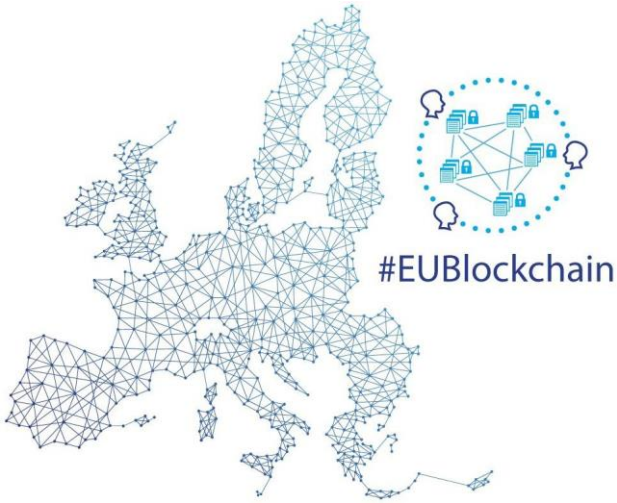
EU Blockchain Observatory and Forum

An initiative of the European Commission

EU BLOCKCHAIN OBSERVATORY & FORUM

Blockchain and Smart Contracts – Online workshop, March 10, 2022



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

Author: White Research
Published: March 2022
Comments and inquiries may be addressed to the following email:
info@eublockchainforum.eu

Table of Contents

WELCOME

Christian Hauschildt, Managing Director at White Research, welcomed everyone to the workshop organised by the EU Blockchain Observatory and Forum. In his opening remarks, Mr Hauschildt introduced EUBOF and covered basic housekeeping including how to use the Q&A function, that the workshop is recorded, and both the recording and workshop report will be published on the EUBOF website. After the introduction of the panellists, Mr Hauschildt handed over to the first keynote speaker, Dr Joshua Ellul, the Director of the Centre for Distributed Ledger Technologies at the University of Malta.

Dr. Joshua Ellul began his presentation by explaining what Smart Contracts are and how technology and law are colliding. He described how in the beginning, we exchanged money through peer-to-peer cash transactions, but as we moved to online payment systems, we needed to go through a bank and lost this direct peer-to-peer payment option. Cryptocurrencies like Bitcoin reintroduced a peer-to-peer payment to digital spaces. Dr Ellul notes that this achieved the decentralisation of monetary systems, where there is no central point of authority. Going into more detail about what cryptocurrencies are, Dr Ellul described how a number of different computers work together to create a single shared ledger to keep track of all transactions, all accounts and all balances. He then mentioned the creation of Ethereum in 2013, which provided a method for executing programmes and software on a blockchain. It operates in the same way as cryptocurrencies, whereby computers work together to create a system of accounting as well as the abstraction of a single shared computer with no centralised controller that software and programmes can be uploaded to and used around the world. These software and programmes, or Smart Contracts, have achieved the decentralisation of computer systems. With the computing system embedded on a blockchain, no one can alter the functioning of this system like the way website owners can. Dr Ellul then provided examples of what a smart contract may do. In his first example, a few lines of code were presented to automatically dictate payment. In another example, the code implemented a voting process, from keeping track of votes and to the actions to be taken to determine who won the vote. In these examples, these Smart Contracts do exactly as they are written, nothing more and nothing less, and no one can interfere with this. Dr Ellul points out that this is what makes blockchain so special—that not even the developer can change a given code. This system is perfect for automating agreements, since code will do exactly what it was written to do, forever. Nevertheless, Dr Ellul brings up that code can fail, and in the past, this has led to millions in losses. He states that this will continue happening, so we must create methods of minimising the risk of code failing. Although code failing is a weakness of Smart Contracts, Dr Ellul provides an example of a legal contract failing to be interpreted in the way it was intended due to a single comma missing, which resulted in a $13M pay-out, pointing out that it is not only Smart Contracts that can have bugs. Dr Ellul then goes on to distinguish the differences between Smart Contracts and legal contracts. Legal contracts define obligations and the consequences if these obligations are not met. They can be subjective, especially as they involve the interpretation of judges, lawyers and involved parties. Smart Contracts do not allow for individuals to break agreements, because the code operates exactly how it is written regardless of the actions or interpretations of others. Smart Contracts also typically do not require third parties, such as lawyers or judges, for their interpretation, as enforcement is automated. While Smart Contracts have the potential to be legally binding contracts, they are not always legally binding. This is an area in which further research is being done—how to ensure parties are legally protected if something goes wrong with the smart contract and how to create rapports in the legal world to ensure individuals are legally secured. Research being done at the University of Malta is looking into how to bridge the gap between the legal world and the tech world in cases where code has malfunctioned or Smart Contracts need to be legally enforced. This requires both lawyers and IT professionals to work together, or law-grammers / law-velopers who are familiar with both law and code. The view of the University of Malta is that this will likely be done through multi-disciplinary teams, which is why they strongly support multi-disciplinary education, which is very common in the blockchain

sector. Dr Ellul closed by providing another example of code that had the re-entrancy bug coded within it; software developers without experience in Smart Contracts would likely not catch this bug. Code cannot be updated, as Smart Contracts are immutable. Original code can allow for workarounds that can change logic, but this loses the decentralisation that Smart Contracts bring. This leads to the final question of governance – who should be able to decide on changes to code?

PANEL 1

The first panel was moderated by Dr. Kristina Livitckaia from CERTH, member of the EU Blockchain Observatory and Forum, who introduced herself and then made her opening remarks for the first panel, followed by a short introduction to the panellists.

