APRIL 2019

FSBC Working Paper

Blockchain Business Models for Autonomous IoT Sensor Devices

Marc Higgins, Philipp Sandner

Cryptocurrencies have been experiencing a tremendous hype since the beginning of 2017. Their underlying blockchain technology opens the possibility to a wide range of new peer-to-peer network applications without intermediary oversight. Besides, new technology advancements create the leeway for innovations of the Internet-enabled device into our everyday lives. With the emergence of the Internet of Things (IoT), new business models have to be created, capable of handling machine to machine communication and the facilitation of micropayments. In this paper, it is examined, how blockchain characteristics and other distributed ledger technologies benefit the IoT development. Furthermore, a new blockchain business model framework for autonomous IoT sensor devices is presented.

Frankfurt School Blockchain Center
www.fs-blockchain.de
contact@fs-blockchain.de

Follow us
www.twitter.com/fsblockchain
www.facebook.de/fsblockchain

Frankfurt School of Finance & Management gGmbH
Adickesallee 32-34
60322 Frankfurt am Main
Germany

Introduction

The Internet of Things (IoT) and process automatization will revolutionize many industrial and consumer business applications. The term "Internet of Things" describes network connectivity and computing capability extended to objects, sensors and everyday items, normally not to be considered as computers (Rose, Eldridge, & Chapin, 2015). As a result, these devices can generate, exchange and consume data with minimal or no human intervention. Machines can connect directly to the Internet and therefore participate by themselves in an independent ecosystem (Christidis & Devetsikiotis, 2016). An electric car sensor, for example, could detect and connect to an inductive charge pole under the road. It searches for the cheapest electricity contract and automatically starts the charging process. As soon as the car leaves the charging pole, the car sensor automatically conducts the payment (slock.it, 2017). It is estimated that there will be more than 75.4 billion IoT devices by 2025, giving the leeway for various new developments like autonomous machines or swarm robotics (Statista, 2016). However, the lack of decentralized control and collective behavior hinder the evolution into real-world practice (Castello' Ferrer, 2017).

Blockchain technology, for the first time in history, enables various non-trusting members to interact with each other through a peer-to-peer network in a secure and verifiable manner. These disruptive characteristics attract a lot of curiosity throughout various industries (Voshmgir, 2016). Transactions which were formerly only possible through intermediary oversight can now be conducted in a decentralized consensus finding network.

Smart contracts specify a set of promises, digitally, in a protocol that automatically executes the terms of the contract (Szabo, 1996). Combining blockchain technology with the idea of smart contracts becomes a powerful technology which can transform simple sensors into decentralized autonomous corporations (DACs). DACs can make independent decisions and interact autonomously in a person to machine (P2M) and machine to machine (M2M) network. The consensus finding characteristic of blockchain technology and the possibility of self-executing programme code make the technology appealing to scientific research and IoT developers. In the current stage, business is most often conducted through an intermediate party which guarantees a trustworthy environment for person to person (P2P) and P2M transactions. The above-mentioned technology has the potential to entirely revolutionize the way of conducting transactions securely through smart contracts in a trustless peer-to-peer network with people and machines as independent actors.

Due to the novelty and technical complexity of blockchain technology, this study first outlines the shortcomings of blockchain technology and describes further developments of the distributed ledger technology (see Section Understanding blockchain technology). Secondly, a theoretical model for an IoT sensor device taxonomy is set up, that builds upon established theories (see Section Internet of Things analysis and categorization). Subsequently, a new framework for an IoT business model is presented, overcoming the proposed IoT barriers by utilizing the described blockchain characteristics (see Section IoT blockchain business model). Finally, the theoretical and practical implications are summarized in the Conclusion.

Understanding blockchain technology

Distributed Peer-to-Peer network

Blockchain technology was first introduced by Satoshi Nakamoto in 2008 in his whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System". He developed a decentralized peer-to-peer network in which an online currency, the Bitcoin, is maintained without any backing from a central authority. His idea included a distributed authoritative ledger, in which all transactions are mutually validated by a peer-to-peer network (so-called miners) to establish a secure, consenting environment and eliminate the double spending of money by one party (Nakamoto, 2008). Since then, blockchain technology has evolved into the development of distributed ledger technology. A distributed ledger is a consensus replicate of an asset database, which is shared and synchronized across a peer-to-peer network of multiple sites, geographies or institutions (Walport, 2016). In a blockchain cryptographically secured algorithms enable transactions to be aggregated into 'blocks' which are irrevocably attached to the blockchain, serving as a distributed ledger. The peer-to-peer network consists of so-called computing "nodes" which replicate and share the blockchain data structure throughout the network (Rosic, 2017). The network is open source and therefore accessible for everyone who wants to participate as well as providing resilience against attacks and system failures. All transactions are verified and approved by the consensus mechanism of the network in order to prevent payment fraud. Additionally, the chronology of events is stored in the blocks, leaving a public transaction trace on the network (Takahashi, 2017). These fundamental characteristics of the decentralized peer-to-peer network, enable secure trustless transactions between unknown parties without the oversight of a central intermediary. Moreover, blockchain technology can also be used for a secure transfer of any other digitalized good, besides cryptocurrencies.

However, the distributed blockchain technology also comes with some disadvantages to conventional centralized transaction platforms. The current blockchain networks have a lower transaction throughput and higher latencies for transaction settlements, compared to centralized platforms (Vukolić, 2015). Bitcoin and Ethereum, for example, have a transaction validation rate of 3-4 and 20 transactions per second, while Visa, as one of the largest transaction settlement providers, can handle up to 56,000 transactions per second (Vermeulen, 2017). Furthermore, the computational work for the consensus mechanism requires large amounts of energy which are compensated with transaction fees. Additionally, the transference of large data amounts, via the distributed network, clog the blockchain nodes. Lastly, the identification mechanism via the public/private key, which can be observed publicly on the blockchain, enables inferences about the user's identity. These technical conditions hinder the blockchain dissemination into real-world practices and require further developments of distributed ledger technologies, which are outlined in the chapter Evolutions of blockchain technology.

ICOs and Tokens

Internet protocols like HTTP and IP for Internet communication or SMTP for e-mail services have been providing a free infrastructure for online applications throughout history. Current Internet business models built their applications and services on top of these free to use protocols. The application layer captures all the created value, while the protocol itself solely serves as a free infrastructure layer. Therefore, these protocols can be specified as "Thin-protocols" (Monegro, 2016).

Blockchain technology is a decentralized protocol technology that rewards and motivates the user for their usage and computing power with cryptographic tokens. These new generations of protocols are referred to as "Fat-protocols" (Monegro, 2016). Blockchain protocols can be open source, allowing anyone to use them as application infrastructure. In comparison to "thin-protocol" applications, most of the value is now captured by the protocol and not the application layer (McKie, 2017). Users need protocol tokens as digital assets to access and transfer value through the blockchain network. The token gains value due to increasing demand if the protocol is commonly used, rewarding early adopters. For example, in the Bitcoin and Ethereum network, these tokens are simply called Bitcoin and Ether respectively. A suitable analogy for all tokens is a paid API key (Srinivasan, 2017). With a purchase of a token, the user can redeem access to the protocol or application. This redemption value gives the token inherent utility. In contrast to a paid API key, tokens can also be transferred to other parties without the consent of the issuer. In general, tokens can be categorized into 1st and 2nd layer tokens, varying in their underlying blockchains and codebase (Srinivasan, 2017).

1st Layer Token. The native token (currency) of a blockchain based fat-protocol is the 1st layer token, in which the transaction fee on the blockchain is paid (e.g., Bitcoin, Ethereum). The miners in the blockchain network, validating the transactions, are also rewarded in the native cryptocurrency. The overall supply of the 1st layer token of a blockchain protocol is mathematically controlled depending on the consensus mechanism. 1st layer tokens can be created in three different ways (McKie, 2017):

- Tokens based on new chains and forked code: A new blockchain is created with a modification of an existing blockchain protocol code.
- Tokens based on new chains and new code: A new blockchain protocol is created with a new codebase.
- Tokens based on forked chains and forked code: An existing blockchain is used and continued with a new or modified codebase.

Often blockchains with a 1st layer token, allow the creation of 2nd layer tokens.

2nd Layer Token. Tokens issued on top of an existing blockchain are known as 2nd layer tokens. The founder of the underlying application usually determines the supply of these tokens and is not determined by the cryptographic mining activity (McKie, 2017). These tokens are a sort of public I owe you (IOU) intended for redemption in a future new chain or other digital good. 2nd layer tokens can be "pre-mined" or sold in a “crowdsale”. Pre-mining refers to the allocation of tokens to the creators and related parties. The crowdsale, also known as Initial Coin Offering (ICO), can be compared to crowdfunding. Internet users pay for a key to use a specific application or protocol, which is often in its very early development stage. The earned money from a sold token is received by the company or organization issuing the token (Swan, Blockchain Blueprint for a New Economy, 2015). It is noteworthy to say an ICO differs from an equity sale. An equity sale underlies strict regulatory requirements while a token is only an access key to a protocol or application. Therefore, a profit sharing mechanism of an application with its token holders or the creation of legally binding voting rights is with the absence of compliance to regulatory requirements impossible. With the development of blockchain technology and the accompanying value capturing mechanism of fat-protocols, new business models can be developed which can be grouped in the following two main categories (McKie, 2017).

Decentralized business model with no dependence on a trusted 3rd party. In the first business model, a new open source protocol is developed with a native token as currency (1st layer token). This business model aims at decentralizing the Internet infrastructure with all its applications. The code is open source and publicly available on the blockchain. Participants and developers of the protocol are rewarded with its cryptocurrency. If the project is successful, demand for the cryptocurrency increases, rewarding early adopters. Due to its decentralization, the project and its business model are owned by the token holders. The level of decentralization can vary throughout the development process. New blockchain protocols can be launched in a centralized manner to convert them into a decentralized protocol (McKie, 2017).

Decentralized business model with some dependence on a trusted 3rd party. If the token is a 2nd layer token owned or issued by a private company, then the business model is partly depended on a 3rd party. The developed business model supports the proliferation of other blockchain protocols. The 2nd layer token is transferable via the decentralized underlying blockchain protocol and tradable on cryptocurrency exchanges. However, the overlaying platform/application which the token belongs to requires trust in 3rd parties. The infrastructure and application environment in which the token is used belongs to company shareholders.

