Blockchains for Pay-per-use Business Models of Industrial Equipment: Insights From a Design Research Study

Daniel Beverungen and Sebastian Overhage and Albert Gorlick and Pascal Moerchel and Sebastian Schuermann
Paderborn University
daniel.beverungen@upb.de

Abstract

A blockchain features an immutable, encrypted, and distributed ledger that enables transactions even if trust and trusted intermediaries are absent. Despite research on their technological properties, few papers are on record to demonstrate (a) what business scenarios blockchains can enable and (b) under which circumstances they outperform rival technologies. This shortfall of design knowledge obscures blockchains' value proposition, its conceptual limitations, and its positioning towards rival classes of IT artifacts. We set out to design a blockchain-based IS that enables pay-per-use business models for industrial equipment—a business model that suffers from high transaction costs and complex agency dilemma caused by asymmetric information. We demonstrate how smart contracts deployed in a blockchain can level these information asymmetries. However, we also find that blockchains will only outperform rival technologies if the business scenario fulfils a set of specific properties, narrowing down the scope of application scenarios for applying blockchains substantially.

1. Introduction

Blockchains are presented as a game-changing technology that might enable trusted transactions in situations in which other means to establish trust fail [1]. Based on foundational concepts that emerged in the early 1990s [2], blockchain gained popularity as an "electronic payment system based on cryptographic proof instead of trust" [3, p. 1]. *Cryptographic proof* refers to the technical irreversibility of the transactions documented in a blockchain, which de-emphasizes the importance of establishing trust in other parties, a foundational assumption for traditional payment systems [3]. The irreversibility of transactions is guaranteed by a distributed ledger, in which transactions are stored immutably and which is maintained by a peer-to-peer network [1, 4, 5]. Apart from its technical core, blockchains can feature more elaborate business logics by establishing smart contracts [6, p. 9ff]—self-executing programs deployed to the blockchain to steer transactions [1, 7, 6, p. 9ff]. With smart contracts, complex transactions can be designed and applications other than payment systems can be developed, paving the way for using blockchains in diverse networked business scenarios [7, 8, 6, p. 9ff].

Inspired by the IS discipline's focus on applying technology for serving organizational and societal goals, current research on blockchains focuses on identifying platform features and use cases in which they can be applied [9, 5]. Advances have been made towards explaining what value blockchain technology can render to improve information systems [10] and what types of blockchains might fit different use cases best [11, 12]. However, the discipline still lacks compelling evidence to identify (a) in what business scenarios blockchains can be applied to enable trust-free transactions [9, 10], and (b) in which of these scenarios blockchains outperforms traditional classes of information systems substantially enough to offset the costs of organizational transformations for shifting to this technology. Research needs to provide compelling answers, to identify blockchains' decisive advantages and limitations.

Approaching both research directions inductively, we set out to explore if blockchain technology can enable pay-per-use business models for industrial equipment—a context that has been insufficiently explored for its potential to apply blockchains, even if it seems to fit the properties of the technology rather well. We find that smart contracts can remedy some of the information asymmetries that limit establishing pay-per-use business models in industrial business scenarios. However, the design process also raised led us to identify some profound challenges related to designing blockchains that require further investigation.

The paper unfolds as follows. In Section 2, we reflect on the properties of blockchains and on information asymmetries in pay-per-use business scenarios. In Section 3, we describe and justify our research

URI: https://hdl.handle.net/10125/71297
978-0-9981331-4-0

approach. In Section 4, we report on the design, implementation, deployment, and evaluation of smart contracts. In Section 5, we identify seven insights into the advantages and drawbacks of blockchains compared to rival technologies. We derive five properties that business scenarios must display to accommodate blockchains. We conclude the paper in Section 6.

2. Related Research

2.1. Core Features of Blockchains

We explored the body of knowledge on blockchain technology in Information Systems research by conducting a systematic literature review in September 2019. We queried the AIS Electronic Library (AISeL) for papers on "Blockchain". We categorized the resulting 124 hits by their type of publication, research method, targeted industry, type of technology, and their consideration of blockchain technology. 34 publications reported on qualitative studies, 27 conducted design science research, 24 applied conceptual research approaches, and eight were quantitative studies.

Blockchains evolved from a technology for transferring electronic coins to platforms that enable fully programmable transaction processing based on smart contracts [9, 4, 6, p. 9ff]. Blockchains are based on four principles: With a transaction, an electronic coin can be send (partly) from one *address* to another one; public-private-key encryption is used to authorize transactions; transactions are validated and added to a central ledger, subject to distributed consensus mechanisms; and the ledger is stored block-wise in a decentralized network acting as a distributed timestamp server to make the ledger tamper-proof [3, 4].

Every block contains a limited amount of transactions published by miners—also called *nodes*—to the blockchain network. Miners are rewarded with a transaction fee paid by senders for every transaction that is recognized in a new block [3]. The fee depends on the desired execution time, the amount and fees of other transactions, and the conversion rate between crypto-currency and real-world currencies [3].

