Zarządzanie Przedsiębiorstwem. Enterprise Management
Volume 25 • Number 3–4 • December 2022 • pp. 10–14
DOI: 10.25961/ent.manag.25.02.02

TITUS-RESEARCH: BLOCKCHAIN STRATEGY FOR AUTONOMOUS SYSTEMS

Sebastian Henningsen, Abdalla Rashwan, Evrim Demircan, Duc Tran, Uwe Meinberg

TITUS-Research, Germany

Corresponding author:
Abdalla Rashwan
TITUS-Research
Schmiedestraße 2 B, 15745 Wildau, Germany
phone: (+49) 3375 52309 39
e-mail: abdalla.rashwan@titus-research.eu

Abstract

Distributed ledger technology has been getting an increased attention in a wide range of applications where a centralized solution is not favorable. One of the most popular DLTs is the well-known Blockchain technology which is currently being adopted in various domains where several independent agents write to the same shared data collection and it has shown a significant potential when it comes to increasing transparency and providing better security. With autonomous systems gaining more momentum and becoming an inseparable part of our day to day lives from autonomous vehicles to wearable devices therefor this article presents the strategy at TITUS-Research for harnessing the DLT potential in the context of autonomous systems by laying the base knowledge behind DLT and highlighting different use cases where it can improve autonomous systems.

Keywords

Distributed ledger technology, blockchain, autonomous systems.

1. Introduction

Over the years, Blockchain technology (or, more general, distributed ledger technology, DLT) has gained more and more traction as well as increased adoption in various industry use cases. The application domains of DLT range from supply chains, over fintech to government registries. In these use-cases Blockchain-related systems are employed to facilitate processes, cut costs, increase transparency and provide better security in a decentralized manner.

"Blockchain" in these examples is used very broadly – these usages of Blockchain do not have much in common with the original Blockchain data structure introduced with the cryptocurrency Bitcoin. Nevertheless, the technologies employed in those use cases, like Hyperledger and Corda, which are commonly subsumed under the Blockchain umbrella, provide significant value in a variety of deployments.

Blockchain solutions are useful in scenarios with several independent agents who all write to the same data sink. These shared writes have to be mediated somehow, and if a centralized solution is not available or desired, DLT can play the mediating role. This in turn enables a consensus of all participants on the shared data. Thus, DLT is mainly used in supply chain networks and decentralized marketplaces. But also, in the field of autonomous systems, DLT can play an important role. The interaction of autonomous vehicles, (wearable) devices and an increased number of sensors in cities and homes needs to be managed in some fashion – depending on the use case scenario, Blockchain can yield significant benefits.

Therefore, as of Q3 2022, Titus Research will delve into the topic of Blockchain technology in the form of a cross-sectional team anchored in different projects. This team will not conduct research on DLT per se, but rather investigate if and how projects in the context of autonomous systems can benefit from integrating distributed ledger technology. In addition to DLT, the team will have a strong focus on IT security.

2. Primer on distributed ledger technology

The term "Blockchain", refers to a multitude of different technologies and concepts – comparable to similarly hyped terms, e.g., "Artificial Intelligence".

The subsumed technologies range from so-called permissionless Blockchains like Bitcoin & Ethereum, to permissioned systems (public and private) such as Hyperledger & Corda with each type having its own pros and cons. In the following we will give a short introduction to these different technological concepts, their strength and weaknesses and when a Blockchain solution is reasonable. A summary of the differences between these concepts is illustrated in Table 1.

There are three large categories of Blockchain systems: permissionless, public permissioned and private permissioned.

Table 1
Different types of Blockchain & their properties.

	Public	Private
Permissonless	Bitcoin, Ethereum, ... + existing infrastructure − slow +/− data transparent	–
Permissioned	Hyperledger, Corda, . . . + fixed set of participants + fast +/− publicly verifiable data	Hyperledger, Corda, ... + hidden data (potentially among participants)

In a permissionless Blockchain, anybody can join and participate in the consensus of the system. Examples are prototypical cryptocurrencies such as Bitcoin, Ethereum, Monero, etc. To enable a consensus among this open and fluctuating set of participants, most permissionless Blockchains employ a form of Proof-of-Work or Proof-of-Stake. The current state of the ledger is replicated by every (full) node in the system and the state of the ledger is advanced through transactions, which are gathered into blocks. Each block references it predecessor, thus the name Blockchain.

