SCALABILITY INTEROPERABILITY AND SUSTAINABILITY OF BLOCKCHAINS

a thematic report prepared by

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM

EU Blockchain 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.
- 'Blockchain scalability, interoperability and sustainability' by Arthur Gervais – an academic research paper prepared by the Lucerne University of Applied Sciences and Arts – an academic partner of the EU Blockchain Observatory & Forum. Available online at www.eublockchainforum.eu/reports.
- Input from participants at the 'Scalability, interoperability and sustainability' workshop held in Berlin on 2 October 2018.
- 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, Ken Timsit
Thematic Report Series Editor: Tom Lyons
Workshop moderator: Reto Peter Gadient
Report design: Benjamin Calméjane

v1.0 - Published on 6 March 2019.

DISCLAIMER

ACKNOWLEDGEMENTS

The authors would like to expressly acknowledge the following for their direct contributions and feedback to this paper:

Observatory Working Group Members:
- Javier Sebastian Cermeño
- Tamás Chlepkó
- Cristina Carrascosa Cobos
- Arnaud Le Hors
- Phillip Sandner
- David Suomalainen
- Konstantinos Votis
- Vlad Zamfir

Scalability Workshop Panelists:
- Peter Broadhurst
- Cyril Cassagnes
- Jesus Ruiz
- Gilbert Verdian

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

In this paper we take a look at the current and likely future state of blockchain in Europe through the lens of large-scale blockchain platforms. Along the way we ask ourselves what factors, technical and organisational, are likely to shape how platforms develop, and make some observations and recommendations for entrepreneurs and policy makers about best practice.

The timing seems right for such a paper. The blockchain ecosystem has been steadily maturing over the past several years, and projects are getting both larger and closer to going live, or have already dones so. This is exciting, as we can expect several large platforms to attract significant user bases over the course of the year. Observing these projects and the development of the technology also allows us, perhaps for the first time, to see the outlines of what a "live" blockchain ecosystem might look like in the near term, as well as identify the main challenges and success factors involved.

Our vision is that **the first wave of blockchain adoption will be characterised by a large number of permissioned, purpose-built blockchain platforms geared towards a specific use case** or user base. These blockchains will, however, not be completely walled off gardens. Instead, they will need to interact with the off-chain world as well as with each other. Just as TCP/IP and the rest of the Internet stack became the open, freely accessible backbone of the Web of Information, we think that a small number of global blockchain networks will also emerge as the backbone of a Web of Value. To get there, the blockchain community will need to solve an array of challenges that we have gathered into three categories:[1]

- **Scalability**: the ability to handle large volumes of transactions at high speeds.
- **Interoperability**: the ability to exchange data with other platforms, including those running different types of blockchains, as well as with the off-chain world.
- **Sustainability**: a) the ability to run a large-scale blockchain platform or decentralised application in an environmentally responsible way, and b) the ability to govern projects, platforms and the core technology in such a way that they remain viable over the long term.

1 Note that, while they represent important challenges for the blockchain ecosystem as well, we do not explicitly address issues of privacy and confidentiality in this paper. We intend to handle these themes as part of our workshop and thematic report on security to be held in the second half of 2019.

EXECUTIVE SUMMARY

A lot of time and effort is being expended on surmounting the above challenges, and we examine each in some detail both in the main text and in a series of technical "deep dives" in our appendix. Privacy and confidentiality, the last main technical discussion not mentioned so far, will be covered extensively in another paper.

As an increasing number of large projects reach maturity, we can also begin to identify the characteristics of the successful ones. In sum, **we believe that projects need a clear vision of what they want to accomplish, a clear reason for using blockchain instead of traditional database technology, and strong governance structures that provide clarity on roles and responsibilities** and support collaboration and sharing of effort and expertise among diverse stakeholders.

We think government can play a role in fostering success as well through supporting the development of the base blockchain infrastructure. We therefore take a look at the key success factors for such an infrastructure, and some of the principles we believe policy makers should follow to support its development.

We end with a set of recommendations as well. First priority remains basic research: Europe has been very supportive in this area, but there is much still to be discovered and developed. To ensure its place as a leader in this new technology, Europe will need to continue to fund work on next-generation solutions. As blockchain matures, there will be an increased need for standards both for the technology as well as how best to work with it (governance). Getting this right will require a balancing act between harmonisation and fostering technical diversity. We therefore believe that a light-touch approach, allowing for experimentation, is the right one for the moment. Last but not least, we believe European governments need to be open to these changes, employing blockchain themselves in government services where it makes sense and so preparing themselves for the potential mass adoption of this technology.

The good news is that Europe already has a relatively good track record in all of the above. That makes us optimistic that our vision of a maturing ecosystem on the brink of mass adoption is a correct one.

