

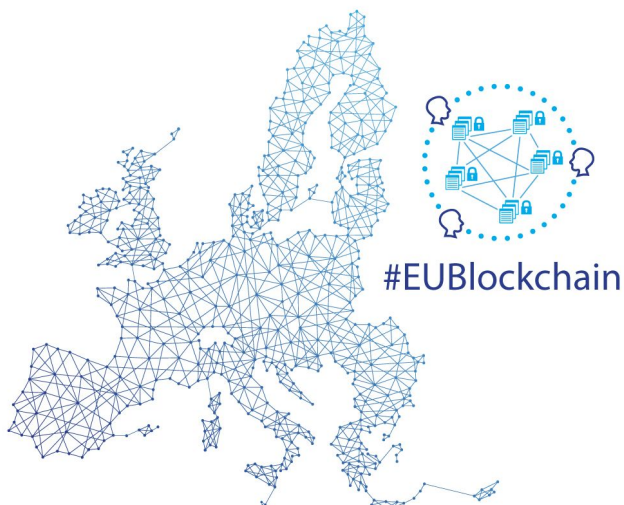


An initiative of the



EU BLOCKCHAIN OBSERVATORY AND FORUM

Workshop Report - Scalability, Interoperability and Sustainability Berlin, October 2, 2018



By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Reproduction is authorised provided the source is acknowledged.

Author: Tom Lyons

Published on 14 November, 2018

Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents

Context	3
Introduction to the day – Ludovic Courcelas	3
Presentation – Arthur Gervais: Scalability methods and state of the art	4
Panel discussion – Scalability, interoperability and sustainability: state of the art	5
Presentation – Peter Broadhurst: What does it take to deploy large-scale decentralized applications	7
Working session – Requirements for a large-scale blockchain infrastructure	8
Appendix	10
Workshop slides	10
Workshop videos	10
Related links and information	10
Official agenda	10
List of registered participants	11

Context

As blockchain technology turns 10 years old, much has been achieved, but we are still waiting for mass adoption. While predictions that 2018 would be the year that blockchain “becomes real” have proven premature, there are a significant number of large-scale projects that look certain to go into production in 2019.

While this is good news for the industry, there are still hurdles to be overcome before reaching any significant milestones on the road to mass adoption of this technology. Among the obstacles to the implementation of truly large-scale, broad-based blockchain platforms are scalability of blockchains and the ability of different blockchains to talk to each other (or “interoperate”). First generation blockchain technology, based on Proof of Work consensus, has also proven very costly in terms of energy consumption, raising questions about sustainability.

At the fourth workshop of the EU Blockchain Observatory & Forum, held on October 2, 2018 in Berlin, blockchain thought leaders and practitioners gathered to look at the state of the technology today in terms of these three important parameters, and to look at what needs to be done to build a truly large-scale blockchain infrastructure in Europe, both in terms of the technology and platform governance.

Below we have summarised the main points of the discussion. Links to the slide as well as videos from the workshop can be found in the appendix at the end of this document.

Introduction to the day – Ludovic Courcelas

Ludovic Courcelas is a member of the ConsenSys France team and Project Manager of the EU Blockchain Observatory & Forum. He opened the workshop by introducing the agenda and themes of the day.

- As the ecosystem is maturing, larger projects are expected to go live. If 2016 was the “year of education” when people learned about blockchain and its uses, and 2017 the “year of proofs-of-concept”, during which people experimented to validate theses, then 2018 has been 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 10+ major platforms slated to go into production.
- This development is creating challenges for governments and businesses regarding how best to manage these large scale solutions. Such challenges include how to create solutions that can scale, how to ensure such solutions are energy efficient, choosing the right technology, deciding what interoperability functionalities should be implemented as

well as the required building blocks (e.g. identity system), and deciding and implementing the right governance models.

- It is becoming clear that we are moving to a world of multiple blockchains. In place of the concept of single, all-purpose blockchains we are seeing architectures arise comprising a central, highly decentralised layer that is surrounded by very efficient blockchain networks specialised on a particular use case. These latter can be very fast and highly scalable, but are not very decentralised. The benefits of decentralisation come instead from the aforementioned base layer, which acts as a backbone.

Presentation – Arthur Gervais: Scalability methods and state of the art

Arthur Gervais is a lecturer at Imperial College London and the Lucerne University of Applied Sciences, the latter of which is an academic partner of the EU Blockchain Observatory & Forum. He is also the author of the research paper on scalability, interoperability and sustainability commissioned by the Observatory ahead of the workshop.

