

# Blockchain technology in the chemical industry: machine-to-machine electricity market

Janusz J. Sikorski<sup>1</sup>, Joy Haughton<sup>1</sup>, Markus Kraft<sup>1,2</sup>

Draft of December 9, 2016

<sup>1</sup> Department of Chemical Engineering  
and Biotechnology  
University of Cambridge  
New Museums Site  
Pembroke Street  
Cambridge, CB2 3RA  
United Kingdom  
E-mail: [mk306@cam.ac.uk](mailto:mk306@cam.ac.uk)

<sup>2</sup> School of Chemical and  
Biomedical Engineering  
Nanyang Technological University  
50 Nanyang Avenue  
Singapore 639798  
E-mail: [mk306@cam.ac.uk](mailto:mk306@cam.ac.uk)

Preprint No. 178



---

*Keywords:* blockchain technology, chemical industry, electricity market, machine-to-machine communications

**Edited by**

Computational Modelling Group  
Department of Chemical Engineering and Biotechnology  
University of Cambridge  
Philippa Fawcett Drive  
Cambridge CB3 0AS  
United Kingdom

**E-Mail:** [c4e@cam.ac.uk](mailto:c4e@cam.ac.uk)

**World Wide Web:** <http://como.ceb.cam.ac.uk/>

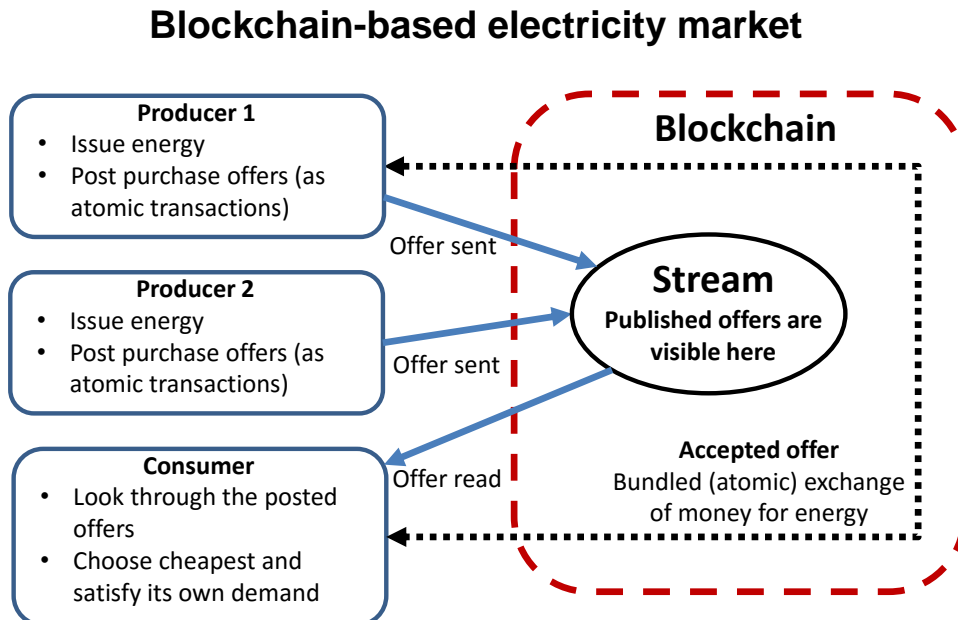


## Highlights

- It is demonstrated that it is possible to successfully employ blockchain technology to facilitate machine-to-machine (M2M) interactions and establish a M2M electricity market in the context of the chemical industry via the Internet of Things.
- The presented scenario includes two electricity producers and one electricity consumer trading with each other over a blockchain.
- This paper describes and discusses the research and application landscape of blockchain technology in relation to Industry 4.0.

## Abstract

The purpose of this paper is to explore applications of blockchain technology related to the 4th Industrial Revolution (Industry 4.0) and to present an example where blockchain is employed to facilitate machine-to-machine (M2M) interactions and establish a M2M electricity market in the context of the chemical industry. The presented scenario includes two electricity producers and one electricity consumer trading with each other over a blockchain. The producers publish exchange offers of energy (in kWh) for currency (in USD) in a data stream. The consumer reads the offers, analyses them and attempts to satisfy its energy demand at a minimum cost. When an offer is accepted it is executed as an atomic exchange (multiple simultaneous transactions). Additionally, this paper describes and discusses the research and application landscape of blockchain technology in relation to the Industry 4.0. It concludes that this technology has significant under-researched potential to support and enhance the efficiency gains of the revolution and identifies areas for future research.



# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Background</b>	<b>3</b>
2.1	What is blockchain technology? . . . . .	3
2.2	Explored areas and applications . . . . .	5
<b>3</b>	<b>Blockchain-enabled M2M electricity market</b>	<b>9</b>
3.1	Design and implementation . . . . .	9
3.2	Results . . . . .	11
<b>4</b>	<b>Conclusions and future work</b>	<b>12</b>
	<b>References</b>	<b>16</b>
	<b>Appendices</b>	<b>22</b>
	<b>Appendix A Key concepts and definitions of the blockchain technology</b>	<b>22</b>
A.1	Definitions . . . . .	22
A.2	Consensus mechanisms . . . . .	24
A.2.1	Proof-of-work . . . . .	25
A.2.2	Proof-of-stake . . . . .	25
A.2.3	Deposit-based . . . . .	26
A.2.4	Byzantine agreement . . . . .	26
A.2.5	Round robin . . . . .	27

# 1 Introduction

Industry 4.0 (or the 4th Industrial Revolution) introduces into industry the concepts of machine-to-machine (M2M) communication, cyber-physical systems (CPSs) and the Internet of Things (IoT) [37, 40]. M2M communication refers to the ability of industrial components to communicate with each other. CPSs can monitor physical processes, create virtual copies of the physical world and make decentralised decisions. IoT is a dynamic network where physical and virtual entities have identities and attributes and use intelligent interfaces. An eco-industrial plant (EIP) refers to an industrial park where businesses cooperate with each other and, at times, with the local community to reduce waste and pollution, efficiently share resources (such as information, materials, water, energy, infrastructure, and natural resources) and minimise environmental impact while simultaneously increasing business success [28, 49, 50]. Implementation of the principles of Industry 4.0 and EIPs in the industry could be aided by blockchain technology. For example, blockchain could be used to facilitate M2M commodity (e.g. electricity) trading. Such a system would benefit from reduced administration cost and increased speed over the traditional practice.

The purpose of this paper is to explore applications of blockchain technology related to Industry 4.0 and to present an example where blockchain is employed to facilitate M2M interactions and establish a M2M electricity market in the context of the chemical industry. This paper is structured as follows: section 2 introduces the readers to blockchain technology using the biggest digital currency (Bitcoin) as case study; section 2.2 describes and discusses the research and application landscape in relation to the engineering industry; section 3 provides implementation details of the example, including the interactions occurring on the blockchain; section 4 summarizes the main findings.

## 2 Background

Blockchain technology is a relatively new research area. Whilst the topic is currently ubiquitous on the news, many readers may not be familiar with the technical terms. For readers' benefit this publication provides a background section with a description of the inner workings and key concepts of blockchain technology and a brief literature review.

### 2.1 What is blockchain technology?

Blockchain is a type of distributed, electronic database (ledger) which can hold any information (e.g. records, events, transactions) and can set rules on how this information is updated [29]. It continually grows as blocks (files with data e.g. transactions) are appended and linked (chained) to the previous block using a hash (the chaining is visualised in Fig. 1 using Bitcoin as an example). The hash is produced by running contents of the block in question through a cryptographic hash function (e.g. Bitcoin uses Secure Hash Algorithm - 256 bit, SHA-256). An ideal cryptographic hash function can easily produce a hash for any input, but it is difficult to use the hash to derive the input. Additionally,

any changes in the original data should result in extensive and seemingly uncorrelated changes to the hash [43, 54]. Finally, it should be infeasible for two different inputs to result in the same hash. Using the cryptographic hashes in this manner ensures that in order to alter an entry in a past block all subsequent blocks also need to be altered [43, 54]. The ledger is validated and maintained by a network of participants (nodes) according to a predefined consensus mechanism (a set of rules allowing the network to reach a global agreement [25]) so no single centralized authority is needed. Multiple (but not necessarily all) nodes hold a full copy of the entire database.