Since the introduction of smart contracts—programmable sets of rules for transaction processing—into what is known as Blockchain 2.0, complex interactions can be supported in a way that requires a minimum of trust among the parties interacting. [4, 6, p. 17]. Smart contracts help to "formalize and secure relationships over public networks" [13]. They execute autonomously, are self-sufficient in their allocation of resources and assets, and execute in a decentralized ecosystem [6, p. 16]. While the technology has matured, the third generation of blockchains focuses on the technology's application in different industries and ecosystems [9, 4, 6, p. 27]. Blockchain 3.0 refers to applications that either focus on other domains than the financial sector [8, 6, p. 53] or provide interfaces to other information systems [7].

Current research on blockchains focuses on applications in finance and logistics, while few implementations target the public sector [14, 15, 16] or health care [17, 18]. Financial applications focus on initial coin offering, a blockchain-based crowd-sourcing concept [10]. Logistics applications aim at improving transparency, providing trust, or simplifying and accelerating processes for the inter-organizational and inter–national flow of information or documents [7, 19]. However, many interactions in supply chains still require physical trust and integrating technologies proves complex, while convincing incentives to use blockchains are still missing [8].

Blockchains seem best suited for scenarios in which multiple parties are involved, trust is absent, and relying on an intermediary is not an option [11, 12]. Different types of blockchains can be instantiated [5], depending on the desired permissions, data access, investment-weighting for transaction consensus, chain modularity, scalability, interoperability, centralization of regulation, and anonymity. Two types frequently discussed include *public blockchains* and *private blockchains*, in which access to data is restricted [12, 5].

While it is a myth that blockchains can offer transactions that are entirely free of trust, they might enable scenarios that were impractical to implement due to trust issues before [20, 6, p. 17]. Blockchains substitute interpersonal trust with cryptographic proof, so as to enable trust-free transactions [1, 3]. Interpersonal trust is "the willingness of a party [trustor] to be vulnerable to the actions of another [trustee] based on the expectation [trusting beliefs] that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party [trustee]" [21, p. 712]. Whereas from a mathematical perspective interpersonal trust can be replaced with cryptographic proof, from a socio-technical perspective, interpersonal trust rather shifts towards trust in technology [20, 22]. Trust in technology depends on "the willingness of a trustor to behaviorally depend on a piece of software to do a task"[23, 24, p. 330, p. 2]. Thus, blockchains' disruptive potential is disputed: While some envision them to make interpersonal trust obsolete, others content that they replace personal with artificial trustees [25, 26].

Blockchains are argued to allow implementing new

organizational forms. For instance, decentralized autonomous organizations (DAOs) enable automated and transparent self-organization by building on the governance mechanisms and decision processes defined in smart contracts [27, 28]. DAOs can act autonomously without the need to establish a central authority.

2.2. Pay-Per-Use Business Models for Industrial Equipment

Dating back to the Total Care business model invented by the aircraft engine company RollsRoyce in 2003 [29], pay-per-use (or: power-by-the-hour) business models have been accumulating attention. With this business model, aircraft operators rent engines based on their hours of operation. This business model can make costs more predictable for customers and increases the engines' availability and predictability, while it expedites maintenance processes and yields substantial cost savings [29]. For service providers, advantages include economic factors (additional revenues with after-sales services), demand conditions (satisfying more complex customer demands with bundled solutions), and competitive advantage (services are more difficult to imitate by competitors) [30, 29]. Due to their potential benefits, pay-per-use business models might be applied successfully for other "capital goods including computing, cranes, trains and aerospace"[31, 29, p. 987].

However, establishing pay-per-use business models is challenging [32]. Economic theory explains why business relationships that involve specific assets require monitoring the other party, contractual agreements, appropriate incentives, and/or high amounts of trust among the actors involved [33, 34]. A service provider can only keep an equipment available if informed on the equipment's usage and condition. With principal-agent theory, new institutional economics outlines that a *principal* (i.e., a service provider), who is unable to monitor an *agent's* (i.e., a service customer's) actions is subject to negative effects, including *moral hazard*, *hold-up*, or *adverse selection* [33]. Customers might use an equipment in inappropriate ways that might cause damage to the product, while providers would need to put the equipment back into operation. Preventing these adverse effects requires leveling information asymmetries. The agent might, for instance, signal that use of the equipment is consistent with agreed-on specifications. This signal can be send by providing data detailed enough to allow providers to monitor and assess their equipment's condition at all times. Trust has been argued to (partially) substitute the need to supervise an agent's actions.

Anecdotal evidence and case studies [35] illustrate why a complete record of an equipment's condition data often cannot be established and analyzed, while stakeholders often do not trust each other enough to offset the limitations caused by asymmetric information. Amongst others, service customers often do not want external parties to monitor the usage and condition data of their machines [35], for instance, to prevent business analysts to evaluate their stocks based on the data obtained from their machines. Due to this limitation, we currently lack a class of information systems that levels asymmetric information among service providers and service customers appropriately.

Blockchains might be the information systems to satisfy the feature set required for establishing pay-per-use business models in an industrial scenario. From a technological perspective, establishing the technology in this scenario might be a convincing business cases that blockchain enthusiasts have long been searching for to demonstrate the applicability and superiority of blockchains.