Panellists:

- Daniel Szego – DLT Architect
- Tooba Faisal - work item leader for Smart Contracts at ETSI PDL, King's College London
- Mark Cudden – CTO we.trade
- David Arroyo – Member of the Spanish delegation to ISO TC 307

Presentation 1 – How not to be agile in smart contract delivery, by Daniel Szego, DLT Architect

Daniel Szego, software architect in DLT, began by introducing himself and his work, which focuses less on the public blockchain and more on enterprise and consortium work. Mr Szego then discussed what agile methodologies are. Agile methodologies began as a software development methodology, but is now used in many spaces, including project management and organisational development. The focus is on fast reactions, adaptations of changes, and experimentation. This is realised in different techniques, such as cross-functional teams, self-managing teams, and quick decision making. On the contrary, smart contract governance tends to be completely different. Blockchains were designed to be mission critical systems. For example, Bitcoin was designed with a core 'money' function; this central logic cannot and should not be changed. This stability is a core principle, and this is the same for Smart Contracts as well. To be more specific, there tends to be two requirements of a system: one part which is highly stable and shouldn't be changed unless there is a bug, and another part of the system that can be changed through a predefined governance process. Any change will typically require the involvement of multiple parties, often consisting of hundreds to thousands of individuals. This use-case typically exists in every smart contract development, with the exception of cases where the administrator is given control to make changes. Mr Szego provided an example of a specific research and development use-case that focused on digitised money research and experimentation. In such payment vs. payment or payment vs. delivery use-cases, which include commercial banks, supervisory authorities and central banks, defining the governance model can be difficult. Deciding who should be able to make changes is not always straightforward; whether it should be individual actors, such as central banks, or a majority / supermajority consensus of banks is something that needs to be decided by the group. The conclusion of Mr Szego if one wants to implement something agile in smart contract delivery is to incorporate three phases in the life cycle of the smart contract. The first phase is the proof of concept or prototype phase, where one can be as agile as they want and experiment with different potential systems. The next phase should be a pause in the development process, where the details on specifications and governance models are finalised and the quality assurance, security audits and testing take place. After this break, one can go live, but it should not be expected that the production system changes much at all after this phase.

Dr Livitckaia said thank you for a great start to the first panel and then introduced Tooba Faisal.

Presentation 2 – Smart Contracts and their applications in 5G and Beyond, by Tooba Faisal, work item leader for Smart Contracts at ETSI PDL, King's College London

Tooba Faisal introduced herself and King's College London, which she was representing. Ms Faisal began by introducing Smart Contracts. Smart Contracts are software codes installed on distributed ledgers, which are immutable data structures where all the participants keep a copy of the ledger. The properties of the ledgers are transferred to the Smart Contracts, so they are immutable, auto-executable, and transparent. In Hyperledger fabrics, the level of transparency can be specified per node; for example, it can be specified that only direct parties in the contract keep a copy of the ledger. Ms Faisal then highlighted specific security challenges to Smart Contracts. The first being transparency—because ledgers are transparent, Smart Contracts are visible to all parties in the network, which is not always ideal as unintended parties may have access to this information. The second security challenge is that Smart Contracts are auto-executable. Erroneous code can trigger unwanted functions of the code, which may cause monetary losses such as unwanted payments. The last security challenge is that Smart Contracts are immutable. Smart Contracts cannot be changed once they are published, so erroneous code and dormant contracts can be dangerous if they are not properly secured. While old codes can be deleted, this ultimately defeats the purpose of distributed ledgers. Because of these concerns, Smart Contracts should only be installed after very careful planning. Ms Faisal provided an example of what the lifecycle of smart contract development should look like, based on the research project being conducted at KCL. The first phase is the planning phase where all the stakeholders are involved to define what the specific needs of the group are for this specific smart contract and whether the contract meets the standards of the supervisory body. The second phase is the code testing and verification phase. This is done on test beds and per specifications that the research group outlines in their upcoming report. After the code is tested properly, the contract moves on to the deployment phase. Although Smart Contracts cannot technically be terminated, the research group advocates that termination should be incorporated into the smart contract through internal self-timers. This would result in the smart contract becoming securely dormant. After following this process, properly secured Smart Contracts can be used as service level agreements between service providers and consumers that are accountable, automated, and transparent. Ms. Faisal provided two different scenarios in the telco sector in which this process was followed. In the first architecture, service contracts were digitised on the distributed application system that was accessible by all users. Users could then choose their service contracts as per their own needs and requirements at any given time. For example, if one needed an extremely strong internet connection for the next three hours, they could choose that service contract and pay extra for the specified time. Further details on how quality and security in this architecture are insured is explained further in the research paper linked on the presentation. Ms Faisal also discussed whether permissioned or permissionless distributed ledgers should be used for Smart Contracts. In a comparison between two different fabrics, there was a significant difference in the execution latency between the permissioned and permissionless ledgers. Based on these results, the group advocates for permissioned ledgers. The second scenario concerned infrastructure sharing. This consisted of an open architecture whereby multiple parties can own and use the network, which was based on how infrastructure is expected to be shared in 5G and 6G. All devices were equipped with a PDL node, which then forms the actual telco infrastructure and enabled devise sharing. This was evaluated on Ethereum and used GNS 3. Algorithms were in place to monitor the device usage and a governance node monitored the network resources to ensure that no party was abusing the system. Ms Faisal highlighted that the nodes were run on a laptop that shared software, so the execution latency in their testing took longer than would be expected when using specialised hardware. Smart Contracts should take into consideration the protocol for permissioned distributed ledgers as well as the design of the network. To conclude, Ms Faisal argued that Smart Contracts provide a viable mechanism because of their transparency, auto-execution and immutability. However, there needs to be proper planning and consideration to enable their viability, such as through management and standardisation initiatives.

Dr Livitckaia said thank you for the crucial details and introduced Mark Cudden.

Presentation 3 – Using Smart Contracts in Trade by Mark Cudden, CTO we.trade innovation DAC