Therefore, the token only serves its purpose as long as the application is not closed or removed from the application. In general, the token represents the right to use a specific application. If a lot of users demands an application, the 2nd layer token will rise in value. This means that early adopters or users are rewarded with an increase in their token value (McKie, 2017).

These two business models are also known as "Better than free" spreading the wealth and success to its user base (Srinivasan, 2017).

Evolutions of blockchain technology

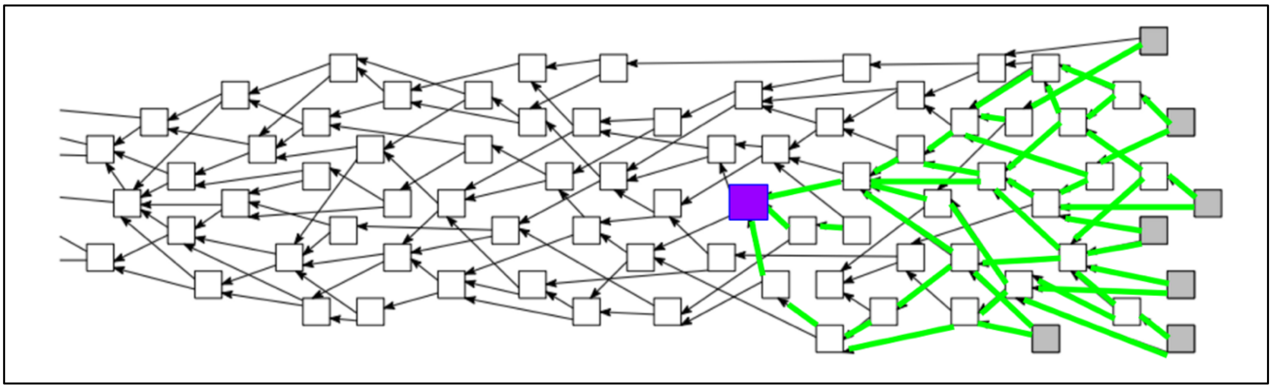
In the previous chapters, the basic ideas and mechanisms behind blockchain technology were presented as well as their shortcomings for potential deployment on a large scale. These shortcomings led to the development of a new generation of distributed ledger technologies that are fast, feeless and minerless (FFM) (Ryszkiewicz, 2017). The most prominent one of these new distributed ledger technologies is IOTA, a cryptocurrency designed for the Internet of Things (IOTA, 2017).

IOTA. IOTA is a cryptocurrency based on an open source technology, which was founded in 2015 with the aim of serving the economy of things. The open source protocol enables machine to machine communication guaranteeing interoperability, scalability and no fee transactions. The IOTA project is led by the IOTA Foundation as a registered not-for-profit entity ("gemeinnützige Stiftung") under German law and is the first German non-profit foundation capitalized solely in cryptocurrency (IOTA Tokens) (Sønstebø, IOTA Foundation, 2017).

The IOTA team identified four main weaknesses of the existing blockchain technology, being scalability, transaction fees as well as high hardware and resource requirements (Schiener, A Primer on IOTA (with Presentation), 2017). Transaction validation takes too much time with the conventional blockchain distributed ledger technology. The reward system of the high computational proof-of-work consensus mechanism for the network nodes aggravates the conduction of micro-payments. Furthermore, the proof-of-work requires a network of enormous computational power, which is vulnerable to a 51% attack, where someone supplies most of the total network's computation capacity. Therefore, IOTA developed its own distributed ledger technology, a 1st layer protocol, called the tangle. In contrast to conventional blockchain mechanism, the tangle uses a directed acyclic graph (DAG), to validate transactions in the IOTA network (Popov, 2017). Every occurring transaction in IOTA's network needs to approve two previous transactions by conducting a small amount of proof-of-work for them. Figure 1 shows a graphical interpretation of the tangle.

Figure 1

The IOTA tangle



Source: IOTA Whitepaper (2017)

The purple block symbolizes a transaction in the IOTA network. This transaction is verified directly or indirectly by subsequent transactions indicated through the green lines. It can be seen, that after a few generations of transactions, the system reaches a state in which all new indirectly verified transactions indirectly enforce the verification of the original purple transaction. The consensus mechanism works through the attachment of weights after each conformation. If a transaction carries enough weight, it is labeled as confirmed by the network. The premise is that the more transactions occur, the network increases in speed and security (Popov, 2017).

One significant difference between the IOTA tangle and conventional blockchains is the parallelization of validation, increasing transaction throughput. Furthermore, the IOTA consensus mechanism removes the arbitrary time interval of a block creation, allowing asynchronous settlement (IOTA Support, 2017). Besides, it is possible for branches to break off the network and propagate their transactions once they reconnect to the network, enabling offline transactions. This is a crucial feature for IoT because it cannot be guaranteed that IoT devices maintain Internet connectivity at all times (Schiener, A Primer on IOTA (with Presentation), 2017). Another advantage of the IOTA protocol is masked authenticated messaging (MAM). This unique feature allows the encryption of data streams on the publicly available tangle. The MAM can be used in two ways, public and private. For a public message distribution, the key to unlock the message is also the address of the message. In that way, the message is broadcasted through the tangle, allowing every participant to see its content, similar to a radio. If a message is for a private purpose, the message can only be decrypted by parties provided with the encryption key, preserving privacy and data integrity (Handy, 2017). Another advantage of IOTA is the deployment of flash channels. Some use cases require rapid and high throughput of transactions. This is realized through the setup of an off-tangle payment channel which provides a way to transact at high frequency without the need of validations through the IOTA network. These off-tangle payment channels open the possibility for instant and feeless transactions of token- and data-streams. Flash channels work as follows. Each of the participants deposits an equal amount of IOTA into a multi-signature address, which is controlled by the participating users. Once the network confirms the initial deposits, the channel does not require further network interaction until it is closed. The parties can conduct multiple transactions while the flash channel keeps track of the balances. When the parties are finished, the final balance is validated through the IOTA tangle, reducing thousands of transactions to two transactions (Freiberg, 2017).

Internet of Things analysis and categorization

The rise of IoT sensor devices - challenges and solutions

The Internet of Things (IoT) is the result of major advancements in technology and network infrastructure. Wireless Internet connectivity with IP technology as a global standard became ubiquitous available. As Moore's law predicted, computing power increased at a lower price and lower power consumption (Koomey, 2013). Miniaturization allowed computers to be implemented into tiny objects and advances in data analytics and cloud computing allow a consolidated analysis of data. These developments encourage the continuous development of Internet connectivity and computing power to a variety of objects, devices, sensors and everyday items not ordinarily considered to be computers, known as the Internet of Things (Rose, Eldridge, & Chapin, 2015). It is estimated by the International Data Corporation (IDC) that by 2020, the IoT network will consist of more than 29 billion connected devices (Business Wire, 2013). The Internet traffic of IoT devices will make up to 70% of the total Internet traffic (Cisco, 2015). Global economists expect that data generated through the IoT will drive the economic value of more than $11 trillion by 2025 (Manyika et al., 2015). This makes IoT one of the most significant and disruptive developments of our time, affecting the world environment in every aspect. A sensor network of interconnected things can achieve a much higher information collection of our world, which will result in detailed knowledge, improving efficiencies and delivering advanced services in a wide range of applications (Dorri, Kanhere, & Jurdak, 2016). IoT shifts the traditional human to human (P2P) interaction model towards a human to machine interaction (P2M) and enables a machine to machine communication (M2M).

However, the invisible pervasive collection, analysis, and dissemination of data in all aspects of the peoples' lives, as well as the coordination of millions of sensor devices, raises key challenges around IoT that have to be resolved. Security, privacy, interoperability, and standards as well as legal frameworks, are the main challenges of a further IoT development (Perera, Zaslavsky, Christen, & Georgakopoulous, 2014). Data collected from various sources, for example, can be used to offer a wide range of personalized services. Yet algorithmic data analysis could also construct a virtual bibliography revealing private behavior and lifestyle patterns. In this case, a sensor and its owner have to be uniquely identified and authenticated. The generated data has to be traceable and secured against manipulation and theft. In addition, a micro-payment system has to be established, since not everybody is willing to share their sensor data for free (Noyen, Volland, Wörner, & Fleisch, 2014).

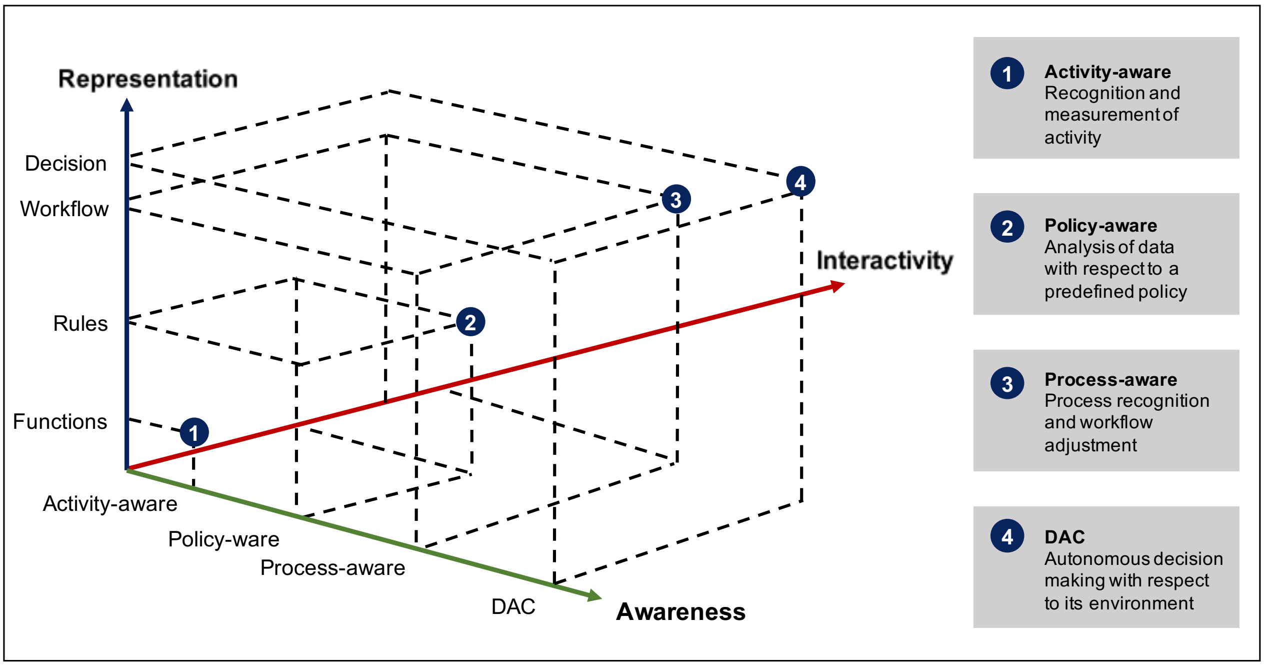
Therefore, IBM's Institute for business value, suggests a decentralized architecture for a growing IoT sensor device ecosystem. From the manufacturer's perspective, it is too expensive to maintain a centralized system, providing continuous maintenance to every sensor. From the consumer's perspective, trust into sensor devices in terms of data security can only be established through transparency. The above-mentioned issues can be resolved through a decentralized blockchain environment utilizing its core characteristics (Brody & Pureswarana, 2014). Blockchain allows decentralization and openness, granting the owner control over the sensor's data. Pseudonymous identification through hash functions grants anonymity. A peer-to-peer network decreases fees and frictions, which result from intermediary participation and facilitates a micro-payment system. Scriptability and cryptographic verifiability allow the deployment of smart contracts, putting IoT applications and services into a structured legal framework (Noyen, Volland, Wörner, & Fleisch, 2014).