- It is easy to see, among other things in the number of unconfirmed transactions or volatility in transaction fees, that current blockchains do not scale well.
- Efforts to scale permissionless blockchains are happening in different areas:
 - **Network layer:** Advances including a faster Internet, professionally hosted nodes or optimised propagation protocols can lead to scaling improvements in today's blockchain technology of 10-15x without great expense or altering trust assumptions.
 - **Consensus algorithm:** Another potential way to scale blockchains is by changing the consensus algorithm from Proof of Work. There are many alternatives out there, but they are very hard to compare with each other, with among other things often fundamentally different trust assumptions than proof of work and question marks around security.
 - **Sharding (partitioning):** By dividing the blockchain into partitions (shards) that are worked on concurrently by a subset of nodes, you can greatly increase capacity. While sharding technology is very promising, it is also highly complex and remains to be proven.
 - **Off chain:** Capacity can also be dramatically increased by moving transactions off chain. Here there are a number of different methods, including collateralised 2-party payment channels or off-chain payment hubs with periodic settlement. Such second layer solutions, some of which are production ready, are extremely promising, offering instantaneous and low to zero-cost transactions.
- In permissioned blockchains we change the trust framework by introducing a consortium of a few trusted entities, which is a well-known approach and typical of how businesses work today. Generally consortium members agree contractually that they are all

validators, which among other things allows them to run more efficient consensus algorithms like proof of authority.

- To sum, comparing permissioned vs permissionless blockchains:
 - in permissionless settings trust is placed in an open algorithm (trusting that no single entity can become dominant) while in permissioned blockchains trust is placed in a consortium;
 - permissionless blockchains are inefficient compared to permissioned;
 - permissionless blockchains are not (yet) privacy preserving, while permissioned blockchains are typically privacy preserving.
- In terms of how mature the scalability approaches mentioned above are, both network layer and off chain approaches are closest to being production ready (or are already in production), consensus algorithms are rather far along, and sharding probably the farthest off.

Panel discussion – Scalability, interoperability and sustainability: state of the art

Gervais' presentation was followed by a panel discussion among:

- *Peter Broadhurst (Co-Founder Kaleido)*
- *Cyril Cassagnes (Technical Lead Infrachain)*
- *Jesus Ruiz (CTO Alastria)*
- *Gilbert Verdian (CEO Quant Network, Chair UK delegation to ISO TC/307)*
- *Reto Gadiant (B.ACADEMY) (Moderator)*

Highlights of the discussion included:

- When it comes to choosing the best solutions design and identifying the key functionalities to ensure interoperability and scalability, a lot depends on what the problem is that you are trying to solve. This requires asking questions like what level of trust you want to place in the nodes, what kind of performance you are looking for, what kind of tradeoffs between consistency and availability you are prepared to make, and so on.
- Efforts like Overledger, which currently connects six different blockchains, support interoperability and user choice. Alastria, the Spanish national blockchain, started with Quorum because it was the only production-ready choice available last year, but is now evaluating other blockchains suitable to its public, permissioned approach. Much more research into scalability of public, permissioned chains is however needed.
- Kaleido, which wants to provide businesses the tools to move quickly from concept to production, chose Ethereum among other things because of its large community, but within that environment looks to provide a lot of choice, whether in consensus algorithm,

permissioning, etc. The hope is to get the tech out of the way so businesses can focus on the organisation, business model and governance aspects of their platform.

- Asked about energy sustainability panelists agreed that there needs to be more energy-efficient alternatives to proof of work, and that these are indeed on the way. In the meantime, projects could also look to recycle the energy needed for mining, for example by using mining data centres as heat sources.
- There was also lengthy discussion of governance, which was a key topic for all. At Infrachain the goal is not to form consortia but to work on governance models for P2P networks, and the projects feels it is close to having developed a gold standard for such a model.
- Looking at the past, with issues in projects like Tezos or the Ethereum fork, it is clear that governance is quite tough. That is why the ISO blockchain working group has a governance stream, though this is not meant to be prescriptive but rather to make it clear that the right governance needs to be in place.
- At Alastria, which has 300 entities and is growing at a rate of 20/month, the mix of experiences of consortium members – drawn from large and small companies as well as public and private entities – is proving to be very helpful for governance discussions.
- At Kaleido it is interesting to see how governance issues are addressed among the communities the company works with that are trying to build the technology. Of note here is the shift we are seeing from a world where a standard gets set and everyone implements it to a world where standards evolve after implementations exist and we have the experiences of adoption. In this light, the announcement of the cooperation between the EEA and Hyperledger was excellent news.
- From the standpoint of the EU Observatory, one goal is to challenge the community to among other things look at how it measures success. Wouldn't one real measure of success for a governance model be if it can, along with the technology, contribute to volumes in the 1 million transactions per day or even second range?
- It is also important to consider that there are many levels of governance: governance of the user communities as well as of the development of the technology, for example. It is also important to differentiate between on- and off-chain governance.
- Governance is first and foremost about managing risk: technological risk, operational risk, regulatory risk, corporate risk, etc.