Introduction: The blockchain landscape in Europe

Survey the blockchain ecosystem in Europe today[1] and you will find an impressive number of startups and projects building platforms and decentralised applications, not to mention literally thousands of white papers, proofs of concept and Github repositories. You will also find a vast and vibrant community of associations, non-profit organisations, foundations, meetups and local, national and supranational government initiatives working to further the development and adoption of this new technology. What is harder to find are live platforms or applications with large, active user bases.

We think this is about to change.

If 2016 was the "year of education", when people learned about blockchain and its uses, 2017 the "year of proofs-of-concept", during which people experimented to validate theses, and 2018 the "year of large-scale projects", with a number of significant projects announced and in development, there is now very good reason to believe that 2019 will indeed be the "year when projects go live", with a number of major platforms slated to go or already in production.

A by-product of this evolution is a bit more clarity: we begin to see the outlines of what the technology and ecosystem will look like in the near future, what the hurdles to mass adoption are, and what some of the best practices and success factors for surmounting these hurdles are likely to be. This, broadly speaking, is the subject of the present paper.

A MULTIVERSE OF CHAINS

So where is blockchain adoption headed in the near future?

From today's vantage point, it seems likely that the first successful implementations of large-scale, live blockchain platforms will come in the form of very efficient, "permissioned" blockchains developed by

1 A good place to start is the 'EU Blockchain Map' we have developed at the EU Blockchain Observatory & Forum, which counts over 550 entries and is continuously growing.

INTRODUCTION: THE BLOCKCHAIN LANDSCAPE IN EUROPE

industry or other types of consortia, and focused on a single sector and/or use case.[2]

Such consortia can take on many different forms and involve different kinds of stakeholders. Below are examples of three of the most prevalent consortia models:

- **Multi-stakeholder-managed industry consortium**. A popular approach involves a group of market participants (who might very well be competitors) that come together to build a market platform. Such consortia are governed collectively by their members.[3]
- **Single stakeholder-managed, blockchain-based industry ecosystem**. In other cases, a single provider may build a platform and open it up for others to use.[4]
- **Geographically based blockchain consortia**. Another approach, less common but with interesting implications, is to build a general purpose, large-scale platform for more or less general transacting within a defined community that provides an infrastructure for members to build upon.[5]

There are many advantages to such market- or use-case-focused approaches.

Limiting the blockchain to a single or small set of related use cases means that developers can design the platform to meet the specific needs of the users. This provides a great deal of flexibility. For example, builders of "private" blockchains currently have more leeway to design for performance and security than designers of public blockchains do (more on this in our discussion of the blockchain trilemma in the next section). A private or semi-private undertaking with a limited number of stakeholders and a well-defined focus will also likely have an easier time of defining and agreeing to a governance model than is the generally the case with large, open, public platforms. Finally, considering how new, and in certain respects untried, blockchain technology is, working in a "walled garden" can be prudent from a software development and data security perspective.

2 For a short overview of blockchain, see Appendix 2 below.
3 A good example is Komgo: https://komgo.io/
4 See for example the IBM Food Trust: https://www.ibm.com/blockchain/solutions/food-trust
5 The pioneer here is Alastria in Spain: https://alastria.io/index_en.html

INTRODUCTION: THE BLOCKCHAIN LANDSCAPE IN EUROPE

A GLOBAL "BACKBONE" OF DECENTRALISED CHAINS

There is, however, a flaw in the walled-garden approach: the walls.

Networks are powerful in proportion to their size. As we know, large private versions of the Internet like AOL eventually disappeared as the maturation and adoption of the world wide web provided average people with user-friendly access to the open, decentralised, global version. This model won the day mostly because it proved the most inclusive and most useful.

Something similar is likely to happen in blockchain.

It seems clear to us that a multiverse of independent blockchains that cannot interoperate would be severely limited. Users of blockchain platforms will find it beneficial to be able to exchange data and make transactions between chains too: a healthcare chain connecting to an insurance chain, a real-estate chain connecting to a construction-materials or manufacturing chain, and so on.

Just as TCP/IP and the rest of the Internet stack became the open, freely accessible backbone of the Web of Information, we think that a small number of global, decentralised blockchain networks will also emerge as the backbone of a Web of Value.

These will allow these permissioned chains to work with each other by helping to facilitate data exchange and interoperability between chains, or even simply serving as a timestamp and settlement layer for other chains, and so providing that key layer of trust.

This is, however, by no means the only possible scenario. We may also see interoperability technologies arise that allow for seamless interaction between blockchains, resulting in a mesh network of directly interoperable chains.

Main issues and challenges in blockchain

SCALABILITY

If blockchain-based platforms and applications are to succeed, they will need to be able to scale sufficiently to meet the needs of their target markets or users. Due to the way blockchains work, scaling poses challenges that are not present with conventional database technology.