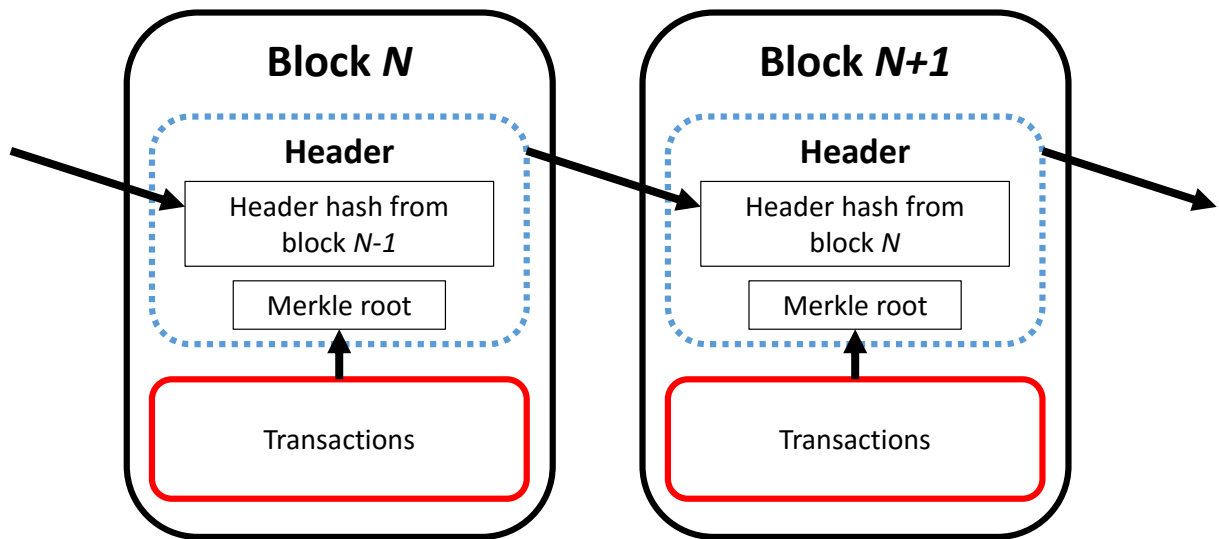
Blockchain technology is relatively new, continues to evolve and comes in many different shapes and forms. In this paper Bitcoin is used as a case study as it is the most well-known and successful implementation of blockchain technology. Bitcoin is a payment system based on a permissionless (i.e. anyone can read or write to the chain) blockchain maintained by a peer-to-peer network (P2P) [5]. It features its native currency (bitcoin or BTC), a proof-of-work consensus mechanism (note that there exist other types of consensus mechanisms; for more see A.2), timestamped blocks not larger than 1 MB (number of transactions per block varies depending on their size), anonymity, a financial incentive to publish blocks, optional transaction fees, a cap of the total BTC supply and BTC fungibility. The blocks primarily record BTC transactions, although additional data can also be included. An example of Bitcoin's block and its contents can be viewed in Fig. 2 and 3, respectively. A transaction is a transfer of BTC from a wallet address (or addresses) to another wallet address (or addresses). For creation transactions, only a receiving wallet is required. Wallets are a public representation of the public and private key pairs that are used to store and transfer coins. One or more such key pairs are generated for each participant so business can be conducted in a secure and anonymous manner. The keys are a result of an encryption method called public-private key cryptography, which uses pairs of parameters: public and private. A public key can be used to verify that a message was created by an owner of the paired private key (verification of a digital signature) and to encrypt a message such that only the aforementioned owner can decrypt.

Bitcoin employs a proof-of-work consensus mechanism where the ability to verify and publish transactions is dependent on the computing power of a node [5]. In order to publish a block, a node is required to complete the following steps:

1. Build a candidate block using valid transactions (i.e. compatible with the rest of the chain) from among the submitted transactions.
2. Calculate a hash of the block header using SHA-256 and compare it with the current target (a specific number of leading zeros; for more information see *Hash target* in A.1), which is imposed by Bitcoin's protocol.
3. If the hash is not correct, the nonce of the header (an arbitrary number in the header) will be repeatedly altered until a solution is found or the target is changed (which means that another node's block was added to the chain).
4. If the hash is correct, the block is broadcast to the Bitcoin network.
5. If majority of the network (weighted by computing power) accepts the block it is permanently added to the chain and the publisher is rewarded with newly created BTCs.

6. If another node's block is added to the chain, the current block will be discarded entirely and the process needs to start all over again.

Note that in a case where multiple suitable blocks are broadcast almost simultaneously, the chain will temporarily split into two or more branches (forks) which will be pursued until one is backed by a majority of the network. Bitcoin's protocol ensures that a block is added to the chain roughly every 10 minutes (ideally 2016 blocks would be added every 1209600 seconds) by adjusting the difficulty of the hash target [5]. However, this mechanism results in significant confirmation latency (order of tens of minutes) and can be resource exhaustive.



**Figure 1:** Chaining of the Bitcoin blocks (adapted from [5]). Note that merkle root is a hash based upon all transactions in a block (for more details see entry "Merkle tree" in A.1).

## 2.2 Explored areas and applications

Blockchain is yet to be fully explored in the academic literature, particularly in relation to the chemical industries. The review of the literature that informed this section therefore included technical reports, industrial and governmental position papers and news articles, which provide better access to the latest work in several areas.

The findings were divided into the following areas:

### Explored areas

Security and privacy

Wasted resources and usability

### Applications

## Block #438995


Summary		Hashes	
Number Of Transactions	1527	Hash	000000000000000042b6b0a7bfa7f43b648167a5c0547d6b3a676e23d4c226
Output Total	12,726.25791485 BTC	Previous Block	00000000000000000257616ab8ed39e0e7bca056d13faf1652075a34e335e7ed
Estimated Transaction Volume	965.70420589 BTC	Next Block(s)	00000000000000000257616ab8ed39e0e7bca056d13faf1652075a34e335e7ed
Transaction Fees	0.41251118 BTC	Merkle Root	4a6be460a67526fd576788cf737713ae614003989706a0675e9d946ec58ca030
Height	438995 (Main Chain)	Network Propagation (Click To View)	
Timestamp	2016-11-15 08:26:59		
Received Time	2016-11-15 08:26:59		
Relayed By	GBMiners		
Difficulty	254,620,187,304.06		
Bits	402936180		
Size	749.146 KB		
Version	536870912		
Nonce	173727158		
Block Reward	12.5 BTC		

Figure 2: General information about Bitcoin block no. 438995 [6].

