CONVERGENCE OF BLOCKCHAIN, AI AND IOT

a thematic report prepared by

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM

EUBlockchain Observatory and Forum

An initiative of the European Commission

About this report

The European Union Blockchain Observatory & Forum has set as one of its objectives the analysis of and reporting on a wide range of important blockchain themes, driven by the priorities of the European Commission and based on input from its Working Groups and other stakeholders. As part of this it will publish a series of thematic reports on selected blockchain-related topics. The objective of these thematic reports is to provide a concise, easily readable overview and exploration of each theme suitable for the general public. The input of a number of different stakeholders and sources is considered for each report. For this paper, these include:

- Members of the Observatory & Forum's Working Groups as well as the Obeservatory's Convergence Sub-Working Group (please see next page).
- "Tokenization of physical assets and the impact of IoT and AI", by Prof. Dr. Tim Weingärtner, Lucerne University of Applied Sciences & Arts – School for Information Technology, an academic partner of the EU Blockchain Observatory & Forum
- Input from participants at the "Convergence of blockhain, AI and IoT" workshop held in Brussels on 28 March, 2019.
- Input from the Secretariat of the EU Blockchain Observatory & Forum (which includes members of the DG CONNECT of the European Commission and members of ConsenSys).

CREDITS

This report has been produced by ConsenSys AG on behalf of the European Union Blockchain Observatory & Forum.

Written by: Tom Lyons, Ludovic Courcelas
Thematic Report Series Editor: Tom Lyons
Report design: Benjamin Calméjane

v1.1 - Published on 21 April, 2020.

DISCLAIMER

ACKNOWLEDGEMENTS

The EU Observatory & Forum would like to expressly acknowledge the following for their direct contributions and feedback to this paper as members of the Convergence Sub-Working Group:

- Anastasios A. Antoniou
- Nadia Filali
- Janis Graubins
- Julian Hosp
- Marta Ienco
- Stefan Junestrand
- Iwona Karasek-Wojciechowicz
- Manuel Machado
- Marina Niforos
- Philipp Sandner
- Jolanda ter Maten
- Professor Tim Weingärtner

We would also like to acknowledge the contributions of the following reviewers:

- Kripal Attawar

NOTE

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this paper.

Contents

Executive summary

No technology exists in a vacuum, blockchain included.

In this paper, we look at how blockchain technology can be used in conjunction with two other important emerging technologies – the Internet of Things (IoT) and artificial intelligence (AI) – to complement each other and build new kinds of platforms, products and services.

We start by examining the interplay of blockchain with the IoT – the realm of sensors, smart devices and robots. The IoT promises many benefits for how we live and our environment, but there are numerous challenges, from monitoring and controlling millions (if not billions) of heterogenous devices, to helping them to communicate and transact with each other, to keeping them secure. As the IoT continues to grow, the centralised approaches to these challenges that are in use today are reaching their limits. Blockchain can help by offering a decentralised alternative for IoT platforms – one in which devices "package" data and share it in a peer-to-peer fashion instead of routing it through a centralised cloud server. Such an approach could be more scalable, more robust and more direct than centralised, cloud-based solutions, and free from potential problems like data bottlenecks and vendor lock-in. By providing secure audit trails of information coming from a sensor, blockchains can make it easier to monitor individual machines and spot anomalies. Blockchains can also support the interoperability of IoT devices by providing a trusted, common communications layer. Via smart contracts, blockchain can also facilitate autonomous machine-to-machine transactions, bringing automation and other efficiencies to large platforms.

Like IoT, AI promises great benefits for society. But to reap these benefits, AI models need access to large amounts of data. As the cost of gathering, storing and processing these large data sets, not to mention of hiring and maintaining AI experts, is prohibitively high, the value of AI is currently being concentrated in the hands of a few large companies. This is of concern to many. Blockchain can help mitigate such concerns in different ways. Blockchains can be used, for instance, to develop open, decentralised data markets in which data producers, whether individuals or enterprises, can sell, rent or share their data. In the same way, blockchains can be used as the basis for open, decentralised markets for AI models, allowing independent AI developers to directly sell their wares, more easily collaborate with each other on large projects and even share computer resources. Such markets could also help make access

EXECUTIVE SUMMARY

to AI models more readily available to individuals and small companies. Using newer technologies, blockchain could also help "bring compute to data", allowing AIs to train on data sets in privacy-preserving ways and potentially opening up more data sources.

In the real world, especially in large-scale use cases, blockchain, AI and IoT are likely to work in concert. In a smart city, blockchain could be combined with IoT and AI on an infrastructure level to manage critical systems that cities depend upon, as well as improve quality of life for residents through safer and better designed urban environments.

While these are all important benefits, realising them will mean tackling a number of difficult challenges. The performance of the technology, in particular blockchain, will need to improve to be able to manage large-scale implementations. The larger and more interdependent these platforms become, the greater the cyber security challenges will be as well. There are also legal and regulatory hurdles that will need to be addressed, for instance around data protection legislation like the GDPR or with regard to the legal standing of blockchain-based transactions. Perhaps of most concern to many, at least in large-scale, public implementations like our smart city example, will be the safe and ethical use of data.

We think that technologists, entrepreneurs and researchers will be able to tackle these hurdles. Policy makers can help. To conclude our paper, we make a number of recommendations as to how. These include ensuring adequate funding for research, helping to foster and disseminate best practice and – if necessary – adapting regulatory processes. We also think that public/private partnerships could be good vehicles for research and development of these new types of platforms. Last but by no means least, we think policy makers should keep ethical considerations in mind, particularly within the context of smart cities and other large-scale platforms involving personal data. In this way we can avoid undesired consequences and truly reap the benefits that the convergence of these technologies can potentially bring.

Introduction

While our focus at the EU Blockchain Observatory and Forum is squarely on blockchain, we are well aware that blockchain does not exist in a technological vacuum. Rather, it takes its place among a host of significant breakthroughs in many fields – from quantum computing and 3D printing to biotech and nanotechnologies – that are significantly reshaping the world in which we live.

