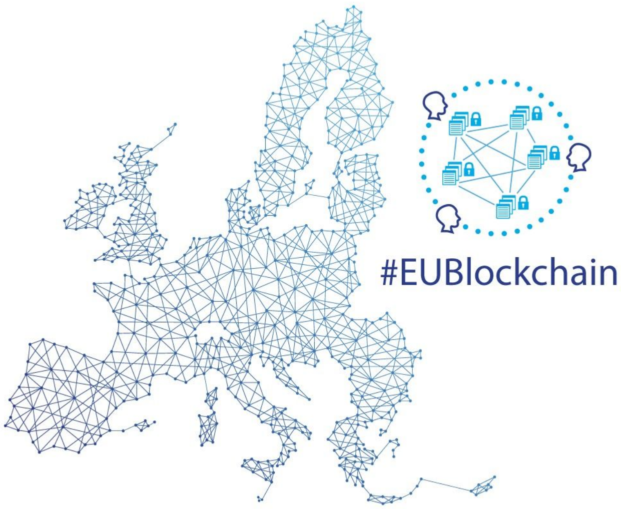
EUBlockchain
Observatory and Forum
An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY & FORUM

Workshop Report -
Research priorities –
Brussels, 18 February, 2020



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.

Author: Tom Lyons
Published on 30 April, 2020
Comments and inquiries may be addressed to the following email: info@eublockchainforum.eu

Table of Contents

Introductions and objectives of the day

- This workshop was intended to explore the state of play of blockchain research in the EU. The goal is to analyse what set of topics are currently being researched within the EU and how the EU compares to other regions. What is at stake is ensuring that Europe has enough blockchain-related research efforts and that they reflect the needs of the ecosystem.
- With that in mind, an area of focus is to identify market needs that are likely to lead to practical and widely used implementations. Here what's at stake is to help prioritise the emergence of flagship projects in Europe by fostering collaboration between academia and private actors.

Presentation: Examples of blockchain related research

Nicolas Liochon (ConsenSys)

- The field of blockchain research can be categorised in terms of 4 + 1 problems.
- The 4 problems are:
  - **Scalability:**
    - Increasing transactions per second
    - Parallelisation (sharding, sidechains)

        - Proof-of-Execution (rollups)
    - **Privacy:**
        - You want to be able to hide things (balance, transactions, fact that you are doing transactions) and to choose for whom they are hidden (some participants, everyone).
        - Partial solutions include: Account-based systems, UTXO based systems, but there are issues of scalability
    - **Generalisation:**
        - Can you do any type of transaction? Are you Turing complete, and if so, is it efficient? What are the risks?
        - Are contracts compatible with privacy and scalability? How easy is it to analyze what the contract is doing?
    - **Decentralisation:**
        - Bitcoin and Ethereum were supposed to be decentralised, but mining has become centralised: economies of scale lead to centralisation.
        - There are ways to increase decentralisation: e.g., sharding.
- The +1 problem is **User experience**:
        - Can we safely implement the system? Is it easy to use, administer, regulate?
- So how can we solve them?
    - First you have to pick what to work on. Often, however, that leads to too many topics. So it can be useful to group them into generalisations. One way to solve a number of problems is by distribution (sidechains, sharding). Another by specialising (state channels). And so on.
    - You can also combine solutions: state channel on a sidechain; rollup on a shard; plug a state channel on a rollup plugged into a shard.
- An incremental approach is often good. Some examples.
    - **Scalability.** Blockchain is a trustless system: we verify by re-executing all transactions. This is very slow. Zero knowledge proofs (ZKP) are a method to provide a large incremental boost. With ZKP you can prove you know something, without revealing it. Examples: you want to rent a flat, you need to show that your earn enough money to pay the rent, but you don't want to reveal your salary; or you are a mathematician asked to find a solution to a problem and you want to prove that you found the solution without revealing it. On a blockchain we can use ZKP to replace the re-verification of all transactions. The blockchain becomes a place where we store proofs, not all transactions.
    - **User experience:** As you improve the system, you need to have checkpoints to ensure that user experience is also evolving along with the improvements. This too is working incrementally towards improvement.
- Designing improvements brings new challenges, and so has a big impact on research
    - Developing new protocols to address scalability, privacy, etc.
    - Implementing these protocols
    - Devising new cryptographic schemes, implies new cryptographic primitives