### Transactions

<p>Transaction ID: fcd6e8933105bf17f9d91c5b26c17c405a07f229fe519063003da262f2995c91</p> <p>Timestamp: 2016-11-15 08:26:59</p> <p>No Inputs (Newly Generated Coins) → 1KuWLoZuoJgz3N6sLoAwGth9XGm8YUFTGT</p> <p>Output: 12.91251118 BTC</p>
<p>Transaction ID: 6ebad12706b60350d93fa2c42ce6d47cece8289447508e1a68585f7d289134cd</p> <p>Timestamp: 2016-11-15 08:26:58</p> <p>1YmVfCLU347vM65TN2E3hugCJgTmomLW → 1YmVfCLU347vM65TN2E3hugCJgTmomLW</p> <p>19ycWQ2z2gJ1kZbpz2kq3GKANcBM5Z1r</p> <p>Output: 0.14734068 BTC, 1.707 BTC</p>
<p>Transaction ID: 86733d9ad44ba3d576cd5284ac879e50634e6d0467b6d8c80fa8d5a8afae5254</p> <p>Timestamp: 2016-11-15 08:23:52</p> <p>1ALNTyDtmUzNoZVW5MNMVKB8Leigdk3TJ → 1MnTMW2IMUaxeGUUQzoKWdJSH8wC4TJQ8</p> <p>1KJXeWbX79MUauZiwlLeLRGVWFdXPK3EJqT</p> <p>Output: 64.464 BTC, 5.067 BTC</p>
<p>Transaction ID: cda0f49e16a11b88a2dd3b38450c0b47e56b63bc2caa378aa39d6828b2f5403</p> <p>Timestamp: 2016-11-15 08:26:37</p> <p>1Hun7KCZ7n8aLdsYCOXgNtpfec58ohpvLT → 1GLaaV4sULzW8sXi1EdMjcu8njRozTWpZ</p> <p>1AEBTgEN1eUaE93i8Pvq9ULe5FL5sd2utL</p> <p>1Mu8kppjdHEhrbbe4MhrWvimfx8tns7V7c</p> <p>Output: 0.16903547 BTC, 0.01000052 BTC</p>
<p>Transaction ID: e7d284ca9845d191c3ac0553a0c815cad3723553932e3d650936637c5f6cdcb6</p> <p>Timestamp: 2016-11-15 08:26:25</p> <p>12Z1hL9FYZ2D7Ffidq7iMHUmKAUNqJr8z2 → 1KDNkoQyAeYcaTqDs21LVNLU41ciHtbMNZ</p> <p>1EVCsi5MpUBbQeiTK776JdoMxaQgYv9qJY</p> <p>16fnNokqkuziJ7nDA7awpL4m66fNQdAwn</p> <p>Output: 0.29583096 BTC, 7.29092536 BTC</p>

Figure 3: Sample of transactions from Bitcoin block no. 438995 [6].



Record-keeping and contract enforcement

The Internet of Things

### **Security and privacy**

Security and privacy are among the core issues of blockchain technology as applied to digital currencies and at the same time the most explored areas. The main issues of security include a possibility of 51% attack, which involves attackers collectively controlling majority of the network, scams (e.g. Ponzi scams, mining scams, scam wallet, fraudulent exchanges) and distributed denial-of-service (DDoS) attacks on exchanges and mining pools. A degree of privacy is introduced as every participant may use one or more anonymous wallets. However, it is still possible to uncover information on the wallet openers. For example, Koshy et al. [39] managed to map a subset of Bitcoin addresses to IP addresses by monitoring and analysing transaction traffic.

A comprehensive review by Yli-Huumo et al. [62] found that the majority of research publications are concerned with this area. These issues are also addressed by Koblitz and Menezes [38] who describe two solutions to the problem of creating a digital currency with the advantages of physical cash, namely an elliptic-curve-based version of a construction provided by Brands [23] and Bitcoin. A detailed description of the mathematics and necessary protocols (setup, signature, withdrawal, payment, deposit and double-spending prevention) for currency systems based on cryptographic hash functions is provided. Applications specifically addressing the issues include CoinParty [65], CoinShuffle [30], Zerocash [56] and Enigma [56]. Zerocash is a ledger-based digital currency which allows user identities, transaction amounts and account balances to be hidden from public view, but still with the ability to quickly and efficiently facilitate transactions (not exclusively financial). Enigma combines blockchain and off-blockchain data storage to construct a personal data management platform focused on privacy.

### **Wasted resources and usability**

Maintaining the most popular blockchain network consumes significant amounts of energy on calculations which have no meaning other than the maintenance. According to O'Dwyer and Malone [48] in 2014 the power used for Bitcoin mining was comparable to Ireland's electricity consumption. Furthermore, increasing accessibility of blockchain technology (e.g. via more user-friendly application programming interface, API) should increase its exposure to areas other than technical computer science and thus help to alleviate the problem of wasted resources and many others.

The review by Yli-Huumo et al. [62] identified eight papers focused on the problems of wasted resources and usability (four each). The applications aimed at improving Bitcoin's usability include BitConeView [36] and BitIodine [58]. English et al. [31] demonstrate how Semantic Web and blockchain technology can enhance each other: the former could facilitate implementation of the latter for several novel applications (e.g. Industry 4.0 platforms for online education or for supply chain management), while the latter could contribute towards the realization of a more robust Semantic Web (for a definition see A.1). An ontology for capturing data within a blockchain was created in order to increase usability of the technology, to facilitate a shared understanding of this technology between humans and to enable interlinking with other Linked Data (for a definition

see A.1) to conduct formal reasoning and inference. A number of consensus mechanisms were developed which are not primarily based on performing intensive computations and typically enjoy lower electricity consumption for a similar blockchain network. Those include the following mechanisms: proof-of-stake [32, 47, 60], deposit-based [57, 63], Byzantine agreement [27, 35, 46, 60] and a rotation scheme [33]. Goodman [32] and Greenspan [33] employ those concepts in their projects, respectively, Tezos and Multi-Chain. The first is a generic and self-amending crypto-ledger employing proof-of-stake consensus mechanism. The second is an off-the-shelf platform for the creation and deployment of private blockchains aiming to facilitate easy deployment of blockchain in the organisations of the financial sector.

### **Application to record-keeping and contract enforcement**

Keeping and creation of records and enforcement of contracts are among the most promising applications of blockchain technology across a wide range of industries from finance to construction. In the context of Industry 4.0 such capability could facilitate logging and sharing data (e.g. emissions) and advanced M2M trading (e.g. bonds).

Watanabe et al. [61] presents a blockchain-based system for confirming contractor consent and archiving the contractual documents. Cardeira [26] argues that employment of the blockchain technology might remedy the major problems of construction industry, namely timing and guarantee of payments, via smart contracts (for a definition see A.1). Smart contracts would ensure that sufficient funds are available to finance the project and that everyone is paid in a timely manner. The governmental report by Condos et al. [29] assesses the opportunities and risks of blockchain technology from the perspective of the American state of Vermont. It is identified that a valid blockchain could be a reliable way of confirming the party submitting a record, the time and date of its submission, and the contents of the record at the time of submission. The final conclusion states that currently the costs and challenges associated with the technology for Vermont's public recordkeeping outweigh the identifiable benefits. O'Dair et al. [47] discuss various applications in the music industry, including a networked copyright database, efficient royalty payment system and provision of access to alternative funding sources for artists. Organisations using blockchain in the music industry include Bittunes [11], Dot Blockchain Music [17] and Mycelia [18]. In the local infrastructure field, a number of projects have adopted blockchain technology to enable residents to choose where to buy renewable energy from (their neighbours or others) and to support communities in keeping energy resources local, reducing dissipation and increasing micro- and macro-grid efficiency. Those include GridSingularity [1], LO3 [2] and SolarCoin [4], as described by a number of technology news [41, 44, 45, 55].

Furthermore, a number of applications were found in finance including: chain.com [12] (deployment of blockchain networks); Augur [13] (prediction trading); Everledger [14] (certification of precious gemstones); Stroj [15] (sharing service for internet bandwidth and spare disk space); Namecoin [10] (an open-source Internet infrastructure such as DNS and identities).

### **Application to the Internet of Things (IoT)**

Employment of blockchain technology for the purpose of introducing transactional functionality to the IoT has been addressed by a number of ideas and applications including:

- IoTcoin [64] - a currency based on BTC intended to facilitate proof of ownership and exchanges of IoT commodities (e.g. sensor data or smart property).
- Community currency [59] - a proposed crypto-currency issued by a non-government entity to serve the economic or social interests of a group of people.
- Enigma [66] - whilst primarily a blockchain-based platform for personal data protection, an assessment by Atzori [21] deems it a suitable solution for the issue of privacy in the IoT.
- IOTA [21, 24] - a crypto-currency developed for the IoT and M2M economy based on Tangle, a blockchain "without blocks" (i.e. each transaction is confirmed separately).
- ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) [21, 51] - an architecture designed for a dynamic democracy of objects connected to a universal digital ledger, which provides users with secure identification and authentication.
- Filament [16] - a technological framework developed to enable devices to hold unique identities on a public ledger and to discover, communicate and interact with each other in an autonomous and distributed manner.

At present there are no documented examples in the literature of M2M commodity trading via IOT. The example presented in the paper explores the potential of that scenario.