It is likely that many of these technologies will be used in conjunction with each other, "converging" in new kinds of platforms, products and services. To see how this might be the case with blockchain, in this paper we discuss the convergence of blockchain with two of the more important emerging technologies – the Internet of Things (IoT) and artificial intelligence (AI). We have chosen this triumvirate because we believe that there is great potential overlap and opportunity for them to work in concert to address a number of important use cases.

In particular, we believe that engineers, developers, entrepreneurs and government authorities, among others, will find it fruitful to combine these technologies in large-scale, often public and increasingly autonomous "convergent platforms"[1] that will on the one hand mirror the physical world and be increasingly able to manipulate it and on the other offer important new capabilities and properties not available outside the digital realm.

As we try and show in more detail below, each of these technologies can contribute important elements to the mix, and each also has pain points which could be addressed by the others. IoT devices, for instance, gather data from the environment (think sensors) and can be used to interact directly and autonomously with it (think smart locks, self-driving cars or robots). They can also be susceptible to hacking and, to be useful, need a means to securely transmit and receive information and interact with each other. AI in its various guises is, to a large extent, about autonomous analysis and decision making based on large data sets. But to be useful and safe, AI needs access to trustworthy data, ideally in privacy-preserving ways.

This is where blockchain can help. A technology designed to enable consensus on data among large groups, it can add a much-needed,

1 Here the term "convergent platform" means a platform that relies on blockchain and at least one of the other two technologies discussed in this paper – that is, that combines blockchain with AI and/or IoT in a significant way.

INTRODUCTION

native "trust" element to the digital realm. As a decentralised data store[2] based on consensus and an immutable ledger, blockchain can provide trusted, auditable records that large-scale communities can use as the basis for a single, agreed-upon version of the truth. Smart contracts run on blockchains can be used to automate transactions and processes, providing trust in agreements and confidence that instructions will be carried out as intended. By providing unique, non-forgeable, non-duplicable representations of people (digital identities) or objects (digital assets), blockchain can be used to forge strong, direct links between the physical and digital worlds in ways that have not been possible up to now.

Yet blockchains have their pain points too. To reach their potential as platforms for trusted information, blockchains often need ways to connect with the outside world in a secure and trustworthy way. To flourish as the backbone for large-scale, decentralised and highly autonomous marketplaces, they will increasingly need to become "smart". Here IoT sensors or AI tools can potentially be of great service.

In the following sections we examine how our three technologies can work together. We first look at how blockchain and IoT might interact with each other, and then how blockchain might interact with AI, before looking at the convergence of the three using the example of a smart city. We follow this with a short look at technological, legal and governance challenges and risks facing convergent platforms, and conclude with a set of recommendations for European policy makers looking to foster such platforms.

In the hope of making what are in many cases complex technologies and use cases more clear for the reader, we have made reference to a number of different projects and companies working in this space. We ask the reader to note that these are meant to be illustrative, and **do not in any way represent an endorsement by the Observatory, the European Commission, or the authors of this paper.** For each example there are many other projects of merit that could have served this purpose equally well.

2 Or, in many cases, an index for off-chain stores of data.

Blockchain and IoT

When we speak of the Internet of Things, we generally refer to networked-connected devices whose purpose is to gather and disseminate data autonomously and, increasingly, to act autonomously upon this data to carry out tasks, as for example a network-connected printer that orders its own supplies when they run low. For the sake of this paper we employ a very broad definition of IoT, including all types of connected sensors and meters, actuators (devices that do something in the physical world, like robots or drones) as well as the software that runs them.

While such devices have been around for a long time, we are currently experiencing an explosion in their numbers and significance. Current estimates indicate that there will be over 20 billion IoT devices in operation by the end of 2020, and that this should grow to over 60 billion by 2025.[1]

The IoT promises a great deal of benefit for how we live and our environment. This includes everything from consumer applications like smart homes or in-home elder care, to commercial applications in sectors like healthcare (the Internet of Medical Things) and transportation (self-driving cars), to smart manufacturing and automated farming, to infrastructure applications in construction, civil engineering, all the way through to smart cities.[2]

But realising this potential means overcoming a number of difficult challenges. Large-scale IoT implementations can mean managing data from and coordinating the activities of millions, perhaps even billions of devices. These need to be monitored and controlled, repaired when they malfunction, protected against manipulation, secured against hacking and the like. They are often at their most useful when they are autonomous, interacting directly with each other, which requires a secure, reliable means for communicating and transacting directly on a peer-to-peer (P2P) basis. As there are not only large numbers and types of devices, but also a large number of different manufacturers and platforms, these devices will need some common way of interoperating.

One way to handle this is through conventional, client-server-based approaches in which one centralised system handles the data and communications. While this model has worked up to now, the explosive growth of IoT threatens to stretch it to the limits. Centralised systems also represent single points of failure: if the system goes down, millions of devices and critical infrastructure could be threatened. Centralised approaches typically involve devices sending data to a cloud-based platform that analyses it and sends back instructions. This intermediation can lead to bottlenecks. Today, most of the major IoT platforms are offered by large tech companies.[3] Such proprietary platforms threaten vendor lock-in as well as exposing data to the vendor, which is not always desirable to customers. There is a great deal of innovation in IoT, meaning that, along with vast numbers of devices coming online, new types of devices are constantly appearing as well. Engineering a centralised system with sufficient scale and flexibility to meet the increasingly complex demands of the IoT environment seems a

1 Comprehensive Guide to IoT Statistics You Need to Know in 2019, vxchange, 26 July 2019.
2 See Wikipedia, Internet of Things#Applications.
3 Major platforms include: AWS IoT, Google Cloud IoT, MS Azure IoT, Oracle IoT, and IBM Watson IoT. Cisco, Bosch, and Salesforce all have IoT platforms and capabilities. See 10 Best IoT Platforms in 2018, DA-14, 9 May 2018.

daunting challenge for a single entity to meet.[4]

HOW BLOCKCHAIN AND IOT CAN WORK IN CONCERT

By employing blockchain with IoT we can potentially mitigate some of these issues, for example by replacing a centralised solution offered by a single vendor with a decentralised IoT platform developed and run by a consortium of interested stakeholders.