- Hardware developments are important too: New CPUs, GPUs, FPGA, ASICs. All have an impact. This is not the realm of mathematics but of low-level electronics.
- When designing new protocols/cryptography, planning is key.
    - First, you ask if you can devise a universal scheme for your problem, then research that. For example, can you have a universal scheme for zero knowledge?
    - Then implement and test, have it analysed.
- The amount of time it takes to solve the problem is important. It may take 10 years for a full solution; but perhaps it is possible to implement partial solutions along the way. If so, do so.
- In terms of research priorities, there are two fronts to tackle simultaneously:
    - **New cryptographic tools.** These are generating a lot of excitement, but will take time to perfect, yet some short-term benefits can be expected.
    - **Developing good UX.** This another set of key research problems, should be tackled in baby steps.
- Implementation is its own research problem. Just because you have the mathematical tools, doesn't mean implementation will be easy. Implementation research has two parts:
    - user experience (how can I make it easy to use);
    - implementation (how can I implement it)

Panel discussion: Academic collaboration in the EU for blockchain

Roman Beck (IT University of Copenhagen); Bodo Balazs (University of Amsterdam); Giacomo Vella (Politecnico di Milano); Astrid Stroobandt (Howest University of Applied Sciences)

- To start the panel discussion, Giacomo Vella presented some of the findings of the Blockchain & Distributed Ledger Observatory of the Politecnico di Milano.
- Key findings in 2019 included:
    - The number of worldwide business applications of Blockchain is growing (+56% in 2019). But the number of concrete projects worldwide is still low (158 in 2019).
    - The market is still more focused on platforms than applications.
    - 65% of the projects in 2019 developed by companies created a new platform. This trend could be a risk for interoperability and for the "Internet of Value".
    - There is still a lack of international projects. The great majority (73%) of projects in 2019 is located only in one country. EBSI could be of great help in Europe.
    - Investments in Blockchain in Italy are growing (+100% in 2019) but are still only around 30 mln €.
    - There is a strong lack of competencies and skills. Companies struggle to find talents with Blockchain competencies and training.
- The EU blockchain ecosystem could benefit from:

    - **Best practice:** Academia should identify best practices and disseminate knowledge among companies and public bodies. This is essential to avoid mistakes being made by less experienced companies.
    - **Collaboration:**
        - Academia should collaborate with regulators to help draft laws and regulations on Blockchain. The role of Academia could be also to express the needs of the market in an impartial way.
        - Universities (especially those with also technical skills) should actively participate in projects (eg. becoming a node of EBSI). The collaboration with the private sector should be enhanced.
        - Academia in the EU should collaborate to give a critical and unbiased view on the EU Blockchain ecosystem. Today most researchers are focused only on one country.
    - **Education:** Universities should provide more courses on Blockchain and DLT both for students and for professionals.
- The event then moved to the panel discussion
- Regarding the maturity of the technology, and how far we are from solving the main technological issues, things already work on a simple application level, like payments. This can be done today at no great risk. On a larger infrastructure level, for cross-border applications, doing business abroad, transferring credentials, that is not ready yet. In terms of larger-scale platforms in production, China is probably ahead.
- It is hard to isolate different trends in different countries, but you can observe that in many countries the blockchain use cases reflect the strengths of the country. Spain and Italy are focused on food track and trace, protecting for instance the Made in Italy brand. That said, financial use cases are important in all countries to a degree.
- There is lots of academic research on technical topics associated with blockchain; less on analysing how business could use blockchain.
- Mapping the ecosystem remains a huge challenge. The only way to do that today is to read all the media reports and then analyse every project. It is time consuming and not very precise. A better approach would be to get companies with successful initiatives to work with academics or authorities and report their experiences and best practice.
- Looking at the development of the technology from an ethical/societal standpoint, one concern is that much research today is very short-term, often sponsored by corporations. We need research on the longer term, ethical and societal consequences. There are three main visions underpinning blockchain now: the crypto anarchist vision of avoiding all authority, the authoritarian vision of using these technologies for societal control, and the corporate/Libra vision of creating large, privately-owned jurisdictions. The question is whether there is a fourth vision for Europe, where these technologies develop with democratic oversight.
- In terms of best practice learnings from other technologies, a good case is copyright protections and P2P file sharing. Here we saw a divergence: very strict regulation on the one hand, and a vibrant piracy underground on the other. We need policies that don’t

push users into evasion. That is a learning. We also need policies that serve the public interest, not just business or geopolitical ones.

