UNIVERSITY of NICOSIA

Week 3 – Session 5

Algorithmic Governance with Smart Contracts

BLOC 512: Blockchain Systems and Architectures

Session Objectives

- In this section, we will go through yet another area, that is bound to be shaken by blockchain technology and its implications of decentralization – ***governance***
- In this regards, blockchain can be helpful not only for enabling transparent decision-making, but also increasing public participation. Nonetheless, when algorithms take over ever larger parts of our lives, we need to be aware of many risks this brings.

- Overview of decentralized/distributed autonomous organizations
- Understand the various aspects of algorithmic governance
- Explore various aspects of algorithmic governance, its benefits and pitfalls

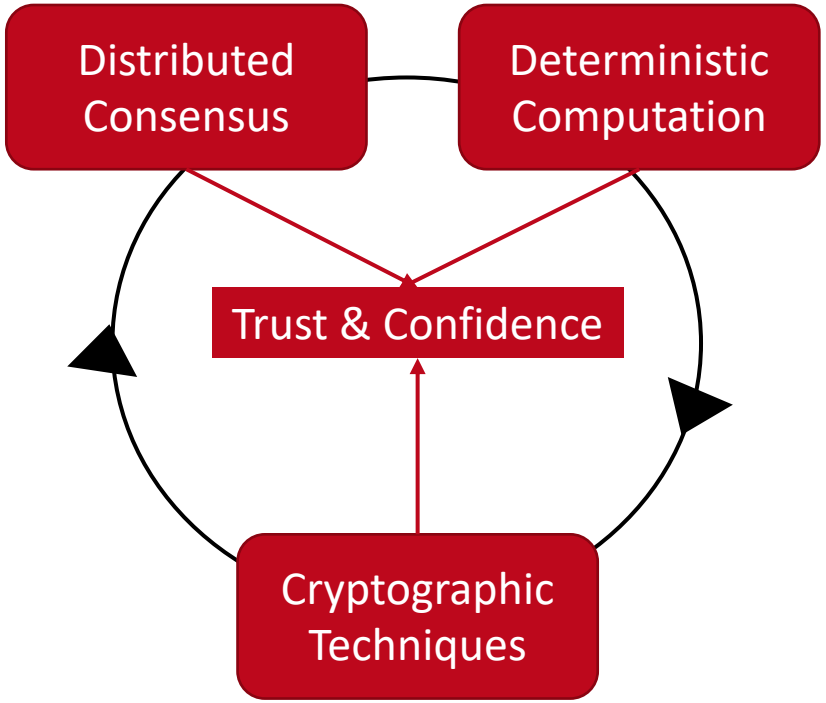
Agenda

1. Re-establishing Trust
2. Governing Open Protocols
3. Decentralized Autonomous Organizations
4. Potentials of Algorithmic Governance
5. Resolving conflicts
6. Conclusions
7. Self-Assessment Exercises and Further Readings

A new movement…

Re-establishing Trust

- As previously discussed Nakamoto proposed an alternative perspective of building trust.
- This trust machine has motivated by:
  - the global financial crisis in 2008, which has been commonly attributed to the failure of trusted institutions such as banks and other financial institutions.
  - abuses of information and communication technologies for surveillance, dissemination of disinformation, and public coercion have come to light.
    - A growing loss of trust in governmental authorities [3]
    - Centralization of Tech giants like Facebook, Google and Twitter [1, 2]
- These developments have triggered a ***new attitude*** towards sociotechnical systems where the requirement to trust a third party is considered a disadvantage.



[1] https://theintercept.com/2019/08/19/twitter-ads-china-uighurs/ [2] https://theintercept.com/2019/08/18/google-egypt-office-sisi/
[3] https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Trust & Confidence

- In blockchain systems we can distinguish between the definitions of trust and confidence
  - **Trust:** refers to potential vulnerabilities of such systems and how risk is mitigated
  - **Confidence:** refers to expectation guarantees deriving from knowledge that builds from past experiences
- The above characteristics relate with the shared expectations to the way the technology operates, and how correct the operations are.
- Therefore, the increased trust and confidence that ultimately the technology provides depends on a variety of factors that relate with the collective operation of the network.