### 3 Blockchain-enabled M2M electricity market

This section presents an example in which blockchain technology is employed to facilitate M2M interactions and establish a M2M electricity market in the context of the chemical industry and the IoT. Electricity is a convenient example as its transfer is near-instantaneous (as are the corresponding blockchain transactions), but in principle any other commodity (e.g. steam, natural gas, coal) could be used here. However, the likelihood of a discrepancy between the blockchain record and reality is more likely for commodities which require significant delivery time.

#### 3.1 Design and implementation

This scenario consists of two electricity producers and one electricity consumer which trade with each other over a blockchain. The producers publish exchange offers of energy (in kWh) for currency (in USD) in a data stream, which functions as a publishing board. The consumer reads the offers, analyses them and attempts to satisfy its energy demand at a minimum cost. When an offer is accepted it is executed as an atomic exchange (i.e. two simultaneous transactions are executed and both must either succeed together or fail together). The scenario is visualised conceptually in Fig. 4. It is envisaged that the machines participating in this system would each be equipped with a computer containing

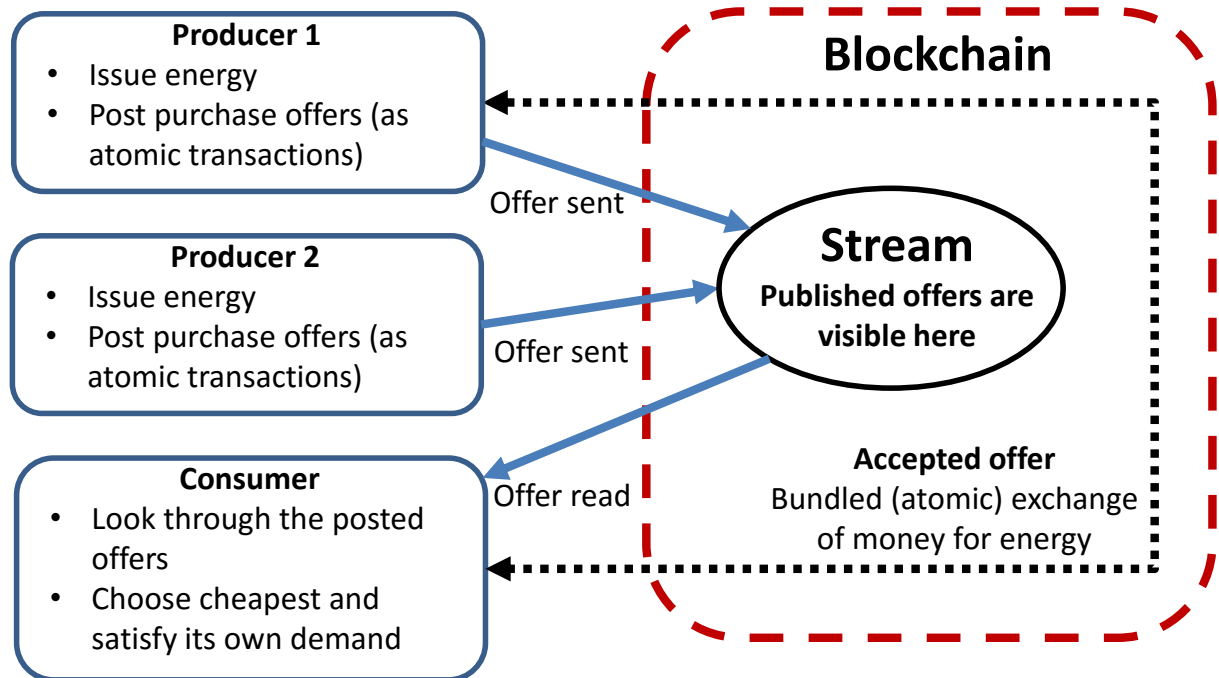
their digital representation enabling them to interact with a blockchain and provide relevant sensor data. Here, the physical machines are replaced with physical simulations of industrial processes in Aspen Plus (AP) [20].

The example was implemented on a Windows 10 machine hosting three Fedora 24 [53] virtual machines. These used MultiChain [33] to establish a blockchain (named BE2) and AP to simulate industrial processes.

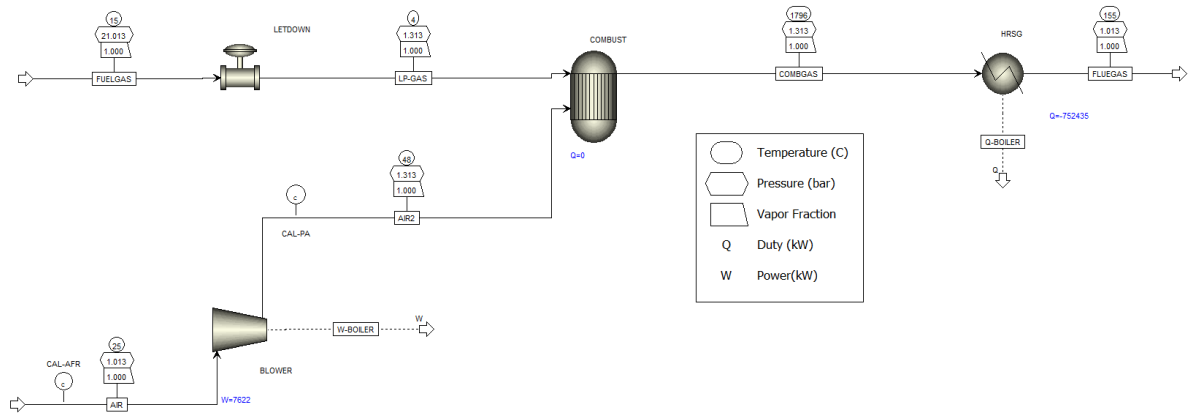
MultiChain is a software package, in development, designed as an off-the-shelf platform for the creation and deployment of private blockchains. In this implementation the primary features of BE2 include round robin consensus mechanism (for in-depth description see section A.2.5) and native assets (here, a digital currency created on top of the chain’s native currency; see *Assets* in section A.1).

Aspen Plus is a process modelling and optimisation software used by the bulk, fine, specialty, biochemical and polymer industries for the design, operation and optimisation of safe, profitable manufacturing facilities. The AP simulations corresponding to the producers model a process in which natural gas is burnt to produce energy, see Fig. 5. The energy demand of the consumer is modelled by a compressor increasing steam pressure, see Fig. 6.

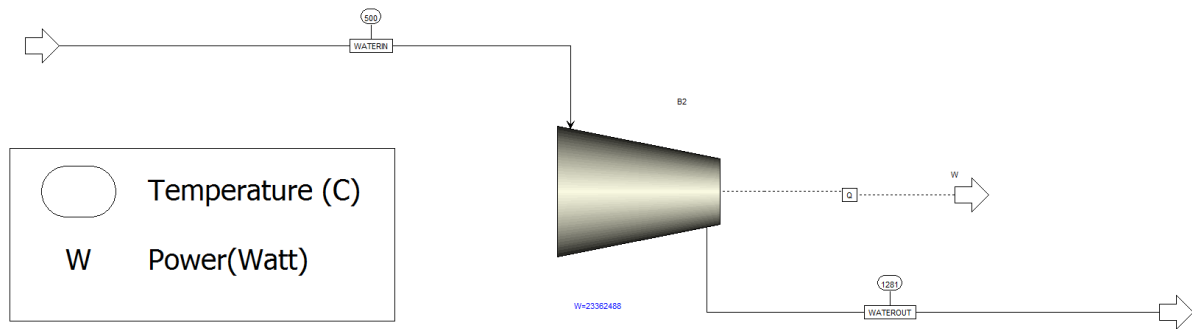
The machines running Fedora represent the producers and the consumer on chain BE2 and receive data from the AP simulations. Fig. 7 shows a section of Fedora terminal immediately after it has connected to BE2 and printed general information about it. All data transfers outside the blockchain, interpretation and analysis of the posted offers, electricity pricing and automation were facilitated using scripts written in Python 3.5.