In such a setup, instead of routing all information through a centralised server, an individual IoT device on the network would package its data together with metadata like the device ID and a timestamp, hash the data and electronically sign it with its own private key and then send it to the blockchain. In this way the data would be both sealed (by the hash) and made uniquely identifiable and so findable (through the public key of the data record). It would then be shared throughout the network and available to all participants, whether humans or other devices.

This approach has certain advantages. It is highly scalable in the sense that it can grow organically: as long as they follow the protocol, new devices can come online as needed.[5] It is also more secure in the sense that there is no single point of failure. If one or even a multitude of nodes go offline, the remaining nodes will keep the network running. Such a platform could easily support trusted peer-to-peer data sharing between devices, facilitating machine-to-machine communications and transactions. This could eliminate the data bottlenecks found in centralised systems. As a community-built and -run platform, it also avoids issues around vendor lock-in and allows stakeholders greater say over who owns and controls data.

There could be other advantages too. As the unique identifier of the device interacting with the system is stored with the data, the blockchain could be used to secure the provenance of information entering the platform. This in turn could be used to create a history of data from an individual device and with it an audit trail of information. Such audit trails can help with monitoring the device, making it easier, among other things, to spot anomalies that could indicate either malfunction or manipulation. In a similar way, such a system could make it easier for IoT devices to verify the authenticity of information being sent to them, for example instructions to perform an action in the physical world, like opening a lock.

Such increased confidence in the quality of the data entering and leaving the chain is crucial, since blockchains are often used to provide a seal of approval for data and so can potentially magnify the potential damage caused by bad data entering a blockchain by accident or design. For example, if a temperature sensor on a refrigerated container containing food malfunctions or is manipulated it could erroneously report that the food was maintained at the correct temperature during shipping, providing a false sense of security in the quality of the shipment.

At the network and connectivity level, blockchain can help provide a common,

4 Atlam, et.al, Blockchain with Internet of Things: Benefits,Challenges, and Future Directions, International Journal of Intelligent Systems and Applications, 8 June 2018. (Retrieved at academia.edu)

5 This assumes that blockchain technology evolves to the point that it can handle the high volumes needed for many IoT settings. That is not the case today. See: Scalability, interoperability and sustainability of blockchains, EU Blockchain Observatory and Forum, 6 March 2019.

trusted communications layer between devices of different types and manufacture, supporting interoperability. Blockchain can also help harden the network, for instance by providing decentralised device logs, which are easier to audit and far harder to hack than centralised logs.[6]

Blockchain and IoT can also work in concert in the important task of providing verifiable identities to the real-world actors in the network. IoT devices are, for instance, often used to provide identity information for objects in the physical world. Fingerprint and iris scanners, face recognition devices and the like provide identities for persons; GPS trackers, built-in sensors, QR codes, etc., do the same for objects. Once identifications have been generated, blockchains can be used to secure a tamper-proof link between them and their source.

At the application level, blockchain can work with IoT in facilitating autonomous machine-to-machine transactions. Smart contracts can be deployed that allow machines to hold funds, make decisions based on complex business logic and carry out transactions, often using blockchain-based tokens or cryptocurrencies as a means of payment. Such capability could also make it easier to manage devices remotely, or to have them manage themselves, for example by caring for their own maintenance, while ensuring a trusted connection to the device and a trusted audit trail of what it has been doing.

COMBINING BLOCKCHAIN AND IOT

TODAY

Using these ingredients, blockchain and IoT can converge in the service of new kinds of applications and business models.

Consider a temperature sensor attached to a refrigerated smart-container in a cold supply chain[7] that constantly sends temperature data to a blockchain-based supply chain platform. This information can be transmitted via the blockchain to the actors involved, from the producer through regulatory authorities to the buyer, all of whom could monitor the condition of the shipment in real time. The container in turn could be outfitted with a smart lock that only allows it to be opened if it receives instructions from the blockchain-based platform that all involved have signed off on the shipment. Information transmitted to the blockchain that the lock has been opened and the buyer has accepted the shipment could in turn trigger an automatic, smart-contract-based payment to the producer via a cryptocurrency or stable coin.

We could envision a blockchain-based decentralised apartment-sharing platform in which short-term renters and tenants deal directly with each other without any intermediary. Along with using blockchain-based identities and, perhaps, reputation scores to allow renters and tenants to negotiate in a trusted way, and smart contracts to handle registration, deposits and payment, IoT scanners could be employed at the rental properties themselves to allow guests to identify themselves. After receiving authorisation from the platform, these could

6 Blockchain-Based Secure Device Management Framework for an Internet of Things Network in a Smart City, Seonghyeon Gong , Erzhena Tcydenova , Jeonghoon Jo , Younghun Lee and Jong Hyuk Park, Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 08826, Korea, 17 July 2019.

7 For more on blockchain and supply chain, see our report Blockchain in trade finance and supply chain, EU Blockchain Observatory and Forum, 9 December 2019.

BLOCKCHAIN AND IOT

activate smart locks to open the property. Sensors, video cameras or other devices inside the property could also be used to verify that a tenant has not only left at the right time but has also left the property in good condition. Once this has been determined, the devices could trigger the release of a security deposit held in escrow in a smart contract.

And these are just two of many, many use cases that might have been cited. The potential seems quite large, and is reflected in the amount of activity and investment we are seeing in this area.