Pay-per-use business models satisfies all items on a checklist for estimating a use case's aptitude for blockchain technology [12]: They assume that data on a machine's condition is shared in a *common database* by service providers and service customers (*multiple parties involved*), while the parties potentially have *conflicting interests and trust issues*. The parties *want to avoid a trusted third party*, since they strive to protect their knowledge about complex assets (service providers) and the assets' use and condition (service customers). The parties are subject to *different rules of access to data*, while the structure of the rules governing the transactions—once established—will remain *largely unchanged* along an equipment's life-cycle. There is a need for an *objective immutable log* that documents how an equipment is used, as advocated by product life-cycle data management [36, p. 2]. While there mostly is no need for making access to data public, *consensus needs to be determined inter-organizationally*—provided that service providers and service consumers are different legal entities—pointing at designing a *private blockchain*. In contrast, we assume that establishing a conventional enterprise system will fit the requirements of intra-organizational scenarios better than a blockchain.

3. Research Method

Design science research is on a dual mission, focusing on both designing IT artifacts that provide utility to solve real-world problems, and contributing innovative theory to the discipline's knowledge base

[37, 38]. Against this backdrop, we set out to design components of a blockchain-based application system that can remedy information asymmetries that impede pay-per-use business models.

More specifically, we designed smart contracts and deployed them into the Ethereum blockchain's testnet. First, the contracts retrieve hours of operation of an equipment from a service customer's ERP system, which is crucial for a service provider to monitor and bill the use of an equipment. Second, the contracts document maintenance activities performed on the machine by a service provider, while they also document an audit trail of aggregated data on customer's use of the machine. Therefore, the contracts assure that both parties fulfil their obligations to use and maintain a machine appropriately. With the smart contracts, the blockchain connects the ERP systems of service providers and service customers, acting as an inter-organizational system.

We evaluated the smart contracts conceptually, to identify their suitability to remedy typical information asymmetries that inhibit pay-per-use business model in industrial settings. Like in other design research projects on blockchains [1, 15], we remained unable to apply and evaluate the IT artifact in a naturalistic setting, since to do so requires making substantial investments in IT infrastructure and application design. Still, our endeavor enabled us to generate substantial insights on verification times and transaction costs associated with deploying and executing smart contracts in the Ethereum blockchain. We condense these results by providing seven insights and five properties that govern the suitability of blockchains vis-á-vis rival technologies used in inter-organizational settings.

4. IT Artifact

4.1. Pay-per-use of Industrial Equipment

In our scenario, a manufacturer provides industrial equipment (machines) to an industrial service customer.

Besides their benefits, pay-per-use services can result in asymmetric information, *hidden* action and *moral hazard* [33, 30]. The service provider depends on the service customer reporting correct data that is required for billing the machine's use. Also, the provider requires service customers to use the equipment within defined parameters. Vice versa, the service customer depends on the service provider to bill machine hours correctly and to guarantee the machine's availability.

While establishing trusted intermediaries can level information asymmetry, monitoring a machine is both complex and costly [11]. Also, sharing usage data of machines with third parties contradicts data confidentiality requirements on the service customer's side, because external parties could estimate capacities and production parameters based on analyzing these data. A private blockchain can be used to counter these issues of public blockchains by limiting the data accessibility to selected third parties. This study uses the public Ethereum blockchain to test our IT artifacts' technical feasibility.

Blockchain technology's properties—replacing the need for trust and intermediaries by proofing data integrity and authenticity—might help to overcome the information asymmetries by storing data transparently in a tamper-proof and authentic record [5]. To do so, data are sent to the blockchain and verified by the network's consensus mechanisms [3]. In verification, one miner is entitled to select the transactions (based on solving a computational puzzle) that may form the next data block, before the network decides about accepting the block and rewarding the miner [3].

4.2. Conceptual Design of a Smart Contract

We designed a two-phase process to enable pay-per-use business models with a blockchain (Figure 1). First, the service provider and the service customer agree on the terms and conditions for supplying/using the industrial equipment on a pay-per-use basis. Just like in a traditional contract, this agreement might include pre-specified service levels, usage details or billing process. Process 1 prepares the execution of the blockchain-based pay-per-use process. The service provider initializes the contract with all relevant terms and conditions and deploys it to the blockchain. Once deployed, the service customer—and all parties that are registered in the smart contract as participants of the business case—can read and verify the contract. After initializing, deploying, and verifying the smart contract, the pay-per-use process is ready to be executed.

For executing the pay-per-use contract itself, we conceptualize the processes 2.1, 2.2 and 2.3. In 2.1, all data required for billing the service are tracked and posted to the blockchain, subject to data privacy restrictions. These data are collected, pre-processed, and provided to the blockchain from conventional enterprise systems, such as the service customer's ERP system. Once the data have been verified by the blockchain network's consensus algorithms, they become tamper-proof and provide a single point of truth. From now on, payments are triggered by the smart contract autonomously. Also, payments can be made using crypto-currencies featured by the blockchain.

