Ben van Lier on Blockchain

Collected blogs 2016–2020

centric

Professor dr. Ben van Lier

Professor dr. Ben van Lier is Director of Strategy & Innovation at Centric, a Dutch ICT company with offices in The Netherlands, Belgium, Norway, Romania, Germany, Sweden and Switzerland. In this capacity, he focuses on research and analysis of developments in the interface between organisations and technology and future technological developments which could influence this interface. Alongside his work at Centric, in 2009 he obtained his PhD from the Rotterdam School of Management (Erasmus University), for which he conducted research into the fusion of man and technology, the interoperability of information and network-centric thinking. In 2013 he was appointed Professor ar Steinbeis University Berlin and in 2015 he has been appointed Lector at Rotterdam University of Applied Sciences. Both roles he fulfils alongside his work at Centric.

CONTENTS

Blockchain: *distributed transactions that will radically change the world*

January 14, 2016

The American mathematician and A.M. Turing Award winner Leslie Lamport is one of the founding fathers of distributed computing and distributed algorithms. Back in 1978, he defined distributed computing thus: *"A distributed system consists of a collection of distinct processes which are spatially separated, and which communicate with each other by exchanging messages. A network of interconnected computers such as the ARPANET is a distributed system."* [1] In an age when there were no such things as the internet, the Internet of Things or advanced manufacturing, he worked on distributed algorithms that have helped make these developments possible. Without the trailblazing by this founding father of distributed computing, today's blockchain technology hype would have been unthinkable.

Read more >

centric

Distributed computing

A key requirement in the development of distributed computing is that a system made up of distributed processes has to be able to keep functioning, even when one or several of its components have ceased to (reliably) contribute to the functioning of the system as a whole. When it comes to reliability, Lamport is unequivocal when he says that a distributed system can only function reliably by using time as a fundamental part of its reliability [2].

As a whole, the system can only function reliably on a permanent basis when the majority of separate components of the system maintain consensus with respect to the functioning of the system as a whole. It is therefore key for a distributed system that all components involved keep a ledger of how and with whom they have performed transactions by exchanging and sharing data and information. All components must have access to information about transactions logged in the distributed ledgers, which are intended to provide an overall view of all approved transactions. In Lamport's age, generating consensus between the various components of a system was a new and complex issue. In 1982, he addressed this consensus problem in an article he co-wrote with Robert Shostak and Marshall Pease, coining it the Byzantine Generals' Problem [3]. In their article, Lamport, Shostak and Pease develop an algorithm that lays the foundation for reliable consensus between systems that are separated in terms of time and space. The essential idea in the solution they come up with is that to establish consensus there have to be at least three plus one components and mutual exchange of qualified messages between them. In 1998, Lamport added a protocol to this consensus principle that regulates the voting that is needed to achieve consensus between the various components within a system. This latter protocol, which is also known as the Paxos algorithm [4], addresses things such as how to handle the voting between the various components, how to record the results of the voting between the components in central and decentralised ledgers, and how to guarantee the consistency of recorded information.

Blockchain technology

Without Lamport et al.'s pioneering work in the field of distributed computing and distributed algorithms, we would not be contemplating the possibilities offered by blockchain technology today. The most widely known application of this technology so far is attributed to Satoshi Nakamoto [5]: Bitcoin. Blockchain's boom as an application for things such as value calculation, currency exchange, data storage in the cloud, or contracts, has received widespread attention in subsequent years. Blockchain technology's potential in developments such as the Internet of Things, (mobile) health care and advanced manufacturing has only been attracting increasing interest in the past two years.

A recent Deloitte publication [6] described blockchain technology as: "*a new solution to a more challenging version of the Byzantine Generals problem that includes the ability to add participants over time. A blockchain is a digital distributed transaction ledger, with identical copies maintained on multiple computer systems controlled by different entities*". Melanie Swan [7] sees blockchain technology as a key innovation in the development of new architectures for transactions between interconnected and distributed systems: *"The blockchain allows the disintermediation and decentralization of all transactions of any type between all parties on a global basis"*. To Swan, decentralised ledgers that enable a transparent structure of recorded transactions are the essence of the blockchain: *"the database that is shared by all network nodes, updated by miners, monitored by everyone and owned and controlled by no one"*. Physical nodes in a network, such as computers, smartphones, sensors and devices such as smart TVs, fridges and cars can thus be interconnected through software and distributed algorithms that ensure consensus in transactions between these nodes. In Swan's words, the blocks that make up the blockchain consist of: *"groups of transactions posted sequentially to the ledger – that is, added to the chain. Blockchain ledgers can be inspected publicly with block explorers, internet sites where you can see a transactions stream by entering a blockchain address (a user's public-key address)"*.

Distributed computing, Blockchain and the IoT

Many agree that Bitcoin is but a first step towards numerous more applications in a wide range of sectors. A Goldman Sachs publication cited by Williams-Grut [8] claims that: *"While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the Blockchain, can change... well everything"*. Silicon Valley's role in developing and shaping blockchain technology is considerable. Insights such as the Byzantine Generals' Problem and the Paxos algorithm have played a major part in the development of solutions such as cloud computing and cloud-based data storage. It is therefore no surprise that Google, Microsoft and Amazon stand to gain a great deal from further development of the concept of distributed computing. Philips Healthcare has recently also announced that it is to research the potential uses of blockchain technology in exchanging and sharing data and information between medical applications. Working closely together with parties such as Samsung, IBM is investing considerable time and money into making a blockchain possible for the Internet of Things. In IBM's view, the basis of today's information revolution lies in: *"the very humble work of transaction processing. From phone calls to electricity metering to airline reservations, each is a transaction to be processed"*[9]. IBM expects the current growth of automated transactions to snowball on the back of the development of the Internet of Things and advanced manufacturing. According to IBM, the exponential growth of the number of objects that are connected to the internet and share information through that connection calls for new paradigms such as the blockchain of distributed computing. In the further development of a decentralised Internet of Things, IBM sees the blockchain as: *"the framework facilitating transaction processing and coordination among interacting devices. Each manages its own roles and behavior, resulting in an Internet of Decentralized, Autonomous Things – and thus the democratization of the digital world"*.

Summed up

In the words of Melanie Swan: *"Perhaps most centrally, the blockchain is an information technology"*. The development of the theory behind this information technology has been ongoing for decades. Despite fundamental breakthroughs and the first advances in this field, the area of distributed computing and distributed algorithms is still one with numerous practical and theoretical issues. Before we can start using this form of information technology globally in developments such as the Internet of Things, (mobile) health care and advanced manufacturing, we need better understanding of the possible development of such a new and technology-based ecosystem over time.

Footnotes

[1] Lamport L. (1978) Time, Clocks, and the ordering of events in a distributed system. Communications of the ACM. July 1978 Volume 21, number 7, pp. 558-565

[2] Wensley J. H., Lamport L., Goldberg J., et al. (1978) SIFT: Design and analysis of a fault tolerant computer for aircraft control. Proceedings of the IEEE, vol. 66, no.10 October 1978, 1240-1255

[3] Lamport L., Shostak R. and Pease M. (1982) The Byzantine Generals Problem

[4] Lamport L. (1998) The Part-Time Parliament. This article appeared in ACM Transactions on Computer Systems 16, 2 May 1998), pp. 133-169. Minor corrections were made on 29 August 2000.

[5] Nakomoto S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[6] Schatsky D. and Muraskin C. (2015) Beyond Bitcoin. Blockchain is coming to disrupt your industry. Deloitte University Press.

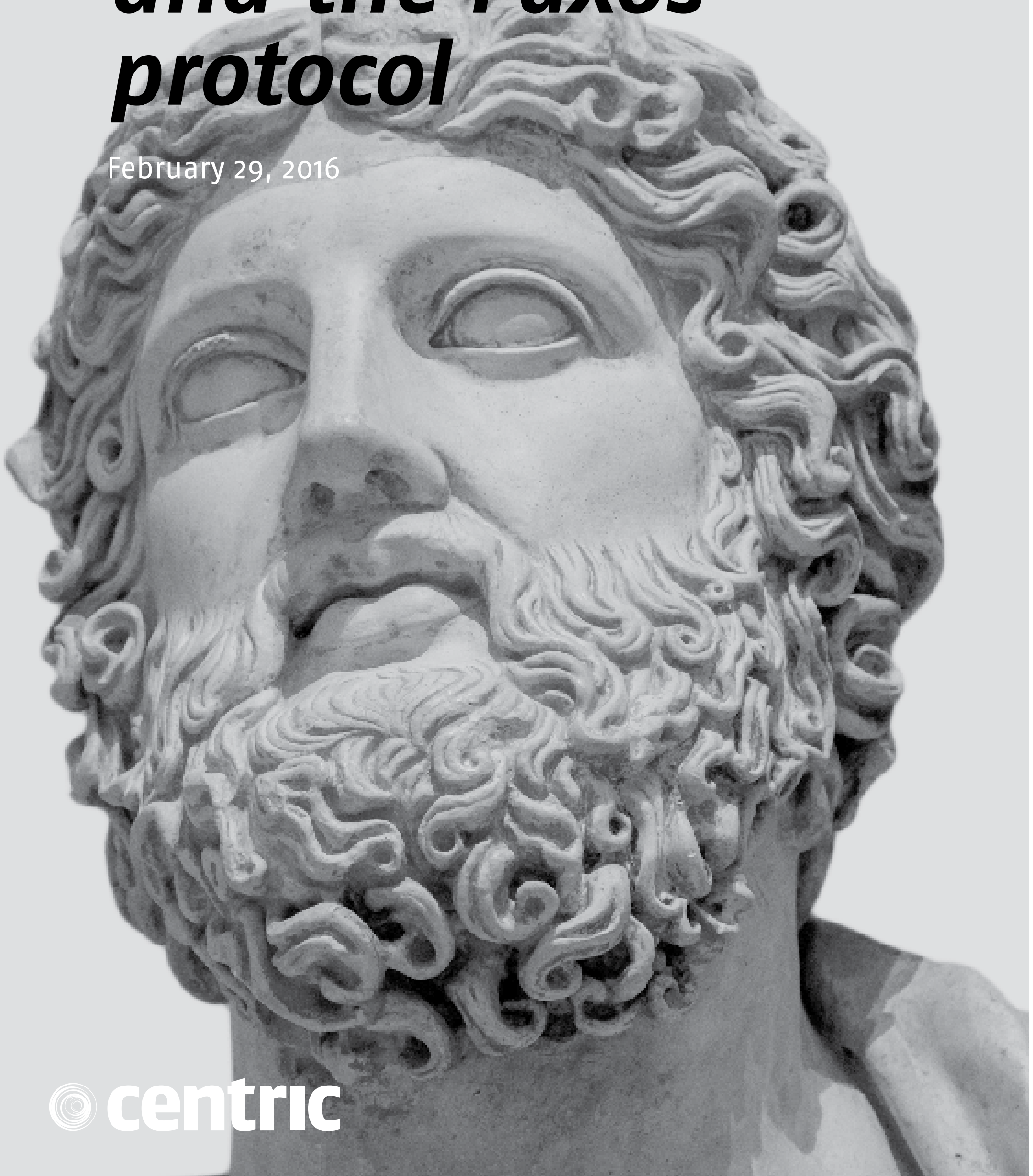
[7] Swan M. (2015) Blockchain. Blueprint for a new economy. Sebastopol, CA, USA, O'Reilly Media ISBN 978141920497

[8] Williams-Grut O. (2015) Goldman Sachs: 'The blockchain can change... well everything'. Business Insider UK. 2 December 2015

[9] IBM Institute for Business Value Executive Report (2015) Device Democracy. Saving the future of the Internet of Things

Blockchain: *distributed ledgers and the Paxos protocol*

February 29, 2016



In his book The Fourth Industrial Revolution executive chairman of the World Economic Forum Klaus Schwab wrote[1]: *"The digital revolution is creating radically new approaches that revolutionize the way in which individuals and institutions engage and collaborate. For example, the blockchain, often described as a distributed ledger, is a secure protocol where a network of computers collectively verifies a transaction before it can be recorded and approved"*. In Schwab's view this blockchain is, in essence: *"a shared, programmable, cryptographically secure and therefore trusted ledger which no single user controls and which can be inspected by everyone."*

Read more >

Distributed ledgers

This view of the blockchain as a distributed and, at the same time, shared (public) form of data and information storage can also be seen in the recently published report of the UK Government Chief Scientific Adviser [2]. This report states that the blockchain is, in essence, a type of distributed database: "... that takes a number of records and puts them in a block. Each block is then chained to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions."

In order to ensure the accuracy (consistency) of the transactions recorded in the distributed ledgers, consensus between the various components of these transactions is required (in network connected devices for example). Through consensus on, and distributed recording of the jointly made decisions concerning transactions, each component involved always has the information about its share in the decision-making for a particular transaction readily available. Every decision or group of decisions (transaction) recorded in a distributed ledger can be viewed as a "block" and any subsequent transaction linked to this block forms a "blockchain" of decisions, linked by means of a protocol, in the form of distributed and stored data and information.

Izabela Moise [3] describes reaching consensus between the components of a system as follows: "*Consensus encapsulates the inherent problems of building fault tolerant distributed systems. Consensus represents the greatest common denominator of the so-called class of Agreement problems such as data consistency, group membership, consistent global states, distributed consensus, atomic broadcast and many others*". In the view of the UK Government Chief Scientific Advisor, the blockchain (distributed computing principles combined with an overlapping protocol) is truly innovative because of the new possibilities it creates to set rules for a particular transaction and ensure these rules remain associated with the transaction itself. This is in contrast to the set-up of a conventional database where rules for recording the data or information are set at the level of the database. When every part serves as an autonomous unit and, at the same time, as a part of the whole system, that system no longer has a central point of failure that can take down the entire system. In a blockchain, the distributed character of recording data and information in distributed ledgers using an encryption-based protocol can also provide a greater degree of privacy and security for the transactions than considered possible using current technological solutions. The UK Government Chief Scientific Advisor states: "*Such ledgers use cryptographic techniques to ensure that anyone can check if a particular record is within the ledger, as long as they possess a small amount of crucial information. At the same time, complex consensus protocols are employed to ensure that everyone in the system gets a consistent view of the ledger (2016:47).*"

The PAXOS protocol

In 1990, Dr Leslie Lamport submitted a research article to the Association for Computing Machinery (ACM) [4]. The article The Part-Time Parliament sat there for eight years before finally being approved for publication. The article centres around what is considered one of the more obscure algorithms in distributed computing. In his writing, Lamport uses the fictional parliament of the ancient civilisation of Paxos as a metaphor to illustrate his algorithm. This parliament operates with part-time legislators who are not always able to be in the parliamentary chamber at the same time when decrees need to be passed. This ancient parliament is a metaphor for consensus and decision-making via random technical units in a system. Lamport goes into considerable detail when describing how such a protocol for reaching consensus and decisions should be given form. In describing this protocol, he works out a detailed algorithm, with which consensus, decision-making and recording of transactions to be carried out can be realised between the entities. The key requirements behind this algorithm are, firstly, fundamental trust between the entities involved and, secondly, consistency where *"...each Paxon legislator maintained a ledger in which he recorded the numbered sequence of decrees that were passed."* An important condition for the individual technical entity (legislator) using the ledger is that, according to the protocol, every decree must be recorded in indelible ink in order to ensure that the decrees cannot be changed once recorded. The main aim of the protocol is to ensure consistency in the recording of the decrees in all the distributed ledgers, meaning, by extension, that no two ledgers can contain contradictory information. The elaborated protocol also contains, among other things, rules to ensure that decision-making procedures are initiated and ballots are conducted, rules on quorums, and how to reach consensus on decrees to be passed. Furthermore, the protocol contains rules on the manner in which the passed decree is to be recorded in the respective ledgers. Because the legislators are required to carry their ledgers with them at all times, they are assured that they will always have the information on the ballots in which they participated. They can also see at what time and in which order these decrees were passed and which legislator took part in a ballot. The ballots are conducted using messengers who distribute messages between the legislators present during the ballot.

This *"Paxos protocol"* appears to have all the characteristics needed for a fault-tolerant and distributed system that operates using a common protocol. In this system, decisions on transactions can be made in consensus and securely recorded in distributed ledgers, which, taken all together, offer at all times and for each component an up-to-date picture of all decisions made.

Conclusion

It is clear that the ideas of Schwab, the UK Government Office for Science and Lamport centre on autonomous entities linked through networks that, with the help of a protocol, make decisions about transactions and how these are to be recorded. This protocol enables the entities to reach consensus and, on the basis of this consensus, make autonomous decisions on transactions, record these transactions in distributed ledgers and learn from previously made decisions. The movement towards transactions that are mutually arranged through technical entities could pose a threat to the role of today's *"trusted third parties"* such as banks, public notaries, government authorities, insurance companies or any other form of physical or technical intermediary. Or, as phrased in the report of the UK Government Office for Science: *"[distributed ledger technologies] have the potential to disrupt the whole economy, and society. Understanding this can help to frame the opportunities and threats afforded by distributed ledger technologies – and how they can inform changes in the role of the government, and the services it delivers."* In addition to praising the unprecedented opportunities afforded by blockchain technology, there is also an urgent need to create a new body of general and technical knowledge, knowledge which, on the one hand, is needed in the short and medium term to build secure and, accordingly, future-proof blockchains and, on the other hand, which can help to make realistic assessments of what is and is not possible the long term.

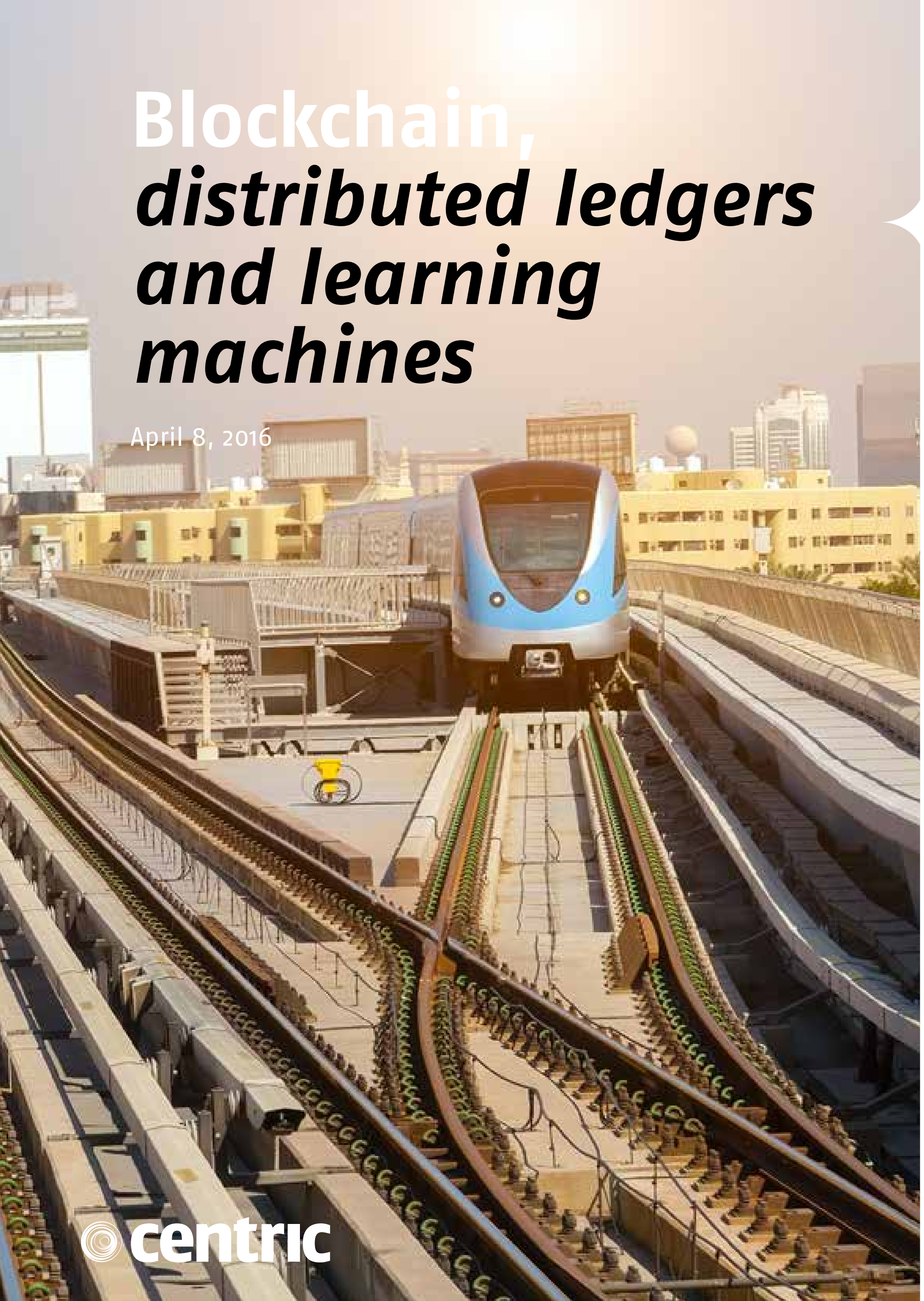
Footnotes

[1] Schwab (2016) The Fourth Industrial Revolution. World Economic Forum ISBN 9781944835002

[2] Government Office for Science. (2016) Distributed Ledger Technology: beyond block chain

[3] Moise I. (2011) Efficient Agreement Protocols for Asynchronous Distributed Systems. Distributed, Parallel and Cluster Computing, Université de Rennes

[4] Lamport L. (1998) The Part-Time Parliament. This article appeared in ACM Transactions on Computer Systems 16, 2 (May 1998)



Blockchain, *distributed ledgers and learning machines*

April 8, 2016

Over the past few decades, the concept of fault-tolerant systems has become essential for the functioning of systems such as aeroplanes. According to Wensley and Lamport et al.[1], fault tolerance is achieved by making as much use of software programs as possible. Software programs enable distributed systems to reach a consensus and run decision-making procedures that let them execute information transactions independently. Running these consensus procedures requires what are known as voter routines, which enable the efficient and effective voting needed for systems to reach a consensus and make decisions. Once made, decisions are recorded in a distributed ledger based on a protocol. Decisions have to be recorded consistently and irreversibly in distributed ledgers as one block, so that the whole can permanently function as a virtual unit, while also offering a steady overview of previous decisions.

Read more >

To run these voting routines quickly and adequately, there are three roles that Lamport deems essential: the proposer, the acceptor and the learner[2]. The interesting question is whether the combination of distributed ledgers, consensus and learning can also play a role in communications between separate and autonomous systems such as machines, factories or entire supply chains in a developing Industrial Internet of Things.

Distributed ledgers and the Industrial Internet of Things

Within a developing Industrial Internet of Things, a diversity of industrial systems and components of these systems will be interconnected in networks. Examples include wind turbines that are networked in a smart grid and communicate with other energy producers or consumers in their environment. Or locomotives that are able to independently communicate with other locomotives and components therein in their environment. In its reference architecture , the Industrial Internet Consortium (IIC) specifies that such industrial systems or components thereof *"must be autonomous, and able to act independently based on the plan and information from other independently operating components nearby."* An essential requirement for communication is that the parties involved trust the communication and the information that is exchanged and shared. The IIC reference architecture therefore states that: *"Trust is established before it is needed, and is necessarily hard to change with very formal procedures in place for transfer between commands."* Communication between such systems must, in principle, be fault-tolerant, which according to the IIC reference architecture refers to *"the ability of the connectivity framework to ensure that redundant connectivity endpoints are properly managed, and appropriate failover mechanisms are in place when an endpoint or a connection is lost."*

As pointed out earlier, trust in intercommunications and in the information exchanged and shared between the parties hinges on factors such as consensus, decision-making and consistent and distributed storage of decisions and related information. Companies of the likes of General Electric are exploring the possibilities for such an industrial fault-tolerant communication system. In a blog post[3], GE already highlighted that: *"the innovative shared-ledger technology offers transparent, immutable and mathematically verifiable record syncing across organisations with no need for trusted middlemen."*

Machine learning

To be able to reach a fault-tolerant decision on an information transaction within an Industrial Internet of Things, the decision-making procedure will have to be executed by four or more autonomous and distributed systems. As stated earlier, Lamport has identified three essential roles in reaching consensus on such a decision: the proposer, the acceptor and the learner. In Lamport's view, it is up to the proposer to propose a decision-making procedure for an information transaction that is to be executed, while acceptors will have to indicate whether or not they can accept this proposal.

"the innovative shared-ledger technology offers transparent, immutable and mathematically verifiable record syncing across organisations with no need for trusted middlemen."

What then becomes particularly interesting in this context is the role of the learner, because, as Lamport explains, the learner: *"can learn what value has been chosen."* According to Domingos , a learner is a learning algorithm that enables systems to learn from data and information. Amir[4] sees machine learning as a sub-area of artificial intelligence that focuses specifically on: *"computerised automatic learning from data of patterns."* The purpose of machine learning is, in Amir's view, *"to use training data to detect patterns, and then to use these learned patterns to automatically answer questions and autonomously make and execute decisions."* In Domingos' opinion, a learner's capacity for learning is still limited within the framework of machine learning, leading him to state that: *"learners can extract some things from data, but nothing you'd confuse with real knowledge."* In Domingos' theory, the learner's learning is only as good as the data available to the learner to learn from. He therefore states that: *"He who controls the data controls the learner."* Domingos claims that, over the coming decade, the development of machine learning will be dominated by deep analogy, i.e.: *"combining in one algorithm the efficiency of the nearest neighbour, the mathematical sophistication of support vector machines, and the power and flexibility of analogical reasoning."* Such deep analogy algorithms are currently primarily used for content or product recommendations that tie in with a specific profile, as used on websites such as Netflix, Amazon, or Bol.com. Such algorithms are also used for real-time monitoring of robotic arms in industrial settings.