Again, just to cite a few examples: on the protocol level, IOTA[8] is being developed specifically to support IoT and the machine economy at scale. Airalabs is building its Robonomics Network on top of Ethereum to provide support for smart cities and Industry 4.0 by aligning "the abilities of robots with the needs of people".[9] Companies like Modum,[10] Ambrosus[11] and Slock.it[12] are also building platforms to connect devices to blockchains for use in supply chains and other contexts.

Other companies are focusing on specific use cases. The mobility sector is one that has proven quite fruitful so far. HireGo,[13] for instance, is a car-sharing platform run on a blockchain, while in Switzerland AdNovum[14] is working with the University of Zurich, the Lucerne School of Information Technology (which is an academic partner of the EU Observatory) as well as industrial partners, insurance companies and government on Car Dossier, a blockchain-based "digital dossier" to securely store data from a vehicle's life cycle.

Energy is another promising use case. At the EU Blockchain Observatory and Forum workshop on the Convergence of blockchain with AI and IoT,[15] the Paris-based company Ledger[16] told how it had partnered with Engie to develop the first blockchain-based hardware to secure data at the source of energy production. In the solution, custom-built sensors are attached to solar panels and provide trusted data to the blockchain regarding how much energy the panel has produced. The sensor has a secure hardware element that takes the data and creates a record using the same fields as would typically be needed for a green energy certificate under EU law. This data record is then secured via hashing and sent to the blockchain.

8 https://www.iota.org/
9 Robonomics: P2P Technologies for Roboteers, Medium, 10 January, 2019.
10 https://modum.io/
11 https://ambrosus.com/
12 https://slock.it/
13 https://www.hirego.io/
14 https://www.adnovum.ch/en/innovation/blockchain_car_dossier.html

15 See Workshop Report: Convergence of Blockchain, AI and IoT, EU Blockchain Obsevatory and Forum, 12 April 2019.
16 https://www.ledger.com/origin/

Blockchain and AI

In this section, we discuss the convergence of blockchain with AI. Before we begin, a note on terminology. As this is a high-level overview, we are using a broad definition of AI as "intelligent machines or software agents that can analyse and process information in some autonomous way, often resembling the way human beings carry out similar tasks". In a similar vein, we refer to "AI models" to broadly mean various kinds of more or less domain-specific machine-learning techniques, and refer at times to "an AI" as a machine or agent that has been or is being so trained.[1] Finally, our reference is for the most part to what is known as "weak AI", or AI trained on data sets to complete specific tasks or solve specific problems, like facial recognition. In some cases, we discuss "strong AI" or artificial general intelligence (AGI), meaning machines that can think at a level on a par with or superior to that of humans. While AGI is still in the research phase, there are increasing expectations among many researchers that this goal is eventually attainable. As with weak AI, AGI raises a number of issues for which blockchains may be relevant.

HOW BLOCKCHAIN CAN SUPPORT AI

To understand how blockchain can support AI, we can look along what we might call an AI value chain involving raw materials (data), production (training AI models) and distribution (the use of AI analyses and decisions).

Democratising AI through decentralised data markets

We start with data, the raw material of AI. As is well known, to be useful, AI models need to train on massive amounts of data. Unfortunately, accumulating and storing enormous data sets as well as finding and hiring qualified AI and data experts to work with them is a complex and extremely expensive endeavour. As a result, the value of AI is being concentrated in the hands of the few companies or organisations with the requisite resources.[2]

The challenge lies both in the exponential rates at which data is being created today, as well as the fact that there are no generally accepted data-sharing standards, meaning data often remains locked in silos. Furthermore, much of the high-value data for AI is sensitive personal information (for example health records), and so is either protected by regulation or the understandable reluctance of individuals to share it. Enterprises also generate a great deal of potentially valuable data that they may be reluctant to share for business reasons.

Those enterprises or individuals interested in selling their data will find that there is no readily available means for them to monetise it or control the use of their data once it has been sold. On the other side of the equation, procurers of data face quality issues, as it is often difficult for data gatherers to trace the provenance of data or judge its merits.

Blockchain could help address many of these

1 We are aware that these terms as used here are inexact, and that we risk oversimplifying a complex technology. We ask the reader's indulgence as we have done so only for the sake of expediency.

2 These are generally large technology companies. See The 15 most important AI companies in the world, Towards Data Science (Medium), 28 January 2019.

BLOCKCHAIN AND AI

issues by supporting the development of decentralised, open markets for AI training data. Blockchains can be used to identify and permanently record individual data points and small data sets at their point of origin, making it possible for information owners or aggregators to package the data they generate. Blockchains could also be used to provide the wrapping around larger data sets, recording their provenance and securing them against tampering. Once packaged, it becomes easier for individuals or organisations to sell, rent or share their data as they choose. This not only provides a more level playing field for data producers, it could also improve the quality of the data as producers would be incentivised to ensure the quality of their offering so as to attract buyers.

This is the idea behind the Ocean Protocol.[3] As described in its white paper, Ocean is a "a decentralized protocol and network of artificial intelligence (AI) data/services. It aims to spread the benefits of AI, by unlocking data while preserving privacy."[4] The Ocean Protocol provides what it calls service execution agreements and decentralised access control to allow AI models to be brought to data to train (as opposed to sending the data to the model), so that the models can learn on the data without it ever leaving its premises (instead the model leaves only with the results of the computation). Ocean also has its own currency, the Ocean Token, to provide economic incentives for sharing and developing the platform, as well as a Curated Proofs Market which provides a reputation-based means of ensuring data quality. As the project describes it, these and other capabilities are intended to create a network that "can be used as a foundational substrate to power a new ecosystem of data marketplaces, and more broadly, data sharing for the public good".

Blockchains could in theory be used to support very large, very broad, highly decentralised data stores that are not curated by humans but rather grow on their own. There are those who believe that any data set that is developed or curated by humans will have inherent limitations, and therefore be a barrier to the development of truly independent, general AI. Decentralised data, it is argued, is therefore a prerequisite for a truly decentralised AI neither restricted by the choices nor influenced by the conscious or unconscious biases of its creators or some centralised entity.[5]

Level playing field for AI developers and entrepreneurs[6]

Just as with AI training data, AI research and development – at least for commercial applications – is dominated by large tech companies. This is not due to a lack of independent expertise. There are many AI researchers in academia and the startup community doing groundbreaking work and developing excellent algorithms. But they face hurdles when it comes to moving their work from the drawing board out into the real world.