For public blockchains:

- Collective management at different levels, from consensus to the protocol's source code
- Verifiable confidence

For private permissioned blockchains:

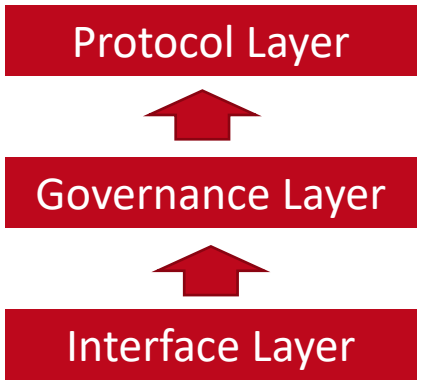
- A pre-existing trust is assumed over the network
- A permissioned governance is enforced to the network by the administrator that restricts how participants are performing actions or access the blockchain.

For consortium blockchains:

- Assuming a level of pre-existing trust over the network - shared values
- Governance is defined as a set of rules that govern the organizational and operational partnership of the consortium
- These rules focus on the operation of the consortium, their roles or responsibilities and the decision making

Governing Open Protocols (Cont.)

- Referring to the abstract architecture of a DLT system and assuming an open, public and permissionless instantiation of such a network. There are different levels of power (influence) and politics that are played out in such systems.
  - These levels are organized under the following layers: protocol, governance, and interfaces.



Internal Actors:

- The consensus algorithm plays a significant role in the governance
- The internal protocol rules, embedded in the technical details e.g., source code, databases, repositories
- Incentivization structures: intended to help governing behavior towards activities beneficial for the system

External Actors:

- The miners, users that participate to the consensus rounds
- The project maintainers, that build the technology
- The developers of smart contracts

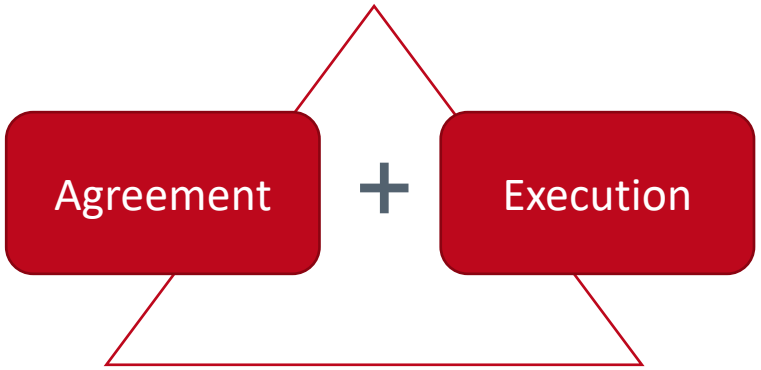
- As we will be discussing it turns out that not all users are the same. Each node has different interests and incentives that are external to the protocol instead (e.g., electricity costs). Therefore, in conflicting events these conditions are likely to influence the evolution of the protocol.

Decentralized Autonomous Organizations

Smart Contracts

"Smart contracts are computer programs that can be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority." – [Bartoletti & Pompianu, 2017]

- Smart contracts are tiny pieces of code, that are executed on "all"* nodes in the network and their output is the same for all nodes. Once deployed on the blockchain, they start their own life, which cannot be altered, stopped or deleted (unless explicitly programmed to be able to do so).
- The "smart" part relates to the certainty of the contract fulfillment, relying on the decentralized and cryptographically secured technology – and not relying on third parties.
- Agreements between parties are inseparable from execution.



decentralized and cryptographically secured

Smart Contract Types

Defining smart contracts depends on the context. Most often they are not really smart, they *don't improve by obtaining new knowledge*, but *they do run autonomously*, interact with others and have a certain degree of "memory". A better term would probably be **chaincode**, coined by IBM for Hyperledger.