Mark Cudden introduced himself and his work with we.trade, which was the first blockchain-based digital trade finance platform. They are a joint venture with eleven European banks and focus on the challenges of SME European trade and deliver a robust digital trade network supported by a concrete Rulebook. Mr Cudden began by discussing the unique value of a blockchain, including that it is a multi-party system and it records data in a way that multiple stakeholders can access and share data at the same time. This allows those who need access to the data to easily have it, while still being able to restrict access to others, as needed. Optimisation and digitisation of current processes does reduce manual steps, but not to the extent that blockchain can minimise the steps in the process. Mr Cudden then outlined the four core blockchain solution building blocks. The first is the shared ledger aspect which avoids duplication and is immutable. Because they use the Hyperledger fabric, they are able to segregate data, determining who can see what, through the private data collections. The second building block is cryptography, which ensures authentication and verifiable transactions. The third aspect is that blockchain is a trust system, which refers to using the power of the network to verify transactions. Mr Cudden prefers to call this a 'trust system' rather than a 'consensus system' because not all validation is done through complete consensus, and the trust comes from the immutability of the blockchain. Lastly, the final building block is the smart contract. These are the business terms that are embedded in a blockchain transaction database and executed with transactions. They are considered to be the 'rules' of a blockchain solution and are needed to define the flow of value and state of each transaction. Mr Cudden then moved on to discussing regulations and certifications. One of the main reasons Smart Contracts are discussed is for the purpose of regulations and certifications. Building a system requires a business mindset, including compliance with relevant industry or geographic regulations such as GDPR, PSD2, ISO 27001, ICC URDTT, SOC 2 Type 2, and FIPS 140-2 (HSMs), which we.trade has set up methods to comply with. In addition to these regulations, we.trade has set up a Rulebook that governs the behaviour of all participants on the network. When designing Smart Contracts, it is important to define first how these contracts would be combined and work together at a business level, such as by creating a ubiquitous language, making sure they understand each other, and bringing in technical staff to understand common terms, rules, and process flows. When this is all taken together, a new business model can be created. As the business or legal flows are fully understood and combined, these can be turned into Smart Contracts that can be executed by the computer. The strength of Smart Contracts lies in their being multi-party systems and multi-party transactions. If this is being created for a single-party system, then the question should be asked whether blockchain is truly the right solution for that case. Smart Contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without the involvement of third parties. They automate workflows, triggering the next action once the conditions have been met. Mr Cudden discussed next how Smart Contracts are used at we.trade. In traditional trade, there can be a lack of trust because not all parties working together know each other intimately and are familiar with the others work. There is a lot of risk involved in traditional trade including interparticipant chatter whereby a lot of detail can be lost, inefficiency, lack of visibility of end-to-end transaction, cyber risk fraud, risk of non-payment, and being prone to error. From a blockchain enabled trade finance platform, such as we.trade, the use of Smart Contracts makes this process significantly more efficient. All parties have easy and efficient access to finance, increased visibility, less paper-based processes, less cyber fraud risk, and use alternative products to Letter of Credits. From a sellers perspective, the risk of non-payment is lower because they can see when payment transactions have been made. It is important to be careful how many Smart Contracts are developed, however, as they do take a lot of overhead to maintain. There has been a great deal of movement in this area because this is an industry that has not been digitised in over 150 years. From a we.trade perspective, they have also created a legal Rulebook enforced through a set of Smart

Contracts since there are not yet set standards for this space. We.trade includes the entire global trade ecosystem. While it can be difficult to do continuous integration and deployment from a blockchain-based solution, from a maintenance and delivery perspective, it is not impossible. Because we.trade is a permissions network and set up through a consortium, it is more efficient for them to use this process.

Dr Livitckaia thanks Mr Cudden for the insights and introduced David Arroyo.

Presentation 4 – Current challenges in the standardization of Smart Contracts, by David Arroyo, Member of the Spanish delegation to ISO TC 307

David Arroyo introduced himself and the Spanish research council, which he was representing. Mr Arroyo began by describing Smart Contracts and potentially problematic usage of language when describing them. It is not an accurate term as they are not always smart, in terms of being auto-executable, and not always contracts that can be enforced. Technology is also not neutral, and it cannot be regarded as such. While the underlying systems can be dependable, they are not totally trustworthy. What needs to be focused on is creating trustworthy systems, not only trusted systems. This is important for Smart Contracts because in many cases they are developed to solve well-known problems in the development of secure software. In a smart contract, many of these issues remain, only with the added complexity and the inability to create continuous integration in a fast and efficient way. Mr Arroyo's presentation provides a summary of aspects that can be assessed in detail in testbeds that often have reoccurring issues across software development, including re-entrancy, arithmetic over / under flows, unexpected ether, delegate call, default visibilities, entropy illusion, external contract referencing, short address or parameter attacks, unchecked CALL return values, race conditions or front running, and denial of service. These are almost the same as what would be found in general web development, which brings Mr Arroyo to the conclusion that security issues in software development are not being solved. While solutions such as blockchain bridges have been put forth, these incorporate a risky scenario that should be tackled in a different way because they introduce a backdoor that then centralises a decentralised system. Mr Arroyo then provided research papers that he has worked on that delve further into these issues. When discussing blockchain, they are presented as trust machines; however, this must be verified, there should not be just blind trust. Algorithmic governance should also be complemented by a corporate or social governance, or else the biggest issues in the digital ecosystem are not being tackled. Related but separate ledgers and actors that are integrated must be integrated properly; it cannot be assumed that a single robust ledger will make the entire system robust. Mr Arroyo brings up the example of cloud systems, which are often used, that are not directly controlled by the parties involved, even by the relevant governments, leading to increased risked and lack of security in otherwise robust ledgers. There is an internet protocol upon which blockchain technologies are deployed, and this must be always taken into consideration. In order to have a proper governance scheme, various intervention systems should be discussed. For example, the creation of interfaces that gather Critical Tracking Events and Key Data Elements can be done in either an automatic way, a semi-automatic way, or through the intervention of a human being. The governance system should not just be set up in the smart contract, but also within separate intervention systems and the entire life cycle of the data. This problem has been well studied in the field of artificial intelligence, in which 'human-in-the-loop' solutions have been put forth so these processes are not entirely automated. While automation is useful and should be used, a level of control should be maintained so that these contracts can be managed in a way that is aligned with the values of transparency and accountability. It would be useful to have systems where humans are involved in the decision-making processes, but eventually to also create 'society-in-the-loop' systems that incorporate proper checks and balance systems and the involvement of stakeholders with competing interests. Without the inclusion of diverse interests and perspectives, these systems in the end may not be very trustworthy. This is something that is being taken into account in several projects worked on by Mr Arroyo. He provided a specific example of the overreliance on external electronic equipment from untrusted vendors, in which it is not transparent what data is maintained and how information is processed by the external devices. This is something

that the European Commission has introduced initiatives to work towards. One cannot have trust without trusted platform models. The approach applied in this project can be applied to many different scenarios in order to create solid and robust identities that perform authentication, authorisation, accountability and auditability, which is required for systems to be trustworthy. Without assurance that systems are trustworthy, we cannot be clear about the credibility of the data and information being accessed. Although information on a blockchain is immutable, it has to have been previously curated by automatic, semi-automatic, or human intervention before it is put there, and this interventions' trustworthiness needs to be ensured. While blockchain is part of the solution that needs to be taken, it is not the solution itself. Mr Arroyo provides a final example of the risks involved in off chain governance and quantum computation, including the use of data validation using classical data signatures and hashes and the constant evolvement of these risks. This is why a robust risk analysis must be included throughout the process.

