disadvantage, e.g., scalability issues, security issues, efficiency issues, and so on [**?**][**?**]. Figure 3 illustrates a collection of consensus algorithms and their scalability as well as performance properties.

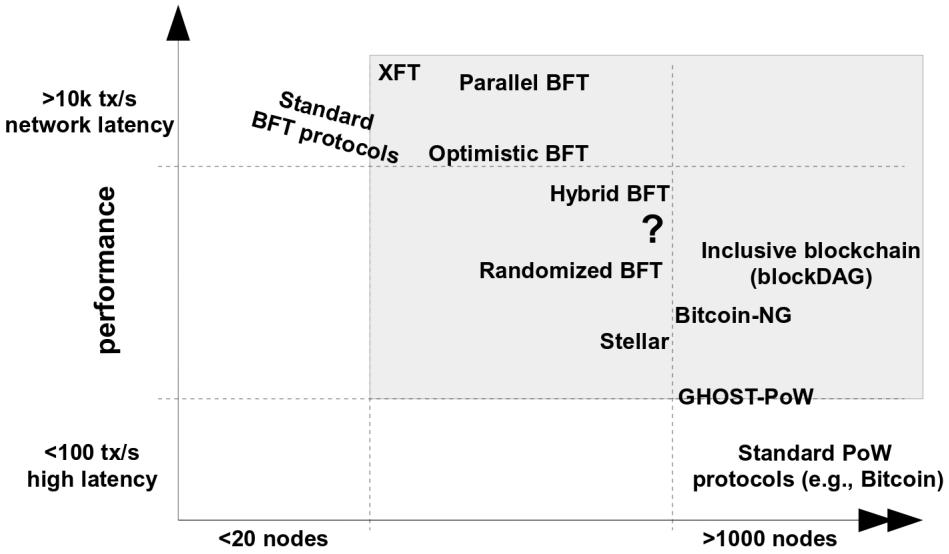

Fig. 3. Caption (Source: [30]).

Those problems become even more complex in the context of mobile- and vehicular ad hoc blockchains due to the large number disjunct chains that exist in parallel as well as the the fact that entities are sometimes only connected in a mesh network without connection to the Internet which makes consensus on a global level even more difficult. In this context, timing assumptions become important. Consensus protocols might be fully synchronous which means that all messages are delivered within a pre-defined time x whereas asynchronous consensus protocols only ensure that all messages are eventually delivered [**?**]. Between those two extrema different sub-categories such as eventually synchronous, partial synchronous and weakly synchronous consensus algorithms exist [**?**][**?**][**?**]. In vehicular ad hoc blockchains a fully asynchronous consensus protocol is desirable due to the sparse connectivity of nodes and missing connection guarantees among nodes.

There are different protocols that aim to offer solutions in this regard. The Babble consensus algorithm [**?**] relies on a leaderless, asynchronous, Byzantine fault tolerant (BFT) algorithm that is based on Hashgraph [3].However, Hashgraph is patent protect in the U.S. and therefore limited in us. Alternative protocols such as [24], [**?**] and [**?**] exist besides Hashgraph with certain limitations. We are currently researching different solutions that enable a leaderless, asynchronous with BFT guarantees that also scales well. Alternatively, VANETs also allow for a hierarchical blockchain solution where RSUs act as *always-on* relay blockchain nodes that accept and process transactions from groups of vehicular ad hoc blockchains, e..g, in a Cosmos-like style [14]. The RSUs then process the

incoming transactions and project them into a blockchain hub block structure as outlined in Section 3.2. C

3.5 Inter-Blockchain Communication

4 Use Cases and Application Scenarios

Waiting for some text input from Will.