We can generalize the concept into 3 types:

1. **Bitcoin script**, executing transactions (scripts) when conditions are met

`smart contract = predicate` (yes/no function)

2. **Ethereum contract**, using Turing complete programming language

`smart contract = automated execution of an agreement` (code)

3. **Ricardian agreements**, using Ricardian contracts

`smart contract = automated execution & enforceability of an agreement`
(code + legal prose)

Towards a “DAOism”

- Vitalik [1] attempts to shed light towards the various concepts mentioned in the literature around **decentralized automation.**
  - **Smart Contracts:** are the simplest form of decentralized automation
  - **Autonomous Agents:** while some degree of human effort might be necessary to build the agent (with software or hardware), in general there is no necessity for any specific human involvement at all for the operation or existence of an autonomous agent e.g., a computer virus
    - What about AI autonomous agents? How can we enforce a level of governance on such agents?
  - **Decentralized Applications:** Vitalik focuses on ***anonymous decentralized applications*** (where each user is anonymous, and the system executes their atomic interactions) and ***reputation-based decentralized applications*** (where the system keeps a history of the interactions in building a mechanism that ensures trust).
  - **Decentralized Organizations:** Instead of a hierarchical structure managed by a humans interacting with each other, a decentralized organization involves humans interacting with each other according to a protocol specified in code and enforced on the blockchain.
  - **Decentralized Autonomous Organizations:** Describes an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.
    - Bitcoin “hires” miners to participate to the consensus
    - AI driven DAOs will be completely autonomous, whereas a DAO still requires heavy involvement from humans specifically interacting according to a protocol defined by the DAO in order to operate.

[1] https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Distributed Business Entities

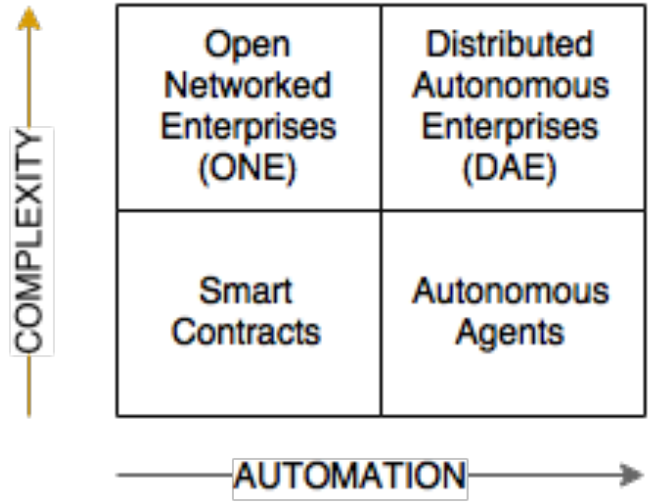
We usually talk about blockchain technology lowering transaction costs and increasing speed in operating a business. However, there is potential for it to impact corporate architecture, also. Don and Alex Tapscott predictions [Blockchain Revolution, 2016]:

- **Search costs** – finding new talent and customers
  - beyond internet search: respecting people's privacy through selective revealing data, multidimensional searching not just data at that particular time, but through all its lifecycle, and account for value in search queries
- **Contracting costs** – reaching an agreement and commit to it
  - smart contracts
- **Coordination costs** – internal managing of people
  - distribution of responsibility, authority and power is easier with blockchain as it provides persistence and stability in an organization, even when there is no hierarchy
- **Costs of (re-)building trust** – preserving integrity
  - transparency and trust codified in software

Distributed Business Entities

Tapscotts also defined **four categories of new business models**, varying in the degree of functional complexity and of human involvement:

- **Smart Contracts** – when considering them on their own, they involve the least complexity and human interaction
- **Open Networked Enterprises** – utilizing smart contracts, enterprises can „open up“ and couple with others in the network
- **Autonomous Agents** – more or less sophisticated devices or software, that adjusts its own actions in order to achieve its goals and can be owned by nobody but themselves
- **Distributed Autonomous Enterprises** – the most complex model, in which members participate through smart contracts to seek common goal, where actions are not triggered only by humans, but by any thing that can interact with blockchain



Introduction to DAOs

- In late 2013, a topic of ***decentralized organizations*** came forward (Bitshares, Dapps, DAC ...). The idea was that along with smart contracts, even the structures of organizations could be managed through "smart" code.

- **Decentralized Autonomous Organization** is an organization that is completely defined online, with all its management rules written in smart contracts. It doesn't rely on people for making decisions, but rather „hires" people to do the things it cannot do: interacting with the real world. By way of example, a DAO can pay a human contractor from its internal capital to do some real-world task, which is determined by the rules of the DAO itself (often participants in the DAO cast votes for what is to be done).