**Figure 4:** Visual presentation of energy producers and a consumer participating in an electricity market over a blockchain.



**Figure 5:** An Aspen Plus [20] simulation in which natural gas is burnt to produce energy. A purchase offer for this energy is later posted on the blockchain.



**Figure 6:** An Aspen Plus [20] simulation in which an electricity-driven compressor increases steam pressure.

### 3.2 Results

This section presents a series of images, see Figs 8, 9 and 10, of commands and outputs related to operations conducted on blockchain BE2. While the entities in the example can conduct automated trade (via Python processes), it was most convenient to capture the aforementioned images during a manual run-through.

A typical trade proceeds as follows:

1. The producer nodes prepare and publish exchange offers of kWh for USD in the stream "elec-market-open", as shown on Fig. 8 for producer 1. The preparations require the producers to lock a sufficient amount of energy asset and encode details of the exchange.
2. The consumer node looks for the offers related to each publisher and decodes them (see Fig. 9 for producer 1).
3. The consumer compares the offers and chooses the one which minimises the energy

```

{"method":"getinfo","params":[],"id":1,"chain_name":"BE2"}
{
  "version" : "1.0 alpha 25",
  "protocolversion" : 10006,
  "chainname" : "BE2",
  "description" : "MultiChain BE2",
  "protocol" : "multichain",
  "port" : 2687,
  "setupblocks" : 60,
  "nodeaddress" : "BE2@10.25.188.105:2687",
  "burnaddress" : "1XXXXXXXX5rXXXXXXXXZbXXXXXXXXYwXXXXXXXXWylsr3",
  "incomingpaused" : false,
  "miningpaused" : false,
  "walletversion" : 60000,
  "balance" : 0.00000000,
  "walletdbversion" : 2,
  "reindex" : false,
  "blocks" : 1103,
  "timeoffset" : 0,
  "connections" : 0,
  "proxy" : "",
  "difficulty" : 0.00001526,
  "testnet" : false,
  "keypoololdest" : 1478514963,
  "keypoolsize" : 2,
  "paytxfee" : 0.00000000,
  "relayfee" : 0.00000000,
  "errors" : ""
}

```

**Figure 7:** *Fedora terminal which has just connected to blockchain BE2 and printed general information about it (e.g. chain's name, protocol version, current number of blocks). MultiChain was used to set up the chain [33].*

cost.

4. The consumer prepares a transaction matching the chosen offer by locking sufficient funds and appending the chosen offer with payment details. It then encodes this and submits the accepted exchange to the chain (see Fig. 10).
5. Finally, the consumer verifies that the transaction was validated by the chain (see Fig. 10).

## 4 Conclusions and future work

This paper demonstrates that it is possible to successfully employ the blockchain technology to facilitate M2M interactions and establish a M2M electricity market in the context of the chemical industry via the IoT. The presented scenario includes two electricity producers and one electricity consumer trading with each other over a blockchain. The producers

```

Issuing wallet for energy          Receiving wallet (Producer 1)          Asset name and quantity produced
BE2: issuemorefrom 1WtUTPFU4KvgHwu4sLjeEMReCfWKqZ6d6D2QAW 1V2qWn6h8hHfGM9wqCgFyx5vDnWCKR7yCCSkW6 'kWh' 1
f1c63bfee5f55b080d19bd9b1de17049ad386ced1e1b87872a513ba0cdda66c9 Transaction ID

Locking wallet                    Asset name and quantity to be sold
BE2: preparelockunspentfrom 1V2qWn6h8hHfGM9wqCgFyx5vDnWCKR7yCCSkW6 '{"kWh":1}'

{
  "txid" : "80810017e87bb51e52d23cd053471ca63a96ad0564fca3de0c34cd3c9a3f7659", Transaction ID
  "vout" : 0 Number of outputs
}

BE2: createrawexchange 80810017e87bb51e52d23cd053471ca63a96ad0564fca3de0c34cd3c9a3f7659 0 '{"USD":0.05}'
Asset name and quantity (price)

Encoded transaction data
01000000159763f9a3ccd340cdea3fc6405ad963aa61c4753d03cd2521eb57be817008180000000006b48304502210086c7ab64676
7ec3cd374a03958bbe78884f6323c41418e6842dc9809fea17b13022074c77be4f3a07564b174d9e378ff7dfa695250a8354ca92939
4fce54f092dd738321034e7710720db985a93a74e504dbb93a27b760c9260163ff42b3d3b47f835ea006fffff01000000000000
0003176a914cf67791abe51c0a431a2d8eab85b98b59a8b571788ac1673706b714a0000000a010000ee0350c300000000000750000
0000

Stream name      Publication tag
BE2: publish 'elec-market-open' 'selling 1.0 kWh' 01000000159763f9a3ccd340cdea3fc6405ad963aa61c4753d03cd25
21eb57be8170081800000000006b48304502210086c7ab646767ec3cd374a03958bbe78884f6323c41418e6842dc9809fea17b130220
74c77be4f3a07564b174d9e378ff7dfa695250a8354ca929394fce54f092dd738321034e7710720db985a93a74e504dbb93a27b760c
9260163ff42b3d3b47f835ea006fffff01000000000000003176a914cf67791abe51c0a431a2d8eab85b98b59a8b571788ac16
73706b714a0000000a010000ee0350c300000000007500000000

7e338fa843fa9c446dd86634e5186d5c661067551679ffa8cca9b86e3804c68f Publication ID

Legend
Commands
Command parameters
Outputs

```

**Figure 8:** Fedora terminal of producer 1 showing commands and outputs related to issuing the energy asset kWh to the wallet belonging to producer 1, preparing a purchase offer of 1.0 kWh for 0.05 USD (prepareunlockedfrom and createrawexchange) and publishing the encoded offer on the stream "elec-market-open".

publish exchange offers of energy (in kWh) for currency (in USD) in a data stream. The consumer reads the offers, analyses them and attempts to satisfy its energy demand at a minimum cost. When an offer is accepted it is executed as an atomic exchange.

Future work will involve employing blockchains in conjunction with J-Park Simulator (JPS) [37, 49]. The JPS is a modelling platform for designing, computer-aided process engineering (CAPE) and managing an eco-industrial park (EIP). This combination will enable the application of the findings from the current example to larger networks and different types of commodities, the implementation of more sophisticated pricing models, balancing of the positions of customers and producers (at the moment the market is purely producer-driven) and the introduction of more complex trade deals using smart contracts. From the chemical engineering perspective, the intention is to use a greater variety of models and to introduce dynamic behaviour (e.g. a simulation of a process line during start-up and shut-down). Blockchain technology has the potential to revolutionise the engineering industry by facilitating the transition to and functioning of Industry 4.0. Furthermore, there remain many unexplored research areas (e.g. latency, throughput, size and bandwidth, forks, side chains, multiple chains and usability from the developer perspective) and application areas (smart contracts, licensing, IoT, and smart properties) leaving significant potential for further innovation.







## References

- [1] GridSingularity. URL <http://gridsingularity.com/#/>. Date accessed: 25.10.2016.
- [2] LO3 Energy. URL <http://lo3energy.com/projects/>. Date accessed: 25.10.2016.
- [3] Merkle Tree. URL <https://bitcoin.org/en/glossary/merkle-tree>. Date accessed: 26.11.2016.
- [4] SolarCoin. URL <http://solarcoin.org/en/front-page/>. Date accessed: 25.10.2016.
- [5] Bitcoin Developer Guide, . URL <https://bitcoin.org/en/developer-guide>. Date accessed: 17.11.2016.
- [6] Block #438995, . URL <https://blockchain.info/block/0000000000000000042b6b0a7bfa7f43b648167a5c0547d6b3a676e23d4c226>. Date accessed: 17.11.2016.
- [7] Botnet. URL <https://www.techopedia.com/definition/384/botnet>. Date accessed: 26.11.2016.
- [8] Fork, Accidental Fork. URL <https://bitcoin.org/en/glossary/fork>. Date accessed: 26.11.2016.
- [9] W3C SEMANTIC WEB ACTIVITY. URL <https://www.w3.org/2001/sw/>. Date accessed: 26.11.2016.
- [10] Namecoin, April 2011. URL <https://namecoin.org/>. Date accessed: 14.11.2016.
- [11] bittunes.org: An Independet Digital Music Market, April 2013. URL <http://www.bittunes.org/>. Date accessed: 14.11.2016.
- [12] Chain, January 2014. URL <https://chain.com/>. Date accessed: 14.11.2016.
- [13] Augur, October 2015. URL <https://www.augur.net/>. Date accessed: 14.11.2016.
- [14] Everledger, July 2015. URL <http://www.everledger.io/>. Date accessed: 14.11.2016.
- [15] Stroj, January 2015. URL <https://storj.io/>. Date accessed: 14.11.2016.
- [16] Foundations for the Next Economic Revolution: Distributed Exchange and the Internet of Things, November 2016. URL <https://filament.com/assets/downloads/Filament%20Foundations.pdf>. Date accessed: 14.11.2016.

