Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain

Thomas Bocek*†, Bruno B. Rodrigues*, Tim Strasser*, Burkhard Stiller*

*Communication Systems Group (CSG), Department of Informatics (IfI)
University of Zürich (UZH)
Zurich Switzerland
E-mail: [bocek,rodrigues,stiller]@ifi.uzh.ch, tim.strasser@uzh.ch

† modum.io AG
Zurich Switzerland
Email: thomas.bocek@modum.io

***Abstract*—Blockchains are on the top of the Gartner Hype Cycle 2016 and many start-ups are integrating blockchains into their technology portfolio. While blockchains have emerged in the context of financial applications, non-financial application areas are of interest as well. In this paper, modum.io is presented, a start-up that uses IoT (Internet of Things) sensor devices leveraging blockchain technology to assert data immutability and public accessibility of temperature records, while reducing operational costs in the pharmaceutical supply-chain. The medical industry has many complex and strict environmental control process (*e.g.*, temperature and humidity) to ensure quality control and regulatory compliance over the transport of medical products. The sensor devices monitor the temperature of each parcel during the shipment to fully ensure GDP regulations. All data is transferred to the blockchain where a smart contract assesses against the product attributes. As modum.io is not the only non-financial start-up working with blockchains, a list of areas and other start-ups is provided that aim to reduce bureaucracy, distribute the infrastructure, and saving costs using blockchains.**

I. Introduction

Smart contracts have gained recently attention, especially in the context of the blockchain technology. A smart contract is a contract that can verify its correctness and enforce predefined rules, thus, smart contracts are self-executing and self-enforcing. However, a smart contract without a proper infrastructure is not ”smart” at all, because it needs such an infrastructure to run, execute, and verify these contracts. A blockchain is such an infrastructure for smart contracts that can operate in a fully autonomous and decentralized manner. Smart contracts can be used for financial services (*e.g.,* Bitcoin) or they can be used for general services *e.g.,* (Ethereum). A blockchain executes, verifies, and collects and stores smart contracts in blocks. Every block has a reference to at least one predecessor, hence the term blockchain.

Blockchains are decentralized and allow for new types distributed applications. A main interest in the financial industry for using blockchains is to automate and digitalizing processes especially when multiple stakeholders are involved. Automated processes can save money and many start-ups believe that these cost savings can be applied in other areas as well. Modum.io AG is a start-up bringing the blockchain into the pharmaceutical supply chain. As many stakeholders are involved in the supply chain, the use of blockchain technology can be used to automate processes and ultimately save costs.

The goal of this paper is a) to showcase the variety of areas where blockchains can be used, and b) to give detailed insights how modum.io AG is using the blockchain in the pharmaceutical supply chain.

The main benefit of using a blockchain with smart contracts is that these contracts can be evaluated automatically. Current solutions produce a PDF that needs to be verified manually. Using smart contracts, the temperatures can be assesses automatically and notify sender and recipient. Furthermore, the stored data is tamper-proof and can be used for audits by external parties. With Ethereum, such a tamper-proof fully decentralized system can be used at a low cost and on a per-contract and per-byte basis.

The remainder of this paper is organized as follows. Section II provides a list of start-ups in non-financial areas and Section III presents concepts and technology used in the modum.io AG start-up. Section IV outlines the technical details, which is followed by a preliminary evaluation, while Section V provides conclusions.

II. Blockchain Start-ups

In the following, new types of distributed applications and ideas besides the financial ones, such as remittance, crowdfunding, or money transfer, are discussed. An example of such an application is CargoChain [1], which is a proof-of-concept that was created at a hackathon to showcase how to reduce paperwork, such as purchase orders, invoices, bills of lading, customs documentation, and certificates of authenticity. The following sub sections discuss the most relevant applications and ideas for modum.io AG, which is fraud detection and identity management.

A. Fraud Detection

Everledger [2] offers a fraud detection system. Their main use-case is to offer a permanent ledger for diamonds. The

verification of diamonds is recorded on the blockchain, and insurance companies, owners, and law enforcers can easily check if diamonds have been verified by everledger. The main goal is to offer digital certificates to prevent fraud as a study [3] claims that 67% of fraudulent insurance claims are undetected. Everledger is a business to business service and runs a private Ethereum blockchain, provided by Eris Industries. The unique properties of a diamond are stored in the private blockchain.