- It is important from an educational perspective to deliver the profiles of tomorrow. So it is important to be multidisciplinary. Technical skills are important, but so are other skills, But also other skills important for consultants, like project management. It is important that students have a good overview of the tech but also of other fields, like social sciences, political science, the law. Sometimes IT students shy away from those kinds of subjects, but they are important.
- When talking about blockchain education you need to ask what kind. Are we educating just technologists, or also philosophers, lawyers, entrepreneurs, C-suite decision makers? You need different tracks, like a protocol track, a use case track. And there are different disciplines.
- There is a good amount of international cooperation among academics in blockchain. Yet there could always be more.
- We need more emphasis on education within the region. It is important to have a national and regional level discourse on a number of blockchain-related topics. Privacy, for instance. So much of the media and public opinion is focused on negative narratives, like energy consumption or use of cryptocurrencies by criminals. But also for policy makers, so they can make evidence-based decisions.
- Collaboration between academia and the private sector is important for blockchain. A lot of companies do not understand blockchain, but there are many also who do, for example consultancies. So a lot of know-how there. But also it is hard to understand the potential of blockchain and its use cases if you don't talk to companies. An academic institution can also provide a neutral, pre-competitive environment for companies to work together on blockchain research and education. This is one of the things the Blockchain Observatory at the Politecnico di Milano tries to do.
- When it comes to research, we need to do more on the impact of technology. Scientists and engineers are building risky technology in the middle of society and not necessarily understanding the impacts. We need to better understand the rules of how technology interacts with society. Just like in physics, we need instruments to measure these effects. We need safeguards. The question is how do we build instrumentation to predict the development of a technological process in society, to monitor the actual development, and to stop it if needed. This isn’t just ethics. The question is also what you can enforce.
- EBSI has an opportunity to improve communication around blockchain, to inform the public on subjects like self-sovereign identity, or digital transformation in general: what these things mean for the individual and also for civil society.
- EBSI could look at interoperability. It won't be the only platform, not all will run on it. So the question is how projects that are already live can interact with EBSI.

Panel discussion: Research priorities for early implementations in live applications

Arnaud Le Hors (IBM); Ivona Skultetyova (Tilburg University); Marc Taverner (INATBA)

- There is innovation happening everywhere in the blockchain space: in technology, regulation, academia, legislation. Lots of the innovation in regulation has to do however with regulatory arbitrage. Europe has to be careful of this. Innovation is not just about new ideas and technologies. It is also about execution and deployment. There are many parts of the world that are outpacing Europe on this score. Europe needs to beware here too.
- Blockchain is about transparency, yet people want privacy, and there has always been a tension in blockchain between these two. This has traditionally been reflected in the difference between the public/permissioned and private/permissionless blockchain world. Yet these two worlds are converging. This is thanks in part to the new privacy-preserving technologies, about which there has been a lot of excitement. With these new privacy-preserving technologies, you can have your cake and eat it too. You can have privacy and auditability. There is a huge demand for this. Hyperledger Fabric is going in that direction, Hyperledger Indy too. WIth each new release there are new privacy features.
- We often talk about interoperability, but it is not clear that there will be a lot of interoperability at the framework level between networks with radically different architectures. We talk less about integration, which is however important, desirable and possible. For example if you have two permissioned networks and you have a payment on one network, and a related asset transfer on the other, you want to make sure that these happen at the same time. That they are coordinated. Hyperledger is seeing an increased number of proposals to do these kinds of things, for example via overlay networks. This is an important area of research. Other important areas of research include quantum safety and how to blockchain and the physical world. We don’t talk about that as much as we used to, but it remains vitally important to ensure that information that makes it onto an immutable blockchain is accurate. A lot of work here for example with IoT.
- Another challenge is to reconcile the legal and regulatory framework with the fast moving technological advances. A good example is digital assets. While the ICO boom is over, the innovation potential was made clear. This was a completely new approach to capital formation, with these digital tokens that are sometimes hard to classify: sometimes utility token, sometimes payment, sometimes a security, sometimes a hybrid, often hard to be sure. This is difficult for regulators and lawyers to imagine. Yet there is great potential in these new approaches. When thinking about how to reconcile these problems, first of all, it is probably not good to change the law too quickly. Better to wait and see how markets

develop. That said, regulatory sandboxes, where regulators and companies can learn together in a controlled environment with near market conditions, are a very good idea. There is a lot of talk about regulatory sandboxes but actually very few countries do them. Perhaps this is something that could be done on a European level.