The point of a blockchain is to create decentralised trust through distributed ledgers that are verified and maintained by a community of peers. In the original Bitcoin blockchain, this is achieved by having all transactions propagated throughout the network and then having miner nodes compete to verify the transactions and append a block of transactions to the ledger, which in turn is propagated to all the full nodes before the process starts over.

The competition to validate the transactions uses what is known as a proof-of-work consensus mechanism, which can be described as a kind of computationally expensive lottery. This lottery forces the miners to pay a price (in hardware, energy costs and time) to take part. That price, in turn, secures the network, among other things by making it prohibitively expensive to cheat.

Most, though not all, blockchain technologies today follow a similar approach, and for a good reason: it works. Despite holding billions of dollars of value, the Bitcoin network has never been compromised.

That said, compared to conventional financial transaction platforms, the Bitcoin blockchain is incredibly slow, processing some seven transactions per second (tps) on average. Many of its blockchain peers do somewhat better, with different configurations able to achieve 10x or even 1,000x this rate. All of which, however, pales against VISA's 24,000 tps.

With the current state of blockchain technology, this lack of performance cannot be avoided, at least in public, permissionless blockchains: it is part of the price of securing the network.

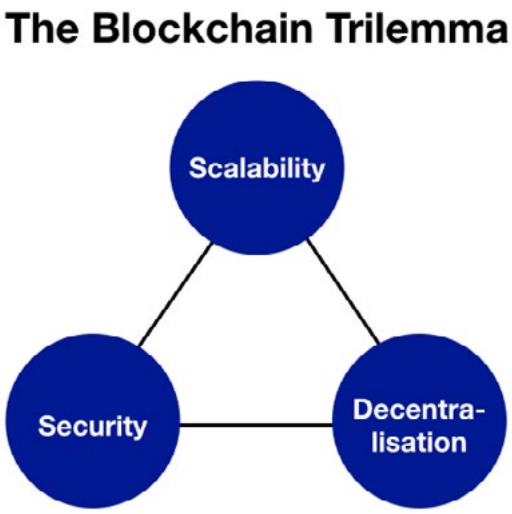
In the blockchain world people often refer to a loose trilemma positing that blockchains can generally have only two of the following three properties: scalability (that is, performance in terms of speed and volume), decentralisation or security.[1]

If a blockchain is to be highly decentralised and highly secure, it will come at the cost of scalability. If it is highly performant and highly decentralised, it will not be secure. Similarly, if one is willing to accept a degree of centralisation, it is possible to build highly secure and performant blockchains.

As a result, designers of blockchain-based platforms need to consider the trade-offs between these three parameters that best fit their particular use case.

1 See https://github.com/ethereum/wiki/wiki/Sharding-FAQs#this-sounds-like-theres-some-kind-of-scalability-trilemma-at-play-what-is-this-trilemma-and-can-we-break-through-it

MAIN ISSUES AND CHALLENGES IN BLOCKCHAIN



If large-scale decentralised trust is important, as is the case for example with a global cryptocurrency like Bitcoin, then decentralisation and security will likely be favoured at the cost of scalability. In closed markets like those created by a consortium, where it is possible to control who is allowed to participate on the network and to "police" their behaviour through both on-chain and off-chain means (for example legal contracts), full decentralisation is less important. That leaves room to design for security and faster performance.

Solving the scalability issue for blockchains – and in particular public, permissionless ones – is one of the most important technical challenges facing the community today. There are many different approaches currently being researched and developed, and as these challenges are met, we may be able to solve the trilemma.

We look more closely at the technology of scalability in our deep dive in the appendix.

INTEROPERABILITY

As we have mentioned, for blockchain-based platforms to succeed they will need to be able to communicate and share data, a property that is usually referred to as interoperability. While interoperability between blockchains can be achieved in a number of different ways, these can be broken down into two basic categories.

One category of interoperability approaches involves the use of trusted third-party authorities to validate transactions or information. Two or more blockchains, for example, might agree to trust an off-chain entity to either transfer information between the blockchains (an exchange) or to record the state of the respective blockchains so that each can trust what has transpired on the other (notary services). A notary service in turn can be either fully centralised (a single trusted third party) or federated (a group of providers of these services). Multiple blockchains can also rely on an outside data source to provide trusted reference information, for example certificates that prove the identity of a person or asset. The common thread in all these cases is that trust is external, vested in some off-chain authority.

The other category of interoperability approaches involves sharing information directly between blockchains without the need for a third-party authority. Such solutions often employ other blockchains or smart contracts to supply the trust needed to carry out inter-chain transactions or exchange data, thus creating a bridge directly between chains.

Like scalability, interoperability is another of the key technological challenges in the blockchain

world at the moment. A lot of time and effort is being invested in developing various approaches and solutions, and we can expect that over time it will become easier and easier for disparate blockchains to work together. This will be to the benefit of the ecosystem as a whole.