The combination of Proof-of-Work together with this chained block data structure was one of the main contributions of Bitcoin, which solved a research problem that had been open for more than 20 years. In essence, Bitcoin allowed an open set of participants to conduct transactions of monetary tokens among one another, even if participants behave maliciously and without previous trust anchors between transacting parties.

Permissionless systems promote openness and transparency of transactions (with the notable exception of Zcash and Monero). This transparency might not always be desirable for industry use cases. The metadata alone, i.e., who transacts with whom how often can give away delicate company secrets to competitors.

In addition, the threat model of Bitcoin and other related systems is harsher most real-world situations actually require, e.g., most of the time we trust the government to issue one identity card to each citizen. The technological measures to cope with the dire threat model leads to scalability problems, in that only a few transactions per second can be processed.

Benefits of permissionless Blockchains (and permissionless systems in general) are: 1) the fact that the system is running and can be used as infrastructure, and 2) the ability to escape regulations and restrictions imposed by central authority; resistant to censorship.

Regarding (1), permissionless systems can be seen as an existing infrastructure that is readily available to be built upon. For example, the Ethereum Blockchain hosts the majority of ICOs and NFTs – with easy-to-use frameworks, documentation and developer experience to develop other forms of systems easily. Thus, it may make sense for companies to choose Ethereum as their infrastructural basis in some circumstances.

Addressing (2), the ability to avoid legislation is mostly associated with criminal activity in western countries. While this association is reasonable, permissionless technologies also enable resistance against censorship and oppression in general.

In contrast to permissionless systems, where anybody can join and partake in the consensus, permissioned Blockchains have a gatekeeping mechanism, i.e., all participants are known in advance. This is more inclined towards most industry use cases. The assumptions on the identity of the participants allows these systems to scale much more easily and allow for more control on data confidentiality. Permissioned systems have to be differentiated whether they are public or private.

In a public permissioned system the consensus is carried out between a (relatively) fixed set of validator nodes, whose actions can be verified by anybody. This form of consensus is oftentimes referred to as Proof-of-Authority, in other words, only authorized nodes form the consensus among themselves.

Private permissioned systems on the other hand are only accessible to the participants of the consensus and are not publicly readable. This is the case for many scenarios in which DLT is used.

The field of permissioned systems is broad, and the employed technologies vary greatly between different use cases. Examples range from spare parts exchanges for airplanes [2], over tracking the origin of goods through supply chains [4] to financial services [5].

Therefore, a summary of the available technologies (as given above for permissionless systems) does not yield much benefit, as the choice of technology depends on the scenario at hand. Instead, in the following we investigate when a DLT solution can make sense and which scenarios are better solved with other technologies.

Naturally, DLT, as any other technology, is a tool with strengths and weaknesses. Therefore, one has to assess whether Blockchain is useful for the specific scenario at hand. An easy-to-use flowchart is depicted in Fig. 1, inspired by Wüst and Gervais [6]. They give the following summary: *"In general, using an open or permissioned blockchain only makes sense when multiple mutually mistrusting entities want to interact and change the state of a system, and are not willing to agree on an online trusted third party."*

We will elaborate on this quote in the following. If no data is written at all, no Blockchain is necessary. The same applies if there is data to be stored, but only one party maintains the data and will continue to do so in the future. In this case a database is the technology of choice.

Similarly, if multiple parties want to write/exchange data, but there is a trusted party coordinating and ordering these writes, then no Blockchain is necessary. If the trusted third party is undesired and should be made obsolete, then a DLT solution might make sense.