Conclusion

Interconnectedness of distributed systems and the availability of increasingly intelligent algorithms will lead to systems acquiring an ever greater level of autonomy in independently making decisions for the execution of information transactions. To be able to adequately perform these information transactions, the distributed systems involved will have to become more intelligent through fast and efficient learning from available data and information. Domingos therefore correctly finds that: *"the role of data and ownership of the models learned from it* *is what many of the twenty-first century's battles will be about – between governments, corporations, unions and individuals."* The importance of reliable and fault-tolerant data and information exchange and sharing between a wide range of different systems can therefore be considered a fundamental precondition in the development of the Industrial Internet of Things.

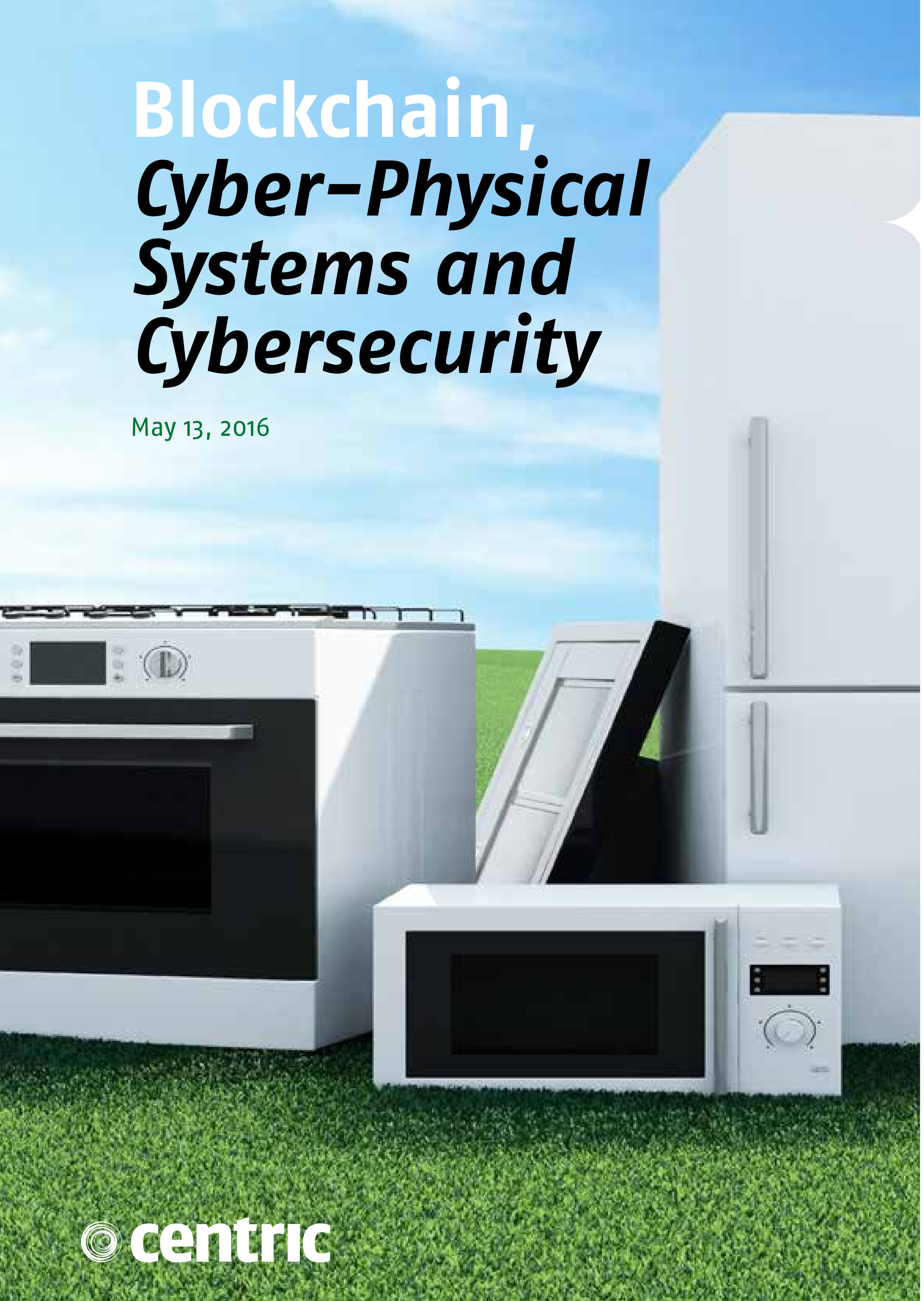
Footnotes

[1] Wensley, J. H., Lamport, L., Goldberg, J., et al. (1978) SIFT: Design and analysis of a fault tolerant computer for aircraft control. Proceedings of the IEEE, Vol. 66, no 10, October 1978.

[2] Industrial Internet Consortium (2015) Industrial Internet Reference Architecture. Version 1.7 June 2015

[3] Domingos, P. (2015) The master algorithm. How the quest for the ultimate learning machine will remake the world. New York, Basic books ISBN 9780465065707

[4] Amir, E. (2014) Reasoning and decision making. in: The Cambridge handbook of Artificial Intelligence. Eds. Frankish, K. and Ramsey, W. M. Cambridge UK, Cambridge University Press ISBN 978521691918 (pp. 191-212)



Blockchain, *Cyber-Physical Systems and Cybersecurity*

May 13, 2016

Cyber-physical systems combine physical objects (such as smart TVs) or systems (such as autonomous cars) with integrated computing facilities and data storage. Such cyber-physical systems can be interconnected in networks, within which they can exchange and share data and information with other objects and systems. Siemens refers to this sort of network of distributed and autonomous systems as a Web of Systems.

Read more >

Cyber-physical systems are increasingly used in networks like smart grids, health-care systems and logistics or industrial production processes. According to the US National Institute of Standards and Technology (NIST), the development of cyber-physical systems needs to include an explicit focus on the cybersecurity of these systems and therefore on increasing resilience against cyberattacks. Blockchains and their inherent combination of consensus algorithms, distributed data storage and secure protocols can be used to increase the robustness and reliability of these networks. This will, in turn, increase confidence in autonomously executed information transactions between cyber-physical systems not resulting in undesired transactions, behaviour or operation of these systems

.

Cyber-physical systems and consensus

Given the critical nature of cyber-physical systems, NIST believes that there must be a constant focus on the uninterrupted and correct operation of these cyber-physical systems in the event of a cyberattack. NIST states that[1] "*cybersecurity for CPS must address how a system can continue to function correctly when under attack, provide mechanisms that support fault-tolerance and/or graceful degradation in accordance with mission- or business-driven priorities, and enable the system to fail-safe in those circumstances in which resilience cannot be provided in the face of threat*". As I have explained previously[2], the achievement of fault tolerance using software is one of the core elements of distributed computing and therefore also of the functioning of a blockchain.

Fault tolerance

Fault tolerance can be achieved by using consensus algorithms that establish consensus between cyber-physical systems on information transactions that are to be executed jointly with one or more other systems. In order to reach consensus on the information transactions to be executed, separate cyber-physical systems exchange and share reliable messages. For Shostak, Pearce and Lamport[3], one of the main prerequisites for establishing consensus is that "*a reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked – namely sending conflicting information to different parts of the system*". Lamport[4] also points out that a reliably functioning distributed system can be developed if it is based on communication between at least three cyber-physical systems which jointly exchange at least six reliable messages in order to reach consensus on the information transaction to be executed.

Consensus and distributed ledgers

Alchieri and Bellami[5] state the following on consensus algorithms: "*In a distributed system, the consensus problem consists of ensuring that all correct processes eventually decide the same value, previously proposed by some processes in* *the system"* (2008:26). When separate systems have reached consensus on the basis of a consensus algorithm and the information transaction has been executed using a secure protocol, each individual system can independently record the value of the decision made and the way in which the decision was made.

The individual systems record this data using the same protocol as the one they used to execute the information transaction. The total of the individually stored values must be consistent and accessible at all times for the systems involved in the decision-making.

> ***"fault tolerant control designs have been developed in order to increase the reliability and maintainability of systems prone to failures"***

By having the protocol used require all systems involved to adhere to the consistency and method of distributed recording of the agreed information transactions, an interconnected information base recorded in distributed ledgers is created. Each distributed recorded decision can be considered to be a block. Once recorded and stored, the block forms the basis for new decisions about new transactions. Basing subsequent decisions on values from previously made decisions, automatically results in a chain of interconnected but distributed recorded decisions about agreed and executed information transactions. As well as agreements on, for instance, ballot procedures or monitoring of the consistency of the stored decisions, the protocol used can also include security features, such as cryptography.

As stated in a recent document published by the European Commission[6], encryption could play a crucial role in the development of a reliable and secure digital environment *"which is impacted by new trends as for instance: the Internet of Things may require more compact and efficient encryption. Without encryption, data in the cloud remains fragile and a target for hackers and criminals"*. The use of a combination of consensus algorithms, distributed storage and cryptography to execute information transactions between cyber-physical systems can prevent the occurrence of single points of failure susceptible to cyberattacks that could cause the system as a whole to malfunction.

Cybersecurity

As posited by Singer[7] and Friedman, one of the risk factors in the development of the Internet of Things is *"that it also enables cyberattackers to penetrate far deeper into our lives than ever before. If everything around us makes important decisions based* *on computerized data, we'll need to work long and hard to make sure that data is not corrupted*".

As well as creating new opportunities, the development of the Internet of Things, the Industrial Internet of Things and cyber-physical systems gives rise to new threats. Cardenas, Amin and Sastry[8] identify a number of conditions that are necessary in order to guarantee the security and reliability of interconnected systems:

- authentication of the systems involved in order to make it clear which system wants to execute an information transaction with other systems;
- access control so that a system can determine which other systems are authorised to execute information transactions with each other;
- a reliable, secure means of communication that enables execution of the information transactions.

Finally, they conclude that "*fault tolerant control designs have been developed in order to increase the reliability and maintainability of systems prone to failures*". The aforementioned developments, which see an increasing number of everyday and industrial systems become interconnected in networks and perform information transactions with each other in these networks, naturally give rise to questions about security and reliability. In the years to come, our lives and our work will increasingly depend on the data and information that these systems exchange and share with each other and with us and security and reliability will therefore become crucial, if not existential, themes.

> ***"In a distributed system, the consensus problem consists of ensuring that all correct processes eventually decide the same value, previously proposed by some processes in the system"***

Conclusion

Thinking in terms of interconnected systems is nothing new. Ashby[9] stated, as far back as 1957, that "*a fundamental property of machines is that they can be coupled. Two or more whole machines can be coupled to form one machine; and any one machine can be regarded as formed by the coupling of its parts, which can themselves be regarded as formed by the coupling of their parts*". This interconnectedness gives rise to a new, complex entity, whose properties cannot be directly traced back to the separate components. Ashby points out that "*such complex systems cannot be treated as an interlaced set of more or less independent feedback circuits, but only as a whole*".

Just like in Ashby's day, we need new insights in order to make the complex entity of people and objects interconnected in networks reliable and safe and to ensure it stays that way. An approach based on distributed and interconnected components that make consensus-based decisions about information transactions to be executed and that ensure distributed, secure and transparent storage of these transactions seems to be a perspective worthy of further research.

Footnotes

[1] National Institute for Standards and Technology. Cyber-Physical Systems Public Working Group (2015) Draft Framework for Cyber-Physical Systems Release 0.8. September 2015

[2] Lier, B. van (2016) Blockchain, distributed ledgers and learning machines, 8 April 2016 http://www.centric.eu/NL/Default/Themas/Blogs/2016/04/08/Blockchain-distributed-ledgers-and-learning-machines- and Lier, B. van (2016) Blockchain, distributed ledgers and the PAXOS protocol, 29 January 2016 http://www.centric.eu/NL/Default/Themas/Blogs/2016/02/29/Blockchain-distributed-ledgers-and-the-Paxos-protocol-

[3] Lamport, L. and Melliar-Smith, P. M. (1984) Proceeding PODC '84, Proceedings of the third annual ACM symposium on Principles of distributed computing, pp. 68-74

[4] Lamport, L., Shostak, R. & Pease, M. (1982) The Byzantine Generals Problem. ACM Transactions on Programming languages and Systems, Vol. 4, No. 3, July 1982, pp. 382-401

[5] Alchieri, E., Bessani, A., Silva Fraga, J. da and Gireve, F.(2008) Byzantine Consensus with Unknown Participants. Baker, T. P., Bui, A. and Tixeuil, S. (eds.) Principles of Distributed Computing, 12th International Conference, OPODIS 2008, Luxor, Egypt, December 15-18 2008. Proceedings, Springer, pp 22-40

[6] European Commission. Scientific Advice Mechanism. Scoping paper: Cybersecurity, 29 January 2016 (Revised)

[7] Singer, P. W. and Friedman, A (2014) Cybersecurity and Cyberwar. What everyone needs to know. New York, Oxford University Press. ISBN 978-0199918119

[8] Cardenas, A., Amin, S. and Sastry, S. (2008) Secure Control: Towards Survivable Cyber-Physical Systems. Distributed Computing Systems Workshops, ICDCS'08. 28th International Conference on (2008), pp. 495–500

[9] Ashby, R. (1957) An introduction to Cybernetics. Second impression. Chapman & Hall Ltd., London.

Smart grids, blockchain and self-organizing systems

August 15, 2016

In his blog post on the 'Fourth Industrial Revolution,' Reidel stated [1] that "The true wonder of the fourth industrial revolution won't be the data produced; it will be intelligent machines' capacity to analyze those data and communicate their findings within a network of similarly intelligent machines. Then, each connected machine will act, altering its processes to be more efficient and communicating those changes back to its network". In this process of preparing and executing information transactions between distributed operating machines, Reidel sees a role for the blockchain. In his view, the blockchain can inspire mutual trust between the machines involved in the information transactions and their stakeholders.

Read more >

The idea of intelligent networked machines that are able to autonomously execute mutual information transactions also lies at the heart of developments such as the (Industrial) Internet of Things. In these developments, distributed and autonomously operating systems are increasingly interconnected in networks and able to mutually exchange and share information and data. Intercommunication and interaction enables autonomous and intelligent systems to self-organise in temporary coalitions that intend to achieve a certain objective in a specific context.

Smart grids

Siemens, the German conglomerate, is currently looking into options for the development of the blockchain for industrial applications. In a recent fact sheet [2] published by Siemens' new Next47 unit, they stated, among other things, that "implementation of blockchain in devices is an interesting but as yet fully untested area". According to Siemens, blockchain applications offer possibilities for: "secure direct interaction between autonomously operating machines". They pointed at possibilities in trading energy between energy consumers and producers. Energy is currently mainly traded through information transactions between energy-producing systems, such as solar panels, wind turbines or power plants, and energy-consuming systems in people's homes or other buildings, such as washing machines, lights and cooling and heating equipment. The information transactions that need to be performed to deliver and receive energy are de facto information transactions between distributed operating systems that are ultimately converted into a value. Of these developments on the energy market, Jimenez [3] said "This along with the latest innovations in smart metering devices, reduction in prices of renewable energy and storage systems are leading towards growth in a decentralized energy market place" (2016). In Jimenez's view, a blockchain has the capacity to play a key role in the development of local marketplaces for producers and consumers through a: "distributed ledgers mechanism combined with the modern communication technologies". He claimed that when the development of smart grids is based on a combination of the Internet of Things and blockchain: "energy networks will become more robust with the inclusion of Internet of Things and blockchain platforms, as every node and asset in the smart grid will be helping to keep the grid stable". A smart grid containing a range of different autonomous distributed operating systems that mutually perform information transactions is similar to the development of the Internet of Things or the Industrial Internet of Things. The latter two concepts are also based on the assumption that increasing numbers of distributed and autonomous operating systems make decisions on a local level about information transactions to be performed.

Blockchain

Goldman Sachs [4] is another company that has identified the potential of blockchain, saying that "combining blockchain with the Internet of Things could enable the negotiation of distributed power transactions" (2016:29). According to experts at this investment bank, it is quite conceivable for producers' systems to negotiate with consumers' applications on a local level about energy consumption and charges. In their view, blockchain could enable reliable and secure information transactions between producers' and consumers' systems, which are not necessarily aware of each other's existence. A blockchain of information transactions would then create a fault-tolerant environment that facilitates reliable and secure message exchange and sharing between unknown and distributed operating systems. In the Industrial Internet Reference Architecture [5], fault tolerance is described as a condition for communication between such systems: "redundant connectivity endpoints are properly managed, and appropriate failover mechanisms are in place when an endpoint or a connection is lost" (2015:75). Based on a fault-tolerant communication system, distributed systems can mutually determine how and with which other system, or groups of systems, they can or have to perform information transactions. The decision-making on the performance of these information transactions between distributed and autonomous systems is based on coordinated voting procedures. By reaching consensus, participating systems are able to jointly decide what information transaction to perform. Each system separately records the details underlying the ultimate decision in its own ledger. The whole of all of the decisions recorded in this way is what we, in terms of blockchain theory, refer to as a block. This block, which is recorded in a distributed manner across different systems, is the basis for participation in subsequent voting rounds, creating a chain of related data and information blocks. For IBM [6], this shift from centralised control by producers to decentralised decision-making by autonomous and distributed operating systems represents a fundamental change: "By shifting the power in the network from the center to the edges, devices gain greater autonomy and can become points of transaction and economic value creation for owners and users" (2015:1). As they reach consensus on transactions, autonomous and intelligent systems become able to play an independent role in economic dealings, leading IBM to conclude that "By transforming every device into a point of transaction and economic value creation for owners and users, the IoT will create new real time digital economies and new sources of value. We call this transformation the 'Economy of Things'" (2015:12).

Self-organisation

The first person to study the possibilities of temporary and permanent forms of self-organisation by systems based on the exchange and sharing of information was Ross Ashby [7]. In 1962, he said "A system is self-organizing in the sense that it changes from parts separated to parts joined" (1962:266). The interconnection of systems in networks, the exchange and sharing of data and information and the ability to assign meaning or value to data and information received are what makes distributed operating systems not only more autonomous, but also smarter and able to self-organise. Dressler [8] (2006) on this: "The interconnected devices have to form a network in an ad-hoc manner i.e. spontaneously, have to maintain the network state and coordinate the information exchange. The grade of interactivity greatly influences the possible solutions for controlling i.e. organizing the network". Developments such as the (Industrial) Internet of Things, smart grids and mobile healthcare all include an element of interconnection of autonomous distributed operating systems in networks, which are becoming smarter and smarter through the use of algorithms, software and data. Historically, a blockchain is also based on algorithms, software and data that enable distributed and autonomous systems to autonomously and consensually make decisions on a local level, also under difficult circumstances. The idea that these two developments can be combined and help us trust the information transactions performed by interconnected systems on our behalf is a more than interesting one. However, not taking economic and other social possibilities into account, it does require greater emphasis on research into the algorithms, software and data that would be needed to enable decision-making by these distributed and autonomous systems.

Footnotes

[1] Reidel, D. (2016) Will Blockchain drive the fourth Industrial Revolution? Readwrite.com http://readwrite.com/2016/05/09/blockhain-new-ir/

[2] Siemens (2016) Blockchain applications Fact sheet for innovation fields. Chained data blocks as a new solution for digital transactions. http://www.siemens.com/content/dam/internet/siemens-com/innovation/innovation/pdfs/next47-fact-sheet-blockchain-e.pdf

[3] Jimenez J. (2016) Blockchain for smart grids can create a decentralized energy marketplace. TOPFUNDED 19 July 2016. http://www.topfunded.com/blockchain/blockchain-for-smart-grids-can-create-a-decentralized-energy-marketplace/

[4] Blockchain. Putting Theory into Practice (2016) Goldman Sachs investment Research. Profiles in innovation, 24 May 2016

[5] Industrial Internet Reference Architecture (2015) Industrial Internet Consortium. tech-arch.tr.001 2015-06-04, Version 1.7

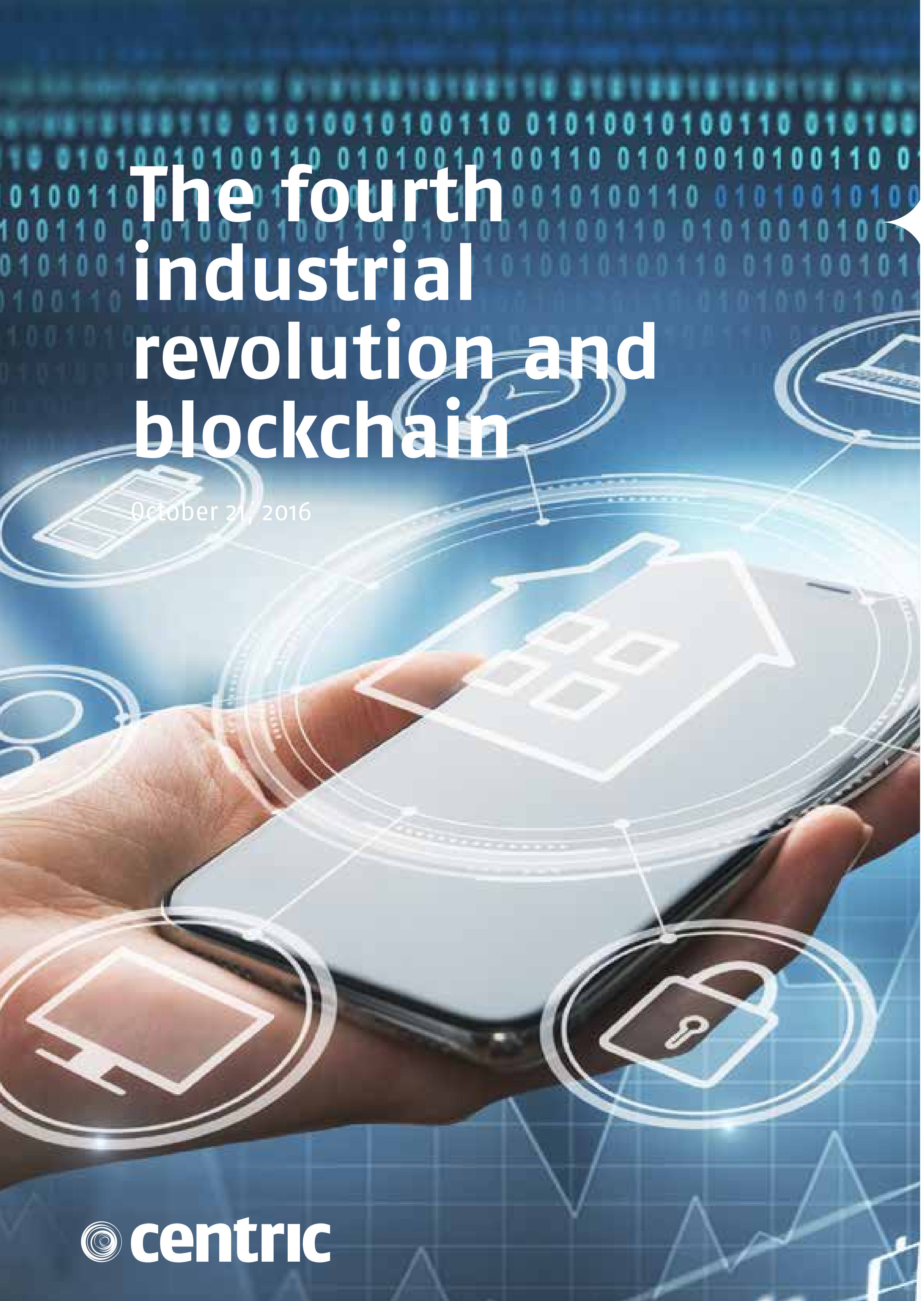
[6] IBM Institute of Business Value (2015) Empowering the Edge. Practical Insights on a Decentralized Internet of Things. Executive report Electronics industry

[7] Ashby, R. W. (1962) Principles of the Self-Organizing system. In: Principles of Self-Organization: Transactions of the University of Illinois Symposium. Foerster, H. von and Zopf jr., G. W. (eds) Pergamon Press, UK, pp. 255-278. Republished in E:CO vol 6, nos 1-2 pp. 102-126

[8] Dressler, F. (2006) Self-Organization in Ad-Hoc Networks: Overview and Classification. Technical Report. University of Erlangen, Dept. of Computer Science 7.

The fourth industrial revolution and blockchain

October 21, 2016



In 1954, German philosopher Martin Heidegger[1] argued that the essence of modern technology *"shows itself in what we call enframing"*. Heidegger uses the concept of enframing to determine how technology develops, surrounds us and conditions our perception of the world. For Heikkerö, the concept of enframing consequently refers to *"a way of disclosing the world"*[2]. Today, the process of technology enframing reality is characterised by networked applications such as smartphones, tablets and an unprecedented range of sensors that enable us and these devices to communicate and interact in both the physical world and the cyber world through networks. This is changing the world and our perception of it, without us wondering what the essence is of this technological shift and what how these changes will affect our lives and work over the coming years.

Read more >

Technology and the technological applications it produces are, according to Arbesman[3], also becoming increasingly complex in people's perception, partially due to their interconnectedness. This interconnectedness enables systems to autonomously make decisions on individual and joint actions. The proliferation of interconnected autonomous systems that are able to work together in random combinations is, in Arbesman's view, creating a situation where "*we become less able to understand them, no matter how smart we are or how prodigious our memory, because these systems are constructed differently from the way we think*".