Dr Livitckaia thanked Mr Arroyo for the energy. Because the first panel had run out of time at this point, Dr Livitckaia immediately introduced the second keynote speaker, Prof. Aggelos Kiayias.

Panel 1 Q&A

Since time ran out for the Q&A discussion of Panel 1, the questions and answers submitted to the Q&A function of Zoom have been included below.

Question 1 :

- **What do you consider the core requirements in smart contract project/architecture?**
- **From which sources could these requirements be identified?**
- **Must a smart contract be stored or installed on distributed ledgers?**

Joshua Ellul : If you have different parties that do not inherently trust each other and require some way to work together in a digital manner, then Smart Contracts are useful for this. If you come to the conclusion that Smart Contracts might be a good option, ask yourself "Would a cloud server (e.g. google, amazon etc) solution that someone manages be an acceptable solution?". If the answer to that is "yes" and that the different parties trust whoever manages that cloud system, then don't use Smart Contracts.
It depends on the definition of smart contract. Some subscribe to a definition of Smart Contracts that must reside on a DLT; some state that automated code in a centralised service provider (e.g. a bank) can also be seen as a smart contract. Besides this, there are ways to execute code off-chain, and then upload results to the DLT, e.g. using zero knowledge proofs.

Question 2

What is the theoretical limit of smart contract size, given that (I assume) there are space limitations to implement code on the chain? Ms. Faisal also just mentioned the need to clear variables, so there needs to be a cache too?

Tooba Faisal: Space limitations are dependent on the chain type. By clear variables I mean that revoke all access rights and make variables inactive (for example, pay to=null)

Question 3

Can you share how is customer protection guaranteed in such model of Architecture?

Tooba Faisal: Please see our paper How to Request Network Resources Just-in time Using Smart Contracts

Question 4
Hi Joshua, to clarify, do you think Smart Contracts run on managed cloud providers contradict the methodology?

Joshua Ellul: It depends. If we are individuals that want to work together, and both trust a cloud provider to execute the smart contract, than it is an acceptable solution in my opinion. Indeed, the cloud provider may have control of the system, but there are also ways to circumvent manipulation (e.g. by replicating beyond the cloud service provider).

Ultimately all solutions in this space boils down to trust. You should question the trust of each stakeholder, and come to an opinion whether that trust and centralized control is acceptable.

Question 5
For all panelists: Is it possible to introduce an 'kill switch button' into the smart contract algorithm that would allow consumers to exercise their right of withdrawal?

Joshua Ellul: Yes. “Anything” can be encoded in a smart contract. The main issue is if the code is buggy, and the kill switch doesn’t work though.

Daniel Szego: It depends how you implement the kill switch. On Ethereum at killing the smart contract withdraws the ether to an account, but you can implement other ways as well, like all customers getting theirs' invested ether.

Tooba Faisal: Yes, but you need to program this at the time of coding the smart contract. We provide details on this in ETSI ISG PDL 11.

Dr. Ioannis Revloidis: What if the requirements to exercise the right of withdrawal are not met? By this I mean, what if the person triggering the kill switch, was not entitled under the law to do so. Is there any way to reverse the effects of the kill switch?

Question 6
Hi Tooba, When comparing permissionless and permissioned blockchains and the latency of smart contract execution, did you consider using Layer 2 solutions like Polygon on top of public blockchains (Ethereum)? This would offer fast execution times while still maintaining the benefits of a public transparent blockchain.

Tooba Faisal: Hi Lisa, we have not looked into layer 2 solutions yet, but I think it will be very interesting research direction.

Question 7
What is your advice and technique to learn Smart Contracts/solidity?

Joshua Ellul: It depends. If you have programming experience, then I would say find tutorials online and just get your hands dirty. You can use remix.ethereum.org which is an easy to use IDE to start trying out some Smart Contracts. There are also other languages supported by different platforms, e.g. cosmos: golang; substrate/polkadot: Rust; Neo/stratis: .NET; Algorand: Python and many more.

If you do not have programming experience, I would recommend starting a programming course in a language like Python.
I had also written a tutorial, that I tried to make as easy as possible to follow:

- http://blockchainthings.io/article.aspx?i=2&t=1
- http://blockchainthings.io/article.aspx?i=3&t=1
- http://blockchainthings.io/article.aspx?i=7&t=1
- http://blockchainthings.io/article.aspx?i=9&t=1
- http://blockchainthings.io/article.aspx?i=10&t=1
- http://blockchainthings.io/article.aspx?i=12&t=1
- http://blockchainthings.io/article.aspx?i=13&t=1

There are also some smart contract platforms that allow for them to be created using templates (e.g. a web based interface), and no-code platforms. As well as some that allow for natural language (English etc.) definition of Smart Contracts.
I haven't tried this, but it may be something to look into: https://transientnetwork.io/.

Question 8

Hi Mark, Do you use traditional ci/cd methods in the deployment processes of Smart Contracts for the we.trade platform?

Mark Cudden: Yes, we use traditional ci/cd methods for deploying out Smart Contracts.

Question 9

It was said that we.trade is a "joint venture". Isn't this against the blockchain spirit of targeting more decentralization of control. What is the difference with a "consortium based blockchain"?

Mark Cudden: We are an industry specific permissioned network that handle financial and trade related data. The key term is permissioned network. Members who join our network are participants at various levels in trade and trade finance. There are different levels when decentralizing control in a blockchain network. This is an early decision to be made when embarking on a blockchain journey, permissioned versus permissionless, and this may be driven by regulatory, legal, security and/or audit requirements.

Dr Livitckaia introduced the second keynote speaker, Prof. Aggelos Kiayias.