Typology of IoT sensor devices

The deployment of smart sensor devices yields the foundation of an IoT economy. In the current literature, there is no standardized classification of IoT sensor devices. Kortuem et al. (2009) were the first to create architectural principles for IoT devices in an industrial environment, which can be used to develop a decentralized system of smart objects. The developed categories can be applied to a broader range of IoT use cases and supplemented with the introduction of decentralized autonomous corporations (DACs). Kortuem et al. (2009) categorized IoT sensor devices into three main architectural principles: activity-aware objects, policy-aware objects and process-aware objects (see Figure 2). Each of them represents a specific combination of the three design dimensions awareness, representation and interactivity. Awareness is the sensor's ability to understand and respond to events occurring in reality (sense, interpret and respond). Representation refers to a sensor's programming abstractions, and interaction denotes the sensor's ability to interact with the user (Kortuem, Kawsar, Fitton, & Sundramoorthy, 2009). In the following sections, each IoT sensor category is analyzed according to their degree of awareness, representation, and interaction as well as their usability in an IoT environment. A summary of the analysis is given in Table 1.

Figure 2

Categorization of IoT sensor devices



Source: Adopted and supplemented from Kortuem et al. (2009)

Table 1

Summary of IoT sensor devices

	Activity-aware IoT Sensor Device	**Policy-aware IoT Sensor Device**	**Process-aware IoT Sensor Device**	**Distributed Autonomous Corporation (DAC)**
Awareness	Collecting activity and event streams related to usage and environment	Data analysis according to a pre-defined policy and methodology	Work processes (sequence and timing of a variety of actions and events)	Reconceiving functions and operations of real physical world businesses
Representation	Time-based data collection and aggregation	Pre-defined rules determine the operation mode	Context-aware workflow model, reacting to measured process conditions	The autonomous and independent decision-making process
Interaction	No interaction with other devices or humans	Basic signaling and communication capability according to pre-defined rules	Context-aware guidance and signaling of workflow adjustments	Capable of autonomous P2M and M2M interaction through smart contracts
Measurement augmentation	e.g. activity state (on/off), activity-based count (in/out)	e.g. activity state (on/off), environmental pollution load,	e.g. supply chain monitoring of just in time activities	e.g. buying input data, value adding, selling data
Use Case	Pay – per use, Statistical observation / measurement	Health and safety applications	Supply chain management, warehouse management	Smart applications, e.g., smart locks, autonomous car charging

Source: Adopted and supplemented from Kortuem et al. (2009)

Activity-aware IoT sensor device. Activity-aware IoT sensor devices record information about their own usage, or about their environmental condition. They can be characterized as follows:

- Awareness: Activity-aware sensors understand event and activity streams which are directly affiliated with their utilization and their environment.
- Representation: Programmed to collect and aggregate activity-based data.
- Interaction: Activity-aware sensors' interaction capability is limited to data collection, accessible via its application programming interface (API).

Activity-aware objects are the most elementary form of IoT sensor devices. They do not include any form of artificial intelligence and often serve as a data collection mechanism for advanced IoT applications. Recognition algorithms detect activities or events in the sensor's data stream and apply simple aggregation functions. These aggregated data streams can be selected via the sensor's API to conduct further analysis and value adding processes. A good example of an activity-aware sensor is the RuuviTag, an advanced open-source sensor beacon, collecting temperature, relative air humidity, air pressure and acceleration (Ruuvi, 2018). The data collected by the activity-aware RuuviTag can be retrieved via its Bluetooth interface, enabling its owner to create customized IoT applications for a value-adding process. Other activity-aware objects can be rental devices, which detect the exact amount of time the object was used. This can then be converted into a financial figure to establish a pay-per-use business model. From a technical perspective, activity-aware objects only collect sensor data and apply application-specific aggregation functions (Kortuem, Kawsar, Fitton, & Sundramoorthy, 2009).

Policy-aware IoT sensor device. Policy-aware IoT sensor devices, are similar to activity-aware objects but can interpret the collected data relative to "predefined organizational policies" (Kortuem, Kawsar, Fitton, & Sundramoorthy, 2009). Their design elements are specified as follows:

- Awareness: Policy-aware sensors analyze their data in terms of their predefined organizational policy compliance.
- Representation: Its operational mode consists of rules, acting on the event and activity streams according to the organizational policies.
- Interactions: Policy-aware sensors can provide context-sensitive information about a specific world condition. They can interact within their predefined operational framework.

Policy-aware sensors are the second form of IoT sensor devices. Before a policy-aware sensor can be installed, rules have to be programmed and assigned to the sensor to fit the specific use case. These rules define, what actions or signals the IoT sensor device conducts, after analyzing the collected data in real time. The interaction with the user can vary in its design. Possible interaction designs can range from simple status information about the object handling or work activity to advanced warnings or shut down mechanisms if a process does not comply with the organizational policy anymore. Compared to activity-aware sensors, policy-aware IoT sensor devices possess computing capacity that monitors whether the collected and aggregated data complies with the predefined organizational policies. Policy-aware sensors can be applied to many use cases in an industrial context. For example, they can be used for employee security, measuring the amount of harmful radiation in a nuclear power plant and alerting the worker, in case the maximum healthy amount is reached. In a consumer context, an automated thermostat can adjust the room temperature in relation to the outside temperature in order to save energy. A policy-aware IoT sensor, therefore, has a higher degree of awareness, representation, and interaction compared to an activity-aware IoT sensor device.

Process-aware IoT sensor device. A process-aware sensor can understand its role in a large conglomerate of process steps. It knows its task in time and space in relation to the process chain. Its design dimensions have the following specifications:

- Awareness: Process-aware sensors understand the organizational process steps they are part of and relate to occurrences of real-world events within the process chain.

- Representation: The application model is a context-aware workflow model adapting its behavior based on changes in the physical world, which are often obtained from various sensor data.
- Interactive: Process-aware sensors can provide users with the context-aware guidance of tasks, deadlines, and decisions.

A process-aware sensor is the third and most advanced category of the conventional IoT sensor devices defined by Kortuem et al. (2009). It can be deployed in complex situations where work activities reach across different organizational and physical levels. A workflow is programmed into the IoT sensor device before the deployment into real-world practice. It then understands the different work steps conducted by various organizational levels. The information used to follow a process is often obtained by sensors from the previous two categories as well as human input. The sensor understands and interprets the input data by evaluating it in the process context. As a result, it can provide context-sensitive guidance about the subsequent process steps to workers or even manage the process itself. For example, in a production scheme, a process-aware object, can relate to real-time tracking of just-in-time supply and let the worker know when he has to prepare the next process step in order to minimize slack and idle time. Another example is that, consumers could use process-aware cooking devices, like the Thermomix by Vorwerk, to learn and improve various cooking steps for sophisticated dishes. Process-aware IoT devices "understand" how they are supposed to be used and guide the user's activities.

Distributed Autonomous Corporation (DAC). In the previous categories, it was shown, how IoT sensor devices benefit the user and create the opportunity for innovative information services. However, only autonomous cooperation between IoT sensor devices would facilitate the full potential of smart IoT sensor devices (Kortuem, Kawsar, Fitton, & Sundramoorthy, 2009).

Blockchain technology and the deployment of smart contracts give rise to the concept of distributed autonomous corporations (DACs). DACs are derived from artificial intelligence as decentralized corporations, with all the practical purposes of conventional corporations (Swan, Blockchain

Blueprint for a New Economy, 2015). The following characteristics are inherent for a DAC (Swan, Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization), 2015). First, its governance and functional principles are outlined publicly on the blockchain. Second, it needs to raise funds to conduct its operations through, for example, issuing tokens in a crowdfunding process. The last characteristic lies within the decision-making process. Since DACs act autonomously without human intervention, they can make their own decisions. They are required to sustain themselves by running their own economy, to earn revenue, spend it on necessary expenditures as well as engaging in a productive value creation process for their customers. This is done through smart contracts relying on the blockchain, executing predefined processes, depending on the environmental conditions of the DAC (Buterin, 2013). It is noteworthy that once a DAC is installed on the blockchain, nobody owns it and it's completely independent of human influence. The personal profit mechanism of a DAC is a result of its stake mechanism and has nothing to do with its decentralized nature (Zhang & Wen, 2016). The economic entity contains a valuable internal property, which can be distributed to various stakeholders. The stake mechanism, however, has to be predefined in the DACs governance. These features make a DAC distinctively different from a conventional software.

In terms of the previously used three dimensions, distributed autonomous corporations can be described as follows:

- Awareness: DACs reconceive functions and operations of real physical world businesses, without human intervention (Swan, Blockchain Blueprint for a New Economy, 2015).
- Representation: The independent decision-making process is learned through the definition of basic rules and automated through machine learning methods (Zhang & Wen, 2016).
- Interaction: DACs are economic independent entities, in a distributed manner and self-determined to finance their operations. They are able of P2M and M2M interaction (Buterin, 2013).