We also discuss interoperability in more detail in our deep dive appendix.

SUSTAINABILITY

Finally, successful blockchain projects will need to be sustainable, in the sense of being viable over a long period of time. When we speak of sustainability, we mean one of two quite different things.

1. Environmental sustainability of blockchains

As is widely known, updating and securing the Bitcoin blockchain – as well as other blockchains that make use of proof-of-work consensus – requires a great deal of electricity. By recent estimates, Bitcoin consumes the equivalent amount of electricity in a day as the country of Singapore[2].

As we have already touched on, this is not a bug in the blockchain protocol, but rather a feature. The proof-of-work consensus mechanism used in Bitcoin is expressly designed to be computationally expensive: it forces miners competing to win mining rewards to run their computers for a certain period of time, and that in turn costs money in the form of the electricity needed to run the hardware.

There are different ways to address the environmental sustainability issues of blockchains. The most promising is by moving to a different consensus mechanism. And indeed, much of the research and development in blockchain today revolves around developing alternative consensus mechanisms, such as proof-of-stake, that use significantly less energy while delivering the same amount of security. We discuss a number of these in our deep dives.

While these alternatives are all very promising, and while the overall trend in the industry is to move towards more sustainable consensus mechanisms, at the present moment proof-of-work remains the most widely used and battle-tested form of blockchain consensus in public networks.

Those employing proof-of-work also have options to reduce their impact. They can – and indeed often do – set up their server farms in areas with cheap, abundant or clean sources of energy. It is also possible to re-cycle the energy, for example by using the heat generated by the servers to heat buildings.

That said, it is clear that the blockchain community considers environmental sustainability a priority concern, and **we can expect blockchain technology to become less energy-intensive over time.**

2. The sustainability of blockchain projects, protocols and ecosystems

One of the peculiarities of blockchain technology is that many of its most significant core technology efforts are open-source, community-run projects.

2 See https://digiconomist.net/bitcoin-energy-consumption.

MAIN ISSUES AND CHALLENGES IN BLOCKCHAIN

Bitcoin, for example, is a purely open-source project with no formal governance structures, developed and managed by a more or less organised group of developers who themselves are often volunteers.

Many of the other significant blockchain protocols under development are open-source projects that have raised funds through an ICO or via sponsors, and are managed by a non-profit foundation.

Such projects are often dependent upon an ecosystem of developers and others for contributions to their ongoing development. For anyone relying on these technologies, the sustainability of that ecosystem is therefore of paramount importance.

Sustainability can be measured along a number of different parameters: the source and amount of funding, the quality of the governance structures, the size and cohesiveness of the development community, and so on. For many people, the market capitalisation of the token associated with the protocol can also serve as an indicator of the health of the project.

In the next section we analyse some of the key success factors for large-scale blockchain projects.

Success factors for large-scale blockchain projects

As we now have a number of major projects that have carried out successful proofs-of-concept and are close to going or have gone live, we can begin to identify some of the common elements that lead to success. In our opinion, these include the following.[1]

CLEAR PURPOSE AND CONCEPT

We think the most important success factor is not technical, but conceptual. More than anything else, projects should be clear about the goals of their endeavour. Without a strong vision and purpose, projects risk failing.

Once the use case is clear, stakeholders should also be sure of the benefits of decentralisation for their particular use case. If decentralisation of some kind does not provide obvious advantages, then it may very well be that a traditional database provides a better alternative. This is a good thing to know before investing time and effort in a potentially unnecessary blockchain solution.

Provided it is a blockchain use case, then projects will want to identify the key functionalities of the platform needed to address the needs of the user base and particular use case, and then choose the most suitable blockchain technology for the job.

This requires asking questions like what level of trust should be placed in the validating nodes, what level of performance is required or what are the acceptable trade-offs between scalability, security and decentralisation. A small consortium of stakeholders well known to each other, with relatively low volumes of transactions, will have different needs in terms of scaling, for instance, than a project catering to a broad user base.

GOVERNANCE

Whether it is building or running a large-scale project or consortium, successful collaboration requires strong governance. This can be challenging, particularly since the question of governance in collaborative consortia for decentralised technologies is still relatively new, and there remains a lot to be learned. That said, we believe the following is important.

The consortium will want a good set of terms and conditions, clearly spelling out such things as the requirements to participate in and/or leave the consortium, a mapping of the on-chain proofs with the relevant off-chain legal and regulatory frameworks, clear service-level agreements spelling out each stakeholder's rights and duties, and so on.