Professor Aggelos Kiayias shared his presentation titled "Blockchain Governance" and mentioned that it is a very difficult topic to understand from different angles. Blockchain systems promise decentralization and one of the main aspects that is being regularly addressed is that "code is law". However, changing the code and the software system has proven to be a very difficult and controversial task. In first and second generation cryptocurrencies (e.g. Bitcoin and Ethereum), the process is mostly centralized or is entirely off-chain. The way that the ecosystem is governed is essentially an unstructured, off-chain process and this has led to quite a disagreement and debates between the community, while it has also created hard forks that divided the community itself. Professor Kiayias provided two examples, Bitcoin Cash and DAO Hack. Bitcoin Cash is considered the result of a fierce community debate, regarding the scalability of Bitcoin protocol. The debate mostly focused on the Segwit upgrade and Bitcoin and has led to quite a disagreement between the community, but also to the creation of other systems, deriving from Bitcoin and in particular Bitcoin Cash. Bitcoin Cash took a different approach concerning how scalability should be handled. DAO Hack was a form of investor-directed venture capital fund on Ethereum and one of the most important Smart Contracts of Ethereum at the time that was introduced. Nevertheless, quite some time after its introduction, DAO Hack was found to be vulnerable. The community was, once again, split and faced significant misalignment on

how to handle this issue, due to users losing great amount of money. Part of the community raised the importance of stopping DAO Hack, while other parts remained in favour of the afore quote “code is law”. The main issue of blockchain governance concerns every distributed and decentralized system. Any system that runs across different organizations becomes an important topic for how it should be properly governed. What has been observed in the next generation cryptocurrencies (e.g. Cardano, Polkadot, Tezos) is that they have taken steps to incorporate formal, on-chain methods to facilitate governance decisions. This is, according to Professor Kiayias, a very complex landscape, thus requiring a deeper approach. It is a multidisciplinary field and all elements originate from either political science or corporate organization, social choice or game theory. The merge of those elements has led to the development of a set of processes and functions that the community wishes to satisfy in the context of an on-chain governance protocol. In terms of defining blockchain governance, there is no unifying theory yet to help someone understand what the requirements are and what are the relevant problems that arise when this system is exploited. The motivation of Professor Kiayias’s joint work with Mr. Lazos is to systematize the properties of this blockchain governance protocols and present a classification of what blockchain projects have done so far. Literature review expands around different areas aiming to understand what the different properties are that governance systems should satisfy and finally project them in the context of the afore blockchain projects. The seven key properties of any governance systems that are identified and presented by Professor Kiayias are:

1. Confidentiality
2. Verifiability
3. Pareto efficiency
4. Accountability
5. Sustainability
6. Liveness
7. Suffrage

Professor Kiayias proceeded with providing an overview of what those key properties mean. Confidentiality is an important property and is considered classical, while it can be broken down to different pieces, i.e. pseudonymity, secrecy and coercion resistance. In all cases, it deals with the fact of personal choice. Verifiability is complimentary to confidentiality and deals with the ability to verify whether the end result is correctly computed based on the input that the system has received. Pareto efficiency is a crucial property from the point of social choice. It specifically deals with whether the outcome of the governance system should align with the desire of the community. Can we extract an outcome that aligns with the desire of the people that participate in a voting procedure? Pareto efficiency concludes that the system will only choose the outcome that people strictly desire.

Accountability deals with the issue of holding the participants responsible to the decisions they have previously taken. Sustainability deals with the fundamental problem of rational ignorance. In liveness it is sometimes crucial that the system acts quickly. Suffrage suggests that the crucial question concludes to who is eligible to participate. According to Professor Kiayias, blockchain can identify huge suffrage. Most systems do not satisfy and miss most of the afore properties. Finally, Professor Kiayias concluded that we still have a lot to learn from the afore processes and thanked everyone for their attention, while remaining open to any questions.

Panel 2

Following Professor Aggelos Kiayias’ presentation, Dr. Ioannis Revolidis, moderator of the second panel introduced himself and the panellists before giving the floor to Ash Costello, Blockchain and Privacy Lawyer.

Panellists:

- Ash Costello – Blockchain and Privacy Lawyer
- Thibault Schrepel – Associate professor of Law at VU Amsterdam, Faculty Affiliate at Stanford University's CodeX Centre
- Jori Armbruster – CEO EthicHub, member of INATBA
- Aura Esther Vilalta Nicuesa (video record) – Prof. Of Civil Law, Open University of Catalonia, Member of the Nat. Centre of Technology & Dispute Resolution, Amherst University

Presentation 1 – DAOs and Smart Contracts, by Ash Costello, Blockchain and Privacy Lawyer

Ms Ash Costello presented a project that she has been working on for the past months and deals with privacy analysis for one of the biggest DAOs. Ms Costello started her talk by defining the meaning of a DAO. A DAO is a decentralized autonomous organization, an organization that operates like a company but it is not a traditional company but a rather peer to peer situation. According to Ms Costello's personal view, all companies might transform into DAOs in the future, mostly due to the fact that DAOs work in an automated basis, they use Smart Contracts, they make decentralization possible. The speaker addressed whether or not Smart Contracts can function as contracts. She mentioned that, for example, when a DAO is built, there is the need to address governance issues and later expressed her view on the ability of Smart Contracts to properly incorporate governance. The speaker elaborated on the GDPR and Data Act, launched by the European Commission by explaining that DAOs are governed by GDPR, due to the fact that they are significantly dealing with data and there is the need to acknowledge who is involved and what are the processes followed for data protection. A DAO could be a vague association of people acting together. She wondered, for the sake of the discussion, whether people involved in DAOs could be considered as data processors or data controllers and who is the one to decide what steps should be taken to handle and process all data collected. The answer to this question is Smart Contracts. The speaker reached to the conclusion that all those involved in data handling in a DAO are considered as joint controllers. For these purposes, governance contracts, token Smart Contracts were analysed. All data deriving from the afore analysis led to the conclusion that in DAOs there is an existing joint controllership situation. People joining a DAO can expect meritocracy, by purchasing a token and entering the relevant DAO, they automatically become a member and take part in the decision making process. In addition, DAOs offer an enormous space for GDPR analysis, especially in terms of consent of data sharing. By joining a DAO, everyone volunteers to have their data public and thus, Smart Contracts must capture all the afore processes of decision making and data sharing. The speaker concluded that there is still room for improvement and more adaptations will follow in the future.