Blockverify [4] is an US company trying to introduce Blockchain into the supply chain to avoid counterfeit and forgeries. Their main business areas are pharmaceuticals, luxury items, diamonds and electronics. Blockverify conducted a pilot project in the pharmaceutical sector. International Policy Network estimates that fake malaria and tuberculosis drugs cause about 700,000 deaths per year [5]. Blockverify uses the Bitcoin blockchain together with a private side chain. Every product has its private key stored in the public blockchain that can be verified by anyone. With a track and trace number it is possible to trace change of ownership, thus every change will be recorder in the private blockchain.

Another start-up is Verisart [6], which is certifying, documenting, and verifying artwork using the blockchain. Every artist can scan their artwork and an image identification algorithm with meta-data needs to be provided in order to record those data on the blockchain. The idea is also to track ownership and give artists information, which has their work and where it is. Similar to Verisart is Ascribe [7] that records ownership of artwork using the Bitcoin blockchain.

Provenance [8] is making the supply chain transparent by using blockchain to prove the authenticity of a product and to prove the origin, where it was produced. The blockchain allows to store and record those information without relying on intermediate auditors. This allows for a detailed view on the supply chain, especially on who created and assembled which part.

Chronicled [9] is preventing fraud with a focus on luxury items. They use a tamper proof smart tag, which links the sneakers to the blockchain. The blockchain is an open registry where information about buyers and sellers are stored. Thus, with the tag, everyone can check the history of buyers and sellers.

B. Identity Management

Blockstack [10] offers a service for identities, naming, storage, and authentication. Blockstack has a network of nodes with a global registry of identities, public keys, and other meta-data. A Blockstack operation, such as a transfer of a name, is represented in a Bitcoin transaction and stored in its blockchain. Thus if a Blockstack node joins the network, it can synchronize its registry data via the Bitcoin blockchain. For data storage, a DHT is used to store key value pairs, where the integrity of the values can be verified in the Bitcoin blockchain.

UniquID [11] manages identities on the blockchain, and integrating biometric data such as fingerprints, or vein patters. They use a private blockchain, which can be deployed at the customers premises.

ShoCard [12] provides and identity services on top of the Bitcoin blockchain. A prototype was presented for airline passengers that can encrypt and hash their travel document and store these resulting travel tokens in the Bitcoin blockchain. Airlines can access the blockchain and verify the travel token in a fully decentralized manner.

SolidX [13] offers a blockchain-based identity management software for location access, authentication, fraud prevention and anti-phishing. The blockchain is used to distribute keys in a secure manner.

C. Document Verification

Tierion [14] is a service to record hashes of any data or information on the Bitcoin blockchain. To reduce the load on the blockchain, Merkle Trees are used and only the Merkle Root is stored in the blockchain. Thus for a receipt of any hash in the Merkle Tree, the uncle hashes are encoded in the receipt, allowing to verify the Merkle Root in the blockchain.

Factom [15] is a method of creating an immutable audit trail. It offers Proof of Existence on top of the Bitcoin blockchain. It also allows to track updates of documents and document its process. Furthermore, Factom allows the update document to be verified according to previously specified rules.

D. Other Types of Blockchain Applications

Many other types and applications for the blockchain exists, such as Augur [16] than aims to predict markets with crowd intelligence. Anyone can participate and predict and a reward is granted if the prediction was correct. Swarm [17] is a distributed storage platform and content distribution service. It allows users to pool their storage and bandwidth resources. Resources are traded with ethers and the goal of swarm is to be DDoS-resistant, have zero-downtime, fault-tolerant and censorship-resistant. Further types are dispute resolution systems based on blockchains or Enigma [18], a decentralized cloud platform with guaranteed privacy. ChromaWay [19] has a first pilot carried out with a private blockchain for land registry. They want to use blockchain technology for real estate transactions. The Blockchain Voting Machine [20] is a digital voting solution using their own VoteUnit blockchain, trying to make votes transparent and secure.

The author of [21] argues that many public, governmental applications can be implemented in form of a permissioned ledger, in which the party of the transaction needs to proof access via a dedicated credential. Transaction parties may be authorized governmental or public offices, for which each beneficiary may access his rights from a centralized authority, controlling the distributed ledger systems access. Obviously, only to trusted parties and beneficiaries such credentials will be granted. Upon such an approach, participants may driven by the system-inherent proof of a transaction interact reliably and trustworthy without any third party.