One hurdle – accessing data – could be addressed by the decentralised data markets described above. Another way for independents to compete with larger organisations is by collaborating with each other. But the AI tools environment is

3 https://oceanprotocol.com/

4 Ocean Protocol: A Decentralized Substrate for AI Data & Services, Technical Whitepaper, Ocean Protocol Foundation, 15 April 2015. This paper informs much of this section.

5 See Hosp, Julian. Blockchain 2.0 Simply Explained, 1. Edition 2019.

6 This section is heavily indebted to the SingularityNET: Whitepaper 2.0, SingularityNET, February 2019.

BLOCKCHAIN AND AI

fragmented, and there are no widely accepted standards for collaboration or interoperability between AI models.

Another hurdle is the fact that there is no broad-based marketplace for independent AI services. AI researchers also tend to be academics and not businesspeople and so may lack the skills needed to sell their products in traditional markets. Last but not least, successfully training models on large data sets requires a great deal of computing power, which is often prohibitively expensive for researchers or startups.

The result of this is that much innovative work either remains in white papers or in prototypes, or, for lack of other options, is sold on to one of the tech giants, further concentrating the market.

Blockchains could help stem this tide by providing decentralised platforms for the development and dissemination of AI models, tools and services. In a way similar to what we saw above with data markets, blockchains could provide a neutral collaborative environment that is shared by its users. Such platforms could provide identity, authentication and verification services, as well as economic incentives through cryptocurrencies and automation through smart contracts. The result would be more people developing AI models, and potentially more innovation.

This is the vision of SingularityNET.[7] Designed to be a "protocol for networking AI and machine learning tools to form highly effective applications across vertical markets", the project aims to transform AI from a "corporate asset to a global commons".[8] To do so, it will on the one hand create a commercial launchpad for AI developers that will give them an easy path to market the way that app stores do for mobile developers. On the other, it will provide tools that allow AIs to interoperate and so learn from each other and develop an intelligence and capabilities greater than the sum of their parts.

Other companies are using blockchain to tackle the computing resources problem. iExec,[9] for instance, provides a decentralised cloud computing service that can be used by AI developers.[10]

Spreading the benefits of AI

Finally, blockchain could be employed in the distribution side of AI, by making it easier for more people to benefit from AI results.

As with the data and model markets above, blockchains could be deployed as the infrastructure to provide broad access to trained AI models for individuals and companies, potentially reducing costs and increasing the number of people able to make use of these services. Such services markets can be very interesting, for instance for enterprises who have data but no access to the necessary AI expertise.

The platforms mentioned above all provide AI services marketplaces to one degree or another. Microsoft has also recently released a proposal to use blockchain as the basis for a platform on which "people will be able to easily and cost-effectively run machine learning models with technology they already have,

7 https://singularitynet.io/

8 SingularityNET white paper. Op Cit.

9 https://iex.ec/

10 Both SingularityNET and iExec presented at our Convergence workshop. See the workshop report, Op. Cit., for an overview as well as links to the videos.

BLOCKCHAIN AND AI

such as browsers and apps on their phones and other devices".[11] Here the blockchain is used to both provide trust and security in the data as well as incentives for participants to contribute data.

Blockchains can also support privacy-preserving methods for training AI models and making their results available. These approaches often involve "sending compute to data"[12] or renting data. At an EU Observatory workshop last year, iExec presented a pilot that combines blockchain with trusted execution environments on chips and other technologies to send AI models to hospitals to be trained on brain scan data, and then send the results to clients without the data leaving the hospital or being revealed.[13]

Another important contribution blockchain could make to AI is in supporting transparency of AI models and decision-making. Most AI models are a black box: data goes in and answers or analysis come out, but the learning process remains obscure. While blockchains cannot solve this problem, a blockchain-based data set, with clear data provenance and audit trails, can provide transparency and potentially a degree of traceability of data when it enters a model and is used by it. This could contribute to the "explainability" of AI decisions by increasing our understanding of how these systems work, and so increase trust in AI outcomes.

HOW AI CAN SUPPORT BLOCKCHAIN

AI can also support blockchain in many ways.

At the protocol level, various types of AI methods to analyse and learn from large data sets could be used to increase security. AI, for instance, could be employed at the data "on ramp" to run plausibility tests or detect anomalies, potentially identifying bad or malicious data before it enters the chain. One example could be to use AI analysis techniques to coordinate between different IoT devices that are acting as oracles (data sources) for blockchain-based platforms and/or smart contracts. Such analysis could improve quality by providing a consensus-view of the data and increase security by helping to more easily identify malfunctioning or malicious oracles.

The ability to detect anomalies or otherwise monitor complex systems can also improve security for blockchain platforms. AI-based learning systems could be employed to detect attacks on a blockchain. AI could also conceivably be used to make blockchain protocols more performant. For example, it could monitor transaction levels and potentially increase the frequency of block creation during peak periods, or be used to better employ some of the newer performance-enhancing mechanisms, like sharding, by better sharing loads across the network.[14]

AI could also be of great assistance in helping make smart contracts more secure by analysing them for flaws. As models learn from each smart contract audit, we can expect their ability to detect bugs in smart contracts to continuously improve. We could

11 Justin D. Harris, Leveraging blockchain to make machine learning models more accessible, Microsoft Research Blog, 12 July 2019.
12 Op. Cit.
13 EU Blockchain Observatory & Forum Workshop Report - Convergence of blockchain, AI and IoT, Brussels, 28 March 2019

14 Sharding, a technique common in conventional database technology, is seen as one way to increase blockchain performance. In sharding, you break down the data to be processed into different partitions (shards) and have part of the network validate the individual partitions, thus allowing for parallel processing. For more see Scalability, Interoperability and Sustainability of Blockchains, EU Blockchain Observatory and Forum, 6 March 2019.