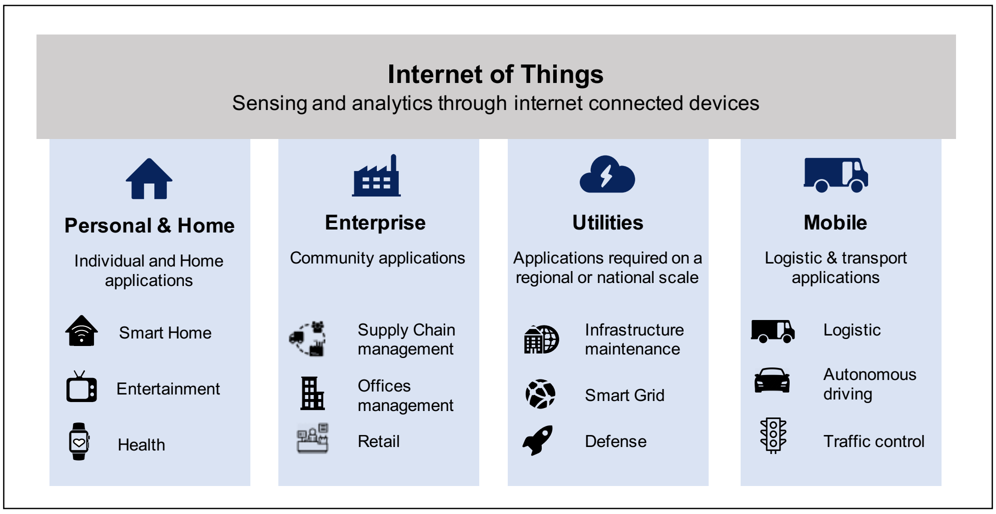
A DAC can consist of various sensors creating and analyzing data. They can independently connect to other IoT devices, trading data, and resources. In an industrial environment, a DAC could operate an entire supply chain or organize a warehouse (Bahga & Madisetti, 2016). It buys, for example, market research data or consumer consumption data provided by smart home devices, to estimate the future demand for a product. This demand estimation can be used by the DAC to adjust the production capacity or the warehouse stocking. In a consumer environment, people could deploy a DAC as a weather sensor. The sensor would buy its electricity demand via smart contracts in the blockchain peer-to-peer network and sell its data autonomously to any kind of consumers (persons / IoT sensor devices).

Areas of IoT sensor device applications

Through the growing presence of Wi-Fi and 4G–LTE wireless Internet access, the development of a ubiquitous information and communication network in the form of IoT sensor devices can be observed. This leaves the question of how our everyday life will be affected by the IoT development. Gubbi et al. (2013) from the University of Melbourne categorized IoT applications into four domains, namely personal and home, enterprise, utilities, and mobile in which IoT sensor devices can be installed (see Figure 3). The domains differentiate in the scale of impact the analyzed data provide for its users. Personal and home represent an individual or home applications while enterprise IoT applications affect a community. The utilities' domain represents applications on a regional or national scale, and mobile represents logistic applications which are cross-linked to the other domains, due to their interconnectivity requirements. Overall, the Internet enables data sharing between different entities in the ecosystem, yielding possible crossovers of applications between the four presented domains (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

Figure 3

Domains of IoT sensor device applications



Source: Adapted from Gubbi et al. (2013)

Personal and home domain. In the personal and home domain, the collected sensor information is mainly used by the individuals who own the sensor. The most common IoT applications in this domain are "healthcare" and "smart home."

For healthcare applications, people attach sensors as wearables or implants on the human body to monitor and maintain the health condition at all time. Policy-aware sensors can measure physiological parameters, notifying the user about the current health condition. This allows a ubiquitous healthcare system which could motivate unhealthy people to change their habits and enables doctors to monitor patients remotely, reducing hospitality cost (Manyika et al., 2015).

In the home setting, energy management, security and the automatization of chores will change how consumers interact with their surroundings. Everyday objects can become smart and independent through Internet connectivity. Their sensing capability enables them to complete domestic chores, like cleaning, washing or gardening. Automated thermostat sensor devices, learn the human behavior and connect to weather stations to adjust the household energy consumption, or order regularly consumed food as a process-aware sensor in a refrigerator (Perera, Zaslavsky, Christen, & Georgakopoulous, 2014). The vision of an automated home can be turned into reality if the consumer feels that, his privacy is protected sufficiently and can access everything through a common interface guaranteeing interoperability (Manyika et al., 2015).

Enterprise domain. The enterprise domain describes a “Network of Things” for enterprise-based applications. The collected information is often only used by the owner, and the data is only shared selectively. Common settings for IoT applications in the enterprise domain are industrial factories, retail shops, offices, and farming. One common application example for the enterprise domain in the industrial IoT setting is the factory management. IoT plays a major role in the current development of factory automatization and digitalization, also known as Industry 4.0. The existing infrastructure of machine sensors for security, automatization, climate control, etc. is being replaced by wireless sensor devices. This gives the flexibility to change the setup, adjust workflows through real-time data analysis and increases the process efficiency (Gubbi, Buyya, Marusic, & Palaniswami, 2013). Policy-aware sensors can improve the working condition by measuring the noise and pollution burden. Process-aware sensors can optimize inventory and predict maintenance for machinery, to guarantee an optimized production environment.

Utilities domain. The utilities domain refers to all IoT sensor data used for service optimization. The aim of IoT utility applications is the resource management, improving the cost vs. profit ratio. The basic setups are often extensive networks on a regional or national scale. Utility-based IoT applications can often be seen in the setting of “Smart Cities” or “Smart Grids.” Smart Cities IoT applications try to improve services, relieve traffic congestions, conserve water, and save energy. A common smart city IoT application is waste management. The various stakeholders (e.g., city council, recycling companies, manufacturing plants, health, and safety authorities) could use unified IoT sensor device data to optimize the collection, disposal and waste monitor mechanisms (Perera, Zaslavsky, Christen, & Georgakopoulous, 2014). Another IoT application example for the utility domain is “Smart Grids.” They could be implemented to monitor the electricity consumption at every point in the city, to efficiently modify the way energy is consumed (Yun & Yuxin, 2010). This ensures the load balance within the grid and saves valuable energy.

Mobile domain. The mobile domain includes all sorts of transportation and logistics IoT applications, due to their necessity of data sharing and interconnectivity to other domains. Applications of IoT mobile domain sensor devices are therefore not mutually exclusive of settings from the previous domains. Mobile IoT applications often relate to just-in-time supply chain management, traffic in smart cities and smart vehicles.

Traffic congestions in cities cause severe cost on social and economic activities. In a Smart City, traffic control is automated through the analysis of the traffic sensor data at various touch points, providing valuable information to stop lights or car drivers (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

Supply chain efficiency is highly dependent on just-in-time operations, enabled through monitoring of travel times and origin—destination route choice data analysis. The mobile domain also includes vehicular navigation — container shipping-, and package delivery applications between urban areas. All applications in the mobile domain are highly dependent on interconnectivity and therefore overlapping in regard to IoT sensor devices of the other domain applications.

Enablers and barriers. It can be seen that IoT applications function in an ecosystem of connected sensor devices with different stakeholders, contributing to specific applications (Rong, Guangyu, Yong, Yongjiang, & Liang, Understanding business ecosystem using a 6C framework in Internet-of-Things-based sectors, 2015). The adoption of the mentioned IoT sensor device applications is therefore mostly dependent on the trustful handling of intellectual property and the interoperability of IoT sensor devices (Manyika et al., 2015). Consumers are only willing to share their data in a trustful relationship. Enterprises are usually reluctant to use and operate technical frameworks, which are controlled by other companies. Utilizing an external platform yields the threat of getting locked in and losing value capturing potential. Therefore, companies create their own company-specific or consortium based system (Seppälä & Mattila, 2016).

However, interoperability can only be guaranteed if large consortium platforms are developed, which agree on an industry standard. This yields the thread of a vertical silo or walled gardens development, in which the platform reduces interoperability to enforce a strong customer lock-in (Filament, 2015). Blockchain technology provides a way to circumvent the trust and interoperability problem by offering a trustless distributed IoT network infrastructure in which all participants can operate freely. Therefore, the introduction of blockchain technology into IoT business models, as explained in the next chapter, can support the proceeding of IoT applications into real-world practices and make our environment more cognitive.

IoT blockchain business model

Previous work

The concept of the business model has been relatively new, with much of the scientific research appearing in the past decade of the 20th century, a time period associated with the "new economy" (Morris, Schindehutte, & Allen, 2005). With the growing practical effects of the business model concept, it receives increasing attention from the field of scientific research. However, so far no unique definition of the business model has been developed in the literature (Zott, Amit, & Massa, The Business Model: Recent Developments and Future Research, 2011). A general description of a business model can be the rational, holistic approach of how an organization does business (creates, delivers and captures value). The latest business model framework, the "business model canvas" was proposed by Osterwald and Pigneur in 2009. They defined key partners, key activities, key resources, cost structure, value proposition, customer relationship management, distribution channels, customer segment and revenue streams as the nine core elements of a business model.