III. MODUM.IO AG

The distribution of medicinal products for human use is highly regulated. Managing the logistics these products from the distribution center until the delivery to those who will use is a task of the utmost importance and involves various

intermediaries. The new EU (European Union) regulation "Good Distribution Practice of medicinal products for human use, (GDP 2013/C 343/01) [22] is effective as of January 1, 2016. It is an obligation to report any deviation such as temperature to the distributor and the recipient of the affected medicinal products as well as to monitor the temperature of every parcel at all times. This forces pharmaceutical companies to order special services from logistic companies, which are often not necessary as temperature categories e.g., from 15° - 25° C are often met in Spring or Autumn, or the category 2° - 30° C are met most of the days in Europe.

Blockchain technology provide a decentralized and trusted consensus in which data of medical products during the logistics process can be stored and accessed by both parties being ensured by a smart contract. The idea of smart contracts is to have a protocol or code representing a contract that is self-executing, making a contractual clause and the inclusion of a trusted third party, like a notary service, unnecessary by exchanging it with the consensus system provided by the blockchain. From a business point of view, blockchain and smart contracts allows to reduce the number of intermediaries, while compliance with GDP regulations is ensured by a smart contract self-executing on the data stored in the blockchain. Therefore, reducing the number of intermediaries in the logistics process, less manual intervention will be required, reducing both the operational expenses and the manipulation risks.

Modum.io AG is monitoring all necessary data during the transport of medicinal products by combining IoT (Internet of Things) sensors with the blockchain technology [23]. The technology guarantees data integrity and makes it impossible to tamper with records. Upon the delivery, a smart contract is executed to ensure temperature category compliance. Once in the Blockchain the data is immutable and verifiable by any party. These results are publicly accessible and reported back to the receiver as well as to the distributor. It is foreseen in the future, that the customer can check the temperatures as well. However, a serial number per pharmaceutical package has to be enforced first. The regulation for such a serial number per pharmaceutical product is in effect (Falsified Medicines Directive (FMD) - EU 2016/161) [24] and on February 2019 all individual pharmaceutical packages are required to have a serial number.

Modum.io AG and University of Zürich (UZH) are working closely together and developing the sensor devices and its software. The project and planning phase started in 2015, development and implementation started in April 2016, and the company modum.io AG was founded in July 2016.

IV. Technical Details

The modum.io AG architecture is structured into back-end, front-end, and IoT sensor devices, as outlined in Figure 1. The architecture is composed by the following components briefly described:

- **Ethereum [25] Blockchain Network**: is used to verify temperature data registered in the front-end. Smart contracts run in a virtual machine, called Ethereum Virtual Machine (EVM) enabling the verification of data by smart contracts.
- **Smart Contract**: is issued for each new shipment, being responsible for ensuring the compliance of temperature data that is associated with the shipment.
- **Database**: a relational database used to store raw temperature data and user credentials.
- **Server**: interfaces the communication between the blockchain network and front-end users, creating and modifying smart contracts, as well as storing data in the database.
- **Mobile Devices**: devices used by the end-users to register new shipments and track/send records of temperature data to the Server.
- **Sensors**: thermal sensitive devices compatible with Bluetooth technology configured to send data in a fixed polling interval to a Mobile Device.

In the back-end, the temperature compliance is ensured by smart contracts written with Solidity [1], a high-level language designed to compile code for EVM. For every new shipment or group of medical product containing specific temperature requirements, a smart contract is configured and deployed in the server-side to ensure the GDP compliance requirements. Therefore, the mapping from the shipment to its corresponding smart contract or address of the contract is made using a relational database with very low additional complexity or cost.

The server at modum.io AG hosts an Ethereum node that participates in the Ethereum network and can watch changes on its smart contracts, create new smart contracts, or call smart contract functions. The Ethereum node communicates with the HTTP (Hypertext Transfer Protocol) server over JSON (JavaScript Object Notation). Data that is sensitive or too large to store in the blockchain is stored in a PostgreSQL[2] database. This includes the raw temperature data, as these are too large to be stored in a smart contract. The smart contract verifies the temperature range, and stores the verification result in the smart contract together with a URL that point to the raw temperature data and its hash.