BLOCKCHAIN AND AI

also potentially employ AI to run simulations to detect unintended consequences of the business or process logic encoded in the smart contract before the smart contract is deployed.

Along with making smart contracts more secure, AI could help make them truly "smart". AI could be used to add more sophisticated analysis and decision-making capabilities to smart contracts, helping them better understand their environments, learn from past experience and so make better decisions or deal with more sophisticated or complex contingencies. This could lead to increased automation and autonomy for smart contracts and software agents based on them.

In a similar vein, AI could be employed in large-scale blockchain platforms to make the platforms themselves smarter. In a global, blockchain-based supply chain platform, for example, an AI could monitor the platform to detect patterns and anomalies, potentially isolating bottlenecks or discovering safety issues faster than humans can. This could help fight fraud and increase safety, as well as help increase efficiencies and support better contingency management. Blockchain and AI could also help secure blockchain-based financial services platforms in the AML/CFT process by tracing transactions and trying to detect AML/CFT risks.

Smart cities: Convergence in action

In the previous two sections we have tried to demonstrate the synergies between blockchain and IoT and between blockchain and AI. In this section we would like to show some of the benefits that could be gained when all three of these technologies are simultaneously brought to bear on a problem. To illustrate these benefits we use the example of a smart city – that is, a city where there is a concerted effort to use information and communications technologies, including sensors and smart devices, along with advanced analytics to help plan and manage city infrastructure and improve quality of life for residents.

A smart city provides an excellent proving ground for our purpose. Modern cities are large, highly complex, interconnected systems that combine different types of often critical infrastructure, like energy, transportation or waste, with complex, interconnected social and economic systems. They are highly dynamic as well, growing at a rapid pace as the world urbanises. Pertinent to our context, smart cities are also highly dependent on data.

Managing this complexity while keeping control of costs and risk and ensuring the needs and rights of citizens are met is a daunting task. We think blockchain can work with IoT and AI to meet the challenge through utilising some of the decentralisation, automation and data-management capabilities we have already discussed.

To take some examples, in a smart city blockchains could serve as the intermediary identity and authorisation layer between IoT devices, like sensors, and AI-assisted infrastructure administration systems, and potentially, through smart contracts, an automated control layer. Blockchains could also be employed as a secure data storage or data coordination platform for heterogeneous data sources, providing data validation and/or managing access to off-chain data repositories. As the data captured for the registration in a blockchain is in general very well structured, it would help AI use this data in real time and support decisions about coordinating city activities or dealing with malfunctions or emergencies. On a macro level, blockchains could also potentially be used as a data substrate to link many smaller, purpose-built systems together into larger systems, turning "fractionally smart" cities, as one writer has put it, into "overall intelligent" ones.[1]

SMART CITY USE CASES: MANAGING INFRASTRUCTURE

On an infrastructure level blockchain could be combined with AI and IoT to manage the critical systems that cities depend upon, as well as automate processes and, where possible, make it possible for these systems to more easily work in concert with each other.

Take, for example, energy and waste management. Here the blockchain layer could help with secure data collection from

1 Smart cities will succeed through systematic planning and a focus on economic vitality, Smart Cities World, 25 November 2019.

sensors fed into an AI that makes decisions about waste pickup and control, smart or green energy, shoring up the power grid and the like. Blockchain could also help facilitate P2P energy markets within the city, in which individuals could buy and sell their excess energy locally, helping to make the city more self-sufficient. Such use cases are already live. Thanks to startups like GridPlus;[2] residents in Texas can buy their energy using a blockchain and AI powered solution that buys and sells energy locally at the best moment and rate.

Sensors, AI and blockchain could also work together in improving public transport. Through people counters and/or blockchain-based online payment systems, as well as other means, the city would have a great deal of real-time data on public transport patterns. This could be used by an AI to manage the system in real time as well as to assist planners in designing improvements and expansions. We can also imagine smart city maintenance systems relying on blockchain, AI and IoT to automate maintenance tasks as well as plan and schedule preventive maintenance work through smart machines. Since blockchains are by their nature transaction platforms, they could also be used to coordinate maintenance operations performed by humans too, providing a platform for validating the credentials of sub-contractors, assigning tasks, bidding for contracts and paying for work done.

These three technologies could help cities with innovative new approaches. For instance, they could help smart cities "help themselves" by supporting self-optimising systems through market-based learning approaches. Consider the following scenario. In the near future, we assume that one feature of smart cities will be fleets of autonomous, self-driving taxis (for the purpose of this example considered to be IoT devices). The individual cars could be outfitted with a specialised AI model optimised to maximise revenues and minimise costs. Yet to do so successfully, they must have data about successful strategies on which to train themselves. We further assume that the most succesful strategies will be those that optimise for the best quality service at the lowest price. A blockchain-based data market would allow the cars in the fleet to transact with each other, buying and selling their ride data using tokens. The more successful cars could also sell their trained algorithms – their knowledge – to the others via the platform, and those successful models would then presumably propagate themselves through the network. This in turn could result in a continuously improving taxi service for residents as the cars become smarter and more attune to their clients' needs and wishes.

SMART CITY USE CASES: QUALITY OF LIFE

For residents, blockchain could work together with AI and IoT to contribute to quality of life through, among other things, safer and more well-designed urban environments. For example, they could help cities better prepare for and deal with emergencies, such as fire or extreme weather, by combinging AI-based monitoring and predictive modelling with autonomous emergency response via connected devices. Human first responders to medical emergencies could be outfitted with devices that access individual medical records of victims in a privacy-preserving way via a blockchain, improving the quality

2 See https://gridplus.io/energy

SMART CITIES: CONVERGENCE IN ACTION

of first aid.[3] A convergent system could help with urban planning as well, with IoT sensors and other devices gathering on people and traffic patterns, population densities, infrastructure usage and the like, and feeding that through the blockchain to the AI which helps analyse and make predictions for future use. Blockchain-based e-voting and citizen participation platforms[4] could make it easier to involve local communities and neighbourhoods in urban planning as well, providing a platform for gathering feedback and perhaps even voting on proposed projects. Blockchain-based platforms could also be used to incentivise residents to behave in desirable ways, for example by offering rewards for using public transportation or clearing up litter.