Enframing by technology and the increasing interconnectedness of humans and technology are forcing us, in fact, to develop new knowledge and insights that, on the one hand, enable us to trust these technological changes. On the other hand, interconnected systems will make more and more decisions and share and exchange data and information ensuing from these decisions, entirely out of humans' sight.

Interconnected systems will thus increasingly condition our daily lives and work, without us retaining any kind of understanding or oversight of how these decisions come about. One key element of this change is the willingness to gain insight into how this increasingly complex technology works, with a view to understanding what it means for the world that we share with technology.

Fourth industrial revolution

The ongoing global development and application of new technology will inevitably change the way we live and work over the coming years. According to Schwab[4], the development that the World Economic Forum has branded the '*fourth industrial revolution*' is the result of the "*fusion of technologies and their interaction across the physical, digital and biological domains that make the fourth industrial revolution fundamentally different from previous revolutions*".

Digitalisation in the form of algorithms, software and data will enable systems produced by the fusion of technologies to operate autonomously in networks and communicate data and information, make decisions and interact within these networks. We are already seeing this development in phenomena such as the (Industrial) Internet of Things, which is based on the interconnection of a wide range of different objects, such as washing machines, televisions, lorries, cars, wind turbines and factories, etc.

This development will engender new systems that are referred to as 'cyber-physical systems'. The US National Institute of Standards and Technology (NIST)[5] defines cyber-physical systems as "*smart systems that include engineered interacting networks of physical and computational components*"[6]. Cyber-physical systems, such as a self-driving lorry, are characterised by the fact that they are designed to be connected in networks, to operate autonomously, to communicate and interact and to be able to independently make decisions in consensus with other cyber-physical systems.

The possibilities offered by a cyber-physical system are not limited to their physical possibilities, but rather determined by the combination of these physical functions with the possibilities offered by algorithms, software and data. This development will change the world around us, while our perception of the world will partly be conditioned by smart, autonomous objects that are able to make more and more decisions for us. We seem to be heading towards a society where man and object live, work and make decisions together as equals.

"enforce property rights, and manage IoT and inter-device interactions"

Blockchain

In Schwab's view, the fourth industrial revolution creates "*radically new approaches that revolutionize the way in which individuals and institutions engage and collaborate*". One of these new approaches is, according to him, blockchain. Blockchain, a unique example of a fusion of technologies, was developed and defined by Nakamoto. Mougayar[7] recently claimed that "*the blockchain can be seen as a 'meta technology', because it is made up of several technologies itself. It is as an overlay of computers and networks that are built on top of the Internet*". Algorithms, software and data enable networked systems to reach consensus on mutual information transactions.

What is particularly revolutionary about this is that blockchain no longer uses centralised data and information storage, as decisions and associated data are stored at the distributed entities that took part in the transaction. In a recent remark, Lael Brainard[8] of the Federal Reserve's Board of Governors stated that "*regardless of the application, much of the industry is at a "proof of concept" stage of development. These proofs of concept are often simple, experimental uses of the technology on a small scale that help stakeholders understand the potential and limitations of the technology for a specific purpose*".

Despite current technological limitations, research into possible applications of this new technological combination is being carried out all over the world. One example is a project by Ant Financial, a subsidiary of China's Alibaba Group[9], to develop a blockchain that raises people's trust in charities and inspires them to donate. Such a blockchain not only potentially increases transparency on the destination of donations, but also allows people to check what funds were actually spent on. Another Chinese company, Wanxiang[10], one of the world's largest manufacturers of automotive parts, has announced plans to develop a blockchain that can be used in their production lines. The company hopes that this technology will not only help them cut costs, but also "*enforce property rights, and manage IoT and inter-device interactions*".

Emergence

In Simon's[11] view, a complex system is made up of a "*large number of parts that interact in a non-simple way. In such systems, the whole is more than the sum of the parts*". Intercommunication and interactions between a diverse range of systems creates a new unified whole, whereby the behaviour of the whole cannot be traced back to its constituent parts. The development of the whole and the ensuing behaviour is referred to as '*emergence*'. Bedau[12] defines emergence as the "*aggregate global behavior of certain systems. The system's global behavior derives just from the operation of micro-level processes, but the micro-level interactions are interwoven in such a complicated network that the global behavior has no simple explanation.*"

In the world of the fourth industrial revolution, we will see more and more fusions of technologies such as the blockchain arise, which will automatically lead to a further progressing process of enframing. This process is driven by an unprecedented number of interconnected systems that communicate, make decisions and interact, and which are thus able to condition our perception of reality. These networks and interconnected systems provide foundations for concepts such as the (Industrial) Internet of Things, smart grids, smart cities and mobile healthcare, as well as Network Centric Warfare.

The new wholes of interconnected people and systems produce new features that are not only unpredictable, but will also inevitably change our perception of the world. In light of this development, we owe it to ourselves to learn more about the new combinations of technology, algorithms, software and data, and about the resulting fusions of technologies that enable this development and that will be a key factor in how we view the world. Without the willingness to learn about how this interconnectedness works and conditions us, we will increasingly feel caught off guard by the development of features that are created in the new wholes into which we are incorporated.

> ***"Despite current technological limitations, research into possible applications of this new technological combination is being carried out all over the world."***

Footnotes

[1] Heidegger, M. (1977). The Question Concerning Technology and Other Essays. New York: Harpers and Row.

[2] Heikkerö, T. (2010). Ethics in Technology. A Philosophical Study. New York: Lexington Books (ISBN 9780739191958).

[3] Arbesman, S. (2016). Overcomplicated. Technology at the Limits of Comprehension. New York: Current (ISBN 9781591847762).

[4] Schwab, K. (2016). The Fourth Industrial Revolution.

[5] National Institute of Standards and Technology (May 2016). Framework for Cyber-Physical Systems Release 1.0. Cyber-Physical Systems Public Working Group.

[6] National Institute of Standards and Technology (May 2016). Framework for Cyber-Physical Systems Release 1.0. Cyber-Physical Systems Public Working Group.

[7] Mougayar. http://blogs.lse.ac.uk/businessreview/2016/07/07/working-as-a-layer-on-top-of-the-internet-blockchain-is-an-instrument-of-change/

[8] Brainard, L. (2016). Distributed Ledger Technology: Implications for Payments, Clearing and Settlement. Remarks by Lael Brainard, member of the Board of Governors of the Federal Reserve System. Institute of International Finance Annual Meeting Panel on Blockchain, Washington D.C. October 7, 2016.

[9] Alibaba. https://news.bitcoin.com/ant-financial-blockchain-philanthropy/.

[10] Wanxiang. Blockchain is Behind a Massive $30B Smart City Project in China. http://futurism.com/blockchain-is-behind-a-massive-30b-smart-city-project-in-china/.

[11] Simon, H. A. (1969). The Sciences of the Artificial. The Massachusetts Institute of Technology.

[12] Bedau, M. A. and Humphreys, P. (eds.) (2008). Downward Causation and Autonomy in Weak Emergence. Emergence: Contemporary Readings in Philosophy and Science. Massachusetts Institute of Technology (ISBN 9780262524759).

Blockchains and ecosystems

December 16, 2016

In 1935, Arthur Tansley[1], a pioneer in the field of ecology, stated that an ecosystem is to be considered a whole that is made up of interconnected constituent parts.

Read more >

This whole, Tansley claimed, is not only the whole of the available organic systems, "*but also the whole complex of physical factors forming what we call the environment of the biome – the habitat factors in the widest sense*." (1935, p.299) For Tansley, there is no distinction between the natural organic elements or physical elements that are present within the whole of an ecosystem. The ecosystem as a whole is made up of separate parts through their mutual relations with their environment. These interrelations, intercommunications, and interactions between the separate elements are precisely what create a whole. Jan Smuts [2] (1926, p.127) defines this whole as follows: "*The whole fuses the action of its elements into a real synthesis, into a unity which makes the result quite different from what it would have been as the separate activities of the parts*." The whole of the ecosystem can therefore not be explained based on knowledge of the separate constituent parts, but rather by acquiring knowledge of the pattern of mutual interaction and communication between the separate parts, which thus make up and further develop the whole of the ecosystem.

Blockchain

In 2008, Satoshi Nakamoto [3] said that "*what is needed is an electronic payment system based on cryptographic proof instead of trust allowing any two willing parties to transact directly which each other without the need for a trusted third party*." The bitcoin ecosystem he describes, and which was created in that era, is based on interaction between people and distributed and random technological nodes (i.e. computers) that are interconnected in a network. With this network, he creates a new way of executing information transactions between peers without the intervention of a trusted third party. Through this new kind of interaction, new people and technological nodes can always join the network (or leave it at any random moment) to execute one or multiple information transactions. The nodes accept that new decisions are made within the network all the time, and that these are linked up as blocks. In Nakamoto's theory, networked nodes vote on these decisions using "*CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism*." The fundamental features of the bitcoin ecosystem are hence the result of communication and interaction between organic and physical entities that operate in a distributed manner and are interconnected in the bitcoin ecosystem or network. The whole of this ecosystem develops itself based on the mutual relations of and communication and interaction between the separate parts. The functioning of the whole depends on the voting that is necessary to reach consensus for the execution of information transactions. With this consensus requirement for information transactions between autonomous nodes, Nakamoto not only lays the foundation for the bitcoin network, but also for current discussions on the possibilities offered by blockchain technology. It isbecoming increasingly clear that it is essential for the functioning of a blockchain that autonomous and distributed nodes update the information on their transactions themselves (in distributed ledgers). Aside from that, it is essential that the blockchain works based on voting and consensus procedures that lead to decisions on the execution of information transactions with other nodes in the network. Connections within the network enable individual nodes to engage in communication and interaction, based on which they can autonomously take part in decision-making procedures in the network. By accepting decision-making procedures completed by technological nodes, humans effectively, based on trust, hand over responsibility for the execution of information transactions to the technological nodes. Humans thus no longer occupy a central position in the decision-making process about information transactions with others in the network, even though this decision-making process was initiated by humans.

"the idea that to understand the world we only need to understand its pieces"

The whole of interconnected humans and technological nodes that communicate, interact, and share information with each other in this network is starting to show similarity to Tansley's description of an ecosystem. In this case, it is a socio-technical ecosystem where combinations of human and physical components naturally strike up interrelations, communicate, and interact, creating a synthesis or a new whole that adds up to more than the different separate activities. Hissam, Klein and Moreno [4] (2013, vii) referred to such a synthesis of man and technology as a socio-adaptive system: "*systems in which humans and computational elements interacts as peers*. *The behavior of the system arises from the properties of both types of elements and the nature of their collective reaction to changes in their environment., the mission they support, and the availability of resources they use.*"

Ecosystems

According to Russell Ackoff [5] (1971), a system is "*a set of interrelated elements*". A system is, in Ackoff's theory, made up of at least two elements and the relationship that keeps these two elements together and unites them with at least one other element in their environment. The functioning of the system as a whole can hence, in Ackoff's view, only be approached from a holistic perspective. He claims that the functioning of the system as a whole is not only driven by the separate elements, but also shaped by these elements and their mutual communications and interactions. For John Miller [6] (2015), the combination of interconnected systems and their mutual communication and interaction are the basis for the complexity of the whole, which tacitly develops in the interconnectedness of the separate elements. Knowledge of patterns of communication and interaction between the separate systems is, in Miller's view, of fundamental importance if we want to understand the behaviour of these complex systems. According to Miller, this is, however, impossible as long as our contemporary science is still driven by reductionism, which is focused on "*the idea that to understand the world we only need to understand its pieces*" (2015, p.22). This leads Miller to state that "*even if we can study and know the world's simplest components, that doesn't imply that we will understand everything just because the world is constructed from these components. Indeed, to reconstruct the world we have to have a theory of how components once put together, interact*" (2015, p.22). Interaction and communication between people and technological nodes based on equality is also the basis of new ecosystems in the form of blockchains. As Tansley already said, ecosystems arise and develop as a whole based on interconnectedness between the separate components and their communications and interactions. Humans and technological nodes communicate and interact in new blockchain ecologies based on trust. Trust between humans and technological nodes is hence the basis for the transfer of decision-making responsibility from humans to technological nodes within a developing blockchain ecosystem. The technological nodes and the consensual decisions made by them lead to information transactions with other technological nodes or humans within the blockchain ecosystem. The development of such a system therefore depends on a new combination of humans and the possibilities (and limitations) of the available technological nodes and their ability to communicate and interact within such a blockchain ecology. Without acceptance of the new whole and the technological possibilities (and limitations) of intercommunication and interaction, any discussion about the development of new blockchains will simply be pointless. As asserted by Murray Gell-Mann [7], this is one of the reasons why ecologists, in their observation of an ecosystem, "*would also include interactions among organisms in the forest, such as those between predator and prey, parasite and host, pollinator and pollinated, and so on*" (1994, p.29). From the perspective of an ecosystem, the creation of new blockchain ecologies is possible only if we accept that this ecosystem will be based on new combinations of man and technology, combined action by humans and technological nodes that strike up equal relationships, based on which they communicate, interact, and exchange and share information.

> ***“The fundamental features of the bitcoin ecosystem are hence the result of communication and interaction between organic and physical entities that operate in a distributed manner and are interconnected in the bitcoin ecosystem or network.”***

Footnotes

[1] Tansley A.G. (1935) The Use and Abuse of Vegetational Concepts and Terms. Ecology, vol 16, issue 3, pp 284-307

[2] Smuts, J. C. (1926) Holism and Evolution. New York, the MacMillan Company.

[3] Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System

[4] Hissam, S., Klein, M. and Moreno, G. A. (2013) Socio-Adaptive Challenge Problems Workshop Report. Chicago, Carnegie Mellon Software Engineering Institute. June 2013, CMU/SEI-2013-SR-010

[5] Ackoff R.L. (1971) Towards a System of Systems Concept. Management Science, vol. 17, issue 11, pp. 661-671

[6] Miller J.H. (2015) A Crude Look at the Whole. The Science of Complex Systems in Business, Life, and Society. New York, Basic Books. ISBN 978465055692

[7] Gell-Mann M. (1994) The Quark and the Jaguar. Adventures in the Simple and the Complex. London, ABACUS. ISBN 9780349106496

[1] Tansley A.G. (1935) The Use and Abuse of Vegetational Concepts and Terms. Ecology, vol 16, issue 3, pp 284-307

[2] Smuts, J. C. (1926) Holism and Evolution. New York, the MacMillan Company.

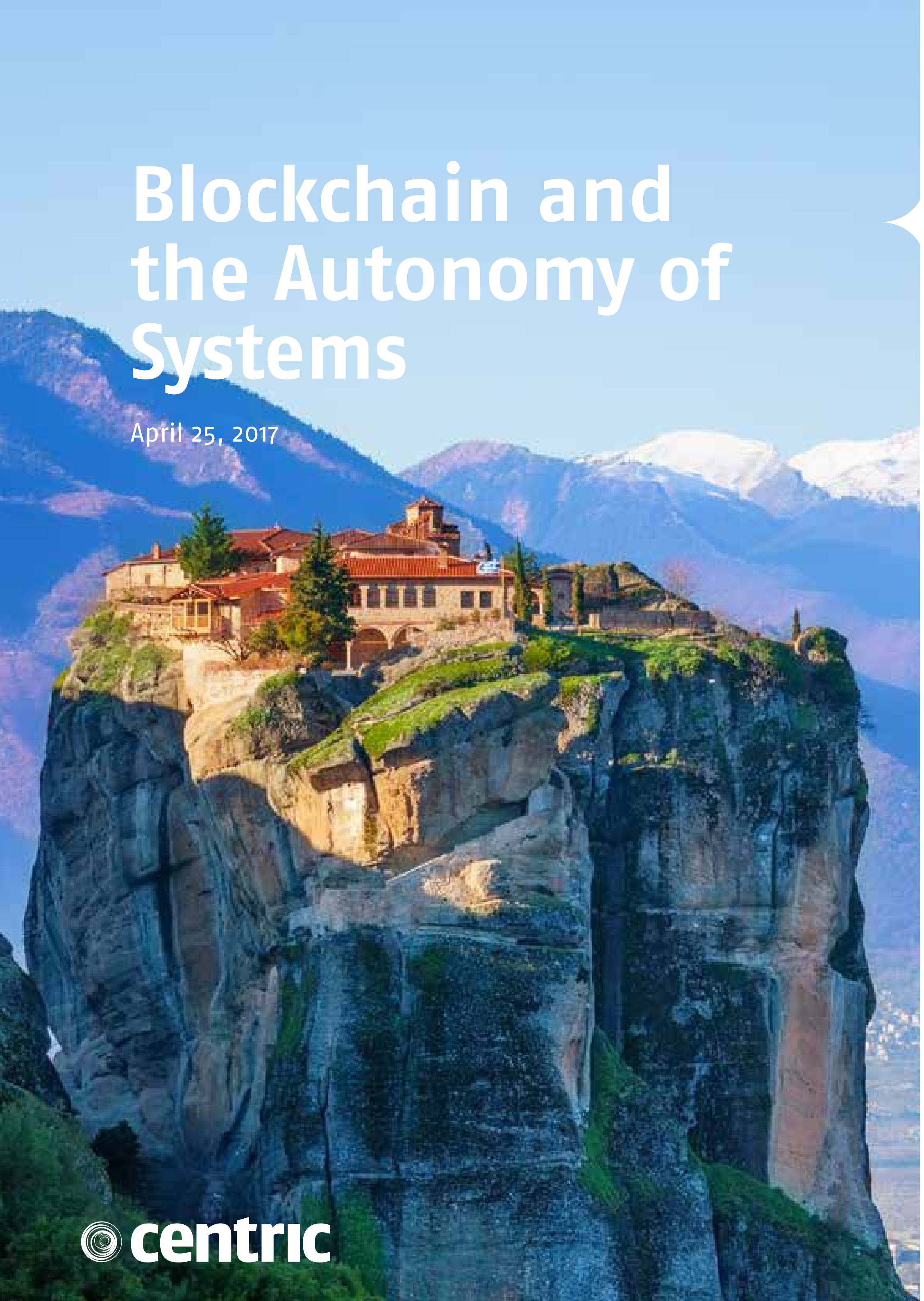
[3] Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System

[4] Hissam, S., Klein, M. and Moreno, G. A. (2013) Socio-Adaptive Challenge Problems Workshop Report. Chicago, Carnegie Mellon Software Engineering Institute. June 2013, CMU/SEI-2013-SR-010

[5] Ackoff R.L. (1971) Towards a System of Systems Concept. Management Science, vol. 17, issue 11, pp. 661-671

[6] Miller J.H. (2015) A Crude Look at the Whole. The Science of Complex Systems in Business, Life, and Society. New York, Basic Books. ISBN 978465055692

[7] Gell-Mann M. (1994) The Quark and the Jaguar. Adventures in the Simple and the Complex. London, ABACUS. ISBN 9780349106496



Blockchain and the Autonomy of Systems

April 25, 2017

The Oxford English Dictionary defines "*autonomy*" as "*the right or condition of self-government or having its own laws*". The autonomy of an individual system can be determined based on the extent to which an individual system is capable of self-government. When an individual system is connected to other systems in a temporary or permanent whole with joint decision-making capability, the autonomy of such a system of systems can be considered to be determined by rules and laws that apply specifically to this whole and its constituent parts, and which are captured in algorithms. The shift of decision making from humans to interconnected machines raises numerous questions, such as, according to Van Lier and Hardjono [1], about the "*necessary trust between participants in such networks*".

Read more >

Blockchain

One example of a system of systems with its own laws and rules is the global bitcoin ecosystem. This ecosystem is partly based on Nakamoto's [2] idea that a new global payment system is needed and must be based on cryptography instead of on trust between people and organisations. By basing information transactions within the payment system on cryptography, you can, according to Nakamoto, enable "*any two willing parties to transact directly with each other without the need for a trusted third party*". In the bitcoin ecosystem, the use of cryptography and other algorithm-based rules replaces the trust between people and organisations with trust in the functioning of the system of systems and its information transactions.

Lamport's PAXOS algorithm [3] is, as he himself explained, a procedure where decision making is based on consensus and getting a "*majority of legislators*" to approve proposed laws and rules needed for the functioning of a system of systems. Problems that may arise in the decision-making process about such laws and rules are, according to Lamport, comparable to those that can arise in fault-tolerant decision making in distributed (computer) systems. In Lamport's view, decision-making procedures executed at any nation's parliament are similar to decision-making processes between different individual and interconnected (computer) systems that have to run a task jointly as a system of systems. Both Nakamoto and Lamport have claimed that trust between people and between people and organisations can be replaced by trust in the functioning of algorithms that enable interconnected systems to operate autonomously and reliably and communicate with each other, and hence allow these systems to make consensus-based decisions on information transactions that have to be executed. When it comes to decision making by interconnected systems, it is, like with a parliament, important to know on which assumptions or choices (included in the algorithms used) the decision-making process is based.

> ***"deploying various forms of machine intelligence and autonomous decision making in the real world without some kind of ethical restraint or moral assurances is both risky and potentially dangerous for human beings"***

Autonomy

Feenberg [4] defined such a form of autonomy as operational autonomy, i.e.: "*the power to make strategic choices among alternative rationalizations without regard for externalities,* *customary practice, workers preferences, or the impact of decisions on their households*". To Feenberg, what is particularly important to consider for this technology-based form of decision making is what ideology, rules, or algorithms underlie the rules, code, or algorithms needed for such decision making. In the cases of bitcoin and PAXOS, for example, the underlying basis is the ambition to create a better global payment system based on interconnected systems and cryptography (bitcoin) and the ambition to create an environment where interconnected autonomous systems can autonomously make consensus-based decisions (PAXOS). According to Barber and Martin [5], increasing trust in the autonomy of interconnected systems is determined by "*the degree to which the decision-making process, used to determine how that goal should be pursued, is free from intervention by any other agent*". In their view, autonomy within a system of systems is a given, and individual systems in any manifestation are therefore self-governing. Autonomy of interconnected systems is, according to them, concentrated around active use of shared capabilities for decision making in realising a specific objective, without other systems being able to influence this. A report published by the US Defense Science Board [6] stated that the autonomy of systems should be considered a result of the delegation of decision making to an autonomous entity to enable this entity to independently execute a task within predefined boundaries. According to the authors of this report, to be autonomous "*a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation*". Wallach [7] sees the increasing autonomy and independent decision-making capabilities of interconnected systems as a threat to the fundamental given that humans are responsible and accountable for possible damage caused by this form of technology. According to Allen and Wallach [8], the current generation of software that interconnected systems use for decision-making procedures is not yet sufficiently developed in an ethical sense, meaning that these systems are insufficiently able to include and process an explicit representation of moral thought in their decision making. This latter point means, according to Gunkel [9], that the development of autonomous and interconnected systems must also look at the need for ethics and moral actions by these systems, which led him to state that "*deploying various forms of machine intelligence and autonomous decision making in the real world without some kind of ethical restraint or moral assurances is both risky and potentially dangerous for human beings*".

Decision making

Today's blockchain technology hype is focused largely on the possibilities and opportunities that this new form of technology seems to offer. We are readily willing to, in our thinking, swap trusted third parties, as created by humans, for interconnected autonomous technological systems. These interconnected systems can, so we think, jointly make decisions, enter into contracts, and perform information transactions based on their own laws and rules as captured in algorithms for these systems. As humans, we trust the growing autonomy with which systems of systems are able to make decisions based on man-made algorithms and software, and subsequently perform a range of information transactions based on these decisions. We are, on the other hand, not interested in the assumptions and choices made by humans in making the algorithms and software that enable the autonomy and decision making of these systems of systems. Our trust in the functioning of these systems of systems is, therefore, not based on our knowledge of the laws and rules underlying the decision making by these systems. Do we, however, not owe it to ourselves to also ask with respect to this readily accepted shift of responsibility from humans to technology, just like Hannah Arendt[10] did, "*what is the nature of the sovereignty of such an entity?*" Should we not focus more on the assumptions and choices that went into the algorithms and software that enable the decision making by these systems of systems and shape the information transactions performed by these systems based on these algorithms and software? Does this hype not ultimately raise the question whether this lack of interest in the essence of this kind of technology could also lead to outcomes that are less positive or different from our current expectations?

Footnotes

[1] Lier, B. van and Hardjono, T. (2011) A Systems Theoretical Approach to Interoperability of Information. Systems Practice and Action Research, 24, pp. 479-497

[2] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system

[3] Lamport, L. (1998) The Part-Time Parliament. ACM Transactions on Computer Science, vol 16 no 2 pp. 133-169. May 1998

[4] Feenberg, A. (2002) Transforming Technology. A Critical Theory Revisited. Oxford University Press ISBN 0195146158

[5] Barber, K. S. and Martin, C. E. (1999) Agent Autonomy: Specification, Measurement, and Dynamic Adjustment. In: Proceedings of the Autonomy Control Workshop at Autonomous Agents. (Agents '99), pp. 8-15, May 1, 1999 Seattle.