In the front-end, Android clients communicate with the server using REST (Representational State Transfer) API (Application Programming Interface) using JSON to encode and decode requests/responses. Screenshots of the Android client are shown in Figure 2. Therefore, using a mobile phone users can register new shipments including regulatory details within the system and that a smart contract is created for each shipment. The API should also allow the receiver of a shipment to upload the temperature measurements recorded by the sensor to the server. Both the sender and the receiver should be made aware of the result of the contract and be able to get access to the temperature measurements, preferably using a graphic visualization.

The API offered by the back-end can be used in different front-end applications in addition to a smartphone or tablet. For instance, one could use a Web application in conjunction with the mobile devices to register compliance data of new shipments and verify their respective states on the run. Therefore, one could benefit from faster ways to input compliance data

[1] https://solidity.readthedocs.io/en/develop/
[2] https://www.postgresql.org/

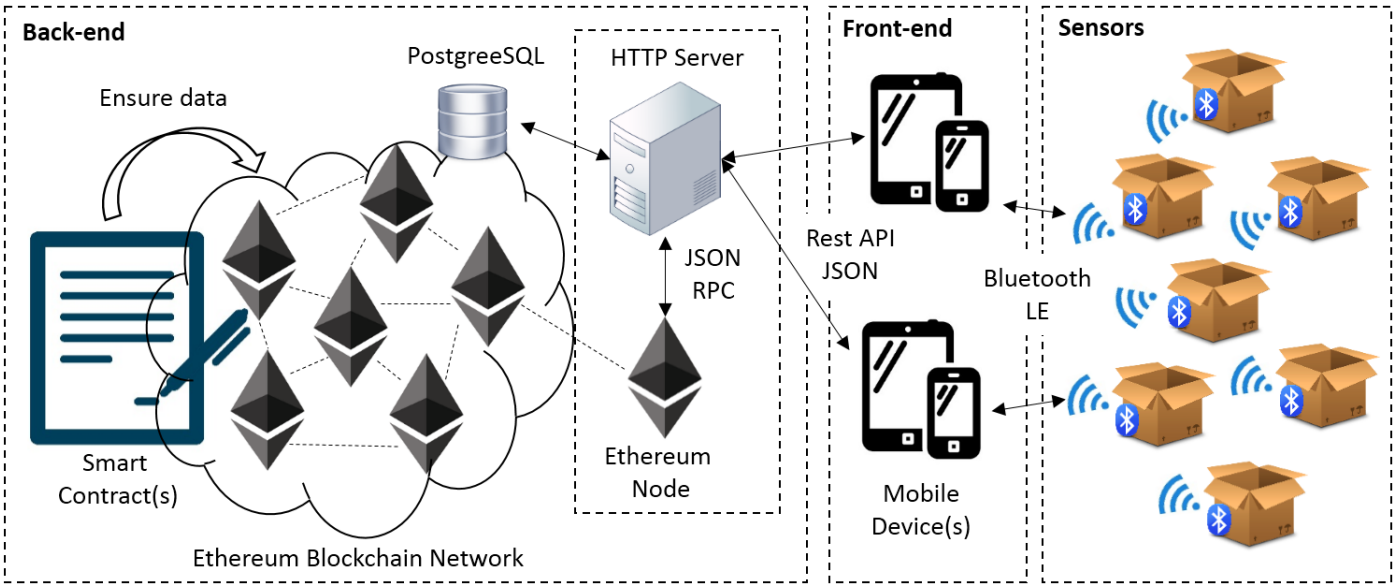

Fig. 1: Modum.io AG Blockchain Architecture

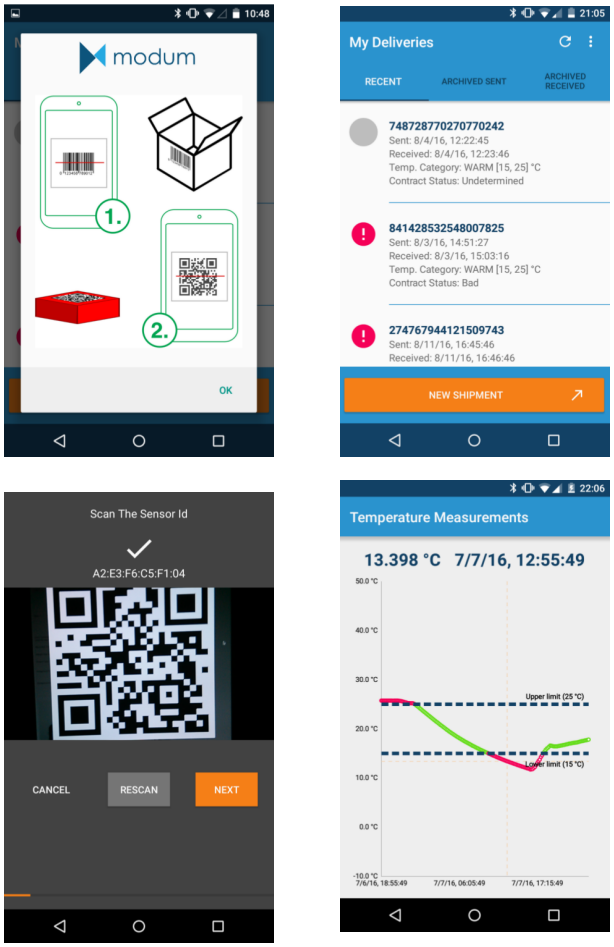

Fig. 2: Modum.io AG Front-end Screens.

in contrast with a smartphone or tablet. However, the logistics environment requires a high mobility of devices reading the sensors, or to register one or multiple barcodes at several points of the end-to-end process.