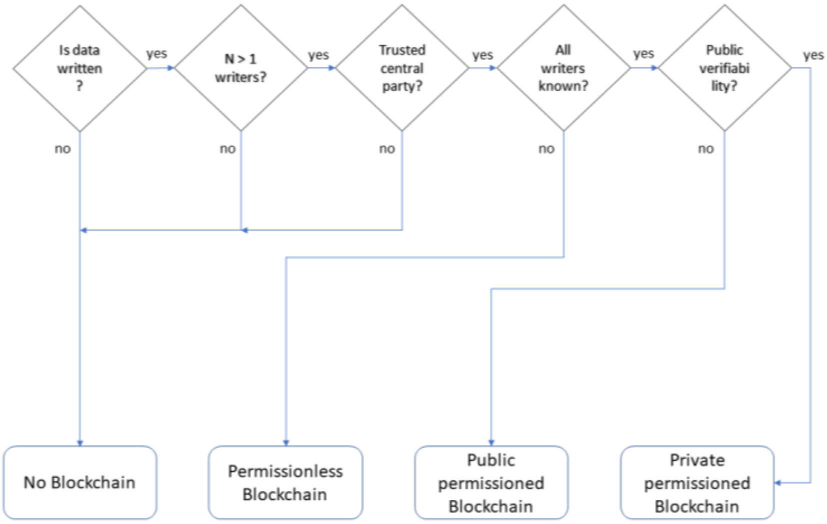

Fig. 1. In which scenarios are Blockchains useful?

DLT is useful in all scenarios when there are multiple parties without a trusted third party. This is often found in supply chains, where no participant should gain a competitive advantage through hosting a central platform, for example. Depending on the concrete scenario, the specific choice of Blockchain follows accordingly.

It is evident that DLT can provide significant benefits in the context of autonomous systems. Especially for self-driving cars or any form of supply chain automation, DLT can help bridge the gap between different data silos and enable a transparent automation of processes.

In the following, we will define the scope of Titus Research's DLT & Security Team based on the guarantees that DLT systems provide and the expectations that people commonly associated with "Blockchain".

3. Distributed ledger technology & autonomous systems @ Titus Research

As outlined above, there are a ton of different frameworks, systems and protocols which are subsumed under the umbrella term "Blockchain", each with different strengths, limitations and trade-offs.

However, a true definition is hardly possible. Firstly, due to the high ambiguity of perceptions and opinions on what "Blockchain" means. Secondly, permissioned Blockchains are mostly realized through Byzantine Fault Tolerance (BFT) protocols – but the field of BFT cannot be fit completely under the umbrella of Blockchain.

Therefore, we take a more demand- and requirements-driven perspective. Users and companies are not interested in Blockchain technology for the technicalities but rather the perceived benefits, to solve open problems, enable new capabilities and to streamline their processes.

We identified multiple key aspects of Blockchain systems that are relevant for autonomous systems:

- Immutable storage/time stamping;
- (transaction) Transparency;
- Trusted infrastructure with different guarantees (not all at once):
  - availability,
  - redundancy,
  - integrity,
  - confidentiality,
  - ...;
- Auditable and partly automated processes ("smart contracts");
- Decentral shared platform among non-trusting entities (e.g., suppliers & competitors);
- Programmable money (requires more regulatory infrastructure).

From this list we can conclude that IT security also has to play a major role, since you cannot have a reasonable DLT setup without thinking about IT security. Especially advanced concepts like homomorphic encryption and zero knowledge proofs have a high potential in these setups where DLT is reasonable.

Homomorphic encryption enables computation on encrypted data, e.g., adding two values and encrypting the result is the same as adding the individually encrypted values. This allows for computations to be performed on the encrypted dataset, without revealing any intel to the computing party. A popular use case for this are computations on medical records.

Zero knowledge proofs on the other hand allow a prover to proof to the verifier the knowledge of some information without revealing said information. This can be used to proof that a number is within a certain range without disclosing the number, or to show membership of a set without revealing the element.

These descriptions alone make it evident that the combination of DLT systems with these advanced protocols may have high potential. Especially in scenarios where multiple non-trusting parties are operating on the same Blockchain platform with the aim of gathering insights by combining their local data sources without disclosing them to the respective others. Therefore, the two pillars of the new team at Titus research: DLT & Security.

The focus of the team will lie on evaluating and providing Ethereum & Hyperledger-based solutions as well as security & cryptography support for projects in the realm of autonomous systems. The latter is especially important in distributed systems with communication between vehicles or vehicles and infrastructure. While providing security support in various projects and settings is one goal of the DLT & Security team, the main focus lies on distributed Blockchain architectures and their integration with advanced cryptographic protocols in the context of research projects in autonomous systems.

4. Example use cases in autonomous systems

In the following we investigate two sample use cases of DLT in the context of autonomous systems. This is aimed to make the concepts and benefits clearer and easier to grasp.

4.1. Privacy preserving and immutable framework for managing vehicle's data

Technological advancements continue to shape our day-to-day life on different aspects, one of which is autonomous driving. Autonomous vehicles are expected to change our current perspective of road traffic by providing solutions to current problems such as accidents and congestions [3]. Modern day autonomous vehicles are defined as cyber-physical systems due to their ability to communicate with other machines as well as gather different types of information using their sensors.