- [17] Dot Blockchain Music, July 2016. URL <http://dotblockchainmusic.com/>. Date accessed: 14.11.2016.
- [18] Mycelia For Music, July 2016. URL <http://myceliaformusic.org/>. Date accessed: 14.11.2016.
- [19] *The Oxford Dictionary*. Oxford University Press, 2016. URL <https://en.oxforddictionaries.com/definition/cryptocurrency>. Date accessed: 26.11.2016.
- [20] AspenTech. aspentech - Aspen Plus V8.6, 2015. URL <http://www.aspentech.com/products/engineering/aspen-plus/>. Date accessed: 19.11.2016.
- [21] M. Atzori. Blockchain-Based Architectures for the Internet of Things: A Survey, May 2016. URL <https://ssrn.com/abstract=2846810>. Date accessed: 24.10.2016.
- [22] C. Bizer, T. Heath, and T. Berners-Lee. Linked Data - The Story So Far. *International Journal on Semantic Web and Information Systems*, 5(3):1–22, 2009. ISSN 1552-6283. doi:10.4018/jswis.2009081901.
- [23] S. Brands. An Efficient Off-line Electronic Cash System Based On The Representation Problem. Technical report, 1993.
- [24] J. P. Buntix. IOTA: Internet of Things Without the Blockchain?, November 2014. URL <http://bitcoinist.net/iota-internet-things-without-blockchain/>. Date accessed: 14.11.2016.
- [25] V. Buterin. Consensus Mechanisms used in Blockchain, November 2014. URL <https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>. Date accessed: 18.10.2016.
- [26] H. Cardeira. Smart contracts and their applications to the construction industry. In *New Perspectives in Construction Law Conference, 2015*, March 2015.
- [27] M. Castro and B. Liskov. Practical Byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI '99*, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association. ISBN 1-880446-39-1. URL <http://dl.acm.org/citation.cfm?id=296806.296824>. Date accessed: 09.12.2016.
- [28] M. K. Catharine A. Kastner, Raymond Lau. Quantitative tools for cultivating symbiosis in industrial parks; a literature review. *Applied Energy*, 155:599 – 612, 2015. ISSN 0306-2619.
- [29] J. Condos, W. H. Sorrell, and S. L. Donegan. Blockchain technology: Opportunities and risks. Technical report, State of Vermont, USA, January 2016.

- [30] C. Decker and R. Wattenhofer. Bitcoin Transaction Malleability and MtGox. In M. Kutylowski and J. Vaidya, editors, *Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II*, pages 313–326. Springer International Publishing, 2014. ISBN 978-3-319-11212-1.
- [31] M. English, S. Auer, and J. Domingue. Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development. Technical report, University of Bonn, Germany, May 2016.
- [32] L. M. Goodman. Tezos - a self-amending crypto-ledger. Technical report, Tezos, September 2014.
- [33] G. Greenspan. MultiChain Private Blockchain. Technical report, MultiChain, July 2015.
- [34] M. Hermann, T. Pentek, and B. Otto. Design Principles for Industrie 4.0 Scenarios. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 3928–3937, Jan 2016. doi:10.1109/HICSS.2016.488.
- [35] S. Higgins. Jed McCaleb Talks Stellar’s New Protocol for Consensus, April 2015. URL <http://www.coindesk.com/stellar-founder-jed-mccaleb-new-protocol/>. Date accessed: 19.10.2016.
- [36] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu. The Blockchain-Based Digital Content Distribution System. In *Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conference on*, pages 187–190, Aug 2015. doi:10.1109/BDCloud.2015.60.
- [37] M. J. Kleinlanghorst, L. Zhou, J. Sikorski, E. F. Y. Shyh, K. Aditya, S. Mosbach, I. Karimi, R. Lau, S. Garud, C. Zhang, M. Pan, J. Moirangthem, Y. Sun, P. Chhabra, K. Nurul, D. Yong, Y. R. Sng, G. Amaratunga, J. Maciejowski, H. Ong, S. Panda, and M. Kraft. J-Park Simulator: Roadmap to Smart Eco-Industrial Parks. Technical Report 174, Computational Modelling Group, University of Cambridge, 2016. URL <https://como.cheng.cam.ac.uk/index.php?Page=Preprints&No=174>. Date accessed: 09.12.2016.
- [38] N. Kobitz and A. J. Menezes. Cryptocash, Cryptocurrencies, and Cryptocontracts. *Des. Codes Cryptography*, 78(1):87–102, Jan. 2016. ISSN 0925-1022. doi:10.1007/s10623-015-0148-5.
- [39] P. Koshy, D. Koshy, and P. McDaniel. *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, pages 469–485. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. ISBN 978-3-662-45472-5.
- [40] M. Kraft and S. Mosbach. The future of computational modelling in reaction engineering. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 368(1924):3633–3644, 2010. ISSN 1364-503X. doi:10.1098/rsta.2010.0124.

- [41] S. Lacey. The Energy Blockchain: How Bitcoin Could Be a Catalyst for the Distributed Grid, February 2016. URL <https://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-for-the-distributed-grid>. Date accessed: 24.10.2016.
- [42] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, July 1982. ISSN 0164-0925. doi:10.1145/357172.357176.
- [43] A. Lewis. A gentle introduction to blockchain technology, September 2015. URL <https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/>. Date accessed: 18.10.2016.
- [44] J. Lilic. Ethereum Enabled Community Energy Market Sharing Economy Phase 2: Here’s How ConsenSys is Building The TransActive Grid, November 2015. URL <https://www.linkedin.com/pulse/ethereum-enabled-community-energy-market-sharing-economy-john-lilic-6071756565017305088>. Date accessed: 24.10.2016.
- [45] J. Lilic. Ethereum Enabled Community Energy Market Sharing Economy Phase 1: Renewable Energy Certificates (RECs), Microgrids, Smart Meters and Ethereum, November 2015. URL <https://www.linkedin.com/pulse/ethereum-enabled-community-energy-market-sharing-economy-john-lilic>. Date accessed: 24.10.2016.
- [46] D. Mazières. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. Technical report, Stellar Development Foundation, April 2015.
- [47] M. O’Dair, Z. Beaven, D. Neilson, R. Osborne, and P. Pacifico. Music On The Blockchain. Technical Report 1, Blockchain For Creative Industries Research Cluster, Middlesex University, UK, July 2016.
- [48] K. J. O’Dwyer and D. Malone. Bitcoin mining and its energy footprint. In *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CICT 2014)*, pages 280–285, June 2014. doi:10.1049/cp.2014.0699.
- [49] M. Pan, J. Sikorski, C. A. Kastner, J. Akroyd, S. Mosbach, R. Lau, and M. Kraft. Applying Industry 4.0 to the Jurong Island Eco-industrial Park. *Energy Procedia*, 150, 2015. doi:10.1016/j.egypro.2015.07.313.
- [50] M. Pan, J. Sikorski, J. Akroyd, S. Mosbach, R. Lau, and M. Kraft. Design technologies for eco-industrial parks: From unit operations to processes, plants and industrial networks. *Applied Energy*, 175:305 – 323, 2016. ISSN 0306-2619.
- [51] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran. ADEPT: An IoT Practitioner Perspective. Technical report, IBM, January 2015.
- [52] A. Poelstra. A Treatise on Altcoins, May 2016. URL <https://download.wpsoftware.net/bitcoin/alts.pdf>. Date accessed: 19.10.2016.