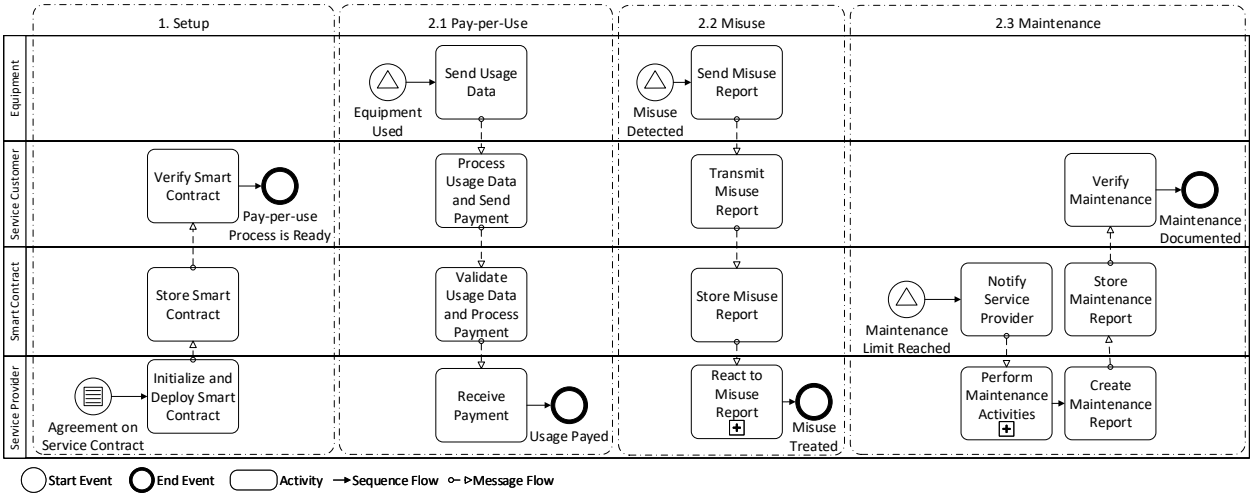

Figure 1. Pay-per-use processes supported by the smart contract

Process 2.2 deals with abnormalities in the usage behaviour. The service provider is subject to customers using an equipment in non-specified or unintended ways. While the service provider must ensure the availability of the machines, the machine must log anomalies and post this log to the blockchain in a tamper-proof audit trail.

Process 2.3 monitors the equipment's condition data and maintenance status. If the equipment is not maintained properly, the customer might face production down-times, probably causing substantial financial damage. Therefore, the service provider must ensure that pre-specified service levels are complied with by performing maintenance activities. However, the service provider might remain unable to initiate maintenance processes if the machine's condition data are unavailable. The other way round, the service customer might lack detailed data about the machine and its maintenance status. To level this bi-directional information asymmetry, the current machine status as well as maintenance processes must be documented in the smart contract.

4.3. Implementation, Deployment, and Evaluation

In our implementation, we used smart contracts and the blockchain as an inter-organizational system, networking the ERP systems of the service provider and service customer (Figure 2). The industrial equipment is traced by the service customer's ERP system. Both the service customer's and the service provider's ERP systems are equipped with a public key, that is also used as address, and a private key. To connect each ERP system to the respective address, we developed a continuously running middleware written in JavaScript and executed in the Truffe Suite,[1] a development environment for Ethereum's smart contracts that uses the web3.js library.[2] The transaction logic is written in Solidity, an object-oriented and high-level programming language for smart contracts.[3]

For initiating the smart contract, the provider must initialize the contract and deploy it from its ERP system into the blockchain. Afterwards, the customer confirms the deployed smart contract[4].

```
function sendUsage(uint256 operatingHours)
  public payable {

  require ((msg.sender == serviceCustomer));
  serviceProvider.transfer(
    operatingHours * pricePerHour);
  this.refund;
}
```

Listing 1. Smart contract for making payments

For executing the pay-per-use billing process, the machine sends its usage data to the customer's ERP system. The customer's ERP system uses our middleware to transmit the relevant usage data to the blockchain, by issuing an transaction including the usage data to the smart contract. Our design prescribes that the payment for using the equipment is transferred within this transaction, using Ethereum's

[1] Project site: https://www.trufflesuite.com/ last accessed 28.01.2020.

[2] Project site: https://github.com/ethereum/web3.js/ last accessed 28.01.2020.

[3] Project site: https://solidity.readthedocs.io/en/v0.6.1/ last accessed 28.01.2020.

[4] Sample in Ropsten at 0x9a7090c7aAaF646F8B5E5Da95349c5402AD54952

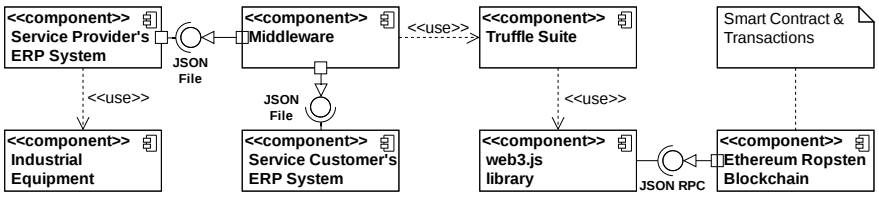

Figure 2. Component model of the implemented software prototype

crypto-currency Ether. The smart contract then redirects the payment to the service provider (Listing 1).