These qualities that autonomous vehicles have make it possible to generate various kinds of data which can be useful for drivers, manufacturers, insurance companies and other service providers [1].

One of the challenges with autonomous vehicles arises in the case of accidents between them or with humans. In this case, liability must be decided based on the accident's forensics. In autonomous vehicles, electronic control units and on-board units are used to gather data from the vehicle's sensors and make decisions accordingly. Hence, the autonomous vehicle's ability to collect data about itself and its environment can have great potential when it comes to forensics in case of accidents. In this scenario, DLT can provide the technical means to immutably and verifiably store the "decisions" of autonomous vehicles, in order to extract them in the case of accidents.

In [1], a partial solution for this situation is proposed. The proposal is based on Blockchain technology for ensuring a vehicle's data integrity. The suggested approach uses a permissioned blockchain framework to manage the vehicle related data. The main desired features of this framework include ensuring data integrity by adopting a tamper proof ledger for storing data, eliminating single point of trust by providing a distributed ledger to all participating nodes, preserving privacy of the participants with pseudonym identities and finally being lightweight in order to ensure useability for participants with different capabilities and resources.

Using such a framework can provide many advantages, but on the other hand many open questions have to be addressed. For example, malicious participants were not considered in the design of the framework, which is of course undesirable for real-world deployments.

In summary, although previous literature exists around the use case of DLT with autonomously driving vehicles, there are still a lot of challenges to be overcome and questions to be answered.

4.2. Spare parts exchange marketplace

Staying the context of self-driving vehicles, we will propose another possible use case of DLT in the context of self-driving vehicles.

As with manually driven cars, autonomous cars will eventually reach the end of their lifetime and will be disassembled. However, not all parts are necessarily junk and can thus be re-used in other cars (which would benefit sustainability as well). These spare parts can still be sold and used in other vehicles. We expect self-driving cars to be heavily regulated, especially regarding safety concerns. In particular, we argue the degree of regulation could be similar to used airplane parts, which must undergo utmost scrutiny and fulfill extensive documentation requirements.

Distributed ledger technology can help to alleviate documentation requirements and facilitate buying and selling of spare parts stemming from self-driving vehicles. In the airline industry, this has already been showcased by Honeywell [2], which built a Hyperledger Fabric-based marketplace for used airplanes parts, leveraging the ledger of transactions to create an easily verifiable trail of documentation for each part.

Similarly, a spare parts exchange market for electronics, sensors, actuators and other parts of self-driving vehicles is conceivable.

The use of DLT could even go further than the end of a vehicles' lifetime. By storing information about frequency of usage, driven distances, previous owners and further data, one can predict the maintenance interval for each vehicle individually which is more cost effective and increases safety in comparison to fixed maintenance intervals.

5. Summery

Distributed ledger technology can be beneficial in a variety of use cases in the context of autonomous systems. Therefore, Titus research will delve into the topic with a cross-sectional research team on distributed ledgers and it security.

In this white paper, we have laid out the fundamentals of Blockchain & DLT and have discussed in which use cases a DLT-based solution can be reasonable. Furthermore, we illustrated the applicability of DLT in the context of autonomous systems at two example use cases involving self-driving vehicles. We have seen that DLT can provide safety benefits, especially when combined with data analytics.

References

[1] Cebe M.E., *Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles*, IEEE Communications Magazine, 2018.

[2] Honeywell, Hyperledger, *Case Study: Honeywell Aerospace creates online parts marketplace with Hyperledger Fabric*, online: https://www.hyperledger.org/learn/publications/honeywell-case-study, 2019.

[3] Martínez-Díaz M.A., *Autonomous vehicles: theoretical and practical challenges*, Transportation Research Procedia, 2018.

[4] Walmart, Hyperledger, *Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric*, online: https://www.hyperledger.org/learn/publications/walmart-case-study, 2020.

[5] we.trade, Hyperledger, *Case Study: How we.trade Helps Businesses Grow with Digital Smart Contracts Powered by Hyperledger Fabric*, online: https://www.hyperledger.org/learn/publications/wetrade-case-study, 2020.

[6] Wüst K., Gervais A., *Do you Need a Blockchain?*, Proceedings of the 1st Crypto Valley Conference on Blockchain Technology (CVCBT), 2018.