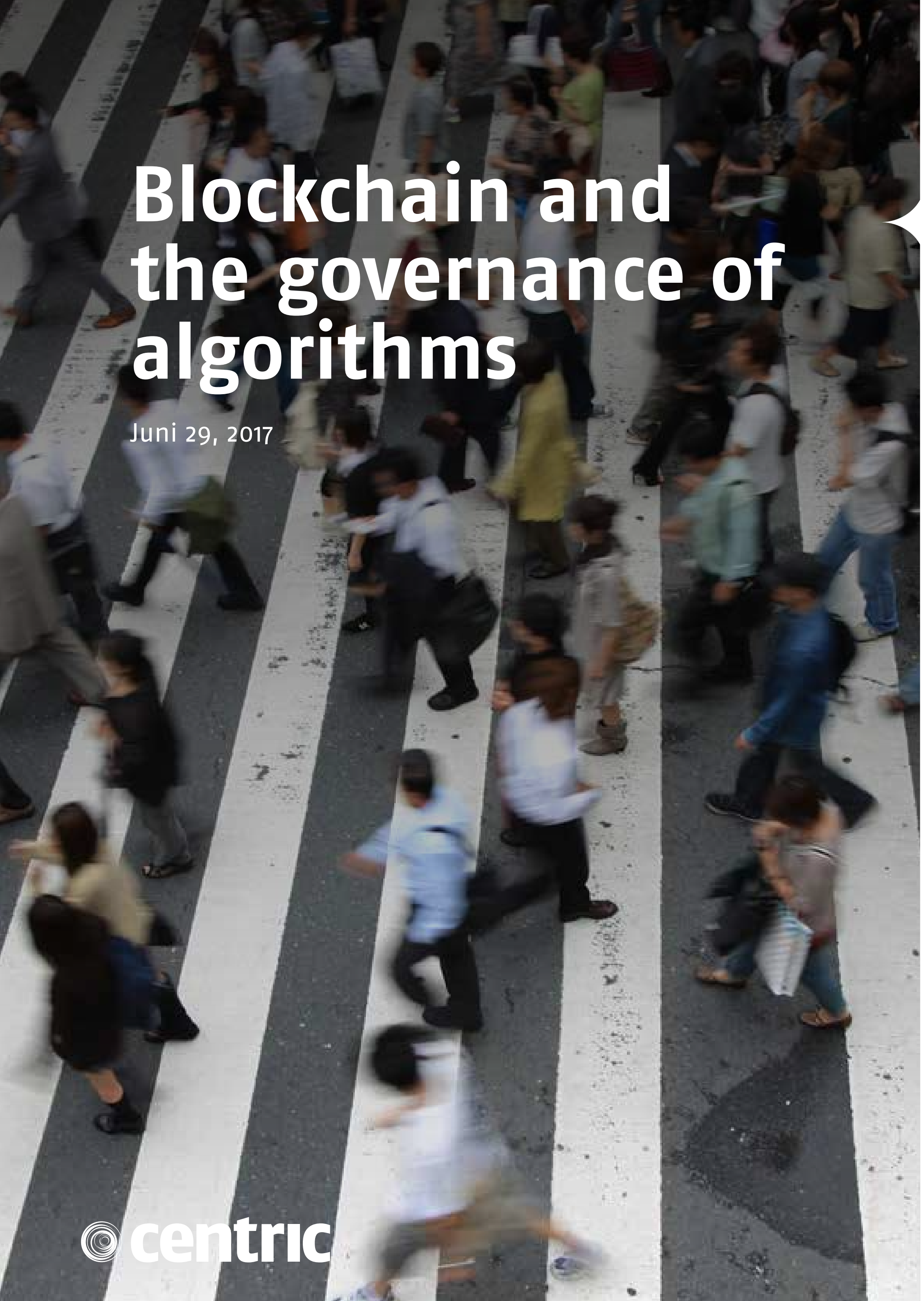
[6] Report of the Defense Science Board Summer Study on Autonomy June 2016 Office of the under Secretary of Defense for Acquisition, Technology and Logistics, Washington D.C.

[7] Wallach, W. (2015) A Dangerous Master. How to Keep Technology from Slipping Beyond Our Control. Basic Books. ISBN 9780465058624

[8] Allen, C. and Wallach, W. (2014) Moral Machines: Contradiction in Terms, or Abdication of Human Responsibility? In: Robot Ethics. The Ethical and Social Implications of Robotics. Edited by Patrick Lin, Keith Abney, and George A. Bekey. Pp. 55-68 MIT Press Paperback 9780262526005

[9] Gunkel, D. J. (2012) The Machine Question. Critical Perspectives on AI, Robots, and Ethics. The MIT Press Cambridge, Massachusetts. ISBN 9780262017435

[10] Ahrendt, H. (Edition 2006) Eichmann in Jerusalem. A Report on the Banality of Evil. Penguin Classics. ISBN 9780143039884



Blockchain and the governance of algorithms

Juni 29, 2017

Governance is the process of governing a collective unit such as a city, an organisation or a group of people and their activities. The governance of such a collective unit or system is made up of a set of rules and regulations that is developed to optimise the functioning of the collective unit or system. The development and application of a blockchain is based on collaboration between people and the rules, algorithms (such as paxos, ripple, etc.) and software (bitcoin, ethereum) they have developed and which enable the independent implementation of these rules and regulations by computers. The whole of man-made rules, algorithms, software and computers determines the functioning of the blockchain

Read more >

Hissam et al.[1] refer to such a combination as a socio-adaptive system: "*systems in which humans and computational elements interact as peers*." According to Hissam et al., the properties of the whole of a system such as the blockchain develop: "*from the properties of both types of elements and the nature of their collective reaction in their environment*." Communication and interaction between people, algorithms and computers creates a new whole, such as a blockchain, which shapes new applications such as cryptocurrencies, smart contracts and smart systems with joint decision-making capabilities. At the same time, however, this throws up all kinds of new issues, such as how to organise the governance of the new whole of a blockchain.

Algorithms

In 1927, the philosopher Heidegger [2] described the way in which we, as human beings, approach phenomena in our world. In Heidegger's theory, a phenomenon is something that presents itself to us without this "*something*" necessarily being an object in terms of structure and inner coherence. That which we humans approach as a whole should, in his view, rather be seen as '*equipment*', i.e. a kind of tool that cannot actually be observed but does give meaning to what we use the equipment for. Interconnected equipment is, according to Heidegger, always connected with other equipment. Together, the equipment shapes what we see as an object, as well as the functionality of this object, or we shape what we perceive as reality.

In Heidegger's view, things are never stand-alone or revealed to us for the first time. They are, in fact, produced by structures and interrelations of that which we perceive or experience in reality. Heidegger's equipment concept is similar to that of algorithms and software that people use nowadays to construct blockchains and shape and use objects such as cryptocurrencies or smart contracts. A blockchain is not something that is entirely new, but is rather a newly constructed structure, an interconnection of modern tools in the form of algorithms, software and computers.

Finn [3] (2017) defines an algorithm as a kind of recipe: "*an instruction set, a sequence of tasks to achieve a particular calculation or result, like the steps needed to calculated a square root to tabulate the Fibonacci sequence*." A constructed algorithm delivers, in his view, a reliable result when realised within a predefined time span by the computers running the algorithms, thereby realising what they were intended to realise.

The results realised in unison are, according to Finn, now becoming so important for us as human beings that we can no longer close our eyes to the assumptions, suppositions and choices that have been incorporated into the structure and the functioning of these algorithms and software. He states the following on this: "*The apparent transparency and simplicity of computational systems are leading many to see them as vehicles for unbiased decision-making*." According to Finn, changes brought by algorithms are also leading to a seemingly automatic reconstruction of our existing legal and ethical frameworks. At the same time, these algorithms are also shaping a new reality, as Finn concluded based on mathematical rules and implicit assumptions incorporated into that, which are not instantly evident to the general public.

Governance

The bitcoin blockchain is shaped by an ecosystem of interrelated algorithms. These algorithms organise consensus on the interrelation of (a block of) information transactions performed within the network. The internal coherence of a blockchain is thus provided by '*Heideggerian equipment*' in the form of interrelated algorithms that create an outcome in the form of, for example, cryptocurrencies or smart contracts. Our perception of how these new currencies or smart contracts are created also leads to a new reality of networked systems that are jointly capable of autonomously performing reliable information transactions for us on a global scale.

For De Filippi and Loveluck [4] (2016), governance of the interrelated set of algorithms is twofold, i.e.: '*governance by the infrastructure*', organised through the bitcoin protocol and 'governance of the infrastructure' which is all about the development and management of algorithms that realise information transactions in the network. The whole of the bitcoin blockchain is, according to De Filippi and Loveluck, much like: "*a highly technocratic power infrastructure, insofar as it is built on the automated technical rules designed by a minority of experts with only limited accountability for their decisions.*" Within this network, De Filippi and Loveluck distinguish two important groups: one of passive users who are only interested in performing information transactions, and one of active users in the form of what are known as miners who make processing power available to the network for transaction validation purposes. In the theory of De Filippi and Loveluck, the second group is: "*the community of developers, who are contributing code to the bitcoin project with a view to maintain or improve its functionalities.*" In this latter group, only a limited number of persons have the capability to edit the source code of the system.

De Filippi and Loveluck provide a detailed description of how a proposal to make changes to the functioning of the source code led to a crisis in the existing governance structure of the bitcoin blockchain. As a consequence of this crisis, according to De Filippi and Loveluck, "*a small number of individuals became responsible for the long-term sustainability of a large collective open source project, and the project rapidly fell prone to interpersonal conflict once consensus could no longer be reached among them.*" The analysis of this crisis made it clear to De Filippi and Loveluck that the '*trustless technology*' in the form of a public blockchain seems to stay outside of the existing frameworks of, for example, the government and other organisations, but that the public blockchain still: "*remains subject to the (invisible) politics of a handful of individuals – the programmers who are in charge of developing the technology and, to a large extent, deciding upon its functionalities.*"

Conclusions

The conclusions formulated by De Filippi and Loveluck tie in with claims by Atzori [5] who said that: "*In a world increasingly reliant* *on technology and ruled by networks, whoever owns and controls these platforms will always have a significant power over civil society on a global scale*." We as human beings still perceive technology and networks as interconnected physical objects. We are barely mindful of how the algorithms needed for the functioning of these platforms are developed and managed. We see the results of the networks as traditional objects that we, as human beings, accept, ignore or reject, but are not interested in the changes these digital objects trigger in our living and work environment.

Our world is changing rapidly due to the increasing intensity, intelligence and autonomy of these interconnected algorithms. The effects of all these developments can, as Boucher[6] claims, "*be found in more subtle impacts upon broad social values and structures. These impacts are associated with the values that are embedded within technology. All technologies have values and politics, usually representing the interest of their creators*." The influence algorithms have on existing social values and structures, and the way in which governance of these algorithms in general, and of the blockchain in particular, has been organised, should therefore be higher on the national and international political agenda. Further research into new governance models for the management and maintenance of such algorithms that intervene in our existing world is of vital importance for that.

Footnotes

[1] Hissam, S., Klein, M. and Moreno, G. A. (2013) Socio-Adaptive Systems Challenge. Problem Workshop Report. Carnegie Mellon Software Engineering Institute, June 2013. CMU/SEI-2013-SR-010

[2] Heidegger, M. (1927) Zijn en Tijd. Dutch edition 1999 [English title: Being and Time], translated by Wildschut, M. Sun, Nijmegen. ISBN 906168675x

[3] Finn, E. (2017) What Algorithms Want. Imagination in the Age of Computing. The MIT Press. ISBN 9780262035927

[4] De Filippi, P. and Loveluck, B. (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review. Journal on Internet Regulation. Volume 5| Issue 3 |September 2016. Pp. 1-26

[5] Atzori, M. (2015) Blockchain Technology and Decentralized Governance: Is the State Still Necessary? (1 December 2015). Available at SSRN: here or here

[6] Boucher, P. (2017) How Blockchain Technology Could Change Our Lives. In Depth Analysis. EPRS | European Parliamentary Research Service STOA – Science and technology options assessment, February 2017. PE 581.948

Blockchain and Servitization of Manufacturing

August 31, 2017

Neely [1] defines servitization as the process by which firms provide services along with the products they manufacture and supply. In Neely's view, servitization is a process of innovation that enables companies to create real added value by selling their products – such as machines, aircraft engines, cars, or television sets – with high-value accompanying services.

Read more >

Servitization is made possible when products such as machines or engines are connected, allowing companies to collect data and information about how these products operate and how they are used. This information can then be used to create new services, such as predictive maintenance. , Neely (2008) identified Rolls-Royce as an example of a company using servitization: *"Rolls-Royce Aerospace no longer simply sells aero engines. Now it offers a total care package, where customers buy the capability the engines deliver – "power by the hour".Rolls-Royce retains responsibility for risk and maintenance, generating revenues by making the engine available for use. [2]"* The servitization innovation process is made possible by developments such as the Industrial Internet of Things (USA-GE), Industries 4.0 (Germany-Siemens), and the Fourth Industrial Revolution (World Economic Forum), which connect growing numbers of machines and devices in networks and allow them to communicate and interact. An interesting question is whether the servitization of products could be supported by another new phenomenon [3]: the blockchain.

Servitization of Manufacturing

The process of servitization naturally leads to peer-to-peer information transactions, which are performed based on a relationship of trust between the manufacturer or supplier and their customer. As they become increasingly connected, machines gain ever greater intercommunication capacity, producing new and thus far unknown data and information streams, which, in turn, can engender new products or services. Evans and Annunziata of GE [4] describe this process thus: *"Over time, these data flows provide a history of operations and performance that enables operators to better understand the condition of the critical components of the plant. Operators can understand how many hours a particular component has been operating and under what conditions. Analytic tools can then compare this information to the operating histories of similar components in other plants to provide reliable estimates of the likelihood and timing of component failure. In this manner, operating data and predictive analytics can be combined to avoid unplanned outages and minimize maintenance costs"*.

Based on this data and information, customers pay a per-unit fee for uninterrupted use of the product and associated services. This unit can be a unit of time or volume. The supplier provides the equipment and makes sure that it works as promised, based on data and information that has been gathered and analysed. Customers only pay for the actual operation or use of the machine. Opresnik et al. [5] put it as follows: *"Informatization and the exploitation of data and information through the information ecosystem have together the potential to create an additional revenue stream for the information ecosystem's members, including the manufacturer"*.

However, the complexity increases as more data and information has to be shared between more suppliers and multiple customers, for example when it comes to billing for products and services. As the number of machines increases, as in-house machines and third-party machines become increasingly interlinked, and as data is shared with other parties, such as maintenance providers, questions are being raised about user rights, transparency and cost calculation based on this data and information. Aspects such as security, reliability, and ownership of the gathered and analysed data and information will also play an ever more important role in the process of servitization.

Servitization and Blockchain

Interconnections and interactions between an increasingly diverse range of machines and organisations on the Internet of Things will not only fire up the debate about the implementation of the process of servitization, but will also make it more complex. This is certainly due to the growing role of consumer electronics in this development. Min, Wang, and Luo [6] pointed out that for Chinese manufacturers developing a servitization strategy "*it should be the key point that providing high value-added complex services for consumers*, *rather than rushing to expand the service business scope by a large number of superficial services*".

Throwing consumer electronics into the mix only increases the complexity of the process of servitization. The development of interconnected systems of distributed operating combinations of humans and machines is bound to raise new questions about the reliability of and confidence in information transactions between machines and humans in these networks, which will ultimately lead to monetary transactions. Not only will '*fault tolerance*' need to be high, but the transparency of performed information transactions also has to be unquestionable. The large number of interconnected devices and the relationships between them means that context-based 'consensus and decision-making procedures' are essential when it comes to information transactions between a broad range of machines and devices.

The level of transparency needed to inspire confidence calls for a form of '*distributed ledging*' where devices and their users can continue to control their own data and information and remain aware of who it is shared with. Decisions made by a device concerning the performance of information transactions are known as '*blocks*', due to the distributed manner in which devices store data and information. Together, these form a '*blockchain*'. Depending on the context and the kind of information transactions, separate protocols can be designed to set requirements for consensus and decision-making procedures and, for example, for security, by means of the '*encryption*' of performed information transactions.

In the words of Martinez [7]: "*Services are the key to creating a more diversified business and to building stronger customer relationships. In the future the interactions of systems, processes* *and technology will provide a route to 'total solutions' for customers*". As the (Industrial) Internet of Things and the process of servitization continue to develop, it will increasingly become standard practice for devices and machines to autonomously exchange and share data and information. By thinking in terms of the possibilities offered by a blockchain, we can keep the information transactions performed between these devices reliable, secure, and transparent and thus retain trust in a system of systems that is going to be of great benefit to human beings.

Footnotes

[1] Neely A. (2011) The Servitization of Manufacturing. An Analysis of Global Trends. University of Cambridge.

[2] Neely A. (2008) Exploring the Financial Consequences of the Servitization of Manufacturing. Operations Management Research. Volume 1, Number 2, December 2008

[3] Lier v. B (2017) Philosophy of Blockchain

[4] Evans P. C. and Annunziata M. (2012) Industrial Internet: Pushing the Boundaries of Minds and Machines. GE Imagination at Work, November 26, 2012

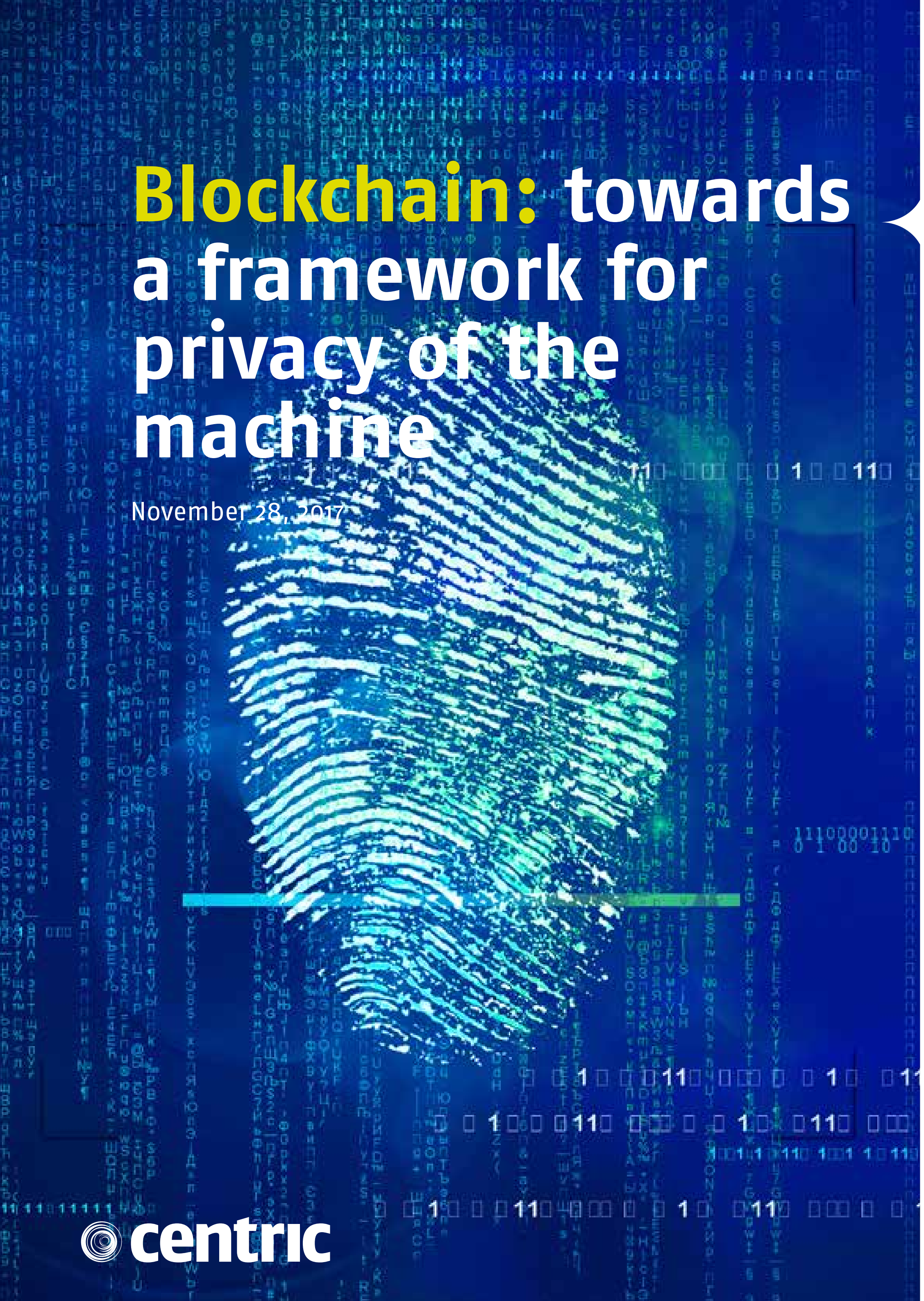
[5] Opresnik D., Hirsch M., Zanetti Chr., Taisch M. (2013) Information – The Hidden the Value of Servitization. 20th Advances in Production Management Systems (APMS), Sep 2013. Springer IFIP Advances in Information and Communication Technology, AICT-415 (part II). Pp. 49-56

[6] Min L., Wang J., Luo Q., (2015) Does the Servitization Strategy Improve the Performance of Manufacturing Enterprises in China? America Journal of Industrial and Business Management. Volume 5, pp. 281-287, 2015.

[7] Cambridge Service Alliance. Annual Report 2016. University of Cambridge. Pp. 19

Blockchain: towards a framework for privacy of the machine

November 28, 2017



centric

According to Hanna Arendt [1], the adjective public “means, first, that everything that appears in public can be seen and heard by everybody and has the widest possible publicity” (1948:51). In Arendt’s view, public refers primarily to the world itself, insofar as it constitutes the realm in which we all live. She distinguished the public from the private, which she defined as ‘the absence of other people.’ Arendt claimed that without these other people: “a human being living as a private person has no shape of its own, and it is therefore as if he did not exist” (1948:60). The concepts of public and private play a major role in the world of blockchain. Cryptocurrencies such as Bitcoin and Ethereum are defined as public blockchains. New technologies such as IBM’s Hyperledger and Microsoft’s Coco Framework are enabling companies to develop private blockchains together with other companies.

Read more >

A recent study of blockchain technology published by the University of Cambridge [2] added to Arendt's definition of public and private, making a distinction between open (public) and closed (private) blockchains. Open blockchains are referred to as '*permissionless*,' meaning that they can, in theory, be accessed by anyone. Examples include the Bitcoin blockchain and the Ethereum blockchain (smart contracts), which rely on consensus algorithms that use principles such as '*proof of work*' or '*proof of stake*' to validate information transactions that have been performed. Such transactions are validated by what are known as miners, most of which are based in China. One specific consequence of using those consensus methods is that it leads to exponentially increasing power consumption by the Bitcoin blockchain, which already consumes power at the same rate as countries like Ecuador. At the same time, public blockchains have a low transaction rate, as shown by Ethereum's 20 transactions per second. These public blockchains let any participant: "*participate in the consensus process (in practice however often limited by resource requirements such as owning suitable hardware or cryptocurrency)*," the University of Cambridge study concluded (2017:13). With a closed or permissioned' blockchain: "*only selected parties can make changes to the distributed ledger*" (2017:13). According to Olfati [3] (2007), realising consensus between networked agents or dynamic systems means: "*to reach an agreement regarding a certain quantity of interest that depends on the state of all agents. A consensus algorithm (or protocol) is an interaction rule that specifies the information exchange between an agent and all of its neighbors in the network*".

Consensus

Cachin and Vukolic [4] defined blockchains, i.e. distributed ledgers, as systems that are able to provide a reliable service to groups made up of random agents, nodes or parties that do not entirely trust each other. In general, this world considers a technology-based blockchain as a trustworthy solution for joint maintenance and management of a status shared between the parties, for mediation in mutual information transactions, and to ensure a secure IT environment. According to Cachin and Vukolic, a private or 'permissioned' blockchain: "*is operated by known entities, such as in consortium blockchains, where a member of a consortium or stakeholders in a given business context operate a permissioned blockchain network*." Permissioned or private blockchains have all the technological resources at their disposal that are needed to enable identification of agents, nodes, or parties taking part in the consensus procedure when managing and editing the shared status between the nodes. And permissioned or private blockchains have the capability to determine which nodes are able and allowed to take part in which transactions. Cachin and Vukolic claimed that nodes communicate through networks, while simultaneously construing the blockchain in consensus through mutual communication. The blockchain consists of blocks containing the result of joint decisions by the nodes, whereby these nodes did not rely on any kind of central authority in making those decisions. To make this jointly shaped service possible, nodes use: "*a fault tolerant consensus protocol to ensure that they all agree on the order in which entries are appended to the blockchain*," Cachin and Vukolic explained. In their view, today's most influential and leading algorithms that are enabling communication and consensus between distributed nodes are the ones from a family of algorithms known as Paxos.

Hyperledger

Back in 2015, IBM and Samsung presented a proof of concept for a blockchain based on the development of the Internet of Things (IoT). They called this concept: Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT). IBM and Samsung claimed that their proof of concept shows the future potential of a blockchain within the development of the IoT. It triggered the following response from Galleon [5]: *"Ultimately, the technology puts digital security and transparency on a whole new level, one that we'll need as we push further into a future of extreme connectivity."* With this trial, IBM ended up laying the foundation for the development of the Hyperledger project. Valenta and Sandner [6] wrote in an article that: *"Hyperledger Fabric intends to provide a modular and extendable architecture that can be employed in various industries, from banking and healthcare over to supply chains"*. Hyperledger includes a broader application of the concept of consensus, extending it to: *"the whole transaction flow, starting from proposing a transaction to the network to committing it to the ledger."* The Hyperledger white paper [7] defines Hyperledger as a protocol for information transactions between business-to-business and business-to-customer applications. This protocol paves the way for a new approach to the traditional blockchain model. From its core, Hyperledger operates like a private blockchain, which enables it to regulate the admission of participants to the blockchain, or in the words of the aforementioned white paper: "validators during network setup can determine the level of permission that is required to transact." *This makes Hyperledger a clear example of a private or permissioned shared ledger that: "responds to the multitude of industrial case requirements by providing a secure, robust model for identity, audibility and privacy."* To achieve consensus between multiple participants on the execution of information transactions, Hyperledger uses the Practical Byzantine Fault Tolerance protocol, which is one of the consensus protocols from the Paxos family.