Presentation 2 - Legal barriers: which clarifications do we need and which new laws do we need - Technical barriers: how to address them by Thibault Schrepel – Associate professor of Law at VU Amsterdam, Faculty Affiliate at Stanford University's CodeX Centre

Thibault Schrepel started his presentation by defining the issue of Smart Contracts and Contract Law. The balance between adopting a smart contract while abiding by the rule of law is a very important aspect, according to Thibault Schrepel. Through Contract law we can clarify the rules that already exist in legal terms. The speaker continued by addressing the complexity in incorporating the application of Smart Contracts under the Contract Law, significantly in terms of exchange of consent. In addition, Thibault Schrepel mentioned that it is very important to choose the medium through which Smart Contracts operate. His thoughts revolved around whether blockchain is a durable medium for Smart Contracts but he concluded that there is no answer to this question yet. He, then, highlighted the terms of data protection, data localization and data sovereignty. Continuing his presentation, Dr. Schrepel addressed the need for new rules and mechanisms and especially the need to discuss about whether a single template for Smart Contracts could solve the problem. According to the speaker's view, a single template would not be ideal, because Smart Contracts differ from one another in nature and scope, thus creating the need for oracle templates. In addition, Thibault Schepel discussed about Article 30 of the newly launched Data Act, and he specifically articulated his thoughts on the interruption of the operation of such contracts to avoid future accidental executions. He further highlighted that there is a constant need to work by combining technology and law, rather than imposing law into the ecosystem. In addition, the speaker pointed out that there are numerous ways to test blockchain immutability and later presented examples of Smart Contracts written in solidity and translation provided in GPT3. He concluded that it is high time that we put oracles to work and design those oracles to help information transmitted to the clause of a Smart Contract, while always bearing in mind trust issues for Smart Contracts. It is imperative to define who is responsible to undertake the task of checking the contract per se: whether it will be a lawyer or an NLP.

Presentation 3 – Smart Contracts use cases and consciousness, by Jori Armbruster – CEO EthicHub, member of INATBA

Mr Armbruster started his speech by quoting that blockchain technology allows for a new stage in human collaboration and he presented the historical evolution of civilization that led to blockchain. He highlighted that the first use case that tried to create decentralized money was Bitcoin. The introduction of Smart Contracts allowed society to think more about decentralized use cases, Fintech, DeFi, ReFi, etc. The speaker addressed the audience and mentioned that we, people, can think of better value chains and can automate more transactions through Smart Contracts and create full traceability, thus more transparency. For this reason, Mr Armbruster suggested that pseudonymous identities could be used instead of digital identities. He significantly pointed that governance helps us think much better tools for Smart Contracts and crypto incentives, thus people is empowered to join public discussions, due to the fact that the world is organized in vertical systems with little participation of people. According to Mr Armbruster, DAOs will be the biggest part of the economy in the future, thus leading to people being in control. However, we are in a super early phase in the technology adoption curve. He further mentioned that the use cases that mostly affected the world were: the Bitcoin in El Salvador, creating digital accounts in the country for the first time and Axie infinity, which led to the creation of more jobs in developing countries' economies. Other use cases that were presented by Mr Armbruster were Klima DAO and Celo. The speaker focused on the constant exclusion of more people from the financial system, thus creating the need for a feasible solution that would target a problem that was not existing before. His company, EthicHub, created crowd collateral, where someone can purchase their token and then all users are able to lend between them. With this system, EthicHub has a trustworthy platform that attracts investors. Mr Armbruster concluded that technology should be used in consciousness to solve world problems.

Presentation 4 – Smart Legal Contracts, by Aura Esther Vilalta Nicuesa (video record) – Prof. Of Civil Law, Open University of Catalonia, Member of the Nat. Centre of Technology & Dispute Resolution, Amherst University

Ms Nicuesa began her presentation by defining the three basic ideas revolving around Smart Contracts, i.e. the nature of smart legal contracts, Smart Contracts ability to enhance legal transactions and access to justice. She mentioned that there is no pressing need for a new legal framework rather than medium adaptations. Smart Contracts are legal transactions where parties enter and perform transactions and there is no need of human intervention. The academia has been struggling to identify the distinction between smart legal contract and Smart Contracts, but consensus has been reached. Smart legal contracts are defined as legally binding contracts. Ms Nicuesa proceeded by providing a classification for Smart Contracts: nature language contracts, hybrid contracts and code contracts. The current legal principles that apply to traditional contracts apply to Smart Contracts as well and, currently, there is no need for a new legal framework, rather than various arrangements and adaptations. The speaker aimed to answer some questions that could be brought forward by the audience, due to the delivery of her speech through video recording. She addressed the formalities for the validation of Smart Contracts by mentioning that there are no additional formalities to be concluded for a contract to be valid. The speaker has also provided useful input on the inability to transform a legal contract to a smart contract, due to the variety of processes that can not be automated, while also highlighting that Smart legal contracts are very difficult to unwind. A serious concern is the language that the contract is written and how could a smart legal contract become binding when it is written in code. The terms need to be comprehensible by all parties involved, some smart legal contracts might be fully codified but natural language will always be necessary. The speaker also addressed various concerns relating to the effectiveness of transcription codes and how this may entitle a part to void a contract. The law has no response to this scenario, parties and intermediaries become vulnerable, thus harmonization with minimum standards of liability is needed. In addition she expressed her view concerning which version of contract should prevail and be the authoritative one in case of controversy, by mentioning that should parties have not reached an agreement, natural language contracts must prevail. She also touched upon the issue of dealing with conflicts where parties are not duly identified. Ms Nicuesa mentioned that it could be considered possible to use pseudonyms for future identification of participation as machine to machine contracts are untraceable. The speaker also endeavoured to address the acceptance of cryptocurrencies as a means of payment and highlighted that this is acceptable. Ms Nicuesa concluded that the law should clarify the nature of these contracts and how to deal with the discrepancies without resorting to the courts. Parties may wish to void the court, due to the fact that smart legal contracts are capable with incorporating solutions, such oracles, arbitration and mediation, but the afore solutions need to be neutral. The speaker noted that there is still room for improvements.

Panel 2 Q&A

The Q&A for the second panel was opened by Dr. Ioannis Revolidis, who decided to address the first question to the speakers.