In a permissioned blockchain, which these projects mostly are, perhaps the most important element of governance is identity. Projects have to consider how they will establish the identity of members and what the rights and responsibilities of the various

1 This section is based on the presentation of Peter Broadhurst at the EU Blockchain Observatory & Forum workshop on Scalability held in Berlin on 2 October 2018. The video is available here: https://www.eublockchainforum.eu/video/workshop/scalability-interoperability-workshop-2-october-2018-berlin-part-4-presentation

roles on the platform are. They will need to think of the appropriate participation levels and how entities qualify for different roles, while having mechanisms in place to ensure that all members are treated fairly. There should be clear criteria for who can vote on consensus, who is allowed to have a complete copy of the chain (which may contain sensitive data), who can put data into the chain and who can process that data.

In a collaborative IT project, especially a big one, participants will likely want to use shared tools and IT standards as much as possible, yet these must also be compatible with the tools and standards of each individual stakeholder. Such tools and standards should be considered carefully and, to the extent this is feasible, agreed upon ahead of time.

Finally, projects should keep in mind that they will grow. A governance model that works for a small group looking to quickly build a proof-of-concept to bootstrap an idea will not work for a large, live platform with hundreds of members. The governance model should therefore also be flexible, allowing the project to evolve and adapt as necessary.

COMPONENT-BASED, SERVICE-ORIENTED ARCHITECTURE

In designing their solutions, projects should be mindful of the fact that the blockchain is often only a small part of the overall architecture and hence of the development effort. There will be many other layers that need to be understood and engineered to fit into the platform as a whole.

A permissioned network will, for instance, need some kind of identity registry to hold the credentials of its users for authentication purposes. Most if not all of the user data will also typically be kept off the chain, so the project will need a shared but encrypted and access-controlled data repository. There should be a means for members of the consortium to communicate and share high volumes of data with each other in a secure way. Then there are the various connections to the outside world, whether data oracles or transaction submissions. A key management solution, with recovery options, is also something projects should consider.

Projects should further keep in mind that blockchain and other technologies evolve quickly. It therefore makes sense to use a component approach for the above-mentioned layers, developing them as microservices that can be swapped out as new options become available.

HOMOGENEOUS PRODUCTION ENVIRONMENT AND POOLED RESOURCES

Sharing is also a key factor. In successful projects, members tend not to build their apps to connect to the platform, but customise standard apps developed by the consortium, saving time and effort and ensuring compatibility. This can, however, be a challenge especially when dealing with groups of well-established enterprises with a long history of IT projects and their own well-developed set of standards, as well as differing levels of blockchain expertise.

SUCCESS FACTORS FOR LARGE-SCALE BLOCKCHAIN PROJECTS

For this reason, successful projects tend to have a centralised, cross-funded shared IT organisation – staffed either by individuals from the member organisations seconded to the project, or set up as a separate funded entity – that develops common practices and tools for the consortium. This organisation can act as a shared pool of skill, resources and expertise, playing an important role not only in developing the platform and keeping it running, but also in answering questions, providing support and generally keeping the wheels greased.

Considerations for a European blockchain infrastructure

A new technology can't become successful on a mass scale without the right infrastructure. This includes such things as the technical hardware and software stacks, standards, the legal framework as well as governance best practices.

Through the European Blockchain Partnership the EU has begun to consider Member State cooperation towards the goal of a European Blockchain Services Infrastructure to support cross-border digital public services.[1]

In this section, we offer some general thoughts on some of the considerations that could influence the development of such an infrastructure, and draw a high-level picture of how such an infrastructure might look.[2]

GOALS OF A PUBLIC SERVICES BLOCKCHAIN INFRASTRUCTURE

We think that government can play a positive role in helping to develop such an infrastructure through policy. To foster the Digital Single Market we believe it makes sense for European policy makers to focus on the following goals for a blockchain infrastructure initiative:

- Create an environment and a set of foundations conducive to the development of an innovative, world-class blockchain ecosystem in the EU.
- Make it easier and cheaper for public and public/private initiatives to design, test and deploy projects based on blockchain technology.
- Establish interoperability standards that make it possible for individual projects to communicate with each other easily and securely, with no leakage of sensitive data.
- Facilitate knowledge transfer between projects.

KEY PRINCIPLES

Such an infrastructure policy should consider the following principles and key points:

- **Technological diversity**. At this early stage of the technology, it would make sense for the EU Blockchain Infrastructure to hedge its bets by allowing multiple technologies to operate and compete on the platform. Similarly, it could be argued that, by allowing multiple identity solutions, payment solutions and other technology components to operate on the EU Blockchain Infrastructure, the platform will protect itself against vendor lock-in and will encourage providers to develop interoperable solutions.
- **Interoperable communications**. The EU should foster interoperability through various policy means. Interoperability is a functionality offered by a specific tool or library, and each tool or library is usually customised to an origin, a destination, a type of data and the level of trust that

1 See https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership

2 The text for the rest of this section first appeared, in slightly different form, in "A public blockchain infrastructure in the European Union?", by Ken Timsit, 14 December 2018.

the origin and the destination have in certain "signing authorities" associated with the data. We cannot request that a EU Blockchain Infrastructure should have "interoperable blockchains". Rather, we ask for specific interoperability functionalities, and expect these functionalities to expand over time.