5 Conclusion and Future Work

This work presents

References

1. Al-Sultan, Saif and Al-Doori, Moath M and Al-Bayatti, Ali H and Zedan, Hussien: A Comprehensive Survey on Vehicular Ad Hoc Network. Journal of Network and Computer Applications 37, 380–392 (2014)
2. Arrivets, M.: MONET: Mobile Ad Hoc Blockchains - Whitepaper. URL: `https://drive.google.com/file/d/1PcI69i_oJpWdsIsOciLliYEsFv9hHCVr/view` (2018), (Accessed September 04, 2018)
3. Baird, L.: The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance - Whitepaper. URL: `https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf` (2016), (Accessed September 06, 2018)
4. Baldessari, R., Bödekker, B., Deegener, M., Festag, A., Franz, W., Kellum, C.C., Kosch, T., Kovacs, A., Lenardi, M., Menig, C., et al.: Car-2-Car Communication Consortium - Manifesto (2007)
5. Bochem, A., Leiding, B., Hogrefe, D.: Unchained Identities: Putting a Price on Sybil Nodes in Mobile Ad hoc Networks. In: Security and Privacy in Communication Networks (SecureComm 2018). Singapore (August 2018)
6. Calcaterra, C., Kaal, W.A., Vlad, A.: Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems. URL: `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125822` (2018), (Accessed April 18, 2018)
7. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303 (2016)
8. Civic Technologies, Inc.: CIVIC - Whitepaper. URL: `https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf` (2017), (Accessed May 01, 2018)
9. Cortright, J.: Sprawl Tax: How the US Stacks Up Internationally . URL: `http://cityobservatory.org/sprawl-tax-how-the-us-stacks-up-internationally/` (2016), (Accessed April 26, 2018)
10. Dai, P., Mahi, N., Earls, J., Norta, A.: Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. URL: `https://qtum.org/uploads/files/a2772efe4dc8ed1100319c6480195fb1.pdf` (2017), (Accessed May 01, 2018)
11. Douceur, J.R.: The Sybil Attack. In: International Workshop on Peer-to-Peer Systems. pp. 251–260. Springer (2002)

12. Faezipour, M., Nourani, M., Saeed, A., Addepalli, S.: Progress and Challenges in Intelligent Vehicle Area Networks. Communications of the ACM 55(2), 90–100 (2012)
13. Goodyear, R., Ralphs, M.: Car, bus, bike or train: What were the main means of travel to work (2009)
14. Kwon, J., Buchman, E.: Cosmos: A Network of Distributed Ledgers - Whitepaper. URL: https://cosmos.network/docs/resources/whitepaper.html (2018), (Accessed September 06, 2018)
15. L. M. Goodman: Tezos - A Self-Amending Crypto-Ledger (White paper). URL: https://www.tezos.com/static/papers/white_paper.pdf (2014), (Accessed September 04, 2018)
16. Lanctot, R.: Accelerating the Future: The Economic Impact of the Emerging Passenger Economy. URL: https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf (2017), (Accessed April 27, 2018)
17. Leiding, B.: Securing the Authcoin Protocol Using Security Risk-oriented Patterns
18. Leiding, B., Cap, C.H., Mundt, T., Rashidibajgan, S.: Authcoin: Validation and Authentication in Decentralized Networks. In: The 10th Mediterranean Conference on Information Systems - MCIS 2016. Cyprus, CY (September 2016)
19. Leiding, B., Memarmoshrefi, P., Hogrefe, D.: Self-Managed and Blockchain-Based Vehicular Ad-Hoc Networks. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. pp. 137–140. ACM (2016)
20. Leiding, B., Norta, A.: Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance. In: International Conference on Future Data and Security Engineering. pp. 181–196. Springer (2017)
21. McCorry, P., Shahandashti, S.F., Clarke, D., Hao, F.: Authenticated key exchange over bitcoin. In: International Conference on Research in Security Standardisation. pp. 3–20. Springer (2015)
22. McKenzie, B.: Who Drives to Work? Commuting by Automobile in the United States: 2013. American Community Survey Reports (2015)
23. Mieke Berends-Ballast et al.: Transport and Mobility 2016. URL: https://www.cbs.nl/en-gb/publication/2016/25/transport-and-mobility-2016 (2016), (Accessed April 26, 2018)
24. Miller, A., Xia, Y., Croman, K., Shi, E., Song, D.: The honey badger of bft protocols. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 31–42. ACM (2016)
25. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf (2008), (Accessed May 01, 2018)
26. Nguyen, Q.K.: Blockchain - A Financial Technology for Future Sustainable Development. In: Green Technology and Sustainable Development (GTSD), International Conference on. pp. 51–54. IEEE (2016)
27. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In: Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523–533. Springer (2017)
28. SALT Technology, Ltd.: SALT - Blockchain-Backed Loans - Whitepaper. URL: https://membership.saltlending.com/files/abstract.pdf (2017), (Accessed April 25, 2018)

29. SelfKey Foundation: SelfKey - Whitepaper. URL: https://selfkey.org/whitepaper/ (2017), (Accessed April 27, 2018)
30. Vukolić, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: International Workshop on Open Problems in Network Security. pp. 112–125. Springer (2015)
31. Wood, G.: Ethereum: A Secure Decrentralized Generalised Transaction Ledger. URL: http://gavwood.com/paper.pdf (2014), (Accessed May 01, 2018)