Public healthcare and social services is another area that could benefit hugely from applying blockchain, AI and IoT. This could be everything from smarter, more efficient systems for entitlements though using data analytics and artificial intelligence to improve both services and health care strategies.[5]

Such convergent smart city platforms could also be used to improve quality of life for residents. To take just one example, we can imagine a smart city parking system. In this scenario, IoT sensors deliver information on free parking spots. AI analyses this information and combines it with current traffic patterns and potentially other relevant information, like an event in the city that day that could lead to increased demand for parking, and uses this to project availability. Using a smartphone, a resident queries the system and receives a recommendation on the best place to park at a given time and location. The blockchain would be used, as in all our scenarios, as the communications layer, but could also be used to handle a parking reservation, "unlock" a parking spot via a smart lock and potentially handle payment.

3 Are Smart Cities The Pathway To Blockchain And Cryptocurrency Adoption?, Forbes, 18 October 2019.

4 Interesting examples of such citizen participation platforms already deployed in cities today include Better Reykjaik and Decidim.

5 Blockchain Revolution in the Governance of Nations and Cities, Stefan Junestrand, OpenLedger Insights, 19 March 2019.

Challenges and Risks

In this section we look at some of the challenges to be overcome and the risks inherent in the convergence of blockchain with AI and IoT. We look at this through three different lenses: a) technology, b) legal and regulatory questions, and c) issues around governance, privacy and data ethics.

TECHNOLOGICAL

The first challenge in building convergent systems will be to ensure the necessary infrastructure.

Individual technologies will need to be performant. This is currently an issue particularly with blockchain, which is still a very young technology and faces scaling and interoperability challenges.[1] The underlying infrastructure needs to be performant too: that means hi-speed connectivity, innovation in devices, improvements in computing technology and so on. Large-scale use cases, such as smart cities or global supply chains, will depend on the appropriate infrastructure being available to all stakeholders. That in turn will require both the appropriate funding as well as research and development efforts, along with timely and forward-looking infrastructure planning.

A key challenge will be achieving interoperability between different technologies. We have written of blockchain, AI and IoT working in concert as if this went without saying, but the devil as always is in the detail. There will be a need for interoperability between large-scale platforms too. If, to take one example, successful smart cities built on blockchain, AI and IoT-based platforms want to come together to form smart regions, these platforms will need to talk to each other. This will be a tall order not only for technologists, but for policy makers and standards bodies as well.

Large-scale convergent platforms will have to deal with serious security challenges and risks too. Designers will need to assure adequate cyber security for all parts of the system – a task which grows more difficult the larger the platform becomes. They will need to ensure adequate data privacy while allowing for the legitimate use of data for the common good. Finally, in a large-scale system mistakes can be not only costly, but also highly disruptive to people's lives and rights. Engineers will have to focus strongly on preventing unwanted or dangerous outcomes, particularly where there is a high level of automation.

They may also have to face new kinds of risks specific to the combination of blockchain with AI and IoT. In our report on the legal and regulatory framework of blockchain and smart contracts we pointed out some of the legal issues with self-executing smart contracts that, once deployed, cannot be altered or shut down. If such smart contracts are used to control infrastructure through IoT, and if an equally unstoppable AI were deployed in the smart contract as well, the damage from a bug or simply unintended consequences could be severe.[2]

1 See: Scalability, interoperability and sustainability of blockchains, EU Blockchain Observatory and Forum, 6 March 2019.

2 See: Legal and regulatory framework of blockchains and smart contracts, EU Blockchain Observatory and Forum, 27 September 2019.

CHALLENGES AND RISKS

LEGAL AND REGULATORY

Turning to the legal and regulatory side, we can identify a number of challenges and risks as well. Many of these are associated with blockchain. As we have written about elsewhere, the open, decentralised, often permissionless, transparent nature of blockchains can raise a number of tricky legal and regulatory questions. These range from how to reconcile a communally controlled, immutable ledger with the personal data protection requirements of a regime like Europe's GDPR, to questions around the legally binding status of data and transactions carried out on blockchains, to questions of applicable law in large-scale, cross-jurisdictional platforms, to questions regarding the legality of and liability around actions taken by blockchain-based autonomous agents. Many of these carry over to convergent platforms, where blockchains may form part of larger autonomous systems that take in data, evaluate it, and take actions and make transactions at their own discretion.

Liability is likely to prove a particular challenge. In our previously mentioned legal report[3] we found the question of liability in blockchain-based platforms to be one of the most complex issues. There are also questions of liability in AI-based decision making. If we cannot know how a machine made a decision, who can we turn to if the decision turned out to be wrong or dangerous? Is it the developer of the model? The model itself? Those who chose to employ it? The larger convergent systems become, and the more autonomous they are, the more likely we are to be faced with deciding difficult questions like these.

3 Op. cit. EU Obser atory paper on legal and regulatory framework of blockchains.

GOVERNANCE, PRIVACY AND DATA ETHICS

The types of large-scale systems combining blockchain, AI and IoT that are under discussion here raise important questions in terms of governance, privacy and data ethics. Here again smart cities can serve as an example. Consider a smart city-wide mobility system using a combination of blockchain, AI and IoT to adjust public transportation availability to demand, propose alternate routes to drivers in real time and adjust traffic lights for optimal traffic flow.[4] While contributing greatly to quality of life, such a system raises significant privacy and data ethics issues as the movement of every citizen can potentially be recorded.