To document maintenance activities, the smart contract keeps track of an equipment's status and triggers corrective actions on the provider's site. When concluding maintenance, the service provider issues documents that are send to the blockchain and verified by the customer (Listing 2). The misuse identification process can be implemented similarly. Once an anomaly concerning the use of a machine is detected, the process is triggered to create and transmit a misuse report which is stored in the smart contract. The misuse is then visible to the service provider, who is enabled to perform corrective action.

```
emit maintenance(serviceCustomer,
  serviceProvider,
  confirmationSC, timestampConfirmationSC,
  confirmationSP, timestampConfirmationSP,
  counterLimit, balanceLimit);
```

Listing 2. Extract from a maintenance log

To analyze the time elapsed between posting a transaction by our middleware and its publication in the blockchain's distributed ledger, we examined the performance of Ethereum's test network Ropsten. New data can be added to Ethereum's ledger only by sending a new transaction. Ethereum is designed to add a new block in an average of 12 seconds. However, the amount of new transactions can exceed this limitation and, therefore, transaction fees are used to prioritize transaction processing. In our test, we discovered that 30 minutes passed before a transaction with a fee of 1 Gwei ($0.01; exchange rate $/ETH from 6th August 2019) was added to Ropsten's ledger, while it only took about 30 seconds until a transaction with a fee of 8 Gwei ($0.08) was mined. While the data retrieved from our test might not correspond one-on-one with the Ethereum network itself, our test indicated that processing transactions on short notice might be subject to considerable fees.

5. Discussion

The processes introduced in Section 4.2 level information asymmetries among principals and agents with a digital machine record, resolving agency dilemma in pay-per-use business models for industrial equipment. The implemented software prototype builds on deploying smart contracts to Ethereum, a public blockchain that can store data in an immutable way.

While we demonstrated how the smart contracts we deployed to the Ethereum blockchain resolve the common information asymmetries present in pay-per-use business models, it is debatable under which circumstances smart contracts deployed to a blockchain can outperform rival IT artifacts that can provide similar functionalities. In order to explore the decisive advantages and disadvantages of blockchains for a pay-per-use scenario, we reflect on the advantages and drawbacks of four classes of IT artifacts that could be used towards this end.

Apart from our prototype that builds on a public blockchain (Option 1), a private blockchain could have been used to host the same smart contracts, leveraging data confidentiality at the expense of immutability (Option 2). Further, the service provider could host the machine record on its ERP system, providing the required functionality to the other actors involved (Option 3). Finally, a trusted third party could act as a neutral intermediary, providing a platform to network the other actors (Option 4). Our assessment of all four options is summarized in Table 1.

5.1. Insights derived from our implementation

Blockchains' basic property is that data are stored immutably due to applying distributed consensus mechanisms [5, 39]. Once committed, transactions and smart contracts cannot be altered, as long as the network is large enough to prevent single entities from taking over control. Then, the ledger in both public and private blockchains is immutable [11].

Insight 1: *Blockchains are superior to rival IT artifacts in terms of providing an irreversible audit trail, e.g., for a machine's use and maintenance history.*

Category	Public blockchain (our implementation)	Private blockchain	Trusted party (Service Provider)	Trusted third party (intermediary)
Control	public ledger subjected to distributed consensus	private ledger subjected to distributed consensus	boundary object controlled by trusted party	boundary object controlled by intermediary
Application logic	deployed in autonomously executed smart contracts	deployed in autonomously executed smart contracts	controlled by trusted party	controlled by trusted third party
Authenticity & trustworthiness	+ + transactions are signed by sender's private key	+ transactions are signed by sender's private key	- - depends on implementation, probably black box	- depends on implementation, probably black box
Irreversibility	+ + transactions and smart contracts are stored irreversibly	+ transactions and smart contracts are stored irreversibly	- - trusted party controls data and application logic	- trusted third party controls data and application logic
Confidentiality and privacy	- - data are publicly accessible	- - data are accessible for members of private blockchain	+ + data transfer between peer and trusted party, access controlled by trusted party	+ + data transfer between peer and trusted third party, access controlled by trusted third party
Transaction costs for including new stakeholders	+ + new actors can join technology at will, low setup costs for new smart contracts	+ new actors can join technology on invitation, low setup costs for new smart contracts	- - identification of hidden characteristics, contracting, process and data integration required	- - identification of hidden characteristics, contracting, process and data integration required
Marginal transaction costs, speed and amount of data exchanged	- - costly distributed consensus, limited transaction processing speed	- less costly distributed consensus, can speed up transaction processing	+ + efficient data processing	+ efficient data processing, mediation fees possible
Predictability of future costs for transaction processing	- costs depend on demand for transactions	+ costs depend on demand for transaction, controlled demand	- - fees controlled by trusted party, risk of hold-up	- - fees controlled by third party, risk of hold-up
Transaction costs (ex post): Monitoring actions of other actors / moral hazard	+ + smart contracts are pre-specified, irreversible and self-executing, providing little room for hidden information	+ smart contracts are pre-specified, irreversible and self-executing, providing little room for hidden information (subjected to network)	- - actors must monitor actions by other peers to verify compliance with contracts	- actors must monitor actions by other peers (including third party) to verify compliance with contracts

Table 1. Comparison of IT artifacts for implementing a digital machine record

New actors can participate in a blockchain at will (public blockchain) or by invitation (private blockchain), subject to making small specific investments. New smart contracts can be deployed with minimal effort, reducing the need for complex contracting to be performed outside the system [40]. Middleware technologies can be used to solve integration problems between applications, including Ethereum and many ERP systems. Connecting additional actors with proprietary application systems often requires that considerable specific investments be made. Thus, blockchains fit well with scenarios in which interactions involve many different participants and in which specific investments and a priori transaction costs need to be avoided as far as possible.