As the ”light-client” is still under development [26], the HTTP server dispatches Ethereum related calls to the Ethereum node. With the ”light-client” the Android client can use Ethereum directly. Currently a full Ethereum node is used. The Android client requires Bluetooth LE connectivity, since it is used to communicate with the sensor devices that record the temperatures. The Android client can start and stop the measurements, read the raw temperature data and send it to the HTTP server, which in turn dispatches it to the Ethereum smart contract. The source code is open and available on Github[3].

Temperature data is provided by IoT sensors by SensorTag[4] that can be placed in strategical points of the shipment. The sensor has both identification and sensing capabilities which allows to communicate the precise temperature in specific points. Furthermore, it requires Bluetooth LE connectivity which is available in most mobile devices nowadays.

With such an architecture, the following use-case is covered as shown in the sequence diagram in Figure 3: temperature monitoring is initiated with the Android client. To start the process, a sensor device needs to be within Bluetooth range. As a first step, a track-and-trace number, which is typically found on the packet, has to be associated with the MAC-address of the sensor device. Since both, track-and-trace number and MAC-address are barcodes, respectively QR-codes, the Android client captures both with its camera. After this process, the Android client starts via Bluetooth LE the temperature measurements on the sensor device, and sends the track-and-trace number/MAC-address association to the server. The sensor also stores the track-and-trace number in case no server