- **Digital identity**. Blockchain-based government services applications are unlikely to be able to operate without a strong underlying digital identity ecosystem. A decentralised identity ecosystem includes a wide universe of applications, devices and authorities, allowing users to store identity credentials in the repository of their choice and use them across multiple blockchains and applications. Such a decentralised identity ecosystem could be designed to interoperate with the centralised national digital identity schemes and eIDAS, the European framework and platform for such schemes.
- **Fiat currency payments**. Many blockchain-based workflows involve some form of automatic payment when certain conditions are met (such as the completion of a workflow). Given that blockchains and banking systems are often two separate environments, these workflows are unlikely to be able to operate unless fiat currencies are given an existence on blockchains, and can be manipulated by smart contracts. The EU Blockchain Infrastructure could allow users to access tokenised fiat currencies, for example by allowing private financial institutions to issue tokens in proportion of the amounts held by these institutions in escrow accounts or by working together with the European Central Bank to issue a central bank-backed form of tokenised euro.
- **Back-ups**. The EU Blockchain Infrastructure should allow users to request regular back-up of their server instances and their data.
- **Roll-back / fork**. The EU Blockchain Infrastructure should, at some point in time, offer "roll-back" functionalities. While blockchains are, in principle, immutable, there may be especially critical situations where processes or data have been corrupted due to a bug or a security issue, making it necessary to roll-back or fork one of the blockchains. Such roll-backs or forks should be exceptional, and decided only by the highest governance bodies of the Infrastructure platform. Nevertheless, if they happen, it is important to have pre-existing governance, processes and functionalities in place in order to make them happen quickly.
- **Migration / living wills**. The EU Blockchain Infrastructure should not, in principle, lock the data of public services within a specific blockchain technology. Governing bodies should request that technology vendors generate "living wills", i.e. high-level guides outlining how the data could be migrated out of their technology into a standard database, should the need arise.

THE LAYERS OF A BLOCKCHAIN INFRASTRUCTURE

In order to meet the functional needs of institutional users and end users, a blockchain infrastructure should likely consist of the following layers, from top to bottom:

- **An application and services ecosystem/ layer**, consisting of applications focusing on specific use cases, service providers, auditors and regulators, and governance

CONSIDERATIONS FOR A EUROPEAN BLOCKCHAIN INFRASTRUCTURE

bodies; some of these applications and services could be made available to end users via some form of app store or marketplace.

- **A platform presentation layer**, consisting of consoles, dashboards, and development environments made available to developers, institutional users, auditors and regulators.
- **A middle layer of services**, callable by the above layers via APIs by entities and users who have the required permissions. Such services would include core APIs for reading/writing data onto the various blockchains and databases, as well as shared utilities such as identity, interoperability bridges, event listeners and oracles, and perhaps even a payment infrastructure.
- **A platform management layer**, consisting of a registry of networks and participating nodes/servers and users as well as their respective permissions, as well as various monitoring tools.
- **A blockchain and database layer**, containing the actual blockchain with the chosen consensus mechanism as well as any ancillary databases.
- **A marketplace of templates**, consisting of a menu of images of machines and containers that can be selected and deployed by institutional users to create as many servers/nodes as they see fit, including blockchain clients, and other technology stacks such as databases, web servers and others.
- **A cloud infrastructure**, in which institutional users can select and deploy as much computing and storage power as they need for their respective application.

Recommendations

Our purpose in writing this paper has been to shed some light on the "potential future states" of blockchain infrastructure and platforms in Europe assuming large-scale adoption, and to examine the characteristics for success in getting there, as far as they can be ascertained at this time.

As we hope we have been able to show, it is indeed an interesting moment for the blockchain ecosystem and industry in Europe, as a number of large projects are beginning to go live and attracting large user bases. While this is encouraging, there are still many challenges – both technical and organisational – that need to be surmounted.

We believe there is a role for policy makers to help support the industry in meeting these challenges, and the good news is that the EU has already shown a clear intention to do so. In this last section, we offer a few concrete recommendations for policy makers to help continue the momentum.