Insight 2: *Blockchains are superior to rival IT artifacts in highly networked business scenarios that involve changing transaction partners, since they eliminate the need for making specific investments and allocating a priori transaction costs.*

Once committed, a transaction cannot be altered by any single actor. Likewise, a smart contract deployed to a blockchain is trustless, executes autonomously, and is self-sufficient. This immutability prevents actors from inflicting others with moral hazard, since data cannot be altered to create benefits or disadvantages [41, 42]. Traditional systems that provide a boundary object that is controlled by a single actor put less powerful actors at the jeopardy of hold-up [43, 44].

Insight 3: *Blockchains disempower single actors, leveraging equal control of the data stored and the application logic executed. Once deployed, contracts execute autonomously, reducing the risk of hold-up and ex post transaction costs on the principal's side.*

A blockchain's immutable transaction log provides data integrity as a build-in functionality that traditional database management systems (DBMS) lack. Furthermore, private key signatures are used to

assure a sender's authenticity. While both technologies are not implemented by many traditional DBMS by default, they could be extended to feature this functionality.

Insight 4: *While blockchains come with particular functionality, rival IT artifacts can be extended to implement similar levels of security and authenticity.*

While all four artifacts depend on data that are correct, providing authentic data [11, 45] is particularly crucial to realize benefits with a blockchain. In our scenario, smart contracts deployed to a blockchain correctly execute a pay-per-use process, whereas flawed data would lead to processing false payments. Inputting false data on purpose are a problem of moral hazard in all four classes of systems.

Insight 5: *Blockchains particularly rely on the authenticity of data provided by other applications.*

Public blockchains allow public access of their data, enabling anyone to track the actions performed by all participants. Even if actors use pseudonyms, there is no guarantee that they will remain covert, but they could be identified and be associated with their transactions even after considerable time. Private blockchains restrict access to blockchains to predefined users [46, 40, 47], increasing the confidentiality of their data. However, using a blockchain presupposes that data can be shared with others, limiting blockchains to data that are de-contextualized and non-critical to the survival of an organization.

Insight 6: *Rival IT artifacts outperform blockchains (particular public blockchains) in terms of data confidentiality and privacy.*

While blockchains display high latency to verifying transactions—limited to committing a few transactions per second and taking minutes to hours to confirm a transaction—rival IT artifacts can be designed to process thousands of transactions per second [44]. Blockchains' latency is due to using distributed consensus mechanisms, requiring the majority of nodes to accept a transaction before committing it to the network [47, 46]. The larger the data volume transmitted, the more time (or money) is needed to confirm a transaction, following an exponential function [48]. The costs for processing transactions on a blockchain, therefore, exceed the costs caused by rival IT artifacts considerably [49].

Insight 7: *Rival IT artifacts outperform blockchains in terms of transaction processing speed, marginal transaction fees, and data volume, limiting blockchains to scenarios that involve very small volumes of data and transactions that tolerate latency.*

5.2. Properties of business scenarios that accommodate blockchains

Based on our insights, we conclude that business scenarios must feature five properties to render blockchains superior to rival classes of IT artifacts. Most importantly, the business scenarios must benefit from the immutable ledger of transactions implemented on a blockchain

Property 1: *1. The irreversibility of the transaction data and/or smart contracts is crucial. The underlying business logic is relatively stable, making historic data valuable.*

Data provided on a blockchain are shared with outsiders or even with the general public.

Property 2: *Confidentiality of the data is not crucial, or other means can be established to protect data from analysis and interpretation by outsiders.*

Compared to rival artifacts (e.g., ERP systems), blockchains are inferior in terms of transaction costs and processing speed. Furthermore, rival IT artifacts might evolve to feature some properties possessed by blockchains. We conclude that business transactions that are mediated by blockchains must feature high asset specificity to compensate their inferior transaction costs and processing speed.

Property 3: *Transactions display high asset specificity, low frequency, and high uncertainty, and involve many participants. They require small amounts of data to be processed, tolerate latency, and provide value that is higher than the transaction fees for mining the transaction.*

Blockchains disempower single parties in terms of data ownership or control, providing a network of actors as a decentralized actor. Furthermore, blockchains are open towards including new participants or tolerating actors leaving the network.