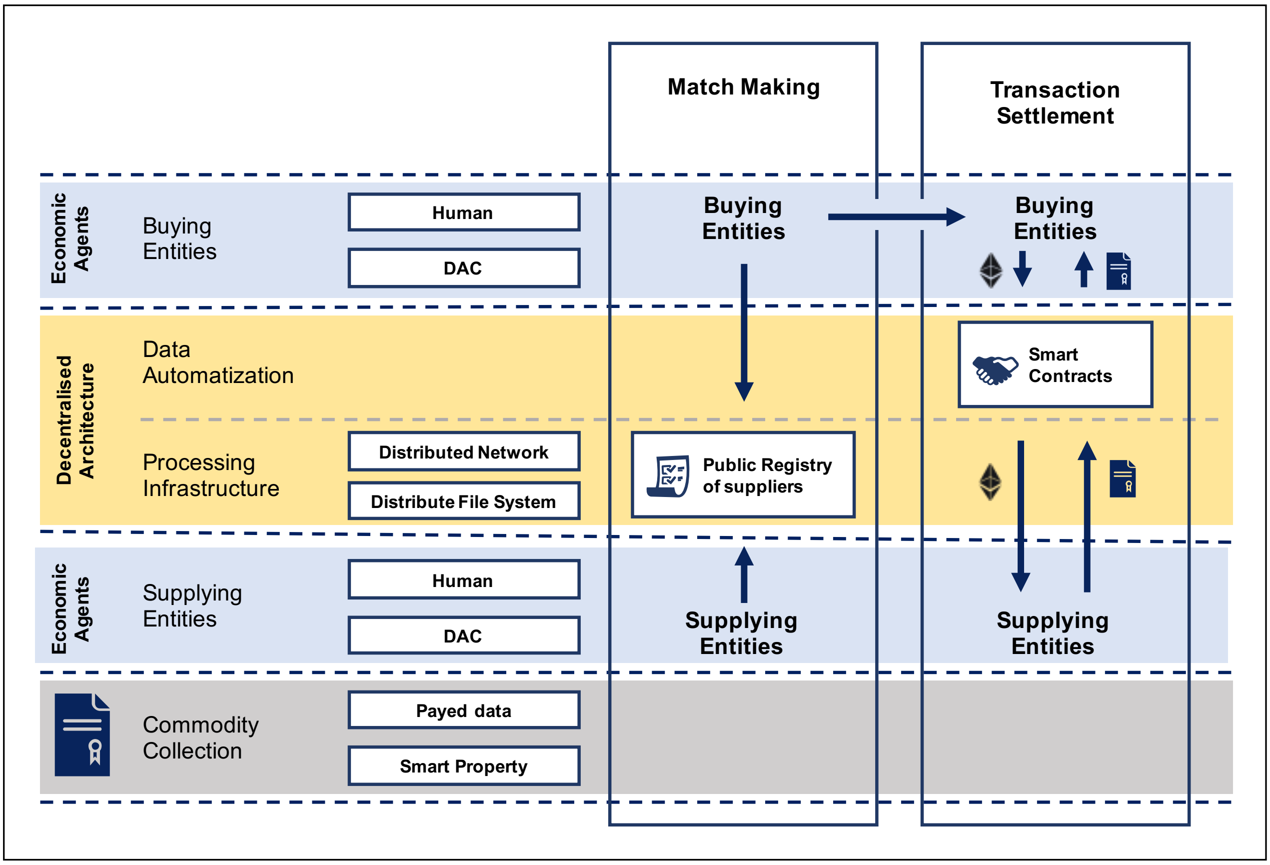
The architecture of the blockchain IoT business model

The business model for autonomous IoT sensor devices distinguishes itself from traditional e-business models. In the previous chapters the following requirements for an IoT business model were determined: 1. entities have to be uniquely identified, 2. values have to be traceable, 3. transactions have to be secured against manipulation, 4. the possibility of low-cost micropayments has to be given and 5. interoperability for machine to machine communication has to be guaranteed. This can be achieved with the "concept of trustless intermediation," in which a decentralized system enforces a set of rules (Klems et al., 2017). The following proposed business model architecture depends on the IoT business model proposed by Zhang and Wen (2016) and the decentralized service marketplace by Klems et al. (2017).

As shown in Figure 4, three different layers can be identified namely the commodity, the economic agents and the decentralized architecture layer. Commodities and economic agents are the basic layers of the IoT business models. The number of economic agents is reduced to humans and DACs (see Section Distributed Autonomous Corporation). They are the providers of the commodities and are also able to consume IoT products. The commodities in the IoT business model framework only include paid data and smart property. Paid data is data collected by sensors or humans, while smart property can be defined as tokenized assets.

Figure 4

The architecture of the blockchain IoT sensor device business model



Source: Own illustration

The core of the IoT business model is the decentralized architecture consisting of a distributed network and a distributed file system (Vermesan et al., 2017). In the decentralized architecture layer, the match making of supplying and consuming economic agents takes place as well as the transaction settlement. This happens through an open source blockchain protocol. The use of a decentralized protocol guarantees that all participants speak the same language, generating interoperability. For the match making process the conventional stages of pre-transaction, negotiation, and the contract signup have to be redefined. The match making mechanism is conducted via a public registry in which all available commodities are listed and published on the blockchain (Klems et al., 2017). Every economic agent has access to this registry (marketplace) and chooses his preferred supplier. The decentralization of the registry reduces entry barriers and decreases the lock-in effects of conventional platforms. The outcome of the matchmaking process is settled via a smart contract published on the blockchain. The legal enforcement mechanism of the smart contract conducts the consequential actions if the participating entities disobey the predefined terms, e.g., conducts the transaction or refunds the payment if programmed with an escrow function (Klems et al., 2017). Moreover, signatures, timestamps, and pseudonymous identification are recorded on the smart contract (Zhang & Wen, 2016). This secures the identification of the economic agents and the traceability of values. The network's token serves as a payment currency and can be exchanged for fiat money in cryptocurrency exchanges. Due to the decentralized architecture of the IoT business model, all transactions are conducted in a peer-to-peer manner, without the help of an intermediating third party. This decrease transaction fees and facilitates micropayments. The transactions have to be cryptographically validated by the network nodes, preventing double spending and securing the network against manipulation. Since the IoT business model follows the idea of trustless intermediation, a possessive token has to be generated for the smart property. The smart property token acts as the title of ownership and as commodity exchange certificate (Zhang & Wen, 2016).

The described architecture allows various value-generating processes and fulfills the requirements of an autonomous IoT sensor device network. Early adopters of the IoT network will profit from an increase of token values if the network gains the attention of an increasing user base (McKie, 2017).

IoT sensor devices are enabled to act independently as DACs, making P2M and M2M transactions possible.

Economic agents. In the conventional business models, three market participants can be identified, being customers, companies and the government. The customers interact with companies, dominating through their demand, consumption behavior, and purchase motivation. Companies have a double role in the conventional business model. On the one side, they are responsible for their organizational structure, manufacturing, and marketing of their commodities and services. On the other side, they also have to purchase material components or services from other companies to run their operations. The last player in the conventional business model framework is the government. The government has an economic supervisory function in advanced economies and is also a consumer for company supplied products and services (Zhang & Wen, 2016).

This setup changes in the IoT business model. In the IoT business model, the number of entities can be reduced to two, humans (private customers, companies, governments) and distributed autonomous corporations. DACs can offer IoT commodities on the public registry and earn money. They can also be required to consume other IoT products like energy or sensor data to maintain their daily operations. In the proposed blockchain IoT business model all transactions are conducted without a third-party oversight and validated by the distributed network, eliminating the threat of manipulation. No third party, including the government, can interfere in the market. The code and regulations are open source and published on the blockchain, enabling trade across state borders under a unified regulatory framework (Koulu, 2016). Smart contracts guarantee the ordered procedure of transactions. In this approach, humans represent all the entities identified in the conventional business model (private consumers, companies, governments), who can also offer their services and goods in the IoT business model (Zhang & Wen, 2016).

Commodities. Two kinds of commodities are traded in the IoT business model: Paid data and Smart property (tokenized assets). Both can be transferred digitally through the network and can be controlled by digital devices. The lack of traditional stages such as storage or shipment enables real-time settlement (DigitalLaw, 2016). The shift of ownership of physical related objects is realized through the digital token transmission of the smart property.

Paid Data. Paid data is the primary commodity in the IoT business model. To access IoT data in the current market set up, consumers have to contact the third party, providing an API which is charged according to their access time. This gives very limited possibilities for the consumer to buy real-time sensor data and does not utilize a large IoT sensor network. The previous introduced DACs are smart sensor devices connected to the Internet, with at least one static IP address (Zhang & Wen, 2016). The owner of these sensors can attribute a set of rules to the DACs which they have to comply with. For instance, these could be, a definition of the data commodity, price guidelines or mechanism on how to buy raw data and energy to maintain the DAC's daily running.

The operating procedure of the DAC is publicly available on the IoT blockchain, and the public register describes the details of the paid data (i.e., type of data, sampling rate, accuracy, and origin), price and trade conditions. Once the rules of a DAC are defined, the owner loses control over the DAC and cannot modify its settings, unless there is a pre-defined setting implemented in its governance, allowing modifications through the consensus of the stakeholders (Swan, Blockchain Blueprint for a New Economy, 2015). The value of the paid data will be determined by the market participants, and can vary to the "true value". Therefore, every sensor owner has to consider the initial and the running cost of a DAC, before deploying it on the network.

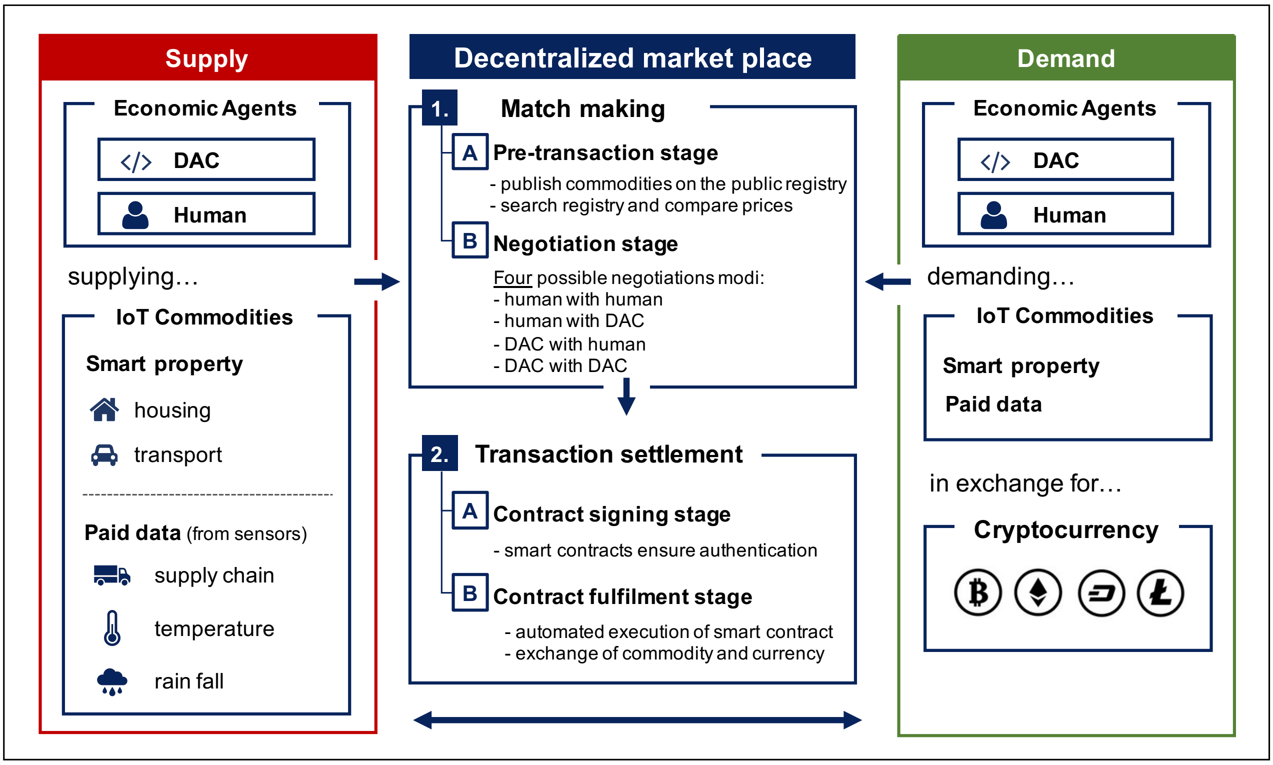
Smart Property. Smart property is controlled via a tokenized indicator of ownership and smart contracts on the blockchain (Cameronhuff, 2017). Smart property includes physical property (e.g., houses, cars, and smartphones), nonphysical property (e.g., stakes of DACs, shares of company ownership) and energies (e.g., power, oil, gas). All these forms of smart property can be controlled via digital devices. Major advantages of smart property are the minimization of fraud and intermediaries, as well as the enabling of transactions in a distributed trustless environment (Swan, Blockchain Blueprint for a New Economy, 2015).