- When looking at the challenges that projects face or the reasons that they struggle or fail, it is often not a technology problem. You need to look at the actual product or service being offered. The uptake of dApps remains very low. They are still very much the domain of enthusiasts who understand the tech and can accept bad user experience. That is one problem. Another is that this is a network technology.
- Unlike other emerging technologies like machine learning that you can run on your own and about which you can make your own choices, there is little value in running a blockchain network by yourself. It is a team game, and you have to be part of an ecosystem. So governance is a real challenge. How to get a group to agree on what they want from the network, and how to get there. The cost of building a dApp or product in this market is not insignificant, so if you don't have a market for your product, you will run out of money quickly. An area with more potential is in applications within the control of governments to “give birth” to, like in identity, healthcare, wealth distribution, areas where there are inefficiencies, large markets, and often lack of trust between citizens and public bodies.
- That said, there are success stories. IBM Food Trust for instance started with a project by Walmart to track and trace certain products, and now has been extended to use by others. Carrefour developed an app where consumers can check provenance of an item on their store on their phone. The companys saw sales of that item go up, so now it is doing this for products throughout the store. These kinds of apps benefit the store but also consumers interested in the provenance of the products they buy.
- One key area where there should be more investment in research is convergence and integration. For example, the convergence of blockchain with IoT, AI and other technologies. We can generate a lot of data with these technologies, but blockchain can help secure that data and prove its provenance. That is very important, for example in things like facial recognition. Focusing on these areas could be an advantage for Europe.
- Research in the area of governance is also important. The governance of applications, of networks, onchain vs offchain governance. We are seeing a lot of experiments in this area and it is a fascinating field of study. This could be something where Europe excels. In terms of regulation, it is important not to make too hasty decisions. We should be pro innovation but also continue to protect the public interest.
- The panel was also asked for examples of projects that have managed to translate research findings into real implementations and if we can already derive best practice from that. In the Netherlands, for instance, there was a bank that, two months after having read a research paper on the subject of how blockchain could improve shareholder voting systems, ran a live test of a blockchain-based voting system at its annual meeting. The blockchain voting took place in parallel to the traditional voting and

was not binding. Because the test was successful, the bank plans on using the blockchain-based system at the next annual meeting.

- Running such tests in parallel to live systems is a good approach, and we have seen that elsewhere. For example, the blockchain-based land registry in the country of Georgia first ran in parallel to the legacy system. This reduced fear of failure and was a natural safeguard against problems. That helped eventual acceptance of the system.
- In large companies doing blockchain development, research is an integral part of the process, and cannot be separated from implementation. This is a function among other things of how young the technology is.
- In the QnA the topic returned to the problems of agreement and governance in permissioned networks, like consortia. Experience has shown that communication among partners is key but can be challenging. It is often good, when contemplating such a network, to make a list of representative players in that sector or industry such that no set of actors feels disenfranchised, but to keep the group manageable, so that communications are not overly difficult.
- Research is often accidental, in the sense that individual teams research what interests them or specific problems related to their project, and sometimes unexpected results lead to the accidental discovery of usefulness in other areas. The question is if there should be a more broad-based, regional or even global research agenda. That could be difficult to do, but efforts to help researchers communicate and connect, so that they have a better idea of what others are doing and what results are being found, could be very useful. The goal is to turn the unknown unknowns to known unknowns as much as possible.
- Europe produces as much research as any other region, but is not always as good at commercialising it or bringing it to market. Patents are an issue in Europe, as it is more difficult to patent inventions here than elsewhere. This can help keep the cost of innovation down, but is also a barrier, because patents can act as an incentive to research and development. It is wrong however to see the patent process in direct contrast to open source. Often they go together: patenting inventions can be a way to protect investment in open source.

Working Session: Research priorities and way forward for the EU

- The final session of the day was dedicated to an open discussion among all participants on the subject of research priorities for the EU.
- Questions revolved around
    - **Technology**: What challenges should be focused on, for instance areas like scalability, privacy, interoperability, energy efficiency. Here are five main sub-challenges: Privacy, Scalability, Decentralisation, Security. Energy use.