Property 4: *The business scenario is subject to new actors entering the network or actors leaving the network. Actors strive to avoid data ownership exercised by any single actor, to relieve their risk of hold-up.*

Once deployed, smart contracts execute autonomously and cannot be stopped or changed by any single party. This continuity reduces the need to monitor transactions, lowering ex post transaction costs. On the other hand, the rules governing transactions must be fairly stable, to reduce the need to update smart contracts frequently.

Property 5: *Actors strive to avoid ex post transaction*

costs for monitoring the transactions performed by other actors, relieving their risk of moral hazard, while rules that govern transactions are fairly stable.

6. Conclusion

Blockchains present themselves as a game-changing technology that can facilitate interactions in scenarios that could not be facilitated with other information systems. One such case is establishing pay-per-use business models for industrial equipment, a case that requires the parties involved to exchange business data to avoid asymmetric information, hidden actions, and moral hazard. However, the trade-off for blockchains competitive advantage in resolving agency dilemmas are technical disadvantages regarding transaction processing speed, throughput, costs and confidentiality. We reason that blockchain's ideal business scenarios depend on highly authentic data with low confidentiality, requires transaction with high asset specificity and can not trust any single (third) party to control data or execute transactions.

We implemented a smart contract that can remedy some of the information asymmetries inherent to pay-per-use business models. On the more general level of blockchain technology's applicability and decisive advantages, our project enabled us to present new insights on designing, implementing, deploying, and operating smart contracts in Ethereum. We argue that this knowledge is urgently required to demystify blockchains' applicability, rather than jumping on the blockchain bandwagon lightly. Further research is required to elicit prospects, limitations, and business scenarios for this technology.

7. Acknowledgment

The research leading to these results received funding from the Ministry of Economics, Innovation, Digitalization and Energy, State of North Rhine-Westphalia, as part of the cluster of excellence it's OWL (project Digital Business, funding no. 005-1807-0106).

References

[1] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain – the gateway to trust-free cryptographic transactions," in *Proceedings of the 24th European Conference on IS, İstanbul, Turkey*, 2016.

[2] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[5] M. Risius and K. Spohrer, "A blockchain research framework," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 385–409, 2017.

[6] M. Swan, *Blockchain*. Sebastopol: O'Reilly Media, Inc, 1 ed., 2015.

[7] J. Kolb, J. Hornung, F. Kraft, and A. Winkelmann, "Industrial application of blockchain technology – erasing the weaknesses of vendor managed inventory," in *Proceedings of the 26th European Conference on IS, Portsmouth, UK*, 2018.

[8] H. Sternberg and G. Baruffaldi, "Chains in chains – logic and challenges of blockchains in supply chains," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 3936–3943, 2018.

[9] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain technology in business and information systems research," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 381–384, 2017.

[10] G. Fridgen, J. Lockl, S. Radszuwill, A. Rieger, A. Schweizer, and N. Urbach, "A solution in search of a problem: A method for the development of blockchain use cases," in *Proceedings of the 24th Americas Conference on IS, New Orleans*, 2018.

[11] B. Betzwieser, S. Franzbonenkamp, T. Riasanow, M. Böhm, H. Kienegger, and H. Krcmar, "A decision model for the implementation of blockchain solutions," in *Proceedings of the 25th Americas Conference on IS, Cancun*, 2019.

[12] A. Pedersen, M. Risius, and R. Beck, "A ten-step decision path to determine when to use blockchain technologies," *MIS Quarterly Executive*, vol. 18, pp. 99–115, 2019.

[13] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[14] A. Bazarhanova, J. Magnusson, J. Lindman, E. Chou, and A. Nilsson, "Blockchain-based electronic identification: Cross-country comparison of six design choices," in *Proceedings of the 27th European Conference on IS, Stockholm, Sweden*, 2019.

[15] R. Benbunan-Fich and A. Castellanos, "Digitalization of land records: From paper to blockchain," in *Proceedings of the 39th International Conference on IS, San Francisco*, 2018.

[16] E. Nagel, J. Kranz, P. Sander, and S. Hopf, "How blockchain facilitates smart city applications–development of a multi-layer taxonomy," in *Proceedings of the 27th European Conference on IS, Stockholm, Sweden*, 2019.

[17] M. Abouzahra, "Using blockchain technology to enhance the use of personal health records," in *Proceedings of the 25th Americas Conference on IS, Cancun*, 2019.

[18] P. Ndayizigamiye and A. Nurudeen, "Adoption of blockchain technology to enhance public healthcare supply chain in south africa: A systems thinking approach," in *Proceedings of the 25th Americas Conference on IS, Cancun*, 2019.

[19] K. Nærland, C. Müller-Bloch, R. Beck, and S. Palmund, "Blockchain to rule the waves - nascent design principles for reducing risk and uncertainty in decentralized environments," in *Proceedingsof the 38th International Conference on IS, Seoul, South Korea*, 2017.

[20] A. Auinger and R. Riedl, "Blockchain and trust: Refuting some widely-held misconceptions," in *Proceedings of the 39th International Conference on IS, San Francisco*, 2018.

[21] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.

[22] V. Sadhya, H. Sadhya, R. Hirschheim, and E. Watson, "Exploring technology trust in bitcoin: The blockchain exemplar," in *Proceedings of the 26th European Conference on IS, Portsmouth, UK*, 2018.