In the current world, one can see early stages of smart property in the form of advanced car locks, or smartphone encryption, which ensures that only the user with the right key can access the device. Smart property in a blockchain environment enables the transformation of ownership via a distributed network. A car or house lock, for example, can be unlocked via a digital wallet, connected to the NFC module in the user's smartphone (slock.it, 2017).

Match making. In the blockchain IoT business model a public registry serves as a marketplace, published on the blockchain network (Klems et al., 2017). This public registry enables the match-making mechanism of supplying and consuming economic agents. Due to the lag of a third party, the operation mode of the match making in the IoT business model differs from the conventional e-business operation mode with a pre-transaction preparation-, a negotiation-, a contract signing- and a contract fulfillment stage (Zhang & Wen, 2016). Figure 5 illustrates the operation stage match making and transaction settlement for the blockchain IoT business model.

Figure 5

Decentralized marketplace in the blockchain IoT business model



Source: Own illustration

Pre-transaction stage: The pre-transaction stage of the conventional e-business model includes the preparation of all participants. For the buyers, this includes, e.g., market investigation and a purchase plan. The sellers have to produce and advertise their goods. Additionally, third-party intermediaries like financial institutions, insurance companies or transport companies have to be prepared for the corresponding trade.

In the decentralized IoT business model, the participation of third-party intermediaries is not necessary. Sellers have to publish their commodities on the public registry on the blockchain (see Figure 5). This is done with the help of a smart contract, containing references to the seller, specific information about the commodity, legal provisions and the price of the commodity (Klems et al., 2017). Buyers can search and filter the registry to find and compare the commodity they need. To keep an accurate registry available at all times, an updated version is shared across the nodes of the blockchain network. All sellers can be incentivized with an escrow function of the public registry to timely update their product portfolio.

Negotiation stage: In the negotiation stage of a traditional e-business model, buyers and sellers settle their purchase agreement in a contract, after the transaction details about the commodity and the settlement have been clarified. This traditional negotiation method does not fit the IoT business since buyers and sellers could be DACs. The following four situations (illustrated in Figure 5) can occur (Zhang & Wen, 2016):

- If seller and buyer are human, the traditional negotiation method can be used to clarify the commodity and the settlement specifications.
- If the seller is a human, and the buyer is a DAC the transaction will be conducted according to the DAC's algorithm. The human publishes his IoT product on the public registry and signs the smart contract in advance. If the product is detected by a DAC, the transaction is conducted automatically, with no negotiation or communication between the parties.
- If the buyer is a human, and the seller is a DAC, the negotiation possibility is limited to the seller's specifications in the public registry. A human buyer can browse and filter the registry until he

finds a DAC which complies with his transaction desires. No further negotiation is possible.

- If both parties are DACs, the situation is similar to the previous one. Buyer and seller act according to their pre-defined rules. If a DAC detects an offered IoT product which it needs, the transaction will be conducted automatically. Market mechanism of prices is important for a liquid DAC to DAC market, adjusting supply and demand.

Transaction settlement. The transaction settlement in the decentralized IoT business model includes the contract signing and the contract fulfillment stage of the conventional e-business operation in the form of a smart contract (see Figure 5) (Zhang & Wen, 2016).

Contract signing stage: In the conventional e-business model contracts are signed by both parties through a hand signature or an electronic data interchange (EDI) to guarantee legal effectiveness of the trade. Additional evidence like negotiation logs or files are kept to settle eventual legal disputes. Often this kind of evidence is stored at a third-party server. Due to the lack of third parties in the IoT business model, this traditional way of a contract signing is useless. In the proposed business model framework, all transactions are settled with the help of decentralized smart contracts publicly available on the blockchain. The contract is signed with the private key of each party, creating pseudonymous identification (Noyen, Volland, Wörner, & Fleisch, 2014). The decentralization of the blockchain network makes this contract accessible to everyone without intermediary participation. The payment and value transferring mechanism of the transaction is conducted through the network's tokens (cryptocurrency) which is compatible with the smart contract. The contract itself contains contractual clauses, which are triggered depending on the transaction parties' behavior.

Contract fulfillment stage: The contract fulfillment stage is drastically reduced compared to the conventional business model. No customs, insurance or packaging have to be prepared (Zhang & Wen, 2016). Furthermore, no third party is involved for the money transfer or the supply of a letter of credit. The entire transaction is conducted via a smart contract, published on the blockchain as safe storage, in a verifiable and impossible to fake manner. The contract itself can monitor and trigger the transaction. Additionally, sellers can sign smart contracts in advance and publish them on the blockchain with a timestamp (Zhang & Wen, 2016). Every buyer can accept the contract within the specific timestamp, through a signature with his private key. Two transaction phases can be distinguished in the IoT business model. One is the price payment, and the other is the exchange of commodities. If the buyer transfers the agreed token price to the smart contract, the transaction is triggered, and the purchased paid data or smart property tokens will automatically be transferred to the buyer.

The analysis of the four operating stages of the traditional and IoT business model shows various differences. As a result of the analysis, the pre-negotiation stage and the negotiation stage can be merged into the match making of the IoT business model (Zhang & Wen, 2016). Buyers and sellers can search the public registry with the help of filters and algorithms to find their desired business partner. The contract signing and contract fulfillment stage are merged into the transaction settlement of the IoT business model (Zhang & Wen, 2016). Both parties sign a smart contract with their private keys. As soon as the smart contract is triggered, the transaction is securely conducted in a peer-to-peer exchange via the blockchain network, without intermediary participation. Features of the smart contract guarantee the compliance with the contractual clauses of the transaction. The proposed business model, therefore, helps to implement IoT applications into real-world scenarios.

Current development and case study

In the present time, various startups and blockchain projects are trying to develop blockchain based IoT business models. IOTA, already described in chapter Evolutions of Blockchain Technology, is the most promising projects in this area. In the following section, it is assessed how the IOTA project complies with the proposed business model framework from the chapter IoT Blockchain Business Model and how it fits the established IoT business model requirements.

IOTA Data Marketplace

IOTA's aim is to serve as the backbone for the Internet of Things, enabling machine to machine communication and the execution of feeless micro-payments, utilizing the tangle as distributed ledger technology. In November 2017 IOTA launched its decentralized data marketplace. With the data marketplace, the IOTA foundation wants to break the so-called "Data Silos" in which most of today's sensor data is locked in, allowing an "open and decentralized data lake, accessible to any compensating party" (Sønstebø, IOTA Data Marketplace, 2017).

The architecture of the IOTA data marketplace is comparable to the proposed business model concept from chapter IoT Blockchain Business Model. The participating economic entities are humans and autonomous sensor devices, which can also be described as DACs. The tradable commodities of the data marketplace are currently limited to paid data. However, the underlying tangle also allows the transfer of every kind of digital data, including digital asset tokens (smart property).

The match making is conducted on the public registry, in form of the data marketplace. DACs can use the marketplace's API to offer their sensing services via the IOTA network. Buyers can search for IoT sensor devices and connect to them. IOTA was able to acquire a lot of official partners like Bosch to join and develop IoT sensors for the marketplace (Schiener, IOTA DATA Marketplace Webinar, 2017). Additionally, the marketplace supports silent partners, who can also use the IOTA API to deploy their IoT sensor devices on the marketplace, without being officially announced.

The tangle serves as a distributed architecture, featuring a distributed network and file system allowing to attach roughly one kilobyte of arbitrary data to a transaction (Ryszkiewicz, 2017). Once two parties agree to trade, the money and the data are directly transferred via the tangle. This form of transaction settlement can be compared to a pre-signed smart contract from chapter IoT Blockchain Business Model. As soon as the buyer orders from an IoT sensor, by transferring the required amount of IOTAs to the sensor's wallet, the paid data is automatically transferred to the buyer. In its current technical stage, the monitoring of the wallet is conducted by the sensor instead of a smart contract. This is due to the technical difficulty of implementing timestamped transactions in the IOTA tangle. The IOTA developer team has announced a smart contract release for the first half of 2018 (DevIOTA, 2017). Furthermore, it is noteworthy that the IOTA protocol guarantees interoperability between all economic entities.

Anonymity as well as private transactions are facilitated through the use of masked authenticated messaging. The transfer of large or real-time data streams can be accomplished through the deployment of flash channels as well as the ordinary use of the IOTA network. The payment is conducted in the network's cryptocurrency IOTA. All IOTA tokens are pre-minded yielding a maximum supply of 2,779,530,283,277,761 IOTAs (IOTA Support, 2017). The zero-fee mechanism enables micropayments. Furthermore, the IOTA foundation can add decimal points if a single IOTA grows too large to be used for micro transactions. According to Statista's (2016) estimations of 75 billion devices connected to the Internet by 2025, this yields an average amount of 37 thousand IOTAS per device, which should be adequate for the implementation of micropayments on a large scale. Table 2 summarizes the key characteristics and advantages of IOTA for the IoT business model.