Question 1

One of the interesting questions after scheming on the EU Data Act is how to create mechanisms in order to mitigate the imbalance in contracts that have to do with the exchange of data. Do you think this is a problem and if yes, which do you think are the next steps to mitigate it?

Dr. Schrepel answered that this is a rather general concern, not only for Smart Contracts. The problem exists even without Smart Contracts. The speaker highlighted that Smart Contracts might be the solution to this and that not all Smart Contracts need to be the same, rather than specific ones. He concluded that this is a great opportunity for the European Commission to put specific Smart Contracts in place to organize data.

Ms Costello agreed with Dr. Schrepel. She mentioned that this is a big problem, and that the recently launched Data Act is trying to address it. The Data Act uses the Smart Contracts as the solution, which is fascinating. We are only in the beginning of seeing how Smart Contracts can be used.

Mr Armbruster shared his view that at the end the main issue is that regulators do not understand the phase that we are at. Always at the beginning regulators think technology is bad and he thinks that this will gradually change. Technology promotes innovation and countries that enable those potentials to arise will take a step forward in the future. The speaker concluded that the most important part is to educate people to use this for a good purpose.

Dr. Schrepel intervened to clarify that internet was thought to be something bad at the beginning. The relationship between law and technology dates back to the code of Hammurabi. It is important to consider that when people regulate problems, they have to deal with problematic potentials as well and take into consideration the evolution of technology.

Ms Costello also concluded that it is too soon and thus, we need to stay back and see what happens.

Question 2

Dr. Revolidis proceeded with the next question that related to Smart Contracts being solution to those problems and asked the speakers whether they see possible limitations of Smart Contracts interpretation? Can someone misinterpret code?

Dr. Schrepel replied positively by highlighting that this is a problem but it is not new. The same problem exists with natural language contracts as well. Someone can run simulations, write in GTP3 to understand and translate code language. The speaker mentioned that interoperability is good when it is bottom up and that we need to impose interoperability standards.

Mr Armbruster replied by admitting that it is a big challenge to interact with Smart Contracts. User experience is super-fast to use and there is a long way until we reach the desired result.

Ms Costello reiterated what the previous speakers mentioned and she continued by replying that we are now beginning to move to interoperability platforms and it is too early to police Smart Contracts.

Dr Revolidis thanked all speakers for their contributions and gave the floor to Mr Hauschildt, as the workshop was finally coming to an end.

Christian Hauschildt reiterated that there is huge potential in Smart Contracts and urged all to keep the debate going and follow all news through the EU Blockchain Observatory and Forum website. Finally, he thanked everyone for participating and the European Commission for providing the opportunity to organize such interesting workshops.

Appendix

Presentations from the workshop can be found here: https://www.eublockchainforum.eu/events/workshop-smart-contracts

Videos from this and all other workshops can be found on the EU Blockchain Observatory and Forum website under the section Reports

Official Agenda

Time	Topic	Speaker
14.30	**Welcome**	**Christian Hauschildt, EU Blockchain Observatory and Forum**
14.35	**Keynote:** Smart Contracts; what are they? Smart Contracts vs Contracts: Exploring challenges and solutions towards tech and law colliding	Dr Joshua Ellul, Director, Centre for Distributed Ledger Technologies, University of Malta
14.50	**Introduction to Panel 1:** Use cases and standardization	**Dr. Kristina Livitckaia – R&D Project Manager - CERTH**
14.55	**Panel 1**	**Dr. Kristina Livitckaia – R&D Project Manager - CERTH**
		Daniel Szego – DLT Architect
		Tooba Faisal – work item leader for Smart Contracts at ETSI PDL, King's College London
		Industry reps – Mark Cudden – CTO – we.trade
		David Arroyo – Member of the Spanish delegation to ISO TC 307
15.35	**Q&A for Panel 1**	**Dr. Kristina Livitckaia – R&D Project Manager - CERTH**
16.00	**Keynote:** Blockchain Governance : Fundamental Properties and Current Approaches	Prof. Aggelos Kiayias, Chair in Cyber Security and Privacy and Director of the Blockchain Technology Laboratory, Uni of Edinburgh
16.15	**Introduction to Panel 2:** Legal and non-technical barriers	**Dr. Ioannis Revolidis – Centre for Distributed Ledger Technologies, University of Malta**
16.20	**Panel 2**	**Dr. Ioannis Revolidis – Centre for Distributed Ledger Technologies, University of Malta**

Time	Topic	Speaker
		Ash Costello- Blockchain and Privacy Lawyer
		Jori Armbruster – CEO - EthicHub, INATBA Member
		Aura Esther Vilalta Nicuesa (Video record) - Prof. of Civil Law, Open University of Catalonia, Member of the Nat. Center of Technology & Dispute Resolution, Amherst University
		Thibault Schrepel - Ass. Prof. of Law at VU Amsterdam, Faculty Affiliate at Stanford University's CodeX Center
17.10	**Q&A for Panel 2**	**Dr. Ioannis Revolidis – Centre for Distributed Ledger Technologies, University of Malta**
17.30	**Closing**	**Christian Hauschildt, EU Blockchain Observatory and Forum**

Speakers Biographies

Dr. Joshua Ellul (https://www.linkedin.com/in/joshuaellul/) is the director of the Centre for Distributed Ledger Technologies (DLT) and a senior lecturer in the Computer Science Department at the University of Malta. The Centre for DLT developed and runs a world-first multidisciplinary Masters in Blockchain and DLT which takes in students having backgrounds in computer science, law, finance and economics. He is also Chairperson of the Malta Digital Innovation Authority which regulates technology aspects of blockchain and safety-critical systems such including those that may make use of Artificial Intelligence sector.

Prof. Aggelos Kiayias (https://twitter.com/sol3gga) is chair in Cyber Security and Privacy and director of the Blockchain Technology Laboratory at the University of Edinburgh. He is also the Chief Scientist at blockchain technology company IOHK. His research interests are in computer security, information security, applied cryptography and foundations of cryptography with a particular emphasis in blockchain technologies and distributed systems, e-voting and secure multiparty protocols as well as privacy and identity management.