Presentation – Peter Broadhurst: What does it take to deploy large-scale decentralized applications

Peter Broadhurst is a co-founder of Kaleido.

- It's an exciting time. In 2019 we can expect a number of permissioned, enterprise grade consortia to move into production. These include the likes of the IBM-Maersk project, the

Interbank Information Network, Alastria, Komgo, LiquidShare, the Australian Securities Exchange, Vakt and the Federation Francaise de l'Assurance

- It is possible to identify some shared key features among these types of successful projects. First off, they are based on strong foundations including comprehensive identity and permissioning frameworks, strong security policies and audits, and evolutive legal terms and conditions. On top of this common enabling features include shared workflows between all actors involved, a service-oriented architecture making it easy to replace and/or upgrade components, a pragmatic approach to interoperability, a homogeneous production environment, and a dedicated team for upgrades and maintenance
- Governance and identity are extremely important. A permissioned chain is first and foremost about identity, so a crucial question is how to establish that identity and decide who will do what while avoiding traps of centralisation.
- Because the technology changes and evolves so quickly, it is also important to have tools and processes that can change and evolve.
- It is interesting to note that the blockchain itself is often a surprisingly small aspect of the technology involved in these efforts. It forms a foundation, but it is not necessarily where most of the activity happens. Other important layers include a shared identity registry, off-chain data repositories, rich-query shared data stores, a private and secure messaging bus and policies and standards governing how people manage keys, submit transactions, and the like.
- It's important to have some kind of centralised, cross-funded IT infrastructure, most likely set up as microservices. Designing and implementing such infrastructure can mean new skills and practices for many IT departments, which are not used to collaborating on a large scale outside their organisations. Decentralised technologies mean new mindsets for technologists too!
- Another important question is how do we connect the logic in our blockchain island with things in the real world? The most practical way is through some kind of oracle to gather data from the outside world and make it available on the chain. There are different ways to do this including building a bridge to another blockchain, utilizing a trusted third party, or having all members submit their own data and employ some kind of validation mechanism (as is done for example with LIBOR today).
- Kaleido is also starting to see consortia joining together to form more interconnected architectures. This can for example be about connecting different consortia who are collaborating in a similar space, generally using cryptographic or oracle-based bridges. It is an area Kaleido expects to grow significantly over the next few years.
- A challenge is to do all this while maintaining the true essence (and benefits) of decentralisation through blockchain. That means finding the balance between consistency, speed and governance, for example mandating on a consortia level how members do things but merging that with enough autonomy so that the project does not become just another database
- Last but not least, the organization of the consortium is very important. It needs a central pool of resources that can be called upon by all. Either each member puts a resource in

or you start a separate company. What's important is to get a central pool of talent to drive things forward.

Working session – Requirements for a large-scale blockchain infrastructure

The workshop ended with a working session among all participants. These split into three groups. Among the findings were:

- In the group discussing governance and business processes a lot of people talked about the importance of crypto regulation as well as starting with use cases and business processes instead of the technology. There was also a debate around if it is realistic to expect a one-size-fits-all blockchain infrastructure (single chain world) or if it's more desirable to have use-case specific blockchains.
- Looking at blockchain architecture, there was clear consensus that we need to think not in terms of a single, monolithic app but a suite of services, among other reasons so that we are not too dependent on a single technology. The group talked about the need to be realistic and anticipate that, while we might start with one or two blockchain technologies now, we might have to migrate to another blockchain technology in future. Other important issues discussed were how to interface with the outside world and identity (both in terms of identity sources, such as governments, as well as the multilayered nature of digital identity in general).
- In the discussion around infrastructure and security requirements for a European blockchain infrastructure, first of all there was debate as to what kind of blockchain is preferable to use. The majority argued for some kind of public, permissioned blockchain, but there was no overall consensus. As part of such an infrastructure we will need clear definitions of who is allowed to be a validator, who can submit transactions, etc. That implies a large registry governed by some administrative function. There was a suggestion for each member state to run a node but also allow independent parties to be validators, as a check and balance on behalf of citizens. We also need governance for who can make structural changes to the network. Looking at security, confidentiality was considered very important, implying there should be no sensitive data on the chain. Code needs to be peer reviewed and audited, and data that goes into the network needs to be validated. Finally, availability is important in two respects: we need clear uptime and return time requirements, but because blockchains are not scalable at the moment, we also need buffers for when the queues are full, as well as triage functions for allowing emergency services (for example) to get through first (priority queue).