- A DAO that seeks financial benefits, usually in the form of receiving dividends, is called **Decentralized Autonomous Corporation or DAC**.
  - Idea was firstly introduced by Bitshares where market participants were able to create decentralized autonomous corporations (DACs) based on smart contracts.
  - This was later evolved into a Decentralized Exchange

Legal status of a DAO

- Considering the traditional legal frameworks in most jurisdictions, a DAO is not easy to define:
  - *general partnership*, in which members own the assets of their business, but are personally liable and any member that could represent a DAO could be sued
  - *unincorporated association*, where some members have limited liability, but generally don‘t create a legal entity, any member that the state first observes the contact with can be sued
  - *joint venture* ...
- There is a problem defining it as a partnership, as participants have only one common thing, they sent some tokens to the smart contract. Also, there is usually no restrictions who can join, either.
- By the ***nearest person theory***, the creator of a DAO would be held responsible for any damages resulting from the operation of DAO. However, what happens when DAO has multiple and even unknown creators? Maybe the members of the DAO could be jointly held liable, as they are funding a DAO and possibly expect direct or indirect profits. If that would be the case, how can users be responsible for others‘ actions or bugs in the code?
- Note, with *in rem* jurisdiction (rights over property), legal actions are taken against the property, even when persons are unknown. The state will not allow illegal actions no matter what, and despite not knowing who the members in a DAO are, it can forbid it nonetheless.

Potentials of Algorithmic Governance

Requirements for Algorithmic Governance

- Organizing businesses and states requires ongoing actions from a hierarchy of delegated people. As we‘ve seen so far, there are central points of control that are necessary for the organization to operate. Even if process automation and controlling were made more efficient through information technologies and *rules of running of organization could already be codified decades ago*, securing it still relied on central entities with administrative privileges – there simply was no other way.

- With blockchain, organization rules and constraints, defined in smart contracts, would be, in essence, self-sufficient, *harder to break* or stop, as their exact replicas would be distributed to all participants – with no central authorities, but with each node independently performing only valid actions.

- A 100% pure algorithmic governance would be a technocratic dystopia. There is no denial about the evolution and proliferation of Robotic Process Automation (RPA), combining artificial intelligence and software robots. No denial about the power that algorithms have over human quirks. No denial about the benefits of transparency in decentralized “autonomous” organizations. There is also no denial about the many problems of contemporary governance models. We just mustn’t forget what would be the *purpose* of an algorithmic governance – and prepare contingency plans.

The Power of Algorithms

The reliance on algorithms has deep sociological and political implications. T. Gillespie analyzed six dimensions of public relevance algorithms that are affecting human discourse and knowledge*:

1. Patterns of inclusion: what data actually gets to the algorithm
2. Cycles of anticipation: the implications of predicting users‘ needs and actions
3. The evaluation of relevance: how algorithms decide what is relevant – to their structure/goals and to users
4. The promise of algorithmic objectivity: can algorithms‘ technicalities provide impartiality *per se*
5. Entanglement with practice: how users reshape their practices to suit the algorithms and how algorithms in turn influence their lives
6. The production of calculated publics: how algorithmic presentation of what is „hot“ or what „others are doing“ shapes users self-image

A deeper examination is beyond the scope of this session, but do think about what implications would a DAO have, when on one hand all its actions and algorithms are completely transparent, yet they are very complex and they might only have informal, voluntary support and no person to be held responsible for any incidents.

* The Relevance of Algorithms, Tarleton Gillespie, 2013

The Power of Algorithms (Cont.)

There are many cases of ***use*** and ***misuse*** of the powers of algorithm, but one should suffice for illustration.

"*If you recognize native advertising, it was insufficiently executed. Good native advertising offers the reader the content, that is of interest to the reader and can help him in his life …*

It is long true, that on the Internet, you don't search for things, but things search for you."

- Igor Lahav, Outbrain, published in 2017 in a commentary for a major Slovenian newspaper.

Outbrain is a large advertising company, using behavioral targeting which serves billions of recommendations and site views per month. It is a global player, with high-profile customers, like CNN and Bild.

What can blockchain do in this case? Several things, but not just