- [53] F. Project. Fedora 24 Workstation, 2016. URL <https://archive.fedoraproject.org/pub/fedora/linux/releases/24/Workstation/>. Date accessed: 25.11.2016.
- [54] P. Rogaway and T. Shrimpton. *Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance*. Springer Berlin Heidelberg, 2004. ISBN 978-3-540-25937-4.
- [55] A. Rutkin. Blockchain aids solar sales. *New Scientist*, 231(3088):22, 2016. ISSN 0262-4079. doi:10.1016/S0262-4079(16)31558-5.
- [56] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy*, pages 459–474, May 2014. doi:10.1109/SP.2014.36.
- [57] Y. Sompolinsky and A. Zohar. Accelerating Bitcoin’s Transaction Processing: Fast Money Grows on Trees, Not Chains. Technical report, Hebrew University of Jerusalem, December 2013.
- [58] M. Spagnuolo, F. Maggi, and S. Zanero. Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security*, pages 457–468. Springer Berlin Heidelberg, 2014.
- [59] D. Vandervort, D. Gaucas, and R. S. Jacques. *Issues in Designing a Bitcoin-like Community Currency*, pages 78–91. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015. ISBN 978-3-662-48051-9.
- [60] M. Vukolić. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In J. Camenisch and D. Kesdoğan, editors, *Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers*, pages 112–125. Springer International Publishing, 2016. ISBN 978-3-319-39028-4.
- [61] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami. Blockchain contract: A complete consensus using blockchain. In *2015 IEEE 4th Global Conference on Consumer Electronics (GCCE)*, pages 577–578, Oct 2015. doi:10.1109/GCCE.2015.7398721.
- [62] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander. Where Is Current Research on Blockchain Technology? - A Systematic Review. *PLoS ONE*, 11(10): 1–27, 10 2016. doi:10.1371/journal.pone.0163477.
- [63] V. Zamfir. Introducing Casper "the Friendly Ghost", August 2015. URL <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>. Date accessed: 18.10.2016.
- [64] Y. Zhang and J. Wen. An IoT electric business model based on the protocol of bitcoin. In *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*, pages 184–191, Feb 2015. doi:10.1109/ICIN.2015.7073830.

- [65] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle. CoinParty: Secure Multi-Party Mixing of Bitcoins. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY '15*, pages 75–86. ACM, 2015. ISBN 978-1-4503-3191-3.
- [66] G. Zyskind, O. Nathan, and A. Pentland. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184, May 2015. doi:[10.1109/SPW.2015.27](https://doi.org/10.1109/SPW.2015.27).

# Appendix A Key concepts and definitions of the blockchain technology

## A.1 Definitions

This subsection contains definitions of terms characteristic to the area of blockchain technology and crypto-currencies.

*51% attack* - an attempt by one or more participants with collective majority control of a network (e.g. by hash rate or stake) to revise transaction history and/or prevent new transactions from being confirmed.

*Assets* - an entity (e.g. currency, commodity) created by sending additional data in transactions of a chain's native currency.

*Block* - a file in which data (e.g. transactions, events) are recorded.

*Blockchain* - a distributed, electronic database which can hold any information (records, events, transactions, etc.) and can set rules on how information is updated [29]. It continually grows as discrete chunks (blocks) are appended and linked (chained) to the previous block using the hash of its content. It also records every change made in its history so in order to alter a past entry all subsequent blocks also need to be altered. It is authenticated and maintained through a distributed network of participants (nodes) according to a predefined consensus mechanism [29].

*Botnet* - a number of Internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control or by passing messages to one another [7].

*Byzantine Generals Problem* (as described by Lamport et al. [42]) - an agreement problem in which a group of generals, each commanding a portion of the Byzantine army, encircle a city. These generals wish to formulate a plan for attacking the city. In the most basic form they need to decide whether to attack or retreat. It is vital that every general agrees on a common decision, for a halfhearted attack by a few generals would become a rout and be worse than a coordinated attack or a coordinated retreat. The problem is complicated by the presence of traitorous generals who may not only cast a vote for a suboptimal strategy, but also do so selectively (i.e. different answers sent to different people). This is analogous to a number of nodes participating in a blockchain attempting to arrive at a global consensus whilst using unreliable communication and under threat of some participants malfunctioning or being malicious.

*Consensus mechanism* - a set of state transition rules enabling an economic set (among which the rights to conduct the transition are distributed) to perform secure update of the state [25]. Bitcoin users are an example of the aforementioned economic set. For further description and examples see section A.2.

*Crypto-currency* - a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank [19].

*Cryptographic hash function* - a type of hash functions (see below) suitable for use in



cryptography e.g. Bitcoin uses SHA-256 (Secure Hash Algorithm - 256 bit) [43, 54]. An ideal cryptographic hash function exhibits the following traits:

- a hash can be easily produced for any message;
- it is difficult to derive the original data from its hash;
- any changes in the original data result in the hash changing so extensively that the new hash value appears uncorrelated with the old hash value;
- it is infeasible for two different inputs to result in the same hash.

*Fork* - the event of a blockchain splitting into two or more chains. A fork can occur when two or more miners publish a valid block at roughly the same time, as a part of an attack (e.g. 51% attack) or when a blockchain protocol change is attempted (such a fork is "hard" if all users are required to upgrade, otherwise it is "soft") [8].

*Hash function* - any function that can be used to map data of arbitrary size to data of fixed size [43, 54].

*Header hash* - a hash of the information contained in a block's header which is used to link the block with the next one. In the case of Bitcoin blocks it contains the blockchain version number, the header hash of the previous block, the merkle root (see *Merkle tree* below) of all transactions in the block, the current time and the current difficulty (see *Hash target* below).

*Hash target* - a set of acceptance criteria imposed on a block's header hash (see *Header hash* above) by the protocol of a blockchain. In the case of Bitcoin, the target is an upper bound on the hash's value.

*Internet of Things (IoT)* - dynamic, global network infrastructure that can self-configure using standards and interoperable protocols where physical and virtual things have identities, attributes, and personalities, use intelligent interfaces, and can seamlessly integrate into the network [21].

*Industry 4.0* - (4th Industrial Revolution) is characterised by the ability of industrial components to communicate with each other. It includes cyber-physical systems, the Internet of Things and cloud computing [34, 37].

*Linked Data* - a method of publishing structured data so that it can be interlinked and become more useful through semantic queries [22].

*Merkle tree* - a tree constructed by pairing data (e.g. in the Bitcoin system it usually refers to transactions), then hashing the pairs, then pairing and hashing the results until a single hash remains, the merkle root [3].

*Mining* - the process of verifying transactions and publishing blocks. The exact procedure varies widely depending on a particular blockchain implementation. In Bitcoin's case miners compete to solve a mathematical puzzle that requires the consumption of computing power [60]. Once the puzzle is solved, the new block of transactions is accepted by the network and committed to the blockchain. The miner is rewarded with newly generated coins. For further description and examples see section A.2.1.

*Node* - any device which is part of a network, and has a unique network address. In the context of blockchain and crypto-currencies it refers to a wallet software such as the Bitcoin client application.

*Nonce* - an arbitrary number that may only be used once. In the case of Bitcoin, it is a part of block's header and mining nodes repeatedly adjust the number in order to meet the target imposed on header hashes.

*"Nothing at stake" problem* - a shortfall experience by blockchain using a proof-of-stake consensus mechanisms where block generators have nothing to lose by voting for multiple blockchain histories leading to consensus never resolving [52].

*Peer-to-peer (P2P) network* - a network of nodes (peers) directly connected with each other. The system relies on the peers, who have equal standing within the network, sharing at least as many resources as they consume.

*Permissioned blockchain* - a blockchain whose use is restricted to known, vetted participants [47].

