Synergy of Distributed Ledger Technologies and the Internet of Things*

Sebastian Kanz
Distributed Ledger Technologies
MaibornWolff GmbH
Frankfurt a.M., Germany
sebastian.kanz@maibornwolff.de

***Abstract*—The telecommunications company Cisco predicts that by 2030, more than 500 billion IOT devices connected to the Internet will have found their way into various areas of our daily lives [1]. Networked objects of our everyday life such as refrigerators, coffee machines, the automated supply chain from the business environment or a smart city are only a few examples of this business field. Although the concept of IOT is still very theoretical, several use cases have already been developed. In order to fully exploit the great potential of IOT and to implement corresponding visions, a suitable IT solution must be provided for the corresponding use case. Many different manufacturers and service providers need a uniform platform on which they can network their IOT devices, services, business logic and customers with each other and integrate a secure payment system. The question arises whether and to what extent the two innovative technologies DLT and IOT can benefit from each other and whether DLT is suitable as a scaling, high-performance and secure technology for IOT use cases. To answer this question, this paper examines an exemplary IOT use case, creates a requirements analysis and determines a suitable DLT for validating the research question by means of a market analysis and a requirements assessment. Finally, the implementation of an exemplary prototype based on the selected DLT is used to validate the results of this thesis.**

***Index Terms*—Blockchain, Distributed Ledger Technologies, Internet of Things, State Channel**

I. Introduction

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

II. Fundamental concepts

A. Distributed Ledger Technologies

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

B. Internet of Things

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

C. State-Channels for asynchronous IOT use cases

Blockchains[1] have predefined limits due to their nature. A natural limit is given by the consensus protocol independent of block size and network capacity: For example, the Bitcoin

[1]Note: This consideration is primarily concerned with public blockchains, regardless of the consensus method used. The scaling problem can usually be solved by limiting the blockchains to a private one.

network is limited to a block time of 10 minutes by the complex calculation of *Proof-of-Work (PoW)*. If the block size is very small, blocks can be propagated over the network very quickly, but only a few transactions can be transmitted at once. If the block size is very large, it is very difficult for nodes to synchronize. Instead, more transactions can be transmitted at once.

Due to this limitation on block size and block duration, Bitcoin currently (as of 01/2020) allows an average of about 7 transactions per second [2]. Other implementations may use different consensus mechanisms and other parameters, but there are natural barriers. It becomes clear that with increasing requirements, especially for transaction processing per time interval (mostly *transaction per second (TPS)*, improved performance and new approaches to solutions become necessary. A solution is sought for the poor scaling of blockchains. [2]

As a possible answer to the scaling problem of blockchains, so-called state channels are being developed. The goal is to process all kinds of status-changing operations off-chain, which are typically executed on the blockchain and stored on-chain. This reduces the number of accesses to the blockchain and the number of transactions, while at the same time improving the interaction time between individual parties. In the context of payments, this enables so-called micro-payments; state channels, which are limited to payment processing, are referred to as payment channels. These can be made faster and cheaper than normal transactions. The costs of such micro-payments can be kept very low because not all transactions are stored on the blockchain. [3]

The basic idea is the following: Alice and Bob reserve a portion of their assets on the blockchain so they can't dispose of them for the time being and open a payment channel to each other. This transaction, i.e. the opening of the payment channel, is stored on the blockchain. The volume of the channel, i.e. the assets that Alice and Bob can now exchange between each other, corresponds to the sum of the reserved assets. Your desired assets, which are to be reserved for the payment channel, can be reserved either by means of a multi-signature wallet (**Reference**) or smart contract (**Reference**). Alice and Bob now have a state of 50 Euro each. Afterwards both can send signed off-chain transactions to each other (i.e. not via the blockchain network). These transactions contain the new state: If Bob transfers 10 Euro to Alice, the state of Alice changes from 50 Euro to 60 Euro. If Bob sends another transaction of 10 Euro, the state of Alice changes to 70 Euro. Both of them can repeat this process as long as they want, as long as they are within the volume of 100 Euro. To close a channel, Alice or Bob send a transaction to the blockchain network containing the final state (in the example, Alice has 70 Euros and Bob 30 Euros). For a theoretically infinite number of transactions between Alice and Bob, only the opening and closing transaction of the payment channel must be stored onchain.

Another major advantage is the asynchronous nature of the transactions made possible by the state channel. If participants are not in the blockchain network (for example, due to connectivity problems), no transactions can be carried out. If real actions, such as opening a barrier or processing an action, are related to a blockchain status update, the real process would come to a standstill until the connection is restored if connectivity is lost. State channels could be used here to create a redundant connection that could also be used when the blockchain is not accessible. Some example implementations of state channels are Bitcoin's Lightning Network [4], Ethereum's Raiden Network, or the implementation of Neo called Trinity [5].

Another way to scale blockchain applications can be created by using side chains [6]. These are separate blockchains that run parallel to the main blockchain (also often called parent blockchain or main chain). To open a side chain, you must first prove that all assets whose status is to be changed in the side chain are locked or reserved on the main chain so that the owner cannot temporarily dispose of them (for example, through zero knowledge proofs, see [7]). These locked assets can then be transferred to the side chain. There the status can be changed; for example, a money transaction can be executed. If an asset is to be transferred back to the main chain, proof must be provided that the asset has been locked on the side chain. This prevents effects such as double spending.

Solutions such as state channels and side chains are known as layer 2 approaches: This term refers to approaches that are not directly executed on the blockchain itself (layer 1), but on a separate system.

Now what are the advantages in the context of IOT?
Keywords: asynchronous processing, offline capability

III. Pay-As-You-Use renting of gastronomy devices

Description of use case goes here.

a) Coffee Machines..: Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

A. Requirements

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus

et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

B. Market analysis DLT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

IV. Implementation

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

V. Conclusion

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

VI. Future Work

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Acknowledgment

Acknowledgment goes here

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

References

[1] Cisco, "Internet of things," 2016. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

[2] M. Macdonald, L. Liu-Thorrold, and R. Julien, "The blockchain: A comparison of platforms and their uses beyond bitcoin," 02 2017.

[3] J. Coleman, L. Horne, and X. Li, "Counterfactual: Generalized state channels," 2018. [Online]. Available: http://l4.ventures/papers/statechannels.pdf

[4] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[5] J. XU, Z. Ji, and Y. Li, "An off-chain scaling solution for neo," 2018.

[6] S. Johnson, P. Robinson, and J. Brainard, "Sidechains and interoperability," *CoRR*, vol. abs/1903.04077, 2019. [Online]. Available: http://arxiv.org/abs/1903.04077

[7] A. M. Pinto, *An Introduction to the Use of zk-SNARKs in Blockchains*, P. Pardalos, I. Kotsireas, Y. Guo, and W. Knottenbelt, Eds. Cham: Springer International Publishing, 2020.