- **Standards**. Today if we want to go in the direction of multi-layered interoperable ecosystem of blockchains, both policy makers and the blockchain industry, ideally working together, should prioritise the development of standards. Among these, we think the most important will be standards for digital identities in a blockchain context, and for interoperability between blockchains.
- **Research**. It is no secret that research is an important element to the success of blockchain. Currently the EU is active in supporting blockchain research in a number of ways, from the EU Blockchain Observatory & Forum, under whose aegis this paper has been written, to the allocation of up to EUR 340 million to support blockchain projects through 2020 under the Horizon 2020 programme. While these are laudable, the EU should not rest on its laurels. Both the US and China have expressed strong support for blockchain research, with the former even going so far as to include it as part of its USD 700 billion defence budget. We therefore recommend that the EU continue its strong support, targeting both basic research as well as supporting implementation of infrastructure-related projects in particular, as well as research into non-technical topics such as governance of blockchain projects (see next bullet).
- **Governance**. Governance, as we've mentioned, is a very important topic and a key success factor for blockchain projects. Governance of decentralised technologies and applications is also not very well understood. Besides supporting research into the topic, the EU should take a wait-and-see approach, giving projects the time to experiment and learn before developing standards or considering governance-related regulations.
- **Ecosystem diversity**. The EU can support the ecosystem in other ways as well, for instance by encouraging project diversity. We think it best, for example, not to mandate specific technologies under the European Blockchain Infrastructure, but rather encourage different technologies

RECOMMENDATIONS

to foster innovation. Policy makers should encourage fiat money on-chain to facilitate blockchain-based payments and the uptake of smart contracts. An open data policy within government, providing bridges to publicly available information in government databases to blockchain-based systems, would help foster the technology, .

- **Be blockchain-aware themselves**. On a broader level, policy makers will want to be mindful of and prepared for the new models and possibilities being brought about by decentralised technologies. As well as using blockchain themselves to provide government services,[1] governments could well be interacting with blockchains as identity providers or data oracles. They will want to be prepared.
- **Legal Framework**. As we have mentioned in previous papers and workshops, the success of the blockchain industry in Europe will depend to a large extent on clarifying many of the legal and regulatory issues thrown up by blockchain. These include resolving the tensions between GDPR and blockchain, the legal, fiscal and accounting status of crypto assets, and the legal status of smart contracts, among others.
- **Education**. Along with research, blockchain adoption will also depend on the education and training of technologists, entrepreneurs, other experts and the general public. This is an area where policy makers can have a significant impact through the support of educational and research initiatives.

1 See Blockchain for Government and Public Services, EU Blockchain Observatory & Forum, 7 December, 2018.

Appendix – Deep Dives

BLOCKCHAIN LAYERS

When dealing with scalability, there are multiple technologies that one can use or improve in order to make a solution work faster. These technologies are related to four different layers:

Layer -1 solutions: Hardware Layer

The hardware layer refers to the machines that are used to run the blockchain client (software). Using better machines can translate into better performance in terms of transaction throughput as the basic computations (e.g. verifications, changes of state) can be performed more quickly. It is important to highlight that all machines on the network need to be upgraded in order to actually realise performance improvements. This solution is often leveraged for specific cases such as consortium chains and dPoS, where a small number of actors are able to deploy high-end hardware.

How much scalability can you gain through this layer?
Up to 5 to 10 times more throughput.

Limitations
This solution cannot be easily leveraged for large networks because machines are heterogeneous performance-wise, meaning that the older nodes would not be able to keep up if the settings make it too hard to keep pace. Minimum requirements could be contemplated for machines to run a client but it means that only a limited number of actors would be able to afford the necessary hardware, resulting in a less decentralised system.

Layer 0 solutions: Network Layer

Layer 0 refers to the network layer, including all communications between nodes. An important concept to keep in mind is the one of network propagation, which describes how fast a certain percentage of the network will have received the latest bits of information (e.g. the last block). There are physical limitations to how fast information can travel around the globe, but also core parameters that will influence

APPENDIX – DEEP DIVES

propagation such as what data is being sent, how much there is of it and which transmission method is being employed. Most blockchain protocols rely on peer-to-peer models for communication between nodes.

How much scalability can you gain through this layer?
Up to 5 times more throughput.

Layer 1 solutions: Blockchain Layer

There is a lot of work going on in the development community to improve the performance of blockchains themselves, also referred to as Layer 1. Innovating on protocols can lead to systems that are faster or more efficient (i.e. use less energy).

Layer 1 solutions can be minor tweaks, for example adjusting the block size or the block time interval. Or they can be major changes. Blockchains can employ sharding, for example, which is a technique common in conventional database technology. This is where 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.

Another approach is to change to a different consensus mechanism. The proof-of-work consensus mechanism is deliberately slow and costly: that is its main means of maintaining the security and viability of the network. There are, however, many other possible consensus mechanisms. The most promising at the moment for public networks seems to be Proof of Stake, which itself comes in a number of variants. There are also non-blockchain systems that allow for decentralised trust through distributed ledgers, such as the Directed Acyclic Graph (DAG). It is, however, important to keep in mind that different consensus mechanisms imply different trust and security assumptions, among other things, and so cannot be compared to each other simply on the basis of transactions per second or other performance metrics.