The Coco Framework [8]

In August 2017, Microsoft launched the Coco Framework. In the white paper accompanying the launch, Microsoft observed that: *"Blockchain technology is poised to become the next transformational computing paradigm"*. The Coco Framework is, as Microsoft pointed out, a consortium-first approach, which means that *"member identities and nodes are known and controlled. Actors are often equally mature, with robust and highly controlled IT environments, security policies, and other enterprise characteristics"*. These lines suggest that Microsoft is trying to harness their experiences with Ethereum on the one hand and with Corda on the other in a new blockchain approach that puts enterprises in the driving seat. The Coco Framework is an open-source system that enables enterprises to team up with partners in a consortium to develop powerful but confidential blockchain networks. Coco uses Trusted Execution Environments (TEEs), such as Intel's SGX or Windows Virtual Secure Mode, to make the network as powerful and confidential as it is. TEEs enable construction of highly reliable networks made up of identified physical nodes that jointly enable the operation of a distributed ledger. The Coco white paper states that, within the network that is created, consensus is needed for all: *"updates to the distributed store, including application transactions, smart contract state, and administrative transactions"*. According to this white paper, consensus is a fundamental aspect of any distributed network, but when compared to public blockchain networks, the Coco network is unique in that each virtual node in this network can blindly trust all other virtual nodes in the network. The Coco white paper goes on to explain that although the framework will initially use Paxos consensus algorithms, it has been designed in such a way that any other consensus algorithm can also be integrated into it at a later stage.

Conclusion

The nature of the development of blockchain technology seems to be slowly but surely shifting from public and permissionless blockchains to private and permissioned blockchains that enable systems to engage in intercommunications and make decisions. Van Lier [9] (2017) worded it as follows: *"The new technological phenomenon that is blockchain, is based on interconnections and intercommunication, interaction and decision-making between a diverse range of systems."* New systems based on a combination of hardware and software are often referred to as cyber-physical systems. Acatech [10] defined cyber-physical systems as software-based systems that are increasingly used in everyday items such as cars, smart TVs, drones, or heart monitoring equipment. By interconnecting these cyber-physical systems in networks: *"in a variety of different ways and incorporating data and services from global networks, they have or are being transformed into integrated, comprehensive solutions that are increasingly pervading and connecting every area of our lives"*. The functioning of these devices hinges on software, as the software enables interconnections between the physical domain – in which the cyber-physical system exists – and the virtual domain of algorithms and software, and the data and information in that domain. The combination of hardware and software and their interconnections enables self-organisation by these systems through the use of standard procedures. Self-organisation by cyber-physical systems has the potential, in Acatech's view, to enable entire factories and their production resources to adapt autonomously and optimise the productionand logistics process based on individual customers' changing requirements to create more personalised products. In Acatech's words: *"Self-organization through goal-oriented negotiation of work-pieces, equipment and material flow systems results in these processes becoming significantly more flexible – whilst today they are based on a central planning approach, in the future will they be characterized by a decentralized optimization approach."* To make Acatech's vision a reality, Swan and De

Filippi [11] (2017) stated that new knowledge needs to be developed within a new context of a combined physical and virtual domain, where, according to Swan and De Filippi: *"tightness of linkage of control relationships is unconfirmed, both initially and persistently. One of the challenges is the quality of correspondence between the domains given their different natures: the virtual world is quantitative (digital ones and zeros), and the physical world is qualitative (messy variable irrational). These are early days in the experimental process of the computational equivalents of human based qualities such as trust and truth"* (2017:615). Hopefully, their call for the development of new and fundamental knowledge will be heard, and this knowledge will help us as human beings in developing, implementing, and using the new interconnected combinations of hardware, algorithms, and software. Only when we develop this kind of new knowledge will we be able to better analyse and understand the rapidly developing new and interconnected combinations of the physical realm and the virtual realm.

Footnotes

[1] Arendt, H. (1958/2015) The Human Condition. The University of Chicago (1958) Dutch edition. Translated by Houwaard, C. Amsterdam | Boom ISBN 9789085066781

[2] Hileman, G. and Rauchs, M. (2017) Global Blockchain Benchmarking Study. Cambridge Centre for Alternative Finance. University of Cambridge Judge Business School

[3] Olfati-Saber, R., Fax, A. J. and Murray, R. M. (2007) Consensus and Cooperation in Networked Multi-Agent Systems. Proceedings of the IEEE, vol. 95, no. 1, January 2007. Pp. 215-233

[4] Cachin, Chr. and Vukolic, M. (2017) Blockchain Consensus Protocols in the Wild. 31st International Symposium on Distributed Computing (DISC 2017) Editor Richa, A.W. Article no 1, pp. 1-16. Leibniz International Proceedings in Informatics.

[5] Galeon, D. (2017) https://futurism.com/ibm-just-launched-blockchain-beyond-currency/

[6] Valenta, M. and Sandner, P. (2017) Comparison of Ethereum, Hyperledger Fabric and Corda. FSBC Working Paper. Frankfurt School Blockchain Center, June 2017

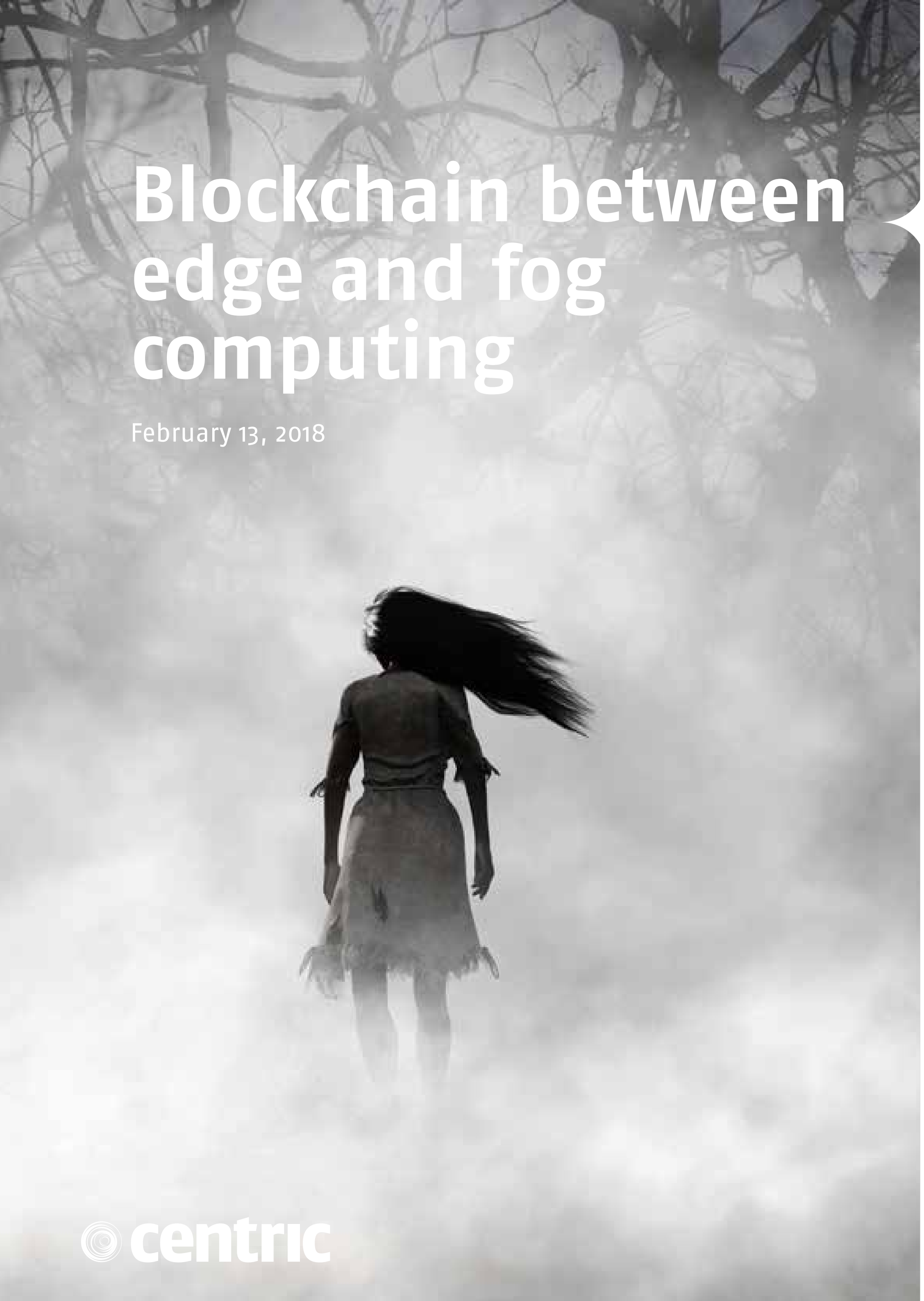
[7] Hyperledger whitepaper. https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/edit#

[8] Microsoft. (2017) The Coco Framework. Technical Overview. Published 10 August 2017.

[9] Lier, B. van (2017) Can cyber-physical systems reliably collaborate within a blockchain? Metaphilosophy, vol. 48, no 5, October 2017, pp. 698-711

[10] Geisberger, E. and Broys, M. eds. (2015) Living in a Networked World. Integrated research agenda. Cyber-Physical Systems. Acatech Study, March 2015

[11] Swan, M. and De Filippi, P. (2017) Toward a Philosophy of Blockchain: A Symposium. Metaphilosophy, vol 48, no 5, October 2017, pp. 603-619.



Blockchain between edge and fog computing

February 13, 2018

The Merriam Webster dictionary defines autonomy as *"the quality or state of being self-governing or the right of self-government"*. The autonomy of physical devices is growing as they converge with software and are connected in networks through new combinations of hardware and software. Interconnection in networks enables such cyber-physical systems to communicate and interact with each other. Such communication and interaction, in turn, makes it possible for these systems to develop self-configuring, self-optimising, self-protecting and self-healing capabilities. When combined, these capabilities give cyber-physical systems great autonomy in the performance of their tasks.

Read more >

The core of blockchain technology consists in cyber-physical systems' ability to autonomously and jointly make decisions about the execution of transactions based on voting and consensus algorithms. An algorithm is, as Steiner [1] put it, basically a set of instructions *"to be carried out perfunctorily to achieve an ideal result"*. As the (industrial) internet of things continues to develop, more and more cyber-physical systems are interconnected in networks at great pace. From a centralist perspective, these cyber-physical systems are placed on the edge of the network, which has led to the term edge computing.

To bridge the gap between the central cloud and the decentralised cyber-physical systems on the edge, the concept of fog computing has emerged. What is interesting is whether blockchain technology and the algorithms used for it are able to operate between the existing centralist perspective of cloud computing and the more decentralised perspective of the (industrial) internet of things. At the same time, the question arises whether the blockchain would then be contributing to increasing the autonomy in the execution of tasks by groups of cyber-physical systems on the edge of the network.

Internet of things

In 2014, Samsung Electronics and IBM developed a proof of concept focused on increasing the autonomy of devices or machines that operate in a decentralised manner within the (industrial) internet of things [2]. For their pilot, they used a Samsung washing machine (W9000). According to Samsung and IBM, these kinds of consumer appliances will increasingly be hooked up to networks such as the internet of things and will perform information transactions in electronic marketplaces and other environments in an increasingly autonomous and self-managed fashion.

The information transactions performed by these devices can, for example, consist in them autonomously ordering detergent or spare parts, negotiating with the electricity company about power supply, or showing adverts on the washing machine's display. To enable devices to do these kinds of things, the project focused on peer-to-peer messaging, distributed file sharing and autonomous device coordination. The software and protocols used for the latter functionality were borrowed from Ethereum. These protocols were needed for the project to, among other things, be able to register and authenticate the various devices in the network, as well as for the agreements and checklists between the devices and the consensus-based rules of engagement. The ADEPT project has led to a pilot of a blockchain of devices, where devices work together autonomously and make decisions about tasks or orders, etcetera. The approach of linking these devices using blockchain technology also further increases these devices' level of autonomy. Software developed as part of the ADEPT project was later used as the basis for the development of Hyperledger fabric.

Edge and fog computing

Edge computing is a new computer paradigm where, according to Satyanarayanan [3] *"substantial computing and storage resources*

– variously referred to as cloudlets, micro datacenters, or fog nodes – are placed at the Internet's edge in close proximity to mobile devices or sensors". The growing number of devices that are interconnected in networks such as the internet of things or the industrial internet of things, such as the washing machines in the above example, produce ever greater volumes of data and information that have to be processed and analysed. All this data and information enables these devices to operate autonomously and to perform their activities on their own or jointly.

Due to the fact that the number of decentralised and autonomously operating devices is increasing rapidly, we need real-time sharing and storage of the data and information they use. According to Cisco [4], the current cloud computing models are, however, not designed to be able to handle "*the volume, variety, and velocity of data that the Internet of Things generates*". This development requires, in the view of Cisco, a new kind of infrastructure that is better positioned for the devices on the edge, and this new infrastructure is what they refer to as '*fog computing*.'

Cisco believes that fog computing can create an intermediate layer between the centralised cloud infrastructure and the devices on the edge of the internet. Dastjerdi and Buyya [5] defined fog computing as "*a distributed paradigm that provides cloud-like services to the network edge*". In their view, fog computing basically takes care of "*deals with IoT data locally by utilizing clients or edge devices near users to carry out a substantial amount of storage, communication control, configuration and management. The approach benefits from edge devices close proximity to sensors, while leveraging the on demand scalability of cloud resources*". Bonomi et al [6] described fog computing as a highly virtualised platform that can provide "*compute, storage and networking services between end devices and traditional Cloud Computing Data Centers, typically, but not exclusively located at the edge of the network*".

These new concepts are making it clear that thinking merely in terms of central concepts, such as cloud computing, will come up short in the long term, as interconnected devices on the edge of the network will be producing huge volumes of data and information that need to be processed, analysed and stored. Between the entirely decentralised and autonomously operating devices and the centralised operating cloud, new facilities will have to arise, such as fog computing, that will have to be able, according to Dastjerdi and Buyya, "*to support the decentralized and intelligent processing of unprecedented data volumes generated by IoT sensors deployed for smooth integration of physical and cyber elements*".

Conclusion

Bieler [7] (2016) argued that both the internet of things and blockchain technology are based on "*decentralized, distributed approaches*". According to him, the decentralised and autonomously operating systems in the (industrial) internet of things need direct mutual communication and interaction *"rather than via existing centralized models"*. Kranz [8] (2017) pointed out that, in the development of the (industrial) internet of things, a blockchain can help *"secure, audit-level tracking of IoT data transactions, eliminating the need for a central, trusted intermediary between communicating devices"*. Given the basic features of blockchain technology, i.e. fault-tolerant communication, a distributed ledger, voting and consensus combined with execution protocols, blockchain technology could be used to lay a secure and reliable foundation for the regulation of data and information transactions between autonomously operating devices on the edge and decentralised fog units of the central cloud infrastructure. Blockchain technology can thus make rules that enable decentralised, autonomous and jointly operating systems to decide and regulate for themselves on what conditions they can provide their data and information, as well as where, how and to whom.

Footnotes

[1] Steiner, C. (2013) Automate This. How Algorithms Took Over Our Markets, Our Jobs, and the World. Portfolio / Penguin, London, UK. ISBN 9781591846529

[2] IBM (2015) Empowering the Edge. Practical Insights on a Decentralized Internet of Things. IBM Institute for Business Value

[3] Satyanarayanan, M. (2017) The Emergence of Edge Computing. Computer, Volume, 50, Issue, 1, Jan. 2017. Pp. 30-39

[4] Cisco Whitepaper (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are

[5] Dastjerdi, V. and Buyya, R. (2016) Fog Computing: Helping the IoT Realize Its Potential. Computer, Volume 49, Issue 8, Aug. 2016. Pp. 112-116

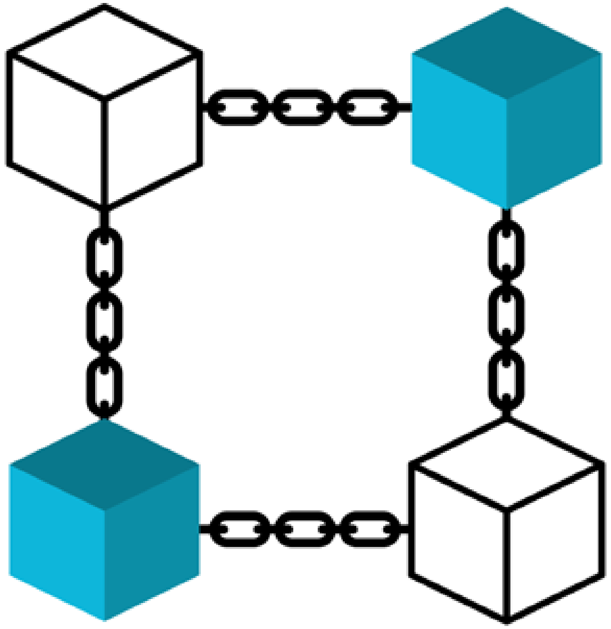
[6] Bonomi, F., Milito, R., Zhu, J. and Addepalli, S. (2012) Fog Computing and Its Role in the Internet of Things. Cisco Systems Inc. Report. August 2012

[7] Bieler, D. (2016) Blockchain's Potential For IoT Solutions. Forrester / Blog: Blockchain's Potential For IoT Solutions

[8] Kranz, M. (2017) In 2018, Get Ready for the Convergence of IoT, AI, Fog and Blockchain. RT Insights, 27 December 2017 https://www.rtinsights.com/in-2018-get-ready-for-the-convergence-of-iot-ai-fog-and-blockchain/

Blockchain of Things

May 16, 2018



In 1954 [1], English scientist W. Ross Ashby described the possibility of machine components establishing mutual connections or the interconnection of machines to create a new whole as a fundamental feature of these machines. Ashby concluded this after studying the functioning of an interconnected whole that he called a homeostat. Kline [2] defined the homeostat as follows: *"The homeostat consisted of four interconnected boxes filled with electronic gear and switches."* (2015:52).

Read more >

In 1962 [3] , Ashby claimed that when adding a feedback loop to these interconnected systems: "the system would be self-organizing if a change were automatically made to the feedback changing it from positive to negative; then the whole would have changed from a bad organization to a good one." (1962:115) In 1978, Lamport called such an interconnected whole a distributed system. In Lamport's [4] view, this kind of distributed but interconnected system can be considered: *"a collection of distinct processes that are spatially separated and communicate with each other by exchanging messages. A network of interconnected computers such as the ARPA net is a distributed system."* (1978:558) Interconnecting machines in networks enables communication and interaction between these machines, thus paving the way for joint decision making about the activities that are to be performed.

Research project

In March 2017, the International Telecommunication Union (ITU) received a research proposal with the following title: Framework of Blockchain of Things as Decentralized Service Platform [5]. The proposal was submitted by Egypt's National Telecommunications Regulatory Authority, in conjunction with China Unicom, the China Academy of Information and Communication Technology (which comes under the Chinese Ministry of Industry and Information Technology), ZTE corporation, AliBaba Group, and the China Electronics Technology Group Corporation.
This research project is focused on introducing a concept for the functioning of a blockchain of things. The scope of the study is to analyse: *"common characteristics and high level requirements, when it is as a decentralized service platform for IoT, and then brings a general framework of Blockchain of Things and relevant capabilities as mapping to IoT reference model."* In this context, the Internet of Things is defined as: *"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving interoperable information and communication technologies."* According to this proposal for a new work item at the ITU, the information transactions performed by things jointly are enabled by a: *"decentralized service platform, based on blockchain-related technologies, enabling the (physical and virtual) things to participate in and make transactions."* (2017:9) Decisions made by a whole of interconnected things are, according to the research proposal, based on: *"consensus: a broader term overarching the entire flow for a BoT transaction, in which the entities involved in a BoT to generate agreements and to confirm the correctness of the BoT transactions."*

Following on from that, the proposal points out that decisions made by a group of things through consensus are logged in each participant's own, and therefore distributed, ledger, which is defined as: *"a distributed append-only transaction log managed by the BoT peers. The BoT ledger stores whole or part of information for the BoT transactions."* The proposal states that the peer-to-peer transactions to be performed between one or multiple things and one or multiple other things can be performed by any independent entity that: *"supports BoT related functionalities, such* *as IoT device, IoT gateway and IoT system"*. Based on the features selected for participation in a blockchain of things, the proposal to the ITU states that every BoT can be classified as either public, consortium or private. In a public blockchain of things, any random thing can be connected in a network and take part in any decision-making process. Aside from that, the proposal also predicts the emergence of consortia of things where: *"parts of the participants are known and trusted with which they provide services for their consumers"*. And finally, the research proposal submitted to the ITU also predicts the emergence of private blockchains, stating that *"in the private blockchain of things all the participants are known and trusted"*.

Networks of things

In 2016, the US National Institute of Standards and Technology stated [6] that within the rapidly developing network of things: *"the tethering factoring is data."* Networked things operate based on interconnections and the ensuing possibilities for communication and interaction between these things. Vermesan et al [7] (2018) claimed that their concept of the Internet of Robotic Things goes further than the Internet of Things: *"beyond networked and collaborative/cloud robotics and integrates heterogeneous intelligent devices into a distributed architecture of platforms operating both in the cloud and the edge. IoRT addresses the many ways IoT today technologies and robotic "devices"* convergence to provide advanced robotic capabilities, enabling aggregated IoT functionality along with novel applications and by extension, new business, and investment opportunities not only in industrial domains but in almost every sector where robotic assistance and IoT technology and applications can be imagined" (92017:99).

According to Vermesan et al, blockchain technology is not only a means for reliable peer-to-peer communication between a varied range of devices in the development of the Internet of Robotic Things, it can also contribute to the prevention of potential threats, vulnerabilities, or consequences of external attacks.

Bahga and Madiseeti [8] (2016) consider the development of the Internet of Things first and foremost as promising for industrial and manufacturing systems. They assume a decentralised peer-to-peer platform that they call a blockchain platform for the Industrial Internet of Things. The blockchain they propose: *"enables peers in decentralized, trustless, peer-to-peer network to interact with each other without the need for a trusted intermediary."* (2016:534) Kott, Swami and West [9] (2016), on the other hand, focused on applications for the armed forces: *"The battlefield of the future will be densely populated by a variety of entities ("things") – some intelligent and some marginally so – performing a broad range of tasks: sensing, communicating, acting, and collaborating with each other and human warfighters."* (2016:70) In their opinion, the things operating in the theatre of war will be able to coordinate and execute their tasks through continuous collaboration based on mutual communication, coordination and negotiation in order to be able to achieve the objectives that have been set. The US government's defence budget, which was presented in December 2017 [10], is testimony to the growing interest in blockchain technology in a defence context, as it asked for: *"a description of potential offensive and defensive cyber applications of blockchain technology and other distributed database technologies."*

Conclusions

In 2008, Nakamoto [11] said the following: *"What is needed is an electronic payment system based on cryptographic proof instead of trust allowing any two willing parties to transact directly with each other without the need for a trusted third party."* (2008:1) Based on the blockchain or network of things created by Nakamoto, machines independently perform reliable information transactions without the involvement of a trusted human third party. The development towards increasing autonomy of machines that jointly perform tasks is something we are now seeing in various social sectors and cultures. This does not only pose questions about the functioning of individual things that autonomously perform tasks, but increasingly also about groups of things that perform tasks for us or will be performing tasks for us without any further human involvement. Following on from that, we as humans should perhaps ask ourselves whether we should focus more on philosophical and/or ethical issues instead of on economic, ideological or technological possibilities, and consider what this development means for our role as humans in a world that is increasingly dominated by interconnected and autonomously operating machines.

Footnotes

[1] Ashby, R.W. (1954) Design for a Brain. New York, John Wiley & Sons

[2] Kline, R.R. (2015) The Cybernetics Moment. Or Why We Call Our Age the Information Age. Baltimore, Johns Hopkins University Press. ISBN 9781421416717

[3] Ashby, R.W. (1962) Principles of the Self-Organizing System. In: Principles of Self-Organization: Transactions of the University of Illinois Symposium. Eds: Von Foerster, H. and Zopf, G.W. London, UK, Pergamon Press. pp. 255-278.

[4] Lamport L. (1978) Time, Clocks, and the Ordering of Events in a Distributed System. Communication of the ACM, Volume 21, Issue 7, pp. 558-565, July 1978.