Such concerns have indeed already been raised with respect to some early projects, for example with Google's plans to develop smart city infrastructure for Toronto.[5] For public use cases like this, it could be possible to use blockchain to replace a centralised, for-profit provider with a decentralised, community or consortium-built platform. While that might alleviate some types of concerns, as we intend to look at in detail in an upcoming paper, governing decentralised platforms comes with its own set of hurdles.

4 We discussed such a scenario in our workshop. See EU Blockchain Observatory & Forum Workshop Report -Convergence of blockchain, AI and IoT, Brussels, 28 March 2019.

5 'City of surveillance': privacy expert quits Toronto's smart-city project, The Guardian, 23 October 2018.

Conclusion and recommendations

In this paper, we have tried to demonstrate potential synergies between blockchain, AI and IOT. To reach this potential, we make the following recommendations for policy makers.

1. Ensure adequate and targeted funding.
All technological evolution requires funding. We recommend that Europe look to fund research on existing convergence use cases, to see what real benefits they have brought and then to look deeper into ways to solve the problems that have been identified.

2. Promote best practice and responsible ownership of these technologies.
Considering the far-reaching nature of the platforms described here, we think authorities should pay extra attention to promoting both best practice and responsible ownership of these technologies and the applications that are built on them. Governments could support these learnings and facilitate testing through such means as regulatory sandboxes and innovation offices.

3. Consider any adaptation of regulatory processes.
If and where relevant, authorities might want to rethink and potentially redesign existing regulatory and monitoring/auditing processes to meet the demands of these new types of platforms.

4. Promote private sector engagement and public/private partnerships.
Private sector engagement with policy makers will also encourage greater interoperability as well as knowledge sharing, which is a key to achieving innovation at scale. We would in particular encourage public/private partnerships, especially in larger, infrastructure-type use cases.

5. Provide regulatory clarity.
Wherever possible, governments should seek to provide regulatory clarity for innovators, and make a strong effort to publicise and educate innovators on the prevailing regulatory environment.

6. Do not regulate too early.
While regulatory clarity is good, as always, regulating too quickly in emerging technologies can hinder innovation. Policy makers should look to strike the right balance between protection and promotion.

7. Consider the ethical issues.
There are enormous ethical considerations in the use cases discussed here, particularly within the context of smart cities and other large-scale platforms involving personal data. These should also be highlighted for examinaition by policy makers, who should look to prevent undesired consequences for society at large, and in particular vulnerable individuals and groups.

8. Consider regulating the activity, not the technology.
When creating or adapting regulatory and legal frameworks to cover activities powered by new and emerging technologies there should be a clear focus to regulate the activity undertaken, not the underlying technology. Technology neutral regulation has the potential to be more sustainable and is less prone to blocking future innovation.

Appendix – Blockchain Terminology

What is a blockchain?
Blockchain is one of the major technological breakthroughs of the past decade. A technology that allows large groups of people and organisations to reach agreement on and permanently record information without a central authority, it has been recognised as an important tool for building a fair, inclusive, secure and democratic digital economy. This has significant implications for how we think about many of our economic, social and political institutions.

How does it work?
At its core, blockchain is a shared, peer-to-peer database. While there are currently several different kinds of blockchains in existence, they share certain functional characteristics. They generally include a means for nodes on the network to communicate directly with each other. They have a mechanism for nodes on the network to propose the addition of information to the database, usually in the form of some transaction, and a consensus mechanism by which the network can validate what is the agreed-upon version of the database.

Blockchain gets its name from the fact that data is stored in groups known as blocks, and that each validated block is cryptographically sealed to the previous block, forming an ever-growing chain of data. Instead of being stored in a central location, all the nodes in the network share an identical copy of the blockchain, continuously updating it as new valid blocks are added.

What is it used for?
Blockchain is a technology that can be used to decentralise and automate processes in a large number of contexts. The attributes of blockchain allow for large numbers of individuals or entities, whether collaborators or competitors, to come to a consensus on information and immutably store it. For this reason, blockchain has been described as a "trust machine".

APPENDIX – BLOCKCHAIN TERMINOLOGY

The potential use cases for blockchain are vast. People are looking at blockchain technology to disrupt most industries, including from automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel. While blockchain is definitely not the solution for every problem, smart contract automation and disintermediation enable reduced costs, lower risks of errors and fraud and drastically improved speed and experience in many processes.

Glossary

The vocabulary used in the context of blockchains is quite specific and can be hard to understand. Here are the essential concepts you should know in order to navigate this breakthrough technology:

- **Node:** A node is a computer running specific software which allows that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network.
- **Signature:** Signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography allows someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key.
- **Transaction:** Transactions are the most granular piece of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network, a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that the transaction content has not been manipulated while being transmitted over the network.
- **Hash:** A hash is the result of a function that transforms data into a unique, fixed-length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data.
- **Block:** A block is the data structure used in blockchains to group transactions. In addition to transactions, blocks include other elements such as the hash of the previous block and a timestamp.
- **Smart contract:** Smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus leveraging the trust and security of the blockchain network. They allow users

APPENDIX – BLOCKCHAIN TERMINOLOGY

to automate business logic and therefore enhance or completely redesign business processes and services.

- **Token:** Tokens are a type of digital asset that can be tracked or transferred on a blockchain. Tokens are often used as a digital representation of assets like commodities, stocks and even physical products. Tokens are also used to incentivise actors in maintaining and securing blockchain networks.
- **Consensus algorithm:** Consensus algorithms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means depending on the specific needs. The most famous consensus algorithms include proof-of-work, proof-of-stake and proof-of-authority.
- **Validator nodes:** Validator nodes are specific nodes in a network that are responsible for constituting blocks and broadcasting these blocks with the network. To create a valid new block they have to follow the exact rules specified by the consensus algorithm.

Learn more about blockchain by watching a recording of our Ask me Anything session.