[3]https://github.com/modum-io
[4]www.ti.com/sensortag

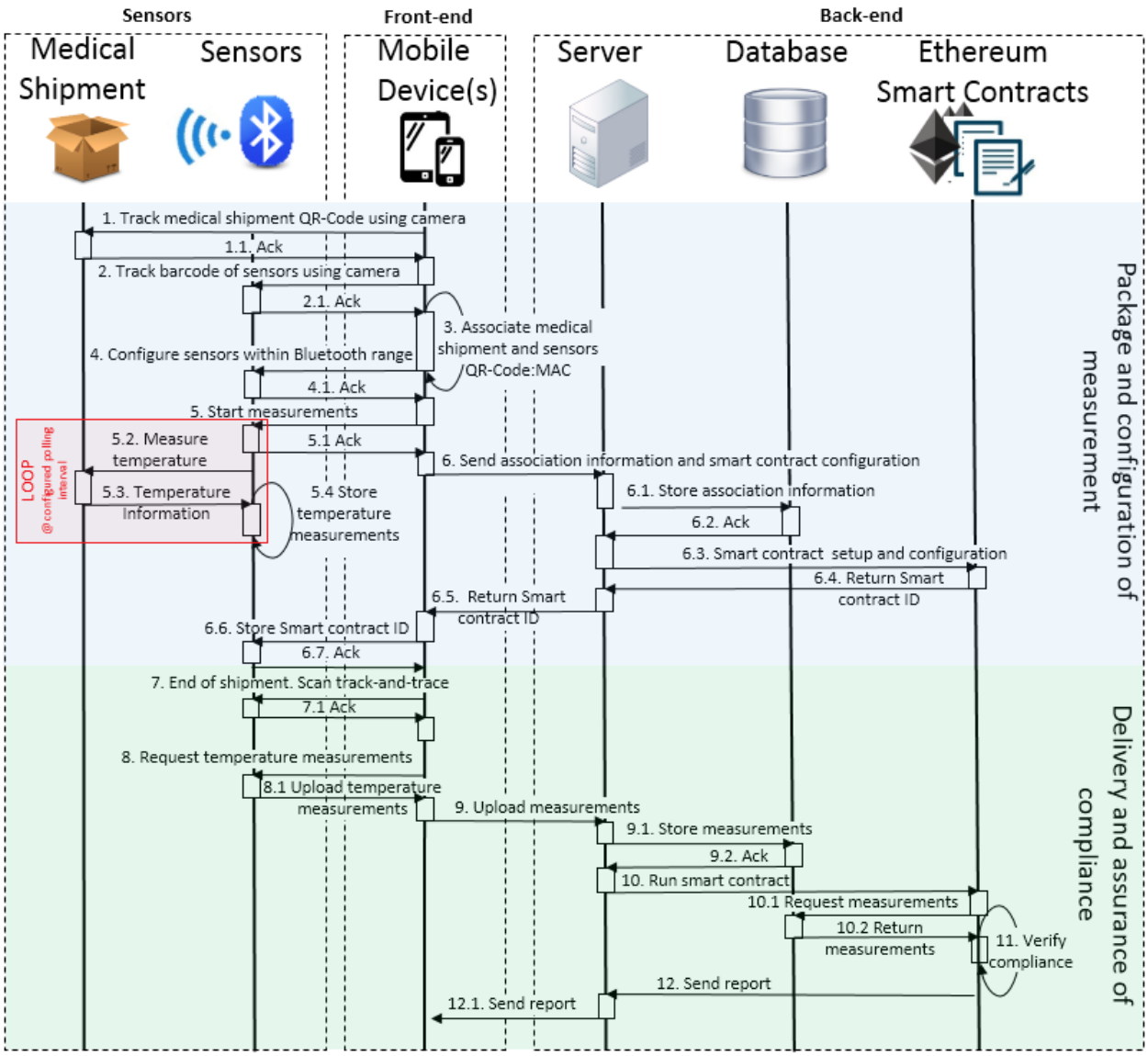

Fig. 3: Modum.io AG Sequence Diagram.

access is provided. Thus, a package that has been sent, always has an association between its MAC-address and the current track-and-trace number. The server stores the association and creates, broadcasts the smart contract, and stores the smart contract ID on the sensor device. Now the sensor device can be placed inside the medical products packet. The sensor device is recording every 10 minutes the temperature and stores it in the internal memory on the sensor device.

After receiving the packet at the destination, the track-and-trace number is scanned. The Android client requests the MAC-Address from the server to connect to the sensor device. Then the Android client automatically downloads all temperature data at once via Bluetooth LE, and sends it to the smart contract. Once the smart contract checks the temperature, anyone interested in that smart contract can verify if the temperature was within its specifications directly on the Ethereum blockchain. Thus, the sender will be notified immediately on such result.

A. *Preliminary Evaluation and Lessons Learned*

Modum.io AG has built a prototype and completed a first pilot project together with pharmaceutical distributors. From July 7th to August 12th 2016, a pilot project was conducted and medical goods were shipped weekly from one supplier to a pharmaceutical wholesaler. A total of 55 shipments were sent, in which 29 to one location selected by the wholesaler, 21 to another location, and 5 shipments were sent internally. As result, 52 were successfully completed and had associated temperature measurements. In total, 7576 temperature data points have been measured, with sensors measuring in an interval of 10 minutes. These pilots resulted in new insights and revealed potential areas to improve the prototype. Currently, modum.io AG is planning for a second pilot project with over 500 shipments with more distributors and wholesalers.

Valuable lessons were learned during these pilots. The following list presents the most important lessons:

- A warehouse has bad Internet connectivity: during the pilots projects, the offline feature (store data internally until it can be uploaded) had to be added with high priority.
- The geth Ethereum clients was not stable: during the pilot projects, the server capacity had to be increased during DoS attacks on Ethereum.
- Go with the fork: waiting to see how the fork turns out (The DAO) requires to resync the blockchain, which may take a couple of days.
- If the smart contract worked before the fork, it may not work after: after the Ethereum fork to fix the DoS attack, operation costs of the contract increased to such a point, where the contract could not be deployed anymore. As a result, the contract had to be rewritten.
- Simplicity is king: A GUI should offer as little options as possible and support only one workflow. The supported workflow should only be changed from a settings menu and not from the main screen. The initial app had two buttons: send and receive. Each pilot user where either sending or receiving, but rarely both. However, some users mixed up these buttons. Hiding the button to switch the workflow solved this problem.