[5] International Telecommunication Union (2017). Telecommunication standardization sector. Study Period 2017-2020. SG20-C.008. Dubai, 13-23 March 2017

[6] Voas, J. (2016) Networks of Things. NIST Special Publication 800-183

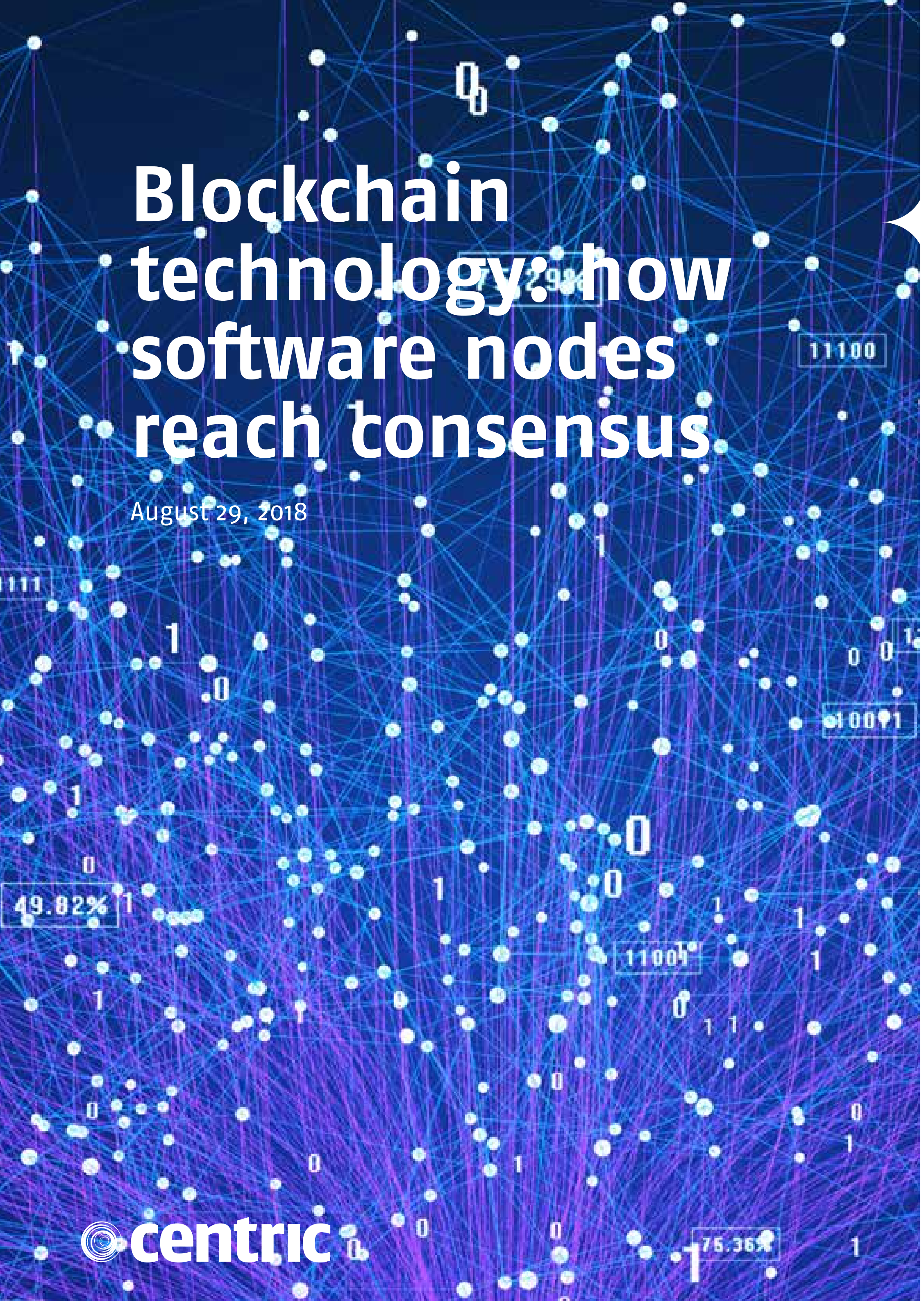
[7] Vermesan, O. et al (2017) Internet of Robotic Things in: Cognitive Hyperconnected Digital Transformation – Internet of Things Intelligence Evolution. River Publishers ISBN 9788793609105 Editors: Vermesan, O. and Bacquet, J. pp.97-155

[8] Bahga, A. and Madisetti, V.K. (2016) Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, Volume 9, pp. 533-546

[9] Kott, A., Swami, A. and West, B.J. (2016) The Internet of Battle Things. Computer Volume: 49, Issue: 12, Dec. 2016, pp. 70-75

[10] https://www.coindesk.com/trump-signs-defense-bill-authorizing-blockchain-study/ SEC. 1646. Briefing on cyber applications of blockchain technology

[11] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf



Blockchain technology: how software nodes reach consensus

August 29, 2018

According to Dasgupta (2014), the development of software started in 1949 at a conference in the UK, when John Wheeler presented rules for the way in which hardware in the form of a computer can be programmed to execute certain tasks. The rules that Wheeler formulated for such computer programming were later referred to as software, Dasgupta explains. In Dasgupta's view, the development of software led to a new symbiosis between *"the physical computer built of electronic and electromechanical components and the liminal, quasi-autonomous 'two-faced' artifact called computer program (or later software) that would serve as the interface between the human user and the physical computer"*.

Read more >

In the 1970s, US computer scientist Leslie Lamport studied how distributed entities can be interconnected through software and be able to strike up error-free collaboration through reliable mutual communication. This leads Lamport to the following argument: *"A distributed system consists of a collection of distinct processes which are spatially separated and which communicate with one another by exchanging messages. A network of interconnected computers, such as the ARPA system, is a distributed system"* (1978 [1], pp. 558). A reliable communication process between distributed entities, which is necessary to reach consensus, is defined by Lamport as a set of events with a predefined structure, or as he phrases it: *"We assume that sending a message is an event in a process"* (1978, pp.559).

Consensus

In 1998 [2], Lamport published an article in which he presents a consensus principle for the reaching of consensus between fault-tolerant and distributed systems. In this same article, Lamport notes that one of the most common problems that distributed systems face is that they can never be sure which systems are available or still adequate for participation in the required communication process to reach mutual consensus. To solve this problem, Lamport proposes a system where *"each entity maintained a ledger in which he recorded the numbered sequence of decrees that were passed"* (1998, pp. 2).

Each system is assigned a ledger in which the entity itself is supposed to record decisions using indelible ink, so as to ensure that these rules cannot be changed or erased later. The entities will always have this ledger with them, allowing them to continuously be able to consult previously made decisions. To take part in voting, the entities need to be physically present in the voting process and use messages that are sent and received between the entities.

In 2008, a person who goes by the name Nakamoto [3] published a paper online, which opened with the following observation: *"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments"* (2008). Nakamoto assumed that the buying and selling of goods and services was, at the time, increasingly performed based on transactions realised through communication between networked – such as the Internet – computers and their software. This led him to claim the following: *"What is needed is an electronic payment system based on cryptographic proof instead of trust."* The electronic payment system called Bitcoin is, Nakamoto explains, intended to enable "any two willing parties to transact directly with each other without the need for a trusted third party".

The rules that Wheeler formulated for such computer programming were later referred to as software, Dasgupta explains. In Dasgupta's view, the development of software led to a new symbiosis between *"the physical computer built of electronic and electromechanical components and the liminal,* *quasi-autonomous 'two-faced' artifact called computer program (or later software) that would serve as the interface between the human user and the physical computer"*.

This payment system furthermore assumes that the random participants in the network, or nodes, can freely leave and rejoin the network, *"accepting the proof-of-work chain as proof of what happened while they were gone"*. When it comes to validation of transactions, Nakamoto uses a consensus algorithm. Nakamoto: *"Any needed rules and incentives can be enforced with this consensus mechanism."* In 2018, a research proposal focused on a Blockchain of Things, which I have referenced in a previous article (2018 [4]), was submitted to the ITU. In this proposal, consensus is defined as *"a broader term overarching the entire flow for a blockchain of things transaction, in which the entities involved in a BoT generate agreements and to confirm the correctness of the BoT transaction"*.

Consensus software

In 2018, two Rotterdam University of Applied Sciences students joined IT firm Centric in Gouda to work on their (final-year) research on blockchain technology. Florian van Herk [5] (Computer Science) studied the realisation of the Paxos consensus using software nodes, while Dirk-Pieter Jens [6] (Business Informatics & Management) did research on the available data that can potentially be used by software nodes in the blockchain pilot that he ran.

Florian departed from a private or permissioned network that includes only identified nodes. He built the Paxos consensus algorithm using .NET code programming software to show how consensus procedures between software nodes work, and what this collaboration can mean. Initially, he split his research brief into two parts, beginning by building a network layer within which software nodes can function well, on which he states the following: *"This network layer would allow nodes to communicate with each other in a peer-to-peer manner, which means that every node communicates which each other"* (2018:18). To be able to build these software nodes, he first analysed Lamport's article and related articles in great depth. Based on the knowledge he thus acquired, he moved on as follows: *"An implementation of the Paxos algorithm was written in .NET core. Besides, multiple tests have been written to understand the qualities and shortcomings of the Paxos algorithm"* (2018:3).

Exceeding his expectations, the software nodes he developed turned out to collaborate effectively in the network. Through a continuous voting process, they are autonomously able to reach consensus on the information transactions they have to perform jointly in an asynchronous communication environment without any kind of third-party intervention. The software nodes record the data used in the procedure in a distributed manner, in a ledger that therefore becomes a distributed ledger. Based on his findings, Florian concludes as follows: *"The protocol works* *well on the built network layer, that is, no abnormalities have been observed, and since .NET has great async support, writing asynchronous functions for an asynchronous environment poses no problem. Various test cases have been written based on the Synod Protocol, to showcase its functionality, and showcase its fault tolerant properties*" (2018:51).

Florian departed from a private or permissioned network that includes only identified nodes. He built the Paxos consensus algorithm using .NET code programming software to show how consensus procedures between software nodes work, and what this collaboration can mean. Initially, he split his research brief into two parts, beginning by building a network layer within which software nodes can function well, on which he states the following: "*This network layer would allow nodes to communicate with each other in a peer-to-peer manner, which means that every node communicates which each other*" (2018:18). To be able to build these software nodes, he first analysed Lamport's article and related articles in great depth. Based on the knowledge he thus acquired, he moved on as follows: "*An implementation of the Paxos algorithm was written in .NET core. Besides, multiple tests have been written to understand the qualities and shortcomings of the Paxos algorithm*" (2018:3).

Exceeding his expectations, the software nodes he developed turned out to collaborate effectively in the network. Through a continuous voting process, they are autonomously able to reach consensus on the information transactions they have to perform jointly in an asynchronous communication environment without any kind of third-party intervention. The software nodes record the data used in the procedure in a distributed manner, in a ledger that therefore becomes a distributed ledger. Based on his findings, Florian concludes as follows: "*The protocol works well on the built network layer, that is, no abnormalities have been observed, and since .NET has great async support, writing asynchronous functions for an asynchronous environment poses no problem. Various test cases have been written based on the Synod Protocol, to showcase its functionality, and showcase its fault tolerant properties*" (2018:51).

The software nodes that he developed enabled Dirk-Pieter Jens to study whether it would be possible to create a reliable blockchain technology-based communication system between software nodes for the logistics industry, such as for warehouse management systems, transport management systems or on-board computers for lorries. What is striking is that, based on the analyses performed, there turns out to be more standard data for use in a consensus network available in the logistics industry than expected. The combination of the development of the software nodes and the analysis of the data available for use in the network turns out to be an effective multidisciplinary collaboration to boost research on the use of consensus possibilities between existing software nodes.

The software is currently, following the graduation of both students, being reused in PhD research focused on reliable exchange and sharing of data and information between distributed software entities based on the Building Information Modelling process. Further research is being conducted on future possibilities for the exchange and sharing of data and information between distributed software entities within government networks. And finally, there is also research ongoing on the application and use of blockchain technology within the realm of cybersecurity.

Conclusion

In essence, blockchain technology is software. Using this software, software nodes that operate in a distributed manner and are combined with hardware can be networked and achieve reliable intercommunication. This intercommunication can subsequently be used by software nodes as a resource that enables joint decision making without third-party, i.e. human, intervention. The thought that software nodes that function in a distributed manner no longer need humans to make decisions with a potential impact on humans is a development that not only calls for reflection on the software itself, but also on the ethical aspects attached to these kinds of decision-making processes.

Footnotes

[1] Ashby, R.W. (1954) Design for a Brain. New York, John Wiley & Sons

[2] Kline, R.R. (2015) The Cybernetics Moment. Or Why We Call Our Age the Information Age. Baltimore, Johns Hopkins University Press. ISBN 9781421416717

[3] Ashby, R.W. (1962) Principles of the Self-Organizing System. In: Principles of Self-Organization: Transactions of the University of Illinois Symposium. Eds: Von Foerster, H. and Zopf, G.W. London, UK, Pergamon Press. pp. 255-278.

[4] Lamport L. (1978) Time, Clocks, and the Ordering of Events in a Distributed System. Communication of the ACM, Volume 21, Issue 7, pp. 558-565, July 1978.

[5] International Telecommunication Union (2017). Telecommunication standardization sector. Study Period 2017-2020. SG20-C.008. Dubai, 13-23 March 2017

[6] Voas, J. (2016) Networks of Things. NIST Special Publication 800-183

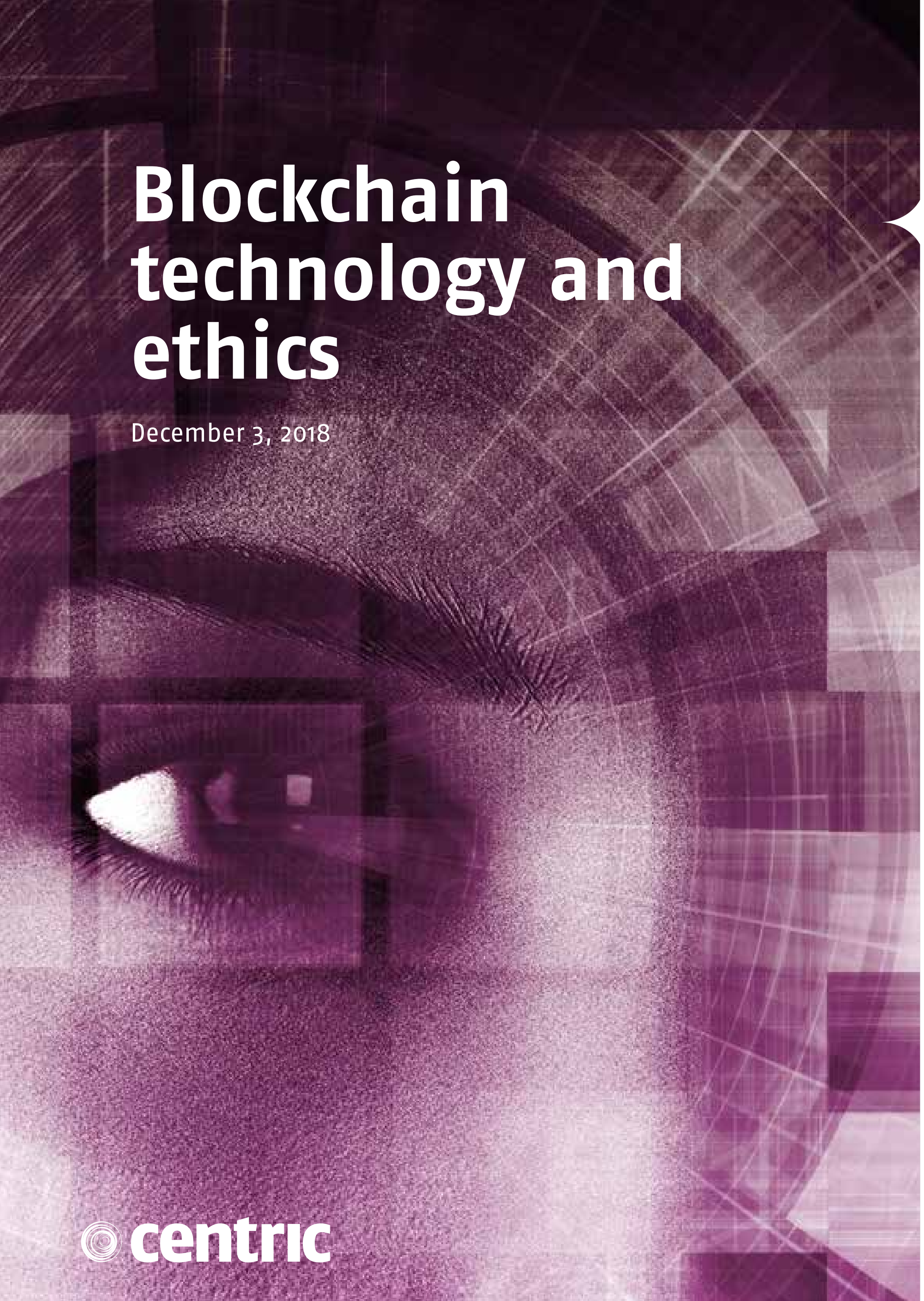
[7] Vermesan, O. et al (2017) Internet of Robotic Things in: Cognitive Hyperconnected Digital Transformation – Internet of Things Intelligence Evolution. River Publishers ISBN 9788793609105 Editors: Vermesan, O. and Bacquet, J. pp.97-155

[8] Bahga, A. and Madisetti, V.K. (2016) Blockchain Platform for Industrial Internet of Things. Journal of Software Engineering and Applications, Volume 9, pp. 533-546

[9] Kott, A., Swami, A. and West, B.J. (2016) The Internet of Battle Things. Computer Volume: 49, Issue: 12, Dec. 2016, pp. 70-75

[10] https://www.coindesk.com/trump-signs-defense-bill-authorizing-blockchain-study/ SEC. 1646. Briefing on cyber applications of blockchain technology

[11] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf



Blockchain technology and ethics

December 3, 2018

The US National Institute of Standards and Technology recently published a report entitled Blockchain Technology Overview [1]. The report starts with background on blockchain technology, saying that “the core ideas behind blockchain technology emerged in the late 1980s and early 1990s.

Read more >

In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The Part-Time Parliament to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue (2018:2). According to the authors of the NIST report, the model that Lamport developed was focused specifically on how networked computers reach consensus.
According to the authors, each instance where computers reach consensus through the use of algorithms and software that leads to the performance of a joint information transaction constitutes interaction between various parties. They write: *"In practice, software handles everything and the user does not need to be aware of these details"* (2018:18).

The possibilities offered by blockchain technology may have great impact on the further development of smart mobility as cars are becoming more and more autonomous, thanks to algorithms and software, in processing information transactions with different parties in a a. This also leads to the question whether, and if so how, ethical aspects play a role in the autonomous processing of these information transactions.

Smart mobility

At a meeting of the US-German standards panel in Berlin in April this year, Kuom [2] of the Federal Ministry for Economic Affairs and Energy dealt at length with the possible relationships between the development of the smart mobility concept and blockchain technology. In his presentation, he explained how German companies such as Daimler and BMW are exploring possibilities for the use and application of blockchain technology for things such as car sharing or access to various forms of transportation. Another focus point in these studies is parking, i.e. finding and paying for parking based on electronic booking and payment systems. He closed his introduction with the following words: *"Mobility will change away from ownership-based models to service models in Blockchain in Smart Mobility"* (2018).

In a blog post, Hacker Noon [3], too, writes about the potential of the combination of blockchain technology and smart mobility, highlighting the following case: *"The latest example of this blockchain transparency across interactions is launched by Renault. The French automaker is piloting a digitized car maintenance program, which uses blockchain as a shared ledger to log all car repair and maintenance history in one place."*
In a working paper, Martin Gösele and Philipp Sandner [4] of the Frankfurt School Blockchain Center write the following about things such as car wallets and payments by cars: *"With an integrated Wallet-App, cars are enabled to make payments on their own. With blockchain, payments concerning every aspect of the car's mobility can be executed fast, secure and automatically."*

A report published by the Roland Berger consultancy firm [5] also draws attention to the combination of smart mobility and blockchain technology: *"Blockchain Technology has clear* *applications in the area of secure communications, both vehicle-to-vehicle and vehicle-to-object. In the future, autonomous vehicles will communicate with other vehicles, traffic lights and other unauthenticated devices. One obvious use of blockchain is to secure this communication and ensure that it only occurs between relevant entities, so that it cannot be hacked into by unauthorized outsiders"* (2018:12).

More autonomy

The examples mentioned here all work on the basis that when combined with an increasing number of algorithms and software, cars as physical devices will acquire increasing autonomy in performing operations and activities with other objects and with humans. The increasing autonomy of these cyber-physical systems enables them to, based on blockchain technology, reliably and transparently communicate with various parties and reach consensus with these parties on information transactions to perform. This does, however, mean that there needs to be mutual trust on the decision-making procedures to execute.

Ethics

Connecting cars to networks in combination with smart algorithms and software creates increasing autonomy for those cars, turning them into cyber-physical systems that autonomously perform information transactions together with other systems. The joint decisions made based on algorithms and software prior to the information transactions ultimately impact on us as humans, which takes these decisions, according to Floridi [6], into the realm of the Ethics of Information. In his view, the world around us is increasingly developing into a *"fully interactive and responsive environment of wireless, pervasive, distributed, a2a (anything to anything) information processes, that works a4a (anywhere for anytime), in real time"* (2013:9). Floridi goes on to define a moral agent in this interactive world as

> ***"any interactive, autonomous and adaptable transition systems that can perform morally qualifiable actions"***

(2013: 135). Based on this description, cars as cyber-physical systems can, due to their increasing autonomy and intercommunication, interaction and transactions, also be considered moral agents. After all, developments are leading to these systems performing more and more operations or actions that can also be qualified as moral. These moral activities are the result of processes of complex communication, interaction and decision-making between systems that operate and collaborate in a distributed manner on a scale that is too great for any individual human to fathom.

The time may, therefore, have come for us to start thinking about a possible ethical framework, as I [7] have said previously, within which these autonomous systems can and are allowed to operate and make decisions independently. If we, for example, take our lead from Immanuel Kant's [8] thinking, we can take a synthesis or convergence of reason (algorithms) and intuition (software) as the basis for the development of rules for these collaborating systems.

This basic synthesis enables us to better understand the new whole that is made up of the underlying components and their interrelationships that jointly make up the smart mobility concept. This understanding of how the new whole works is necessary to be able to gain a clear view of the potential impact of mutual collaboration and joint decision-making by cyber-physical systems. The basic synthesis, in turn, can be followed up with a new synthesis that, according to Kant, ensues from an amalgam of duty, will and autonomy. The need to perform a certain action is, according to Kant, based on the duty or practical compulsion that an individual cyber-physical system has or experiences and that drives it to perform actions within an interconnection with other systems. The duty of an individual cyber-physical system must, in Kant's theory, be a practical and unconditional product of the necessary action.

According to Kant [9], the will of the system is its capacity to autonomously decide what the system will acknowledge or accept as good and its capability to implement the selected option. Morality, therefore, in Kant's view, consists in the duty to perform activities or operations in relation to the will of the system to actually perform the selected operation. The basic synthesis of reason and intuition, and the trichotomy of duty, will and autonomy would have to apply to all interconnected cyber-physical systems that autonomously intercommunicate, interact, make decisions between them and perform information-based actions or operations.

Conclusions

The full scope of the possibilities of application of consensus algorithms and software is currently certainly not yet clear, but will undoubtedly extend far beyond the domain of cryptocurrencies. What is clear, however, is that consensus algorithms will help increase the autonomy of cyber-physical systems in independently and jointly performing operations or activities. Cyber-physical systems' increasing level of autonomy triggers questions about the ethical aspects of the processes that lead to these decisions. Profound reflection on these (ethical) aspects can help us define the essence of this technology and its potential impact on us humans.

Footnotes

[1] Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018) Blockchain Technology Overview. NISTIR 8202. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

[2] Kuom, M. (2018) Blockchains in Smart Mobility. US-German Standards Panel 2018. DLR Project Management Agency. Society, Innovation, Technology. Berlin, Federal Ministry for Economic Affairs.

[3] Blockchain DuDe - Blockchain Writing a New Chapter for Automotive Industries. https://hackernoon.com/blockchain-writing-a-new-chapter-for-automotive-industry-48a8151eec99

[4] Gösele, M and Sandner, P. (2018) Analysis of Blockchain Technology in the Mobility Sector. FSBC Working paper, April 2018. Sandner, P.

[5] Roland Berger Focus. September 2018. The blockchain bandwagon. Is it time for automotive companies to start investing seriously in blockchain?

[6] Floridi (2013) Ethics of Information. Oxford, UK, Oxford University Press. ISBN 9780199641321

[7] Lier, B. van (2018) Thinking about ecologies of autonomous cyber-physical systems and their ethics. Inaugural Lecture, Rotterdam University of Applied Sciences. ISBN

[8] Kant, I. (1781) Critique of Pure Reason. Dutch edition 2017. Translation Veenbaas, J. & Visser, W. Amsterdam Boom. ISBN 9789085060178

[9] Kant, I. (1785) Groundwork of the Metaphysics of Morals. Dutch edition 2005. Translation Mertens, T. Amsterdam, Boom uitgeverij. ISBN 90 53522484

Blockchain technology and Self-stabilising systems

April 15, 2019

In 1954, one of the pioneers behind cybernetics, W. Ross Ashby, defined homeostasis as behaviour of interconnected machines that *"is adaptive if it maintains the essential variables within physiological limits"*. [1] Ashby based his definition on experiments he conducted with four interconnected machines that formed a new whole that he called the Homeostat. Operational stability of this new whole is achieved as one of the whole's properties. In fact, Ashby considered this particular property a form of autonomous coordination of activities by and between the various machines.

Read more >

In today's age, devices and machines are increasingly interconnected in networks such as the (Industrial) Internet of Things, offering not only new possibilities but also creating rapidly growing threats that we are still insufficiently aware of and to which we certainly still lack an adequate response. Research into the essence of seemingly new technology such as blockchain technology or cybersecurity may produce new combinations for the development of new knowledge and applications.