Appendix

Workshop slides

- [Full day presentation](#)
- [Slides Arthur Gervais presentation](#)

Workshop videos

- Videos from this and all other workshops can be found on the [EU Observatory website under reports](#)
- Videos specific to this workshop:
 - [Part 1 Introduction \(Courcelas\)](#)
 - [Part 2 Scalability presentation \(Gervais\)](#)
 - [Part 3 Panel discussion](#)
 - [Part 4 Presentation Kaleido \(Broadhurst\)](#)
 - [Part 5 Conclusion](#)

Related links and information

- [Alastria](#)
- [Infrachain](#)
- [ISO TC/307](#)
- [Kaleido](#)
- [Quant Network](#)

Official agenda

9:30	30min	Guests' reception
10:00	15min	Introduction of the day - Agenda and objectives of the day
10:15	45min	Presentation - Arthur Gervais, Scalability methods and state of the art (25min + 20min discussion) Why is it difficult to create blockchains that scale? What are currently existing solutions to scalability? Improving scalability by improving the protocol layer - Technical explanation Improving scalability by using layer 2 solutions - Technical explanation
11:00	1h30	Panel discussion - Scalability, Interoperability and sustainability: state of the art (50min + 40min discussion) Gilbert Verdian (CEO Quant Network, chair UK delegation to ISO TC/307) Peter Broadhurst (Co-Founder Kaleido) Jesus Ruiz (CTO Alastria) Cyril Cassagnes (Technical Lead Infrachain)
12:30-13:30 Lunch break		

13:30	45min	Presentation - What does it take to deploy large scale decentralized applications (25min + 20min discussion) Presentation from Peter Broadhurst (Co-Founder Kaleido)
14h15	1h30	Working session - Requirements for a large scale blockchain infrastructure What are the main requirements and specifications of a blockchain infrastructure? What challenges need to be addressed? What should be the role of the EU and its priorities? How to get there?
15:45	15min	Conclusion
16:00		End of the day

List of registered participants

Alain Roset	La Poste
Aleksander Kampa	Sikoba
Andreas Heider-Aviet	T Systems
Anne Leslie	Pikcio
Arthur Gervais	Imperial College
Arvin Kamberi	DiploFoundation
Avijit Sarkar	CapOne Research
Benjamin Howard	
Benoit Abeloos	European Commission
Chiara Mazzone	European Commission
Clémence Olivier	Arcturus Group
Cyril Cassagnes	Infrachain
Dave Remue	B-Hive
Elizabeth Renieris	Evernym
Eusebio Felguera	Telefónica
Franz von Weizsäcker	GIZ
Frédéric Ocana	NenyA
Frederique Danjon	Ordre des Experts-Comptables français
Garrett MacDonald	Energy Web Foundation
Gilbert Verdian	Quant Network
Greta Solomon	Cognitive
Gunther Walden	CircularTree

Herve Francois	ING
Javier Sebastián	BBVA
Jean-Luc Verhelst	Hive
Jesus Ruiz	Alastria
Jonathan J. Attia	DL4T
Joséphine Quioc	GIZ
Joshua Muzza	
Julian Richter	NEM
Kai Wagner	Jolocom
Ken Timsit	EU Blockchain Observatory & Forum
Kestutis Rudzika	RoyaltyRange
Konstantinos Votis	CERTH/ITI
Leonardo Vidal	TorlaBix
Ludovic Courcelas	EU Blockchain Observatory and Forum
Maik Hesse	PwC
Maria Marengo	MentFort
Martin Schollm	
Matt Hancock	
Michael Neaves	Logos
Mirko De Maldè	Lynkeus
Monica de Oliveira Gonçalves Vidal	TorlaBix
Nadia Filali	Caisse des dépôts
Nathan Williams	Minespider
Nicolas Liochon	Pegasys
Nina Siedler	DWF
Nino Richter	
Oliver Krause	Untitled INC
Panagiotis Georgiadis	Alpes Lasers
Patrick Guay	Vanbex
Peter Broadhurst	Kaleido
Peter Danko	eDelivery

Peter Milan Trapp	Untitled INC
Pierre Marro	European Commission
Reto Gadiant	EU Blockchain Observatory & Forum
Ricky Thiermann	Spherity
Simone Ravaioli	Digitary
Stefan Beyer	S2 Grupo
Sven Laepple	ASTRATUM
Thomas Kanga-Tona	AIM International
Thomas Tremel	Microsoft
Tom Lyons	EU Blockchain Observatory & Forum
Ville Sointu	Nordea Bank
Volker Skwarek	HAW Hamburg