[23] D. H. McKnight, "Trust in information technology," in *The Blackwell Encyclopedia of Management* (G. B. Davis, ed.), vol. 7, pp. 329–331, Wiley-Blackwell, 2005.

[24] N. Ostern, "Do you trust a trust-free technology? toward a trust framework model for blockchain technology," in *Proceedings of the 39th International Conference on IS, San Francisco*, 2018.

[25] C. Lustig and B. Nardi, "Algorithmic authority: The case of bitcoin," in *Proceedings of the 48th Hawaii International Conference on System Sciences*, 2015.

[26] B. Notheisen, F. Hawlitschek, and C. Weinhardt, "Breaking down the blockchain hype – towards a blockchain market engineering approach," in *Proceedings of the 25th European Conference on IS, Guimarães, Portugal*, 2017.

[27] R. Beck, C. Müller-Bloch, and J. King, "Governance in the blockchain economy: A framework and research agenda," *Journal of the Association for Information Systems*, vol. 19, no. 10, pp. 1020–1034, 2018.

[28] J. Andersen and C. I. Bogusz, ""self-organizing in blockchain infrastructures: Generativity through shifting objectives and forking"," *Journal of the Association for Information Systems*, vol. 20, no. 9, pp. 1242–1273, 2019.

[29] D. J. Smith, "Power-by-the-hour: the role of technology in reshaping business strategy at rolls-royce," *Technology Analysis & Strategic Management*, vol. 25, no. 8, pp. 987–1007, 2013.

[30] R. Oliva and R. Kallenberg, "Managing the transition from products to services," *International Journal of Service Industry Management*, vol. 14, pp. 160–172, 04 2003.

[31] J. Howells, "Innovation, consumption and services: encapsulation and the combinatorial role of services," *The Service Industries Journal*, vol. 24, no. 1, pp. 19–36, 2004.

[32] V. Wolf, A. Franke, C. Bartelheimer, and D. Beverungen, "Establishing smart service systems is a challenge: A case study on pitfalls and implications," in *Proceedings of the 15th International Conference on Wirtschaftsinformatik, Potsdam, Germany*, 2020.

[33] K. J. Arrow, "Agency and the market," in *Handbook of Mathematical Economics* (K. Arrow and M. Intriligator, eds.), vol. 3, pp. 1183–1195, Elsevier Science Publishers B.V. (North- Holland), 1986.

[34] P. Keil, "Principal agent theory and its application to analyze outsourcing of software development," *SIGSOFT Softw. Eng. Notes*, vol. 30, no. 4, p. 1–5, 2005.

[35] J. Becker, D. Beverungen, M. Matzner, and O. Müller, "Design requirements to support information flows for providing customer solutions: A case study in the mechanical engineering sector," in *Proceedings of the 1st International Symposium on Services Science*, 2009.

[36] A. Saaksvuori and A. Immonen, *Product Lifecycle Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 3 ed., 2008.

[37] S. Gregor and D. Jones, "The anatomy of a design theory," *Journal of the Association for Information Systems*, vol. 8, no. 5, pp. 312–335, 2007.

[38] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action design research," *Management Information Systems Quarterly*, vol. 35, no. 1, pp. 37—-56, 2011.

[39] D. Patel, J. Bothra, and V. Patel, "Blockchain exhumed," in *2017 ISEA Asia Security and Privacy (ISEASP)*, pp. 1–12, 2017.

[40] C. G. Schmidt and S. M. Wagner, "Blockchain and supply chain relations: A transaction cost theory perspective," *Journal of Purchasing and Supply Management*, vol. 25, no. 4, p. 100552, 2019.

[41] M. Avital, R. Beck, J. King, M. Rossi, and R. Teigland, "Jumping on the blockchain bandwagon: Lessons of the past and outlook to the future," in *Proceedings of the 37th International Conference on IS, Dublin*, Association for Information Systems. AIS Electronic Library (AISeL), 2016. null ; Conference date: 11-12-2016 Through 14-12-2016.

[42] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," Working Paper 22952, National Bureau of Economic Research, December 2016.

[43] K. Wüst and A. Gervais, "Do you need a blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45–54, 2018.

[44] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain versus database: A critical analysis," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1348–1353, 2018.

[45] B. Egelund-Müller, M. Elsman, F. Henglein, and O. Ross, "Automated execution of financial contracts on blockchains," *Business & Information Systems Engineering*, vol. 59, p. 457–467, 2017.

[46] O. Labazova, "Towards a framework for evaluation of blockchain implementations," in *Fortieth International Conference on IS, Munich*, 12 2019.

[47] S. Sarmah, "Understanding blockchain technology," *Computer Science and Engineering*, vol. 8, no. 2, pp. 23–29, 2018.

[48] S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke, "A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems," in *Distributed, Ambient and Pervasive Interactions: Understanding Humans* (N. Streitz and S. Konomi, eds.), (Cham), pp. 21–34, Springer International Publishing, 2018.

[49] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu, "Comparing blockchain and cloud services for business process execution," in *2017 IEEE International Conference on Software Architecture (ICSA)*, pp. 257–260, 2017.