  - **Risk assessment challenges**: What critical topics should be explored in areas like security, governance, legal framework.
  - **Use cases / protocols**: What use cases should be prioritised in terms of impact, in areas like energy, public sector use, bitcoin mining system, etc.
- Blockchain convergence with AI/IoT was proffered as one important use case.
- In terms of research priorities we need some kind of generalisation of business applications: Many sectors work on the same underlying use case just in different contexts. If there was an agreed path to follow research learnings and best practice could more easily be shared. New sectors wouldn't have to reinvent the wheel. Indeed, case study methodology is perfect for looking at specific things and then generalising from them, especially when there is not too much data available.
- Design is an important area of research that often gets overlooked. User interface and UX design are also important cross sectors.
- Interoperability was seen as important too, but not necessarily a standard research topic, as most research topics are focused on single issues, while interoperability/integration tend to span multiple topics. Interoperability/Integration is also a question of standards.
- The Observatory's healthcare workshop focused on the use of various privacy-preserving techniques to deconstruct data silos in healthcare to make data generated in hospitals, insurance companies, etc. available for research in privacy-preserving ways.
- Different priorities are more or less adoption-relevant. Quantum security is not necessarily a driver of adoption today, whereas scalability is.
- Sometimes problems that seem like technological ones are actually not. Energy efficiency of blockchains, for example. This can be solved by technology. But on the other hand, energy use in Bitcoin serves to secure the network. If society considers that highly valuable, then perhaps energy efficiency is not an issue. That requires a different kind of research and scientific agreement than just the technology.
- Research into smart contract languages, with formal proofs, could be important. These are often new programming languages and are deployed in high-stakes use cases (value transfer).
- Decentralisation should have overall priority because it is the desire for decentralisation that drives a lot of the efforts in blockchain. So you need to understand what decentralisation means first.
- In terms of readiness, in areas like ZKP it is very hard to assess. It often depends because there are new schemes with different properties, some are close, some are quite far away. Some schemes that are close to being ready are good for some use cases, other schemes that are far away are better for others. In terms of a universal ZKP scheme, probably five years away. But we don't always need a universal one, depending on the use case.
- In terms of risks, focus needs to be on security risks, legal and compliance risks, systemic risks of decentralized technologies and user experience related issues (loss of private keys)

- In terms of systemic risks, one panelist was concerned about the creation of large cartels working together on these technologies.
- To mitigate smart contract risk, it might be good to focus more on deterministic logic than on Turing completeness.
- Blockchain is the technology of trust. We need ways to evaluate how trustworthy blockchain-based platforms really are. Not just a question of technology but also governance and related things.
- Decentralised identity has its risks. There are compliance issues, like KYC/AML, but also security issues, as when someone loses their private keys related to identity information.
- While not a classic risk, we should look at barriers to institutional adoption from institutions not able to adjust to change.
- Unbundling of legacy institutions is also a risk. Banks are unbundling their offerings, and perhaps there is a risk that the benefits banks bring us might be lost without a replacement. This could happen in education, health logistics, anywhere where decentralisation is introduced. We need a way to assess that.
- Fragmentation is a risk. That is what integration is important. It is highly unlikely that we will end up with one blockchain technology. There will be several. So lack of integration capability is a risk.
- User experience is a critical risk in terms of driving mass adoption.

Appendix

Workshop slides

- EU Blockchain Observatory and Forum Research Priorities Workshop Deck

Workshop videos

- Videos from this and all other workshops can be found on the EU Observatory website under reports.
- Videos specific to this workshop:
  - Research Priorities Workshop Video - Part 1
  - Research Priorities Workshop Video - Part 2

Official agenda

Time	Activity
9:30	**Registration & Welcome Coffee**
10:00	**Introductions and objectives of the day**
10:15	**Presentation: Examples of blockchain related research** Nicolas Liochon (ConsenSys)
11:00	**Panel discussion: Academic collaboration in the EU for blockchain** Roman Beck (IT University of Copenhagen); Bodo Balazs (University of Amsterdam); Giacomo Vella (Politecnico di Milano); Astrid Stroobandt (Howest University of Applied Sciences)
12:15-13:30 Lunch break	
13:30	**Panel discussion: Research priorities for early implementations in live applications** Arnaud Le Hors (IBM); Ivona Skultetyova (Tilburg University); Marc Taverner (INATBA)
14:30	**Working Session: Research priorities and way forward for the EU**
16:00	**End of the day**