*Permissionless blockchain* - a blockchain that is accessible to anyone who wishes to use it [47].

*Private blockchain* - a blockchain that limits read access to particular users [47].

*Public blockchain* - a blockchain that grants read access and ability to create transactions to all users [47].

*Public-private key cryptography* - a class of encryption methods that uses pairs of keys (e.g. a pair of two special numbers): public and private. A public key can be used to verify that a message was created by an owner of the paired private key (verification of a digital signature) and to encrypt a message such that only the aforementioned owner can decrypt.

*Smart contract* - a contractual agreement built on computer protocols, whose terms are executed automatically [47].

*Semantic Web* - an extension of the Web through standards by the World Wide Web Consortium (W3C) in order to promote common data formats and exchange protocols on the Web, most fundamentally the Resource Description Framework (RDF) [9].

*Transaction* - a transfer of a digital asset from an address (or addresses) to another address (or addresses) [47].

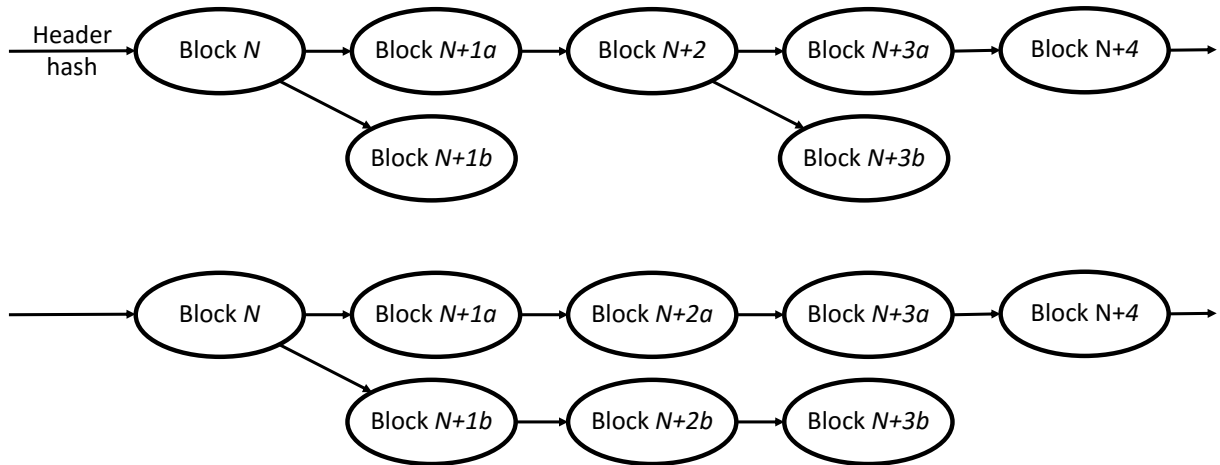
*Wallet* - a public representation of the public and private key pairs that are used to store and transfer coins.

## A.2 Consensus mechanisms

This section briefly describes various kinds of consensus mechanisms (see definition in section A.1) used for blockchain implementations. The following mechanisms are discussed:

- Proof-of-work

## Examples of forking during normal operation: typical (top) and rare (bottom)



**Figure 11:** Diagram demonstrating temporary blockchain forks [5].

- Proof-of-stake
- Deposit-based
- Byzantine agreement (PBFT)
- Rotation scheme

### A.2.1 Proof-of-work

Proof-of-work is a method of achieving network consensus where the ability to verify and publish transactions is dependent on the computing power of the miner [25, 47]. The details have already been explained in section 2.1.

### A.2.2 Proof-of-stake

Proof-of-stake is a consensus mechanism in which the ability to verify and publish blocks depends on the "stake" (e.g. amount of the native currency) already possessed [47]. Verification is performed by the nodes with the largest stake in the network as its correct operation is in their best interest, e.g. mining is easier for those who can show they control a large amount of the blockchain's native currency.

Publishing blocks proceeds as follows [60]:

1. A participant needs to "lock" (e.g. deposit, spend) a number of coins in order to be allowed to publish blocks;

2. The participant needs to generate a block with a valid hash (as in the proof-of-work system, but the more coins consumed, the easier the search for a valid hash);
3. The block is published and validated by other participants.

The system benefits over the proof-of-work mechanism from reduced energy consumption, immunity from hardware centralization and reduced risk of any one member acquiring the controlling stake as its cost might be higher than the cost of acquiring significant mining power. However, it suffers from the "nothing at stake" problem (described in section [A.1](#)).

### **A.2.3 Deposit-based**

A deposit-based consensus protocol requires the participants to register a security deposit in order to serve the consensus by producing blocks [\[63\]](#). In the case of Ethereum, a chain selection rule called GHOST (Greedy Heaviest Observed Sub Tree) serves as an arbitrator governing the security deposits [\[57\]](#). If a node validates a transaction that GHOST considers invalid, the node loses its deposit and forfeits the privilege of participating in the consensus process. This directly solves the "nothing-at-stake" problem (described in section [A.1](#)). This system benefits from strong convergence of history (i.e. every block would either be fully abandoned or fully adopted) and strengthened immutability as blocks that are not in the main chain remain on the record [\[57\]](#). Ethereum is expected to introduce a deposit-based consensus protocol called Casper [\[63\]](#).

### **A.2.4 Byzantine agreement**

Byzantine agreement, also known as Practical Byzantine Fault Tolerance (PBFT), type consensus mechanisms are based on a solution to the Byzantine Generals Problem (described in section [A.1](#)). In this case each node generates a private-public key pair and publishes the public key. Messages from other nodes, which are concerned with issues requiring the network agreement, passing through the node are signed by the node to verify their format. Once enough identical responses are recorded, the consensus about the issue in question is reached. This protocol is suitable for low-latency storage system and digital asset-based platforms that do not require a large data throughput, but need many transactions [\[27, 60\]](#). One of the platforms using it is Hyperledger.

This method does not require any hashing power (hence enjoys reduced energy usage), provides fast and efficient consensus convergence and decouples trust from resource ownership making it possible for the small to keep the powerful honest. However, the system needs to be set up by a central authority or over a course of closed negotiations and all parties have to agree on the exact list of participants [\[46\]](#).

Federated Byzantine Agreement (FBA) is a type of PBFT, but it enjoys an open membership scheme [\[46\]](#), where all nodes know other nodes and can consider some to be important. Whenever a transaction needs to be verified, any given node waits for the vast majority of the nodes it considers important to agree with each other. At the same time,

the important participants do not agree to the transaction until the participants they consider important agree as well. Eventually, sufficiently large part of the network accepts the transaction making it infeasible for an attacker to make any changes. The FBA system relies on small sets of trusted parties which would consist of the nodes that built their trust level over time through good behaviour [46]. A platform called Stellar employs this scheme [35].

### A.2.5 Round robin

For private blockchains, where certain degree of trust between the participants is possible, the network consensus can be achieved without difficult computations. In the case of MultiChain [33] the set of miners is limited to known entities which take turns in publishing blocks. The strictness of the rotation scheme is controlled using a parameter called mining diversity ( $0 \leq \text{mining diversity} \leq 1$ ). This parameter defines the minimum proportion of permitted miners needed to control the network. 0.75 is a recommended value [33], as high values are safer, but a value too close to 1 can cause the blockchain to freeze up if some miners become inactive. In the case that the network splits temporarily (e.g. due to communications failure) resulting in a fork, the branch with the longer chain will be adopted.

The participants are approved for publishing blocks as follows:

1. Any permission changes defined by transactions in the current block are applied;
2. The current number of permitted miners is calculated;
3. The number of miners is multiplied by mining diversity and rounded up to get spacing;
4. If any of the spacing-1 blocks were mined by the current miner, the block is invalid.

The scheme enjoys the following advantages over a centralised database:

- Each participant has full control over its assets via their ownership of private key(s);
- Distributed control prevents an individual or a small group from unilaterally deciding which transactions are valid or will be confirmed;
- More robust as access and validation of transactions will continue even if a server malfunctions (i.e. no single point of failure).