Blockchain technology and self-stabilising systems
Ashby considered it a given that two or multiple systems can be interconnected. By creating interconnections, different systems acquire an ability to communicate and interact, thus forming a new whole. For Ashby, creating stability in this new whole is a form of 'adaptive behaviour'. He claimed that *"change of stability can only be due to change of value of a parameter, and change of value of a parameter causes a change in stability."*
In the early 1970s, Edsger W. Dijkstra raised the question whether self-stability as a feature of a whole made up of interconnected systems could be interesting on a scale "from a world-wide network to a common bus control." Dijkstra defines self-stability in systems in this context as follows: *"We call the system self-stabilising if and only if, regardless of the initial state and regardless of the privilege selected each time for the next move, at least one privilege will always be present and the system is guaranteed to find itself in a legitimate state after a finite number of moves."* [2]
That same year, Lamport added the following to Dijkstra's definition: *"Self-stabilizing systems represent ones which are self-correcting:even if they reach an incorrect state through some transient malfunction, they will eventually resume correct operation."*[3] The nuance that Lamport added to the definition opens up the possibility of having networked machines communicate as neighbours as soon as a specific connection has been established between the neighbours. Lamport thus laid the basis for thinking about distributed operating systems that are interconnected in networks, stating that *"a distributed system consists of a collection of distinct processes which are spatially separated, and which communicate with one another by exchanging messages. A network of interconnected computers, such as the ARPA net, is a distributed system."*

Reliable exchange of messages makes sure that the functioning of the whole of interconnected systems cannot be disrupted by changes to one or several of the connected systems. Lamport ultimately included the principles of self-stabilisation in the PAXOS algorithm, paving the way for the development of a self-stabilising whole of interconnected systems that, based on collective decision-making and information-sharing, are able to keep functioning, even in the face of changes from outside the system in one or multiple connected systems.
In 2018 [4], the US National Institute of Standards and Technology (NIST) established that blockchain technology basically originated in the 1980s and 1990s, evolving largely out of the development of the PAXOS algorithm as a consensus protocol that allows interconnected machines to agree on a specific result. These concepts are, according to NIST, the basis for digital currency such as the Bitcoin cryptocurrency.

Cybersecurity

Singer [5] argued that, in this day and age, the concept of changes that come from outside the system is more relevant than ever, as we increasingly face cybersecurity issues when an outsider *"seeks to gain something from the activity, whether to obtain private information, undermine the system, or prevent its legitimate use"*. Willingly penetrating one or multiple networks of interconnected systems or components of such networks, with a view to disrupting the functioning of the whole, is a growing and very current threat to the workings of our society. The extent of this new threat continues to grow, as pointed out by Schneier when he said that *"everything is becoming one hyper-connected system in which, even if things don't interoperate, they're on the same network and affect each other"*. [6]

Such systems are also referred to as cyber-physical systems. NIST defines such systems as *"smart systems that include engineered interacting networks of physical and computational components."* [7] These smart networked systems are incorporating more and more devices that we use in our everyday life (smartphones, TVs, refrigerators, cars), in our day-to-day work (industrial robots, power grids) and in healthcare (MRI scanners, electronic infusion pumps, implanted glucometers, et cetera). They are all systems that operate in a distributed manner and are connected in networks such as the Internet, communicating and interacting in these networks by exchanging messages.

Security

Systems are furthermore often hard to secure or entirely unprotected. It is becoming increasingly clear that illegally gaining access to one or multiple systems can cause severe disruption of the greater network. Recent incidents such as Operation Cloud Hopper, ransomware attacks on Maersk in Rotterdam and Hydros in Norway, Hatman malware in the petrochemical industry, or crash override attacks on power grids have shown that the vast number of wholes of interconnected systems that we use today cannot simply be assumed to be secure. In light of this, Kello argued that *"understanding the cyber question requires a new paradigm of security commensurate with it, one that privileges not just physical but also nonphysical threats and that elevates nonstate actors to a higher level of theoretical existence than the traditionalist viewpoint allows."* [8]

Understanding the new cyber-threat is impossible without first understanding the essence of the new networks and the devices and machines that operate within them in a distributed fashion, making up cyber-physical systems that communicate and interact in changing combinations. There seems to be, however, real potential in combining the possibilities for self-stabilisation of interconnected systems to enable them to assimilate or correct changes to the behaviour of one or several participating systems, thus protecting their joint security. Still, to further flesh out the new combination, we need greater knowledge of the possibilities for self-stabilisation by collaborating cyber-physical systems and the relation to their joint security.

Conclusions

The technological developments that are shaping our present-day world, such as the Internet, (Industrial) Internet of Things and cyber-physical systems, are the product of rapid development of knowledge over the past seventy years. As knowledge grew, new technologies and applications, as well as new threats, have emerged that together constitute the growing technological enframing of our day-to-day lives and working practices. Heidegger believed that the essence of new technology will only truly manifest itself in a world of ignorance and oblivion. In its current manifestation of interconnected systems that jointly make up a new whole, technology is forcing us to find the essence of this new technology fast, so as to be able to deal with the threats that ensue from this essence and to figure out how it affects us as humans. Like Heidegger said, *"the essence of technology lies in what from the beginning and before all else gives food for thought."* [9]

Research into the essence of new and interconnected technology as it has developed so far should focus not only on new possibilities offered by the technology, but also on the potential threats arising from the autonomous operations of this new whole. Developing new knowledge and insights based on analyses of the history and background to the possibilities and threats that come with interconnectedness can help us overcome our ignorance and oblivion, while also contributing to finding new stability between systems mutually and between systems and humans.

Footnotes

[1] Ashby, R.W. (1954) Design for a Brain. New York, John Wiley & Sons Inc.

[2] Dijkstra, E. W. (1974) Self-Stabilizing Systems in Spite of Distributed Control. Commun. ACM 17 (1974), 11: 643-644

[3] Lamport, L. (1974) On Self-Stabilizing Systems. Massachusetts Computer Associates Inc. 5 December 1974 CA 7412-0511

[4] Yaga, D., Mell, P., Roby, N., Scarfone, K. (2018) National Institute of Standards and Technology. Blockchain Technology Overview 2. Draft NISTIR 8202. January 2018

[5] Singer, P. W. and Friedman, A. (2014) Cybersecurity and Cyberwar. What Everyone Needs to Know. New York, Oxford University Press. ISBN 9780199918119

[6] Schneier, B. (2018) Click Here to Kill Everybody. Security and Survival in a Hyper-Connected World. New York, W.W. Norton & Company. ISBN 9780393608885

[7] National Institute of Standards and Technology (2017), Framework for Cyber-Physical Systems. Volume 11, NIST Special Publication 1500-201 Version 1.0 Cyber-Physical Systems Public Working Group.

[8] Kello, L. (2017) The Virtual Weapon and International Order. New Haven, Yale University Press. ISBN 9780300220230

[9] Heidegger, M. (1964) What is Called Thinking? Translated by Gray, J. G. New York, Harper Perennial. ISBN 006090528X

Blockchain technology and data access to connected cars

July 25, 2019

The US National Institute of Standards and Technology has defined the Internet of Things and cyber-physical systems as "a related set of trends in integrating digital capabilities (i.e. network connectivity and computational capability) with physical devices and engineered systems to enhance performance and functionality". According to the authors of this report, the intelligent vehicle is an example of this trend.

Read more >

In today's In Europe, the intelligent car is often referred to as the *'connected car'*. As more and more electronic and software components are installed in cars, cars' intelligence is developing rapidly. These components enable cars to constantly, in the words of a recently published memo by the International Automobile Federation [1], "*collect, store, process, transmit and use*" data.

The European Commission urges manufacturers of these connected cars to quickly reassess their business models and transform from "developing and producing cars to delivering more and more mobility services". This need to transform their business is, according to EU authorities, prompted by the fact that, "*their current business in hardware-selling is at risk of becoming a commodity play and less attractive because of decreasing margins*" [2]. The drive to develop connected cars and the increasing volumes of data that these connected cars collect and communicate will, as claimed in a report[3] published by the EU, have "*potentially large effects on how and who can access and exploit the data*".

Connected cars

In one of his articles, Kerber[4] specifically deals with governance issues that will arise in the transition to connected cars in relation to questions such as who will ultimately be able and allowed to access data collected by connected cars. Kerber is quite clear when he says that, "*in the case of non-personal in-vehicle data – which might be certain kinds of technical data and, in particular, the huge mass of anonymized data – no clear legal rights exist, especially no property rights for data*". Following on from this, he points out that the discussion on data rights so far has shown "that an exclusive de facto control of non-personal data by a data holder from an economic perspective leads to a de facto (but not legal) 'ownership' of these data".

Kerber goes on to claim that, so far, all data collected by cars and subsequently connected cars "*are transmitted directly to proprietary servers of the OEMs (original equipment manufacturer, BvL), they are obtaining de facto exclusive control of these data*". Neither the user(s) of the car, nor other stakeholders of the car are allowed to use data collected by the connected car without the OEM's consent.

Data access

In the discussion on access to data collected by connected cars, research is currently ongoing in a wide range of areas into things such as safety and security (including cybersecurity), liability, standardisation and interoperability, privacy and ethical issues. The aforementioned report by McCarthy et al. claims, among other things, that the car industry does not object to data being made available to third parties based on pre-approved use cases, the requested type of data, or the purpose for which the data will be used. They do, however, restrict such availability to specific kinds of data.

Data generated by the vehicle, known as operating data, can be made available based on these criteria. Access to data imported by the user from a phone or other kind of device, on the other hand, should be blocked. And data received by connected cars from external sources, such as transport infrastructure or other vehicles, must, according to manufacturers, not be accessible either. This report furthermore states that, in most cases, the manufacturers of connected cars are the de facto owner of *"data that their machines or processes generate, even if those machines are owned by the user. A de facto control of this data can be a source of differentiation and competitive advantage for manufacturers"*.

The new position that the manufacturers of connected cars thus acquire, i.e. that of the de facto data owner, leads to interesting new discussions. Kerber claims, among other things, that, *"the problem of access to in-vehicle data should be seen as part of the more general question concerning how a comprehensive governance solution for the data that are produced in the ecosystem of connected and automated mobility should look like"*. The governance issue in such a digital ecosystem is, according to Van Lier[5], complicated by the fact that a digital ecosystem is made up of an amalgam of new and constantly changing combinations of hardware, software, data, information and people. As a result of mutual communication and decision-making within these combinations, changes to components or combinations of components of the ecosystem can automatically lead to changes to the functioning of the system as a whole. The solutions that the aforementioned report proposes with respect to the data issue around connected cars largely fail to address these specific governance issues within an ecosystem. The possible solutions consist primarily of developing a central data server platform to which all data are sent for analysis and distribution. Or an in-vehicle interface (on-board platform) that is connected to a further developed OBD (On-Board Diagnostics) interface, which can in turn be connected to an external device such as a smartphone. These two solutions could in the long term be combined with a yet to be developed on-board application platform that, *"would allow access to vehicle data and the execution of applications inside the vehicle environment"*. Both these possible solutions include the creation of new central trusted third parties to solve the problem of reliable data access.

Blockchain and Distributed Ledger

The connected car as the outcome of the transformation of the traditional car into the car as a cyber-physical system is a composite system of a traditional physical object combined with algorithms, software and data. As a cyber-physical system, the connected car can be connected in networks as a node and communicate and interact autonomously with other nodes in the network. Given the specific singularity of each distributed operating node in the network, it needs to be able to autonomously decide when and with whom it wants and is able to share data or information based on autonomous procedures on *"how the participants agree that a transaction is valid"*[6].

Such consensus procedures performed based on algorithms, software and data originate, according to Yaga et al., from ideas dating back to the early 1990s. The basic idea for such a consensus procedure was, in the view of Yaga et al., presented by Leslie Lamport in 1991 in a scientific article that Yaga et al. argue described a

"consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable".

The PAXOS algorithm that Lamport works out has as one of its essential conditions that the consensus algorithm must work based on the given that each node in the network autonomously stores and secures its data. As a result, each node can independently log the consensus procedures in which it was involved prior to a data transaction, as well as keep track of the data entities that were processed in transactions. The combination of consensus algorithms and distributed ledgers is currently the basis for ITU research initiated by several Chinese organisations[7] into the standardisation of a blockchain of things. It is an interesting thought that standardisation of a blockchain of things may also offer possibilities for a solution to the data access problem involved in cyber-physical systems such as connected cars, especially where standardisation of a blockchain of things is or will be related to the development and implementation of 5G networks.

Conclusion

Data access is not only an issue in relation to connected cars, it is also an issue to consider for all other traditional objects that are slowly but surely transforming into cyber-physical systems, such as fridges, TVs, production machines, MRI scanners, infusion pumps, container terminals and aircraft. And, as outlined in this article, it plays an essential role in concepts such as smart mobility, and with that also in concepts such as smart cities, smart industries, smart healthcare, etc. Given the fact that we are currently insufficiently aware of the data aspects (ownership, access, security) of these developments, we are constantly taken by surprise by new applications in this context. We are constantly trying to come up with isolated solutions to these new developments based on historically defined rules as they apply to humans or natural persons.

New issues emerging from technological developments, such as data access with connected cars, do however call for new and perhaps far more radical solution approaches based on thinking in terms of new wholes, such as digital ecosystems. New possibilities arise when traditional objects are enriched with combinations of algorithms, software and data. Solutions will, therefore, not be found in the possibilities that ensue from the past. New questions surrounding algorithms, software and data call for new ways of thinking and new insights that accept the autonomy and independence of the intelligent object that communicates and interacts within a whole, and urge us to consider how we, as humans, would be willing to transfer our responsibilities to this whole.

Footnotes

[1] International Automobile Federation (2017), What EU legislation says about car data. Legal Memorandum on connected vehicles and data. Memo by Dr M. Störing of Osborne Clarke. Memo on matter 1060415

[2] European Commission (2017), The race for automotive data. Digital transformation Monitor. (January 2017)

[3] McCarthy, M., Seidl, M., Mohan, S., Hopkin, J., Stevens, A., Ognissanto, F. (2017), Access to In-Vehicle Data and Resources. Final Report. European Commission. Directorate-General for Mobility and Transport.

[4] Kerber, W. (2018), Data Governance in Connected Cars. The Problem of Access to In-Vehicle Data, 9 (2018) JIPITEDC 310 paragraph 1.

[5] Lier, B. van (2018), Thinking about ecologies of autonomous cyber-physical systems and their ethics. Rotterdam University of Applied Sciences publishing. ISBN 9789493012028

[6] Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018), Blockchain Technology Overview. US National Institute of Standards and Technology NISTIR 8202

[7] Adolph, M. (2019), ITU Standards for Blockchain and Distributed Ledger Technology. ITU

Blockchain Technology and Decentralised Autonomous Organisations

November 1, 2019

At a lecture in 1951, Heidegger said the following: *"But so long as the essence of technology does not closely concern us, in our thought, we shall never be able to know what the machine is"* (2004: 24)[1]. With these words, Heidegger referred to the rapid development and application of technology, such as production machines, electricity, television and aircraft, in his day. The manifestations of this technology rapidly changed the world at the time, while people never stopped to think about the essence of these technological developments and the ensuing social impact.

Read more >

Today, we again find ourselves on the eve of a similar global change, where machines as physical and stand-alone devices are no longer centre stage, as they are evolving into devices that, through the use of algorithms and software, can communicate and interact in networks. This development is turning the devices produced by modernity into cyber-physical systems that can function and make decisions autonomously based on data and information. These changes, in turn, reveal new organisational possibilities based on a kind of interconnectedness that enables cyber-physical systems to jointly make decisions. Again, the question that arises is whether we can still fathom, or even want to fathom, the scope and essence of such a technology-based development.

Decentralised Autonomous Organisations

In a white paper published by Ethereum in 2014[2], Buterin states that *"the general concept of a 'decentralized organization' is that of a virtual entity that has a certain set of members or shareholders."* Buterin alludes to the capabilities of a whole of networked individual computers, algorithms and software to make decisions by consensus as a whole or as an autonomous virtual entity and to autonomously perform transactions based on these decisions. The rules governing the virtual entity's decision-making process are recorded in what Szabo (1994)[3] calls *'smart contracts'*, which are, essentially, algorithms and software that jointly make up a protocol based on which transactions can be performed autonomously by the virtual entity, i.e. without human intervention. In 2015, Wright and Primavera de Filippi[4] put it as follows: *"Over time, as internet-enabled devices become more autonomous, these machines can use decentralized organizations and the blockchain to coordinate their interactions with the outside world."* This quote links the application of consensus algorithms, smart contracts, decentralised operating autonomous organisations to the rapid development and application of concepts such as the (Industrial) Internet of Things and cyber-physical systems. A 2019 report by the US National Institute of Standards and Technology[5] claims that although these concepts have different origins, they do overlap to a considerable degree, as they all refer to a similar development, which the report describes as *"trends in integrating digital capabilities, including network connectivity and computational capability, with physical devices and systems"*. The increasing digital capabilities of random combinations of networked cyber-physical systems, which people use every day or that produce information output that is applied, engender new organisational models that, in turn, can be considered decentralised autonomous organisations. These are organisations that are made up of autonomously operating cyber-physical systems that are able to communicate and interact, as well as to jointly make decisions and perform transactions without any kind of human involvement.

Organisation design

In his 2019 dissertation [6], Mark van Rijmenam asks how new technologies such as big data, artificial intelligence and blockchain technology influence our thinking on how to develop organisations and organisational models. He explores *"how blockchain requires* *us to rethink organisation design theory by redefining the decentralised and autonomous form of organisation design; and how agency theory helps us solve the principal–agent problem when dealing with artificial actors that behave differently than intended*". Van Rijmenam defines a decentralised autonomous organisation as an organisation that is made up entirely of networked computers, (consensus) algorithms and software, which operate jointly based on what are known as smart contracts. The data and information transactions that these autonomous organisations perform without human involvement are regulated by protocols that are captured in software code, which is used to manage the rules based on which joint transactions can be performed. According to Van Rijmenam, this development marks the first time in history that "*machines can collaborate automatically and even autonomously with other machines and even humans, while ensuring the outcome aligns with what has been already agreed upon*". This development will lead to organisations becoming increasingly entangled with the technology they use, even more so than they already are. As this entanglement increases, there will be a rapidly growing need to use forms of artificial intelligence/machine learning to manage and control autonomously performed transactions. It is inevitable, in Van Rijmenam's view, that this development will force people at these organisations to (learn to) collaborate with networked cyber-physical systems. This collaboration means, in Van Rijmenam's view, that "*the material and the artificial should exist in coherence and interact with each other without negatively affecting one another*". The latter point leads to questions that potentially touch on the ethical nature of this development. Is it true that, as Van Rijmenam claims, interconnected cyber-physical systems in this development are by definition subordinate to human ethics and that "*the material is bound by the norms and principles of our society and the culture within an organisation and the social is not subordinate to the material and the artificial*"? Is it not more likely that, in a situation where people work with several intelligent or large numbers of interconnected cyber-physical systems that have originated from different cultures, humans inherently become subordinate to this virtual entity? Will this development not see people transfer their (ultimate) responsibility for the performance of transactions to the new virtual entity of a decentralised autonomous organisation a lot faster than expected, based on the excuse that it so complex?

Consequences

As described previously [7], the International Telecommunication Union (ITU) is working on studies into the standardisation of a blockchain of things. The research proposal that the governments of Egypt and China, and a number of Chinese companies submitted to ITU in 2017 concerned only one study. This number has meanwhile grown to twenty-four. The first results are expected in late 2019. The standards that these studies will define are inevitably going to play a role in shaping and implementing a blockchain of things based on the capabilities of cyber-physical systems and their mutual communication in future 5G networks. These standards will enable new and global decentralised and autonomous organisations that can consist of random combinations of cyber-physical systems. These will be organisations that are made up of the cyber-physical systems we use on a daily basis, such as computers, smartphones, cars, toothbrushes and fridges, or more uncommon cyber-physical systems, such as MRI scanners, infusion pumps, patient monitors and implantable glucometers. Electronic or physical infrastructures, such as electronic networks, railways and roads, energy applications or military applications, will also be part of these new decentralised autonomous organisations. Algorithms and software are increasingly being built into all the devices we humans use on a daily basis, enabling these devices to participate in the new form of a decentralised autonomous organisation. It is high time that we in Europe take Van Rijmenam's lead and take a serious look at the increasing autonomy of cyber-physical systems that ensues from the widespread use of algorithms and software. At the same time, we, in Europe, are going to have to think about conditions based on which we want to allow and enable decentralised and autonomous organisations to function within our European culture. Given the great pace of these developments, we do not have a lot of time to develop the new knowledge required for the design and analysis of such virtual entities based on European Software.

Footnotes

[1] Heidegger, M. (2004) What is Called Thinking? Translated by Gray, J. G., New York, Harper Perennial. ISBN 006090528X Original version: Was heißt Denken? (1954)

[2] Buterin, V. (2014) Ethereum White Paper. A Next Generation Smart Contract & Decentralized Application Platform http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] Szabo, N. (1994) Smart Contracts http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[4] Wright, Aaron and De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (10 March 2015). Available at SSRN: https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664

[5] Greer, C., Burns, M., Wollman, D., Griffor, E. (2019) Cyber-Physical Systems and Internet of Things. NIST Special Publication 1900-202, March 2019

[6] Rijmenam, M. van (2019) Sociomateriality in the age of emerging information technologies: How big data analytics, blockchain and artificial intelligence affect organisations. A thesis for the degree of Doctor of Philosophy in Management. UTS Business School, University of Technology Sydney, Management Discipline Group

[7] Lier, B. van (2018) Blockchain-of-Things. https://www.centric.eu/NL/Default/Themas/Blogs/2018/05/16/Blockchain-of-Things

[8] Heidegger, M. (2004) What is Called Thinking? Translated by Gray, J. G., New York, Harper Perennial. ISBN 006090528X Original version: Was heißt Denken? (1954)

Blockchain and the complexity of emerging technologies

April 17, 2020

We humans and our societies in the 21st century are increasingly seeing technological developments emerge that we find engaging, convenient, or useful, but which we are often essentially unable or unwilling to understand. This lack of understanding of technology is not a new phenomenon. In fact, German philosopher Martin Heidegger [1] noted as early as in 1927 that the advent of the radio both broadened and disrupted his everyday reality. Heidegger also wrote that the consequences of the emergence of new technology in the form of radio were completely impossible for him to fathom. Also for us, people of the 21st century, new and networked everyday devices such as cars, television sets, washing machines, MRI scanners, wind turbines and even lampposts are all manifestations of new combinations of hardware, algorithms, software and data that are having an impact on our world that is barely graspable. These new combinations, which are also known as cyber-physical systems, are able to autonomously interconnect themselves in networks, communicate in these networks, and interact with other and similar combinations. The data and information that are autonomously produced and communicated by these systems are rapidly changing our everyday world, as well as the existing economic system, from the inside. The new combinations of hardware and software bring a form of what economist Joseph Schumpeter [2] called *'creative destruction'*. Cyber-physical systems are gradually replacing existing devices and simultaneously developing a process of creative destruction of our world and our economy, without us being able to properly monitor and/or understand this process.

Read more >

centric

Internet of Things

Slowly but surely, it is becoming common practice to use voice commands to operate devices such as a smartphone, a TV, or a Tesla. Without thinking twice about it, we use and pay for content from providers such as Netflix and HBO that is produced in the United States and shown on our networked smart TV. We watch the content wherever we want, whenever we want, and on any device we want, while telling our friends that we don't really watch TV any more. We talk to Siri, Google Assistant, or Alexa, getting our device to order things for us or take care of mundane tasks such as switching the lights on and off. It has long ceased to seem alien to us to get suggestions on our smartphone about the energy generated by our solar panels. All these new capabilities are created by the communication and interaction between devices enabled by the algorithms, software, and data that are available specifically to these devices. It led the US National Institute of Standards and Technology (NIST) to state in March 2019 that *"the phrases 'cyber-physical systems', or 'CPS', and 'Internet of Things', or 'IoT', have distinct origins but overlapping definitions, with both referring to trends in integrating digital capabilities, including network connectivity and computational capability, with physical devices and systems"*. [3] The increasing connections, communication, and interaction between new combinations are converting, unchallenged, our day-to-day reality into a more and more interconnected and complex whole of data and information. One hundred years ago, grasping how an individual and stand-alone device such as a radio works was highly complicated for humans. Today, learning to understand how interconnected individual cyber-physical systems work is virtually impossible for us humans.

Our analysis of the individual device should no longer revolve around the individual device itself, but rather around its connections to other devices, as these connections are what enables new functionality. Existing methods, ways of thinking, and forms of organisation, regulation, or governance no longer seem adequate in light of the rapid increase in the number and use of interconnected cyber-physical systems and their growing autonomy and intelligence.

Blockchain technology

Slowly but surely, we are entering a phase where new possibilities arise for collaboration and decision-making by these interconnected cyber-physical systems. In October 2018, NIST stated in a research report [4] on blockchain technology that *"the core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper 'The Part-Time Parliament' to ACM Transactions on Computer Systems. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable"*. In a previous blog entry (February 2018), I referred to a collaboration project of Samsung and IBM in this area. This pilot project, called Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT), was focused on the possibilities for collaboration between a specific cyber-physical system, in this case a washing machine, and multiple other devices in a specific and permissioned environment. Back in 2018, I [5] wrote the following about this project: *"The ADEPT project has led to a pilot of a blockchain of devices, where devices work together autonomously and make decisions about tasks or orders, etcetera. The approach of linking these devices using blockchain technology also further increases these devices' level of autonomy."* Parts of the algorithms and software used in the project were later used by IBM as a basis in their development of Hyperledger blockchain technology. The pilot run by Samsung and IBM shows that the possibilities offered by blockchain technology can also be harnessed for reliable communication, consensus and decision-making, as well as for autonomously performed information transactions by and between autonomous cyber-physical systems. On the latter possibility, the Industrial Internet of Things Consortium [6] stated the following: *"Entities need to share information; they also need to keep it private. Distributed ledger technologies, such as blockchain, can be used as authentication providers. This means that more data can be shared because the provider has more confidence that the shared data will be restricted to the preselected groups. This could be used to provide attestation of edge elements and software, and track the provenance and completeness of the critical edge-hosted data"* (2019:7). In Europe, there is also ongoing research into the possibilities for reliable information exchange between devices. In 2019, the European Blockchain Laboratory [7] concluded the following: "Blockchain could be connected to new production trends or the 'fourth industrial revolution', which include other emerging technologies, from IoT to artificial intelligence and robotics, and new materials or additive manufacturing" (2019:29). Whether we like it or not, complexity will inevitably increase as more and more interconnected cyber-physical systems become able to autonomously and jointly make decisions on our behalf through an incalculable number of connections and based on algorithms, software, and data.