Table 2

IOTA characteristics relevant for the blockchain IoT business model

Characteristics	IOTA characteristic
Economic Agents	The IOTA tangle is a distributed ledger technology enabling humans and distributed autonomous corporations (DACs) to interact in a P2M and M2M manner. Both can be uniquely identified by their public wallet's address.
Commodities	Paid Data and Smart Property can be transferred via the IOTA tangle network. The cryptocurrency IOTA is used to settle transactions.
Decentralized Architecture	The decentralized architecture is infinitely scalable and facilities fast feeless and miner-less microtransactions. Higher transaction utilization leads to a faster transaction validation. Masked authenticated messaging allows a secure transfer of private and public data as well as a free broadcast through the IOTA network. Flash channels allow trustful and real-time streaming of transactions without delay due to validation time.
Match making	For match making purposes distributed marketplaces can be built on top of the IOTA protocol, serving as a public registry for paid data and smart property.
Transaction settlement	Transactions can be autonomously conducted through the implementation of smart contracts and timestamped transactions in the IOTA network by 2018

In its current stage, the marketplace is supposed to serve as a proof-of-concept. The strategy of the IOTA foundation is to have the industry combining forces and develop marketplaces based on the open source IOTA protocol in the future (Schiener, IOTA DATA Marketplace Webinar, 2017). From a technical perspective, the characteristics of the IOTA developed tangle and the layer two applications like masked authenticated messaging and flash channels fulfill the requirements of the proposed blockchain IoT business model framework (see table2).

The team is currently spread across two continents with offices in Berlin, Oslo, and Chicago. Shanghai will follow in 2018. In the next years IOTA's ecosystem fund, comprising of 10.000.000 USD, will further enhance the technological development of the IOTA ecosystem. Developer teams can apply their application ideas and receive funding to create their proof-of-concept (Sønstebø, IOTA Ecosystem Fund ($10 million), 2017). The market capitalization of IOTA is currently 10,314,753,494 USD making it one of the top ten cryptocurrencies on the market (Coinmarketcap, 2018). The future will show whether the IOTA foundation can fulfill their mission of revolutionizing distributed ledger technology through its tangle and thereby becoming the "backbone of the Internet".

General implication for a commercial realization

The IOTA project shows that the proposed business model is not just a theoretical construct but rather a blueprint for an inevitable IoT economy. The IOTA concept tries to revolutionize the blockchain distributed infrastructure and develops a new distributed ledger technology, which is tailored to IoT requirements. The development of a new fat protocol should not depend on a third party. Compared to conventional business models, IOTA facilitates a distributed network and enable the deployment of DACs and machine to machine communication. The presented projects show the current relevance of blockchain IoT business models and predict, that more blockchain IoT projects will be developed in the future utilizing the blockchain IoT business model framework.

Conclusion

Theoretical implications

The presented results contribute to the existing research of blockchain technology for IoT applications in several ways. First, the characteristics of blockchain networks and its shortcomings for a large-scale implementation are outlined (Christidis & Devetsikiotis, 2016), shifting the focus away from the traditional blockchain infrastructure protocol to advanced distributed ledger technologies. By doing so IOTA's innovative tangle technology is introduced, which enables the implementation of distributed applications to a larger number of use cases.

The taxonomy for IoT sensor devices, which can be deployed in an IoT ecosystem utilizing blockchain technology, add value to the existing literature (e.g., Kortuem, Kawsar, Fitton, & Sundramoorthy, 2009) by introducing the distributed autonomous corporation. DACs are novel IoT sensor devices, which act autonomously incorporating an independent-decision making process and utilizing smart contracts. Furthermore, the paper adds to various visionary concepts of IoT based business uses cases (e.g., Perera, Zaslavsky, Christen, & Georgakopoulous, 2014; Huckle, Bhattachrya, White, & Beloff, 2016; Bahga & Madisetti, 2016) by promoting a new blockchain IoT business model framework. This fills the literature gap for IoT business models in which various actors (person/machine) conduct transactions without the need of a trusted intermediary. In addition, the appearance of the economic entities, the traded goods and the declaration of ownership are outlined in the proposed IoT business model. The combining of the conventional e-business model transaction stages into the match making, and transaction settlement stage shows the fundamental differences between the proposed blockchain IoT business model and the conventional e-business.

Practical implications

Besides extending the academic literature, the present study also has practical impact on the future IoT development as well as the way in which we currently conduct our transactions. For IoT developers, a revolutionary business model framework was proposed, fulfilling the requirements for a large-scale implementation of IoT applications. Furthermore, the taxonomy of IoT sensor devices facilitates the development of future autonomous IoT sensors, customized for specific IoT applications. In the current world, business is conducted through an intermediate party which guarantees a trustworthy environment for P&P and P&M transactions. The proposed blockchain IoT business model will entirely revolutionize the way of conducting transactions through smart contracts in a trustless peer-to-peer network with people and machines as independent actors. This will affect our everyday life in every aspect. It was also shown, that the IOTA project follows the theoretical model, driving the expectation to see more distributed IoT applications in the future. Therefore, start-ups as well as established corporations can use the proposed business model framework as a blueprint for a decentralized IoT environment.

Today the world is on the edge of a technological revolution with the potential to disrupt our economy. This will shift the power of centralized ecosystems into a uniform decentralized network where every human and machine has equal power over their data and property.

If you like this article, we would be happy if you forward it to your colleagues or share it on social networks.

Marc Higgins is graduate of the Frankfurt School of Finance and Management and has recently finished his final thesis on this topic. You can contact him via mail (m.higgins@gmx.de).

Prof. Dr. Philipp Sandner is head of the Frankfurt School Blockchain Center. You can contact him via mail (email@philipp-sandner.de), via LinkedIn (https://www.linkedin.com/in/philippsandner/) or follow him on Twitter (@philippsandner).

Aliessi, M. D. (01 06 2016 г.). How Does the Blockchain Work? Получено из Medium: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Amit, R., & Zott, C. (2001). Value Creation in e-business. Strategic Management Journal, 22, 493-520.

Armstrong , M., & Zhou, J. (2011). Paying for prominence. The Economic Journal , 121, 368-395.

Bahga, A., & Madisetti, V. K. (2016). Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, 533-546.

Bauerle, N. (09 01 2018 г.). What is the Difference Between Public and Permissioned Blockchains? Получено 09 01 2018 г., из coindesk: https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/

bitcoinwiki. (04 03 2016 г.). Block. Получено из bitcoinwiki: https://en.bitcoin.it/wiki/Block

bitcoinwiki. (26 11 2016 г.). Double-Spending. Получено из Bitcoin Wiki: https://en.bitcoin.it/w/index.php?title=Irreversible_Transactions&redirect=no

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005). Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. В W. Weber, J. Rabaey, & E. Aarts, Ambient Intelligence (стр. 5-29). Berlin: Springer.

Brody, P., & Pureswarana, V. (2014). Device democracy Saving the future of the Internet of Things. Somers: IBM Institute for Business Value.

Brown, R. G. (10 02 2015 г.). A simple model for smart contracts. Получено из gendal.me: https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/

Bucherer, E., & Uckelmann, D. (2011). Business Models for the Internet of Things. В D. Uckelmann, M. Harrison, & F. Michahelles, Architecting the Internet of Things (стр. 253-277). Berlin: Springer.

Business Wire. (01 09 2013 г.). The Internet of Things Is Poised to Change Everything, Says IDC. Получено из A Berkshire Hathaway Company: http://www.businesswire.com/news/home/20131003005687/en/Internet-Poised-Change-IDC

Buterin, V. (13 09 2013 г.). Bootstrapping A Decentralized Autonomous Corporation: Part I. Получено из Bitcoin Magazine: https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274/

Cameronhuff, A. (30 05 2017 г.). Op Ed: How Tokenization Is Putting Real-World Assets on Blockchains. Получено из Bitcoin Magazine: https://bitcoinmagazine.com/articles/op-ed-how-tokenization-putting-real-world-assets-blockchains/

Castello' Ferrer, E. (25 6 2017 г.). The blockchain: a new framework for robotic swarm systems. MIT Media Lab.

Chesbrough, H., & Rosenbloom, R. S. (2002). The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies. Industrial and Corporate Change, 11, 529-555.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292 - 2303.

Cisco. (27 05 2015 г.). Cisco Visual Networking Index: Forecast and Methodology, 2016-2021. Получено из Cisco: http://www.cisco.com/c/en/us/ solutions/collateral/service-provider/ ip-ngn-ip-next-generation-network/white_ paper_c11-481360.pdf

Coinmarketcap. (14 01 2018 г.). Cryptocurrency Market Capitalizations Coins. Получено из Cryptocurrency Market Capitalizations: https://coinmarketcap.com/coins/

Davidsen, M., Gajek, S., Kruse, M., & Thomsen , S. (03 04 2017 г.). Empowering the Economy of Things. Получено из Weeve.network: https://weeve.network/papers/weeve_whitepaper

DevIOTA. (13 11 2017 г.). IOTA. Получено из reddit: https://www.reddit.com/r/Iota/comments/7e9cwr/iota_aiming_to_release_smart_contracts_within_the/

DigitalLaw. (26 12 2016 г.). Revolutionize trading with Blockchain technology. Получено из Medium: https://medium.com/@Techexpro/revolutionize-trading-with-blockchain-technology-1affa5f91c24

Dijkman, M. R., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. International Journal of Information Management, 35, 672-678.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in Internet of Things: Challenges and Solutions. arXiv: 1608.05187.

Douceur, J. R. (2002). The Sybil Attack. В K. F. Druschel P., Peer-to-Peer Systems. IPTPS 2002. Lecture Notes in Computer Science (Т. 2429, стр. 251-260). Berlin: Springer .

Einav, L., Farronato, C., & Levin, J. (2016). Peer-to-Peer Markets. Annual review of Economics, 8, 615-635.

Eliaz, K., & Spiegler, R. (2011). A Simple Model of Search Engine Pricing. The Economic Journal, 121, 329-339.

Evans, P., & Gawer, A. (2016). The Rise of the Platform Enterprise: A Global Survey. The Center for Global Enterprise. New York: The Center for Global Enterprise.