Dr. Kristina Livitckaia (https://www.linkedin.com/in/livitckaia/) is an R&D project manager and a researcher associate working at Information Technologies Institute, Centre for Research and Technologies Hellas (CERTH/ITI). Dr. Livitckaia earned her Ph.D. from the Aristotle University of Thessaloniki, has MSc in Telemedicine and e-Health (Computer Science), and Diploma in Economics. She has experience working in academia, industry, and R&D facility in several European countries (Norway, Finland, and Greece) for the past eight years, from project and product management to execution of scientific work and running and mentoring start-ups. Her primary research interests involve a multidisciplinary blend of emerging technologies (i.e., blockchain, AI, IoT, IoV) applied to multiple domains and focusing on healthcare, Pharma, well-being, safety, and city infrastructure.

Daniel Szego (https://www.linkedin.com/in/daniel-szego/) is an independent software architect and advisor having 20+ years in the industry, with around 5 years in research and development, and 15 years with enterprise software applications and use-cases. He has been dealing with the distributed ledger technology for more than 5 years, with the focus rather on consortium and enterprise ledgers with many notable project contributions. He has been running Hyperledger Budapest, a local community group dedicated to open-source enterprise blockchain technologies for more than 4 years.

Tooba Faisal (https://www.linkedin.com/in/toobafaisal/) Tooba is a PhD student at King's College London (KCL) working on Telco-blockchain. Her current research interests are designing secure smart contracts, Distributed Ledger Technology and SLAs. She also has a Master of Research (MRes) in Security Science from University College London, a Master of Science (MS) in Telecommunication and Networks and a Bachelor of Science degree in Computer Engineering from Bahria University, Karachi, Pakistan. She is a KCL's delegate in the ETSI Industries Specifications Group on Permissioned Distributed Ledgers and rapporteur of smart contract Group Report and Specifications.

Mark Cudden (https://www.linkedin.com/in/mark-cudden/) leads the we.trade company's operations, working with the company's board to develop the strategy and leads the organisation in its implementation. He also oversees the company's global expansion efforts. In his previous roles, Mark has held multiple leadership roles with global organisations. He has built and led multi-disciplinary teams in transformation, cost optimisation and operational improvements initiatives and coached organisations towards sustainable growth and through instilling high-performance cultures.

David Arroyo (https://twitter.com/davidalgabri) is Tenured Scientist in the Institute of Physical and Information Technologies (ITEFI) of the Spanish National Research Council (CSIC). He has a MSc in Telecommunication Engineering from the University of Seville (Spain) and a PhD in Physics of Complex Systems from the Polytechnic University of Madrid. As member of the CSIC, David Arroyo collaborates with the Spanish Association for Standardization (UNE) as expert in the CTN 320 "Cybersecurity and Protection of Personal Data", CTN 71/SC 307 "Blockchain and distributed ledger technologies", and CTN 71/SC 42 "Artificial Intelligence and Big Data". From January 2020, Dr. Arroyo is involved in the deployment tools for fake news detection in the context of the H2020 project TRESCA (Trustworthy, Reliable and Engaging Scientific Communication Approaches), and from October 2021 he is in charge of the deployment of Privacy Enhancing Technologies in the H2020 project SPIRS (Secure Platform for ICT Systems Rooted at the Silicon manufacturing process).

Dr. Ioannis Revolidis (www.linkedin.com/in/ioannis-revolidis-85b126179) is a legal academic at the Centre for Distributed Ledger Technologies (DLT), responsible for the legal stream of the interdisciplinary research and teaching endeavours of the Centre. He is also a lecturer in the Department of Media, Communications, and Technology Law at the Law Faculty of the University of Malta. He is an editor of two Legal Journals in his native Greece (Lex&Forum and Armenopoulos), as well as a practicing lawyer, registered with the Bar Association of Thessaloniki, where he supervises cases of civil and commercial law with digital elements. His research interests revolve around the regulation of emerging technologies, especially through contract, consumer protection, copyright, and data protection law.

Ash Costello (https://www.linkedin.com/in/ash-costello-14669a9a/) is a lawyer who advises on financial services law, privacy and blockchain. She works with blockchain technology entities such as DAOs to analyse their structures and practices for privacy compliance. She is the Co-Chair of the Privacy Working Group for the International Association of Trusted Blockchain Applications.

Jori Armburster (https://www.linkedin.com/in/jori-armbruster/) Blockchain believer, decentralization advocate. Igniting the agritech and multi-award winner EthicHub, who aims to disrupt the current financial lending system by creating a fair global crowdlending system for unbanked farmers. I have run a coffee farm in Mexico and also was CEO of an over 880 employees company with prior experience in operations, HR, and M&A to name a few. I am fully committed with Sustainable Development Goals and trying to demonstrate that Impact Investing is not only necessary but a better investment in the long term.

Aura Esther Vilalta Nicuesa (https://www.linkedin.com/in/aura-esther-vilalta-nicuesa-24555019/) Ph.D. Chair in Civil Law at the Open University of Catalonia (UOC). Researcher at the Internet Interdisciplinary Institute (IN3). Member of the National Centre of Technology and Dispute Resolution (NCTDR) and fellow of the European Law Institute (ELI), Dispute Resolution SIG and Digital Law SIG. She has been a Spanish Delegate as an expert in the United Nations, Working Group WG III of UNCITRAL, Director of the Legal Department at the University School of Lleida (EURL), lawyer (ICAB), mediator (AEPJMA and FMA), arbitrator for the Arbitration Tribunal of Barcelona (TAB) and arbitrator for the Chamber of Commerce of Madrid (CAM). Vilalta has served as Deputy Magistrate in the Court of appeal in Barcelona.

Dr. Thibault Schrepel (https://www.linkedin.com/in/thibaultschrepel/), LL.M., is an Associate Professor of Law at VU Amsterdam University where he co-directs the Amsterdam Law & Technology Institute, and a Faculty Affiliate at Stanford University CodeX Centre where he has created the "Computational Antitrust" project that brings together over 60 antitrust agencies. Thibault also holds research and teaching positions at the University Paris 1 Panthéon-Sorbonne and Sciences Po Paris. He is a Harvard University Berkman Centre alumnus, a member of the French Superior Audiovisual Council's scientific board, also, a blockchain expert appointed to the World Economic Forum and the World Bank.