Artificial Intelligence

In 1950, Alan Turing [8] asked himself the following question:

'Can Machines Think?'

Five years later, a group of American scientists wrote a proposal for a study [9] that would answer this question about what they called 'Artificial Intelligence' within two months. In their proposal, they stated *"that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it"* (1955:1). Over the 65 years that followed, artificial intelligence has developed with a great many highs and lows. In essence, the question is still how machines as combinations of hardware (computers), algorithms, and programs (software) can learn from the data made available to such a combination. The foundations of the learning are still under discussion. Today, the key question is whether the owner of a new combination (such as Google, IBM, Amazon, Facebook, Apple) is able to increase the computing power of the technology (such as

Tensor Processing Units) and continue to combine the capabilities created by such an increase in computing power with new and improved algorithms and software, so as to make the technology even better at *'learning'* from analyses from even greater volumes of data. There is increasing discussion worldwide on whether this form of algorithm-based learning could ever match humans' ability to learn. In this discussion, Russell [10] stated the following in 2019: *"The problem is right there in the basic definition of AI. We say that machines are intelligent to the extent that their actions can be expected to achieve their objectives, but we have no reliable way to make sure that their objectives are the same as our objectives"* (2019:11). Machine learning in any form is a dimension of learning that differs from what we humans define as learning. The learning done by machines that are interconnected in networks and make decisions within these networks involves learning from the value associated with these decisions to be able to subsequently make *'better'* decisions. The step to machine learning by interconnected cyber-physical systems is, therefore, not as major as is often thought. The PAXOS algorithm, for example, includes that nodes in a network must learn from the value ensuing from a joint decision-making process between the nodes. In an ever more complex world of interconnected cyber-physical systems, these systems are not only able to autonomously and independently make decisions based on algorithms, software, and data, they can at the same time also learn from the value used to also autonomously adjust and improve the decision-making process. These capabilities will lead to these new combinations drastically changing our lives and work over the coming years, and thus have a far-reaching impact on us humans.

Conclusion

This last statement takes us right back to the beginning.
The current process of innovation creates new technological combinations and makes our world increasingly complex and harder to grasp for many. Having ideas and knowledge in the traditional way, or turning a blind eye to the way in which new technology creates possibilities that seem engaging, convenient, or useful, is impossible without new knowledge to help us make sense of this development. Like Heidegger [11] said, we, as humans, need to *'relearn to think'* about the question of what the essence is of the new technology. This way of thinking will enable us to find new ways to understand technology and the ensuing possibilities and consequences for humans and society. And above all, *'learning to think'* can help us understand what this technology means for us humans.

‘learning to think’

Footnotes

[1] Heidegger, M. (1927) Being and Time. Dutch Edition (1986) Zijn en Tijd. Nijmegen, Uitgeverij SUN (1998). ISBN 9063037945

[2] Schumpeter, J. A. (1943/2003) Capitalism, Socialism & Democracy. New York, Routledge. ISBN 0203202058

[3] Greer, C., Burns, M., Wollman, D. and Griffor, E. (2019) Cyber-Physical Systems and Internet of Things, NIST Special Publication 1900-202. https://doi.org/10.6028/NIST.SP.1900-202

[4] Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2018) Blockchain Technology Overview, NIST 2019, NISTIR 8202

Blockchain Technology Overview https://doi.org/10.6028/NIST.IR.8202

[5] Lier, B. van (2018) Blog entry - Blockchain between edge and fog computing. February 2018

[6] Industrial Internet Consortium (2019) The Edge Computing Advantage. An Industrial Internet Consortium White Paper, Version 1.0. 2019/10/24

[7] European Commission. Joint Research Centre. (2019) Blockchain Now and Tomorrow. Assessing Multidimensional Impacts of Distributed Ledger Technologies. ISBN 9789276089773

[8] Turing, A. M. (1950) Computing Machinery and Intelligence. Mind 49: 433-460

[9] McCarthy, J., Minsky, M. L., Rochester, N., Shannon, C. E. (1955) A proposal for the Dartmouth Summer Research Project on Artificial Intelligence.

[10] Russell, S. (2019) Human Compatible. Artificial Intelligence and the Problem of Control. New York, VIKING. ISBN 9780525558613

[11] Heidegger, M. (1954/2004) What is Called Thinking? Harper Perennial, New York. ISBN 006090528

Blockchain of Things: *global infrastructure made in China*

July 13, 2020

In April this year, the Chinese government signed off on plans for new investments in Chinese infrastructure[1]. The plans are set to be implemented by the National Development and Reform Commission (NDRC), which recently presented a vision outlining its definition of infrastructure. According to the NDRC, the development of new infrastructure is focused on three elements: *"information infrastructure, integration infrastructure and innovation infrastructure."* What is clear is that blockchain technology plays an important role in the first of these three elements, as confirmed by the creation in April of a National Blockchain and Distributed Ledger Technology Standardisation Technical Committee by the Chinese Ministry of Industry and Information Technology (MIIT)[2].

Read more >

As I pointed out in 2018[3], China is a prominent player in the International Telecommunication Union, forging global alliances on a Blockchain of Things, which combines blockchain technology with the Internet of Things. This international standardisation drive, which is focused on the functioning of a blockchain-based Internet of Things and Smart Cities, has meanwhile produced the first reports. The Chinese megalopolis of Chongqing[4], which has a population of roughly 31 million, has already taken the lead and launched its own blockchain technology innovation league. The question is whether we in Europe and the Netherlands, in light of recent developments in China, actually understand the technology behind blockchain in combination with other technological developments, or that we should just bow to the supremacy of China and the US when it comes to these new technological combinations.

ITU

As expected, the reports published by the International Telecommunication Union (ITU) focus primarily on the combination of the Internet of Things and Smart Cities with blockchain technology to create a new technology-based combination of the new Blockchain of Things. Some of these reports were written by an ITU focus group made up of representatives from Renmin University of China, Huawei, Telecom SudParis, Smart Dubai, UN-Habitat and the Kyoto Institute of Technology. The reports present technical specifications and definitions of terms to use in this context. One of the key concepts is *'ecosystem'*, which the focus group defines as a whole of organisations that jointly make up a distributed system with both technical and non-technical features. Smart cities and communities are defined as an effective integration of physical, digital and human systems in a built environment to offer civilians a sustainable, prosperous and inclusive future. The Internet of Things is defined as a global infrastructure, also referred to as the information society.

This global infrastructure makes the development of advanced services possible through the (physical and digital) interconnection of *'objects'* or *'things'* in networks, based on existing and still evolving information and communication technologies. The ITU focus group defines blockchain technology as a "*peer-to-peer distributed ledger based on a group of technologies for a new generation of transactional applications which may maintain a continuously growing list of cryptographically secured data records hardened against tempering and revision*".

According to the focus group, Blockchains of Things can be classed in three categories, with the first being the public blockchain (accessible to everyone and anywhere without restrictions). The second and new category is the consortium blockchain, which seems to be based on the concept of ecosystem. The focus group defines the consortium blockchain as "*usually deployed and maintained by a consortium. The distinction of a consortium blockchain is primarily on the method of making consensus. The consortium decides which participants in the blockchain will have the authority to deploy smart contracts and make transactions, and decides how to open the blockchain data to the participants*[5]" . The term 'consensus' is a key element of this definition. The focus group considers '*consensus*' to be "*agreements to confirm the correctness of the blockchain transaction*". The third and final blockchain category designated by the focus group is the private blockchain. A private blockchain is developed and managed by private parties and is basically the opposite of a public blockchain, i.e. it cannot be accessed without the permission of the private parties that run it[6].

According to the members of the focus group, blockchain technology has major potential for the creation of a new ecosystem that consists of a whole of people, things and decentralised (software) apps[7], which is a whole that creates new possibilities in many sectors of society, such as the financial sector, healthcare, public sector, industry, retail, supply chain and logistics, etc.

China as the frontrunner

As a major advocate for the development and use of blockchain technology, the Chinese leader Xi Jinping believes that this new technology can help propel China's economic developments and position his country globally as a technology-based society. Although Xi Jinping is clearly not interested in public blockchain networks such as bitcoin, China's central bank is exploring options for a Chinese digital currency that runs on blockchain technology.

> ***"the only global infrastructure network autonomously innovated by Chinese entities and for which network access is Chinese-controlled"***

For China, blockchain technology is primarily a means of securely and reliably exchanging and sharing data and information between people and between people and things in a rapidly developing global digital society. In late 2019, several initiatives were launched in China for the development and implementation of what is known as a Blockchain-based Service Network (BSN)[8] [9]. This network is intended to be a precursor to global infrastructure based on '*consortium blockchain technology and consensus trust mechanisms*'.

China has opted for this consortium approach because of the following reason stated in a BSN white paper: "*Under a permissioned blockchain framework, if the application owner is an alliance composed of multiple organizations, then all* *members of the alliance will commonly formulate all internal mechanisms of the application. This type of permissioned blockchain structure is known as a consortium blockchain. If only one organization controls all application rights, privileges, and regulations, then it is known as a private blockchain."* The Blockchain-based Service Network is essentially made up of interconnected nodes that are the responsibility of city governments. For each urban area, one or multiple such urban nodes can be developed as units made up of physical servers or cloud services on one side, possibly hosted by private parties, which jointly form a blockchain operating environment, and a consensus order cluster service on the other.

The urban nodes developed in China are interconnected through the Internet to initially form a national information infrastructure and ultimately, as the white paper states, a new global information infrastructure. The Chinese Blockchain-based Service Network has the potential, so the white paper claims, to develop into "*a second generation of smart and dedicated internet using consensus mechanisms between organizations*". The Chinese megalopolis of Chongqing is already taking the lead in this development, setting up its own blockchain technology innovation league of 110 companies, including Huawei, Tencent, China Mobile, China Unicom, China Telecom and IBM. The possibilities that this new information infrastructure offers enable Chinese software developers to develop what are known as decentralised (software) apps that can function in various frameworks and enable the interconnection and communication between the various '*DApps*' (Decentralised Apps).

At present, 40 cities across China are interconnected through the BSN, and this number is expected to rise rapidly to 100 urban nodes in the BSN following the official launch. The authors of the white paper anticipate that other Asian and European nodes may be connected to the BSN as well soon thereafter. It will enable the BSN to slowly but surely grow into a global network of urban-based nodes. If the BSN does indeed go global, it creates, according to the white paper, "*the only global infrastructure network autonomously innovated by Chinese entities and for which network access is Chinese-controlled*".

What about Europe?

China is currently the global leader when it comes to patents granted to state and private-owned companies for elements of a Blockchain of Things. While the US still manages to stay close to China in this respect, the European Union pales into insignificance next to China in the area of blockchain technology. China's success starts with the combination of a long-term vision, which spans decades and is based on technology in general, and centrally managed developments such as blockchain technology. China has undeniably been very successful in implementing infrastructures driven by technological developments, such as the Belt and Road initiative and Artificial Intelligence. It is therefore highly likely that the

Blockchain-based Service Network will in the long term be successful as an information infrastructure in parts of the world.

The rapid Chinese developments should get us thinking here in the Netherlands and Europe. Do we want to be part of a Chinese blockchain information network that is controlled from Beijing? If we in Europe want to stay autonomous and chart our own digital future, we are going to have to develop our own alternative to the Chinese Blockchain of Things. Such a European alternative infrastructure would then have to be able to communicate with its Chinese and US counterparts.

The development of such a European initiative is, however, impossible without centralised coordination and a long-term vision for knowledge development for the development and application of algorithms and software that make a blockchain what it basically is: a reliable and secure way for things to communicate, interact and autonomously make decisions based on consensus.

Footnotes

[1] China includes blockchain technology under definition of "New Infrastructure" as part of 2020 Investements Ambitions (2020) China Banking News http://www.chinabankingnews.com/2020/04/21/china-includes-blockchain-technology-under-definition-of-infrastructure-as-part-of-investment-plans/

[2] China assembles technical committee for national blockchain and distributed ledger standards (2020) China Banking News http://www.chinabankingnews.com/2020/04/14/china-assembles-technical-committee-for-national-blockchain-and-distributed-ledger-standards/

[3] Lier van B. (2018) Blockchain of Things May, 2018

[4] Chonqing establishes new blockchain innovation league with IBM, Huawei, Tencent (2020) China Banking News http://www.chinabankingnews.com/2020/04/13/chongqing-establishes-new-blockchain-innovation- league-with-ibm-huawei-and-tencent/

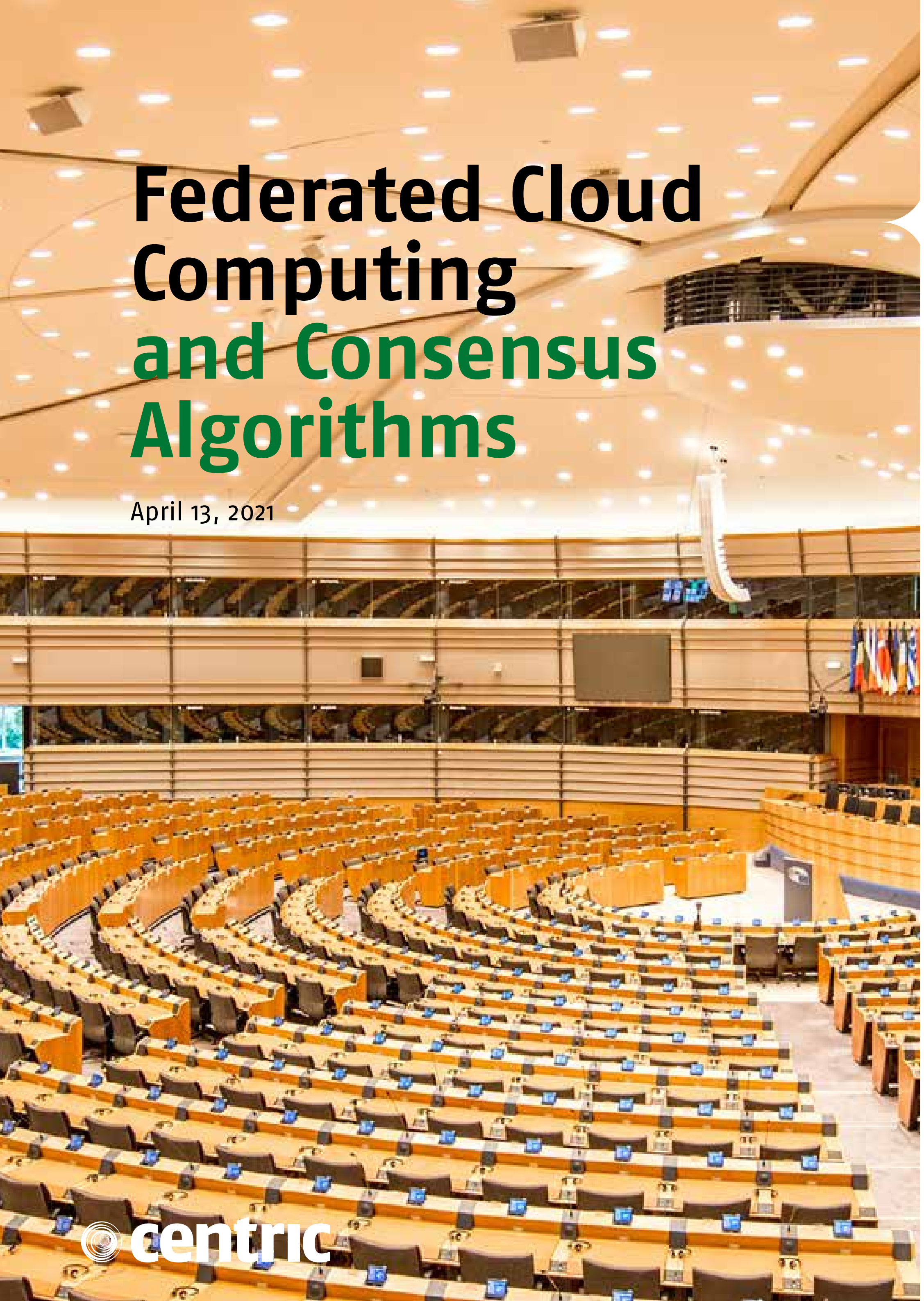
[5] ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (2019) Technical Specification D1.1 Use case analysis and requirements for Data Processing and Management to support IoT and Smart Cities and Communities

[6] ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities (2019) Technical Report D3.5 Overview of blockchain for supporting IoT and SC&C in DPM aspects

[7] Framework of blockchain of things as decentralized service platform (2020) 1.0 ITU-T Y.4464 2020-01-13 20 11.1002/1000/14167

[8] Blockchain-based Service Network Introductory whitepaper (2019) BSN Development Association, September 2019

[9] Blockchain-based Service Network Technical whitepaper (2019) BSN Development Association, April 2020



Federated Cloud Computing and Consensus Algorithms

April 13, 2021

In his 1956 book entitled An Introduction to Cybernetics[1], William Ross Ashby argues that interconnectability is a fundamental feature of machines. In his view, 'two or more whole machines can be coupled to form one machine; and any one machine can be regarded as formed by the coupling of its parts, which can themselves be thought of as small, sub-machines' (Ashby ,1956, p. 48). In 1962, Ashby predicts that these kinds of interconnections between computers or intelligent mechanisms will increasingly become normal and make up the core of self-organisation by computers. He argues[2] that the core of this self-organisation is made up of the conditions under which the interconnections will be created.

Read more >

In 2011[3], the US National Institute of Standards and Technology (NIST) states that *'cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)'* (NIST, 2011, p. 3). This definition of cloud computing teaches us that computers that are interconnected in networks can make their joint capacity available to users based on prior hardware and software configurations. In a document published in 2021[4], NIST broaches the possibility of incorporating these individual cloud configurations into a federated association or, in their words, *'getting two or more cloud providers to interact or collaborate'*, thus coining the term *'federated cloud'*.

Federation

The term *'federation'* has a long history that revolves primarily around the development of political or social entities. In general, 'federation' denotes collaboration between individual, partially self-governing organisations, states, regions or other entities with a view to creating a new and collaborating whole without the constituent entities losing control or command of their own internal affairs. In most cases, the federation as an organisational form is under centralised governance that does not involve itself in the composition or functioning of the individual entities. Therefore, a federation as a whole needs to be governed based on agreements on how the federation should function. These agreements must be such that the participating parties can trust the functioning of the federation as a whole. According to NIST, the term *'federated cloud'* refers to the coordination and organisation of collaboration between individual cloud providers. In this context, coordination and organisation concern the correlation between the separate cloud parties without wanting to intervene in the configuration or composition of the underlying networks or the specific configurations of the hardware and software used by the various cloud providers. In this way, the federated cloud can be seen as a *'permissioned network'* of interconnected cloud providers. Cachin and Vukolic[5] defined permissioned network as a network *'operated by known entities, such as in consortium blockchains, where members of a consortium or stakeholders in a given business context operate a permissioned blockchain network'*. (2017, p. 2). In these networks, participating nodes such as individual cloud parties are not only identifiable beforehand, but these interconnected nodes themselves are also able to check their shared status and, if necessary, update it. A core task of these interconnected nodes is to determine in consensus which node can perform a specific information transaction with third parties outside the network.

Consensus

The 2021 NIST document focuses specifically on the topic of trust and governance of the collaboration within a federation of interconnected cloud parties. According to NIST: *'While* *much trust and governance may be established out-of-band, we recognize that there are tools for establishing trust in an otherwise untrusted environment that are relevant for federated systems.'* (NIST, 2020, p. 45). According to NIST, these tools include consensus algorithms such as Paxos and Raft. What is interesting to note is that NIST[6] previously (NIST, 2018) claimed that the development of these consensus algorithms started in the late 1980s. They considered the Paxos[7] algorithm published by Leslie Lamport in 1998 to be the basis for the further development of consensus algorithms. About this publication NIST says: *'The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable.'* A contemporary example of a consensus network is Microsoft's Confidential Consortium Framework, which is available on an open-source basis. This Coco Framework is based on consensus algorithms such as Paxos and Raft, creating possibilities for secure interconnection of local nodes or virtual machines in a closed network. The Coco Framework also offers ways to securely and reliably exchange and share information between groups of identified nodes. Based on the information shared, these nodes are able to autonomously make decisions on the performance of information transactions between nodes in the network and beyond. Given that there is no trusted third party in the network, it is up to the nodes to autonomously store the data and information they use in their own decentralised ledgers. The first experiments with this framework run by Centric show that it offers many possibilities for further development and application. However, these experiments also show that the thinking about development and application of these closed and secure networks within which nodes can autonomously make decisions requires different and new knowledge. New experiments that are currently being prepared will explore whether this development can also be applied in the context of, for example, multi-party computation where different parties' networked computers can reach a shared outcome without any data and information being transferred.

> ***The first experiments with this framework run by Centric show that it offers many possibilities for further development and application.***

European Federated Cloud Infrastructure

In 2020, the European Commission[8] launched a European strategy for European data. This European strategy is based partly on new technological possibilities such as combinations of blockchain technology/consensus algorithms and digital infrastructures such as a European Federated Cloud Infrastructure, and therefore seems to be running in sync with the developments identified by NIST. In October 2020, the Dutch government signed the EU

Declaration entitled *'Building the next generation cloud for businesses and the public sector in the EU'*[9]. In this declaration, the EU member states agree to pursue a European Federated Cloud to create next-generation secure, energy-efficient, and interoperable cloud infrastructure for Europe as a whole. The EU member states furthermore agreed to jointly *'cooperate towards one set of common technical rules and norms (future EU Cloud Rulebook) and the deployment of interconnected cloud capacities across the EU, including common marketplaces'*. Whether and, if so, how consensus algorithms will play a role in the organisation of the European Federated Cloud is (as yet) unclear. The Franco-German GAIA-X initiative also explores whether and, if so, how a European Federated Cloud infrastructure can be organised and implemented to gain greater control of data produced and used in Europe. The first document published by GAIA-X[10] in 2019 states as follows: *'We understand data infrastructure as a federated technical infrastructure, consisting of components and services that make it possible to access data and to store, exchange and use it according to predefined rules'* (2019, p.2). The development towards a European Federated Cloud infrastructure for greater control and better governance of European data and information can therefore be considered a given.

Conclusion

The whole of a federation of interconnected individual cloud configurations can be considered a form of self-organisation by machines as once described by Ashby. Based on algorithms and software, an autonomous whole can be created that is able to autonomously make consensus-based decisions. These joint and consensus-based decisions serve as the basis for the autonomous execution and settlement of information transactions. This form of self-organisation can be the foundation for the creation of a sovereign European data space. The emphasis in the development of the European Federated Cloud infrastructure will inevitably have to be on the development of new conventions and rules for organisation and governance by this federated infrastructure. The rules for this federation will, however, only work if they can be implemented by the federated participants based on new and transparent algorithms, protocols, and software that underpin the European Federated Cloud infrastructure. The perspective in

> ***'We understand data infrastructure as a federated technical infrastructure, consisting of components and services that make it possible to access data and to store, exchange and use it according to predefined rules'***

this development thus gradually shifts away from human action towards independent and autonomous action by hardware and software configurations that collaborate and make decisions within a federated association. Hopefully, this development will include sufficient focus on European values and the history on which it is based.

Footnotes

[1] Ashby, W.R. (1957) An Introduction to Cybernetics. London, Chapman Hall LTD. Second impression

[2] Ashby, W.R. (1962) 'Principles of the Self-Organizing System'. In: Heinz Von Foerster and George W. Zopf, Jr. (eds.), Principles of Self-Organization (Sponsored by Information Systems Branch, U.S. Office of Naval Research). Republished as a PDF in Emergence: Complexity and Organization (E:CO) Special Double Issue Vol. 6, Nos. 1-2 2004, pp. 102–126.

[3] Mell P. and Grance T. (2011) The NIST Definition of Cloud Computing. NIST Special Publication 800-145

[4] Lee C.A., Bohm R.B. and Michel M. (2020) NIST Federated Cloud Reference Architecture. NIST Special Publication 500-332., February 2020

[5] Cachin C. and Vukolic M. (2017) 'Blockchain Consensus Protocols in the Wild', 31st International Symposium on Distributed Computing (DISC 2017), Vienna, Austria, 16-20 October 2017

[6] Yaga D., Mell P., Roby N., and Scarfone K. (2018) NIST Blockchain Technology Overview, NISTIR 8202, October 2018

[7] Lamport L. (1998) 'The Part-Time Parliament'. In: ACM Transactions on Computer Systems 16, 2 (May 1998), pp. 133-169.

[8] European Commission (2020) European strategy for data. Brussels, 19.2.2020 COM(2020) 66 final: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[9] Joint declaration: Building the next generation cloud for businesses and the public sector in the EU; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[10] German Federal Ministry for Economic Affairs and Energy. (2019) Project GAIA-X. A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. (October 2019): https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4