Filament. (04 06 2015 г.). A Declaration of Device Independence. Получено из Medium: https://medium.com/@FilamentHQ/a-declaration-of-device-independence-b6f83e8b6441

Franco, P. (2014). Understanding Bitcoin: Cryptography, Engineering and Economics. New York: Wiley.

Freiberg, L. (24 09 2017 г.). Instant & Feeless— Flash Channels. Получено из Medium: https://blog.iota.org/instant-feeless-flash-channels-88572d9a4385

Giaglis, G. M., Klein, S., & O'Keefe, R. M. (2002). The role of intermediaries in electronic marketplaces: developing a contingency model. Information Systems Journal, 12, 231-246.

Greenspan, G. (22 11 2015 г.). Avoiding the pointless blockchain project. Получено из multichain: https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (07 09 2013 г.). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645 - 1660.

Hagiu, A., & Jullien, B. (2011). Why Do Intermediaries Divert Search? The RAND Journal of Economics, 42, 337-362.

Hagiu, A., & Wright, J. (2015). Marketplace or reseller? Management Science, 61(1), 184-203.

Handy, P. (04 11 2017 г.). Introducing Masked Authenticated Messaging. Получено из Medium: https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e

Huckle, S., Bhattachrya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. Procedia Computer Science, 461-466.

IOTA. (21 05 2017 г.). IOTA The Tconomy of Things. Получено из IOTA : https://iota.org

IOTA Support. (21 05 2017 г.). An introduction to IOTA. Получено из IOTA Support: https://iotasupport.com/whatisiota.shtml

Klems, M., Eberhardt, J., Tai, S., Härtlein, S., Buchholz, S., & Tidjani, A. (2017). Trustless Intermediation in Blockchain-based Decentralized Service Marketplaces. В M. Maximilien, A. Vallecillo, J. Wang, & M. Oriol, Service-Oriented Computing: 15th International Conference, ICSOC 2017, Malaga, Spain, November 13–16, 2017, Proceedings (Lecture Notes in Computer Science) (стр. 731-739). Berlin: Springer International Publishing.

Koomey, J. (07 06 2013 г.). How green is the Internet? Получено из Youtube: https://www.youtube.com/embed/O8-LDLyKaBM

Kortuem, G., Kawsar, F., Fitton, D., & Sundramoorthy, V. (2009). Smart objects as building blocks for the internet of things. IEEE Internet Computing, 14, 44-51.

Koulu, R. (2016). Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement. Scripted, 13, 40-69.

Kronovet, D. (01 11 2017 г.). Ethereum Wiki Proof of Stake FAQ. Получено из GitHub: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

Lamport, L., Shotstak, R., & Pease, M. (07 1982 г.). The Byzantine Gerals Problem. ACM Transactions on Programming Languages and Systems, 382-401.

Liao, C.-F., Bao, S.-W., Cheng, C.-J., & Chen, K. (2017). On Design Issues and Architectural Styles for Blockchain-driven IoT Services. 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW). Taipei: IEEE.

Lueth, K. L. (02 02 2015 г.). The 10 most popular Internet of Things applications right now. Получено из IOT Analytics: https://iot-analytics.com/10-internet-of-things-applications/

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). Unlocking the potential of the Internet of Things. McKinsey & Company, McKinsey Global Institute. McKinsey Global Institute.

McIntyre, D., & Srinivasan, A. (2016). Networks, platforms, and strategy: Emerging views and next steps. Strategic Management Journal, 38, 141-160.

McKie, S. (30 09 2017 г.). Investing in Tokens and Decentralized Business Models. Получено из Medium: https://medium.com/blockchannel/investing-in-tokens-and-decentralized-business-models-e7629efa5d9b

Monegro, J. (08 08 2016 г.). Fat Protocols. Получено из Union Square Ventures: http://www.usv.com/blog/fat-protocols

Morris, M., Schindehutte, M., & Allen, J. (2005). The entrepreneur's business model: toward a unified perspective. Journal of Business Research(58), 726-735.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Получено из www.bitcoin.org

Noyen, K., Volland, D., Wörner, D., & Fleisch, E. (2014). When Money Learns to Fly: Towards Sensing as a Service Applications Using Bitcoin. CoRR, 1409.5841.

Palo, T., & Tähtinen, J. (2011). A network perspective on business models for emerging technology-based services. Journal of Business & Industrial Marketing, 26(5), 377-388.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulous, D. (2014). Sensing as a Service Model for Smart Cities Supported by Internet of Things. Transaction on Emerging Telecomunication Technologies, 81-93.

Popov, S. (01 10 2017 г.). The Tangle. Получено из IOTA - Next Generation Blockchain : https://iota.org/IOTA_Whitepaper.pdf

r3. (18 07 2017 г.). What is a UTXO? Получено из r3: https://www.r3.com/blog/2017/07/18/what-is-a-utxo/

Rong, K., Guangyu , H., Yong, L., Yongjiang, S., & Liang, G. (2015). Understanding business ecosystem using a 6C framework in Internet-of-Things-based sectors. International Journal of Production Economics, 41 -55.

Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An overview. The Internet Society (ISOC). Reston: The Internet Society (ISOC).

Rosic, A. (13 01 2017 г.). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Получено из Blockgeeks: https://blockgeeks.com/guides/what-is-blockchain-technology/

Ruuvi. (08 01 2018 г.). Ruuvi Tag. Получено из Ruuvi Tag: https://tag.ruuvi.com

Ryszkiewicz, P. (19 12 2017 г.). IOTA vs RaiBlocks. Получено из Medium: https://hackernoon.com/iota-vs-raiblocks-413679bb4c3e

Schiener, D. (21 05 2017 г.). A Primer on IOTA (with Presentation). Получено из Medium: https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621

Schiener, D. (17 12 2017 г.). IOTA DATA Marketplace Webinar. Получено из Youtube: https://www.youtube.com/watch?v=fqdZSafCRhM

Schiener, D. (01 09 2017 г.). The Coordinator. Получено из IOTA Documentation: https://domschiener.gitbooks.io/iota-guide/content/chapter1/current-role-of-the-coordinator.html

Seppälä, T., & Mattila, J. (2016). Ubiquitous Network of Systems. Berkeley Roundtable on the International Economy (BRIE) (стр. 1-3). Berkeley: University of California, berkeley.

slock.it. (2017). Solution. Получено из slock.it: https://slock.it/solutions.html

Sønstebø, D. (28 11 2017 г.). IOTA Data Marketplace. Получено из Medium: https://blog.iota.org/iota-data-marketplace-cb6be463ac7f

Sønstebø, D. (5 5 2017 г.). IOTA Ecosystem Fund ($10 million). Получено из Medium: https://blog.iota.org/iota-ecosystem-fund-2-million-f6ade6a4d8ba

Sønstebø, D. (13 11 2017 г.). IOTA Foundation. Получено из Medium: https://blog.iota.org/iota-foundation-fb61937c9a7e

Srinivasan, B. S. (27 05 2017 г.). Thoughts on Tokens. Получено из Medium: https://news.earn.com/thoughts-on-tokens-436109aabcbe

Statista. (01 11 2016 г.). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Получено из Statista: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

streamr. (25 07 2017 г.). Product, How it works. Получено из streamr: https://www.streamr.com

streamr. (25 07 2017 г.). Unstoppable Data for Unstoppable Apps: DATAcoin by Streamr. Получено из streamr: https://s3.amazonaws.com/streamr-public/streamr-datacoin-whitepaper-2017-07-25-v1_0.pdf

Swan, M. (2015). Blockchain Blueprint for a New Economy. Sebastopol: O'Reilley.

Swan, M. (12 2015 г.). Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization). IEEE Technology and Society Magazine, 34(4), 41-52.

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. Получено из Praat: doing phonetics by computer: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Takahashi, R. (01 08 2017 г.). How can creative industries benefit from blockchain? Получено из McKinsey & Company: https://www.mckinsey.com/industries/media-and-entertainment/our-insights/how-can-creative-industries-benefit-from-blockchain

Täuscher, K., & Laudien, S. M. (2017). Understanding platform business models: A mixed methods study of marketplaces. European Management Journal, 1-11.

TechNet, M. (19 05 2005 г.). Understanding Public Key Cryptography. Получено из Microsoft Technet: https://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

Tikkanen, H., Lamberg, J.-A., Parvinen, P., & Kallunki, K.-P. (2005). Managerial cognition, action and the business model of the firm. Management Decision, 43, 789-809.

Timmers, P. (1998). Business Models for Electronic Markets. Electronic Markets, 8, 3 -8.

Vermesan, O., Bröring, A., Tragos, E., Serrano, M., Bacciu, D., Chessa, S., . . . Bahr, R. (2017). Internet of robotic things: converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT Platforms. В O. Vermesan, & J. Bacquet, Cognitive Hyperconnected Digital Transformation: Internet of Things Intelligence Evolution (стр. 97-155). Gistrup: River Publishers.

Vermeulen, J. (22 04 2017 г.). Bitcoin and Ethereum vs Visa and PayPal – Transactions per second. Получено из Mybroadband: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html

Voshmgir, S. (2016). Blockchains, Smart Contracts und das Dezentrale Web. Berlin: Technologie Stiftung.

Vukolić, M. (2015). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. В J. Camenisch, & D. Kesdoğan, Open Problems in Network Security (стр. 112-115). Zurich: Springer.

Walport, M. (2016). Distributed ledger technology: beyond block chain. Government Office for Science. London: Government Office for Science.

Wright, A., & Filippi, P. (03 2015 г.). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN.

Yun, M., & Yuxin, B. (2010). Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. 2010 International Conference on Advances in Energy Engineering (ICAEE) (стр. 601 - 605). Beijing: IEEE.

Zhang, Y., & Wen, J. (2016). The IoT electric business model: Using blockchain technology for the internet of things. Springer Science + Business Media New York 2016.

Zott, C., & Amit, R. (2008). The fit between product market strategy and business model: implications for firm performance. Strategic Management Journal, 29, 1-26.

Zott, C., & Amit, R. (2010). Business Model Design: An Activity System Perspective. Long Range Planning, 43, 216-226.

Zott, C., Amit, R., & Massa, L. (2011). The Business Model: Recent Developments and Future Research. Journal of Management, 37(4), 1019-1042.