The outcome of this pilot project is a refined architecture, where offline feature were taken into account as well as a higher decoupling of the Ethereum blockchain, to report temperatures at a later time. As users were asking about iOS apps, a new iOS client is currently being developed. With this pilot, security weaknesses could be identified and categorized, thus, future software and hardware development will take these identified issues into account, such as securing the data inside the sensor with signatures or access control schemes to read out the data.

V. Summary, Conclusions, and Future Work

Many financial-related start-ups are looking into blockchain-based solutions in order to reduce bureaucracy and saving costs. However, blockchains can be used in other areas as well as shown by modum.io AG and other start-ups working in non-financial areas. Ultimately, the survival rate of those start-ups and the success rate of the blockchain technology in the private and public application domain will tell, if all or only parts of those technically available characteristics and advantages can be practically exploited.

Acknowledgments

This work was supported partially by the FLAMINGO projects funded by the EU FP7 Program under Contract FP7-2012-ICT-318488.

References

[1] J. Redman, "CargoChain: The Disruptive Force in Global Trade Wins Deloittes Hackathon," Jan. 2016. [Online]. Available: https://news.bitcoin.com/cargochain-disruptive-force-global-trade-wins-deloittes-hackathon

[2] "Everledger," Sep. 2016. [Online]. Available: http://www.everledger.io

[3] "UK Insurance Key Facts," Sep. 2015. [Online]. Available: https://www.abi.org.uk/~/media/Files/Documents/Publications/Public/Migrated/Facts and figures data/UK Insurance Key Facts 2012.ashx

[4] "Blockverify," Sep. 2016. [Online]. Available: http://www.blockverify.io

[5] IPN Press release, "Fake drugs kill over 700,000 people every year - new report," Jun. 2013. [Online]. Available: http://archive.is/ipW8i

[6] "Verisart," Sep. 2016. [Online]. Available: https://www.verisart.com

[7] "Ascribe," Sep. 2016. [Online]. Available: https://www.ascribe.io

[8] "Provenance," Sep. 2016. [Online]. Available: https://www.provenance.org

[9] "Chronicled," Sep. 2016. [Online]. Available: http://www.chronicled.com

[10] "The Blockchain Application Stack," Sep. 2016. [Online]. Available: https://blockstack.org

[11] "UniquID," Sep. 2016. [Online]. Available: http://uniquid.com

[12] "ShoCard," Sep. 2016. [Online]. Available: https://shocard.com

[13] "SolidX," Sep. 2016. [Online]. Available: https://sldx.com

[14] "Your Bridge To The Blockchain," Sep. 2016. [Online]. Available: https://tierion.com

[15] "Bringing the Blockchain to Business," Sep. 2016. [Online]. Available: http://factom.org

[16] "Augur Project," Sep. 2016. [Online]. Available: https://www.augur.net

[17] "Swarm," Sep. 2016. [Online]. Available: https://github.com/ethersphere/swarm

[18] "Enigma," Sep. 2016. [Online]. Available: http://enigma.media.mit.edu

[19] "ChromaWay," Sep. 2016. [Online]. Available: http://chromaway.com

[20] "Blockchain Voting Machine," Sep. 2016. [Online]. Available: http://blockchaintechcorp.com/blockchain-apparatus/blockchain-voting-machine/

[21] Government Office for Science, "Distributed Ledger Technology: beyond block chain," Jan. 2016. [Online]. Available: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

[22] Europen Union, "Guidelines of 5 November 2013 on Good Distribution Practice of medicinal products for human use," http://ec.europa.eu/health/files/eudralex/vol-1/2013_c343_01/2013_c343_01_en.pdf, Nov. 2013.

[23] S. Norton, "CIO Explainer: What Is Blockchain?" Feb. 2016. [Online]. Available: http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/

[24] Europen Union, "Commision Delegated Regulation (EU) 2016/161 ," http://ec.europa.eu/health/files/eudralex/vol-1/reg_2016_161/reg_2016_161_en.pdf, Dec. 2012.

[25] "Ethereum Project," Sep. 2016. [Online]. Available: https://www.ethereum.org/

[26] "Light client protocol," Sep. 2016. [Online]. Available: https://github.com/ethereum/wiki/wiki/Light-client-protocol