Focus on consensus algorithms:
The choice of a consensus algorithm fundamentally affects the characteristics of a blockchain, including the stability of the network, scalability, energy consumption and resilience to failures and malicious attacks. Each consensus algorithm has its pros and cons, and some will be preferred in specific contexts. Even though there are dozens of different types of consensus algorithms, each with multiple different

APPENDIX – DEEP DIVES

implementations, some of them are most often used.

Category of consensus algorithm	Used for	Time before finality	# of nodes on the network	Tolerance to malicious participants	Energy consumption
Proof of Work	Public networks	High	High	1/2	High
Proof of Stake	Public networks	Low	High	1/3	Low
Delegated Proof of Stake	Public networks	Low	Low	1/3	Low
Practical Byzantine Fault Tolerance	Permissioned networks	Low	Low	1/3	Low
RAFT/PAXOS	Permissioned networks	Low	Low	1/3	Low

Fig. 1 Comparison of some consensus algorithms

How much scalability can you gain through this layer?
Up to 10 to 20 times more throughput.

Limitations
It is important to keep in mind that different consensus mechanisms imply different trust, governance and security assumptions, among other things, and so cannot be compared to each other simply on the basis of transactions per second or other performance metrics.

Layer 2 solutions: Application Layer

Another way to improve performance is to move significant parts of the computation - the work of directing and verifying transactions, for instance - off the chain into more conventional, and hence more performant, systems. These are generally referred to as Layer 2 solutions.

A typical Layer 2 solution is a payment channel. In such a case, two parties who want to transact with each other open a direct channel between themselves, generally pre-funded, and then carry out their transactions. At some defined point these transactions are then written to the blockchain, which acts as the permanent record of what had transpired – in effect settling the transactions. Such payment channels can greatly

APPENDIX – DEEP DIVES

increase the performance of a blockchain, but they also imply different trust assumptions and pose challenges of their own.

More complex variants of this concept can be conceived as well, for instance multi-sided payment channels or payment hubs, or even complete sidechains, which are like sub-blockchains that handle transactions quickly and then write the results to the main chain.[1]

How much scalability can you gain through this layer?
Up to 10,000 to 100,000 more throughput.

Limitations
This type of solution is the most promising in terms of scalability. It also often offers interesting tools for privacy. However, it heavily relies on interoperable tools in order to function properly. When fully mature, layer 2 solutions will allow to connect multiple blockchains seemlessly.

ORACLES

An oracle is an agent that allows to transfer external data to the blockchain for on-chain use. This is done through the use of smart contracts that add information about real-world events to the blockchain. Simple examples of data that are useful to import include temperatures, prices or information about flight delays. Once entered on the blockchain, this data can be used to automate processes based on real-world events (e.g. if a train is delayed, an insurance contract automatically and autonomously delivers the indemnification).

How does it work?
Technically speaking, oracles are no different from other smart contracts. However, in order to be useful, oracles need to be trusted: either because they are operated by a trusted third party or thanks to cryptographic attestations.

Why is it interesting?
Oracles provide a data feed about external events. Without oracles, a blockchain would operate only in its own closed environment, limiting greatly its capabilities.

Maturity and real-world implementations

1 The Lightning Network on Bitcoin and Plasma on Ethereum are examples of sidechains designed to help with scaling.

APPENDIX – DEEP DIVES

Oracles are proven and easy-to-implement systems.

Limitations
Applications are only as reliable and trusted as their oracles are.

ATOMIC SWAPS

An atomic swap is the exchange of digital assets happening between assets from two different blockchains, without intermediaries. To take a simple example, Alice can choose to exchange her digital assets (located on blockchain A) against Bob's (located on blockchain B), without relying on a third party to complete the transaction.

How does it work?
Atomic swaps rely on Hash Timelock Contracts (HTLC) and follow three main steps:

1. Alice generates a secret key s, calculates its hash h and sends h to Bob.
2. Alice locks her assets into a contract that Bob can redeem the funds with s provided within time y or the funds will be sent back to Alice. Bob then locks his assets into a contract that Alice can redeem the funds with s provided within time x, such that y is larger than x, or the funds will be sent back to Bob.
3. Alice reveals s within time x to redeem coins from Bob. Bob then learns s and can redeem coins from Alice.

Why is it interesting?
Atomic swaps increase the level of interoperability between chains that are not otherwise linked. They are not specific to a certain type of blockchain and can theoretically be implemented on any chain that deals with digital assets.

Maturity and real-world implementations
Atomic swaps is a technology that is already available and was first experimented with in 2017. It can be used to set up decentralised exchanges where no third party is required to complete the transaction. Example: https://komodoplatform.com/.

Limitations
Atomic swaps have so far only been successfully used in order to exchange simple assets; the technology has not proven its usability to transfer information.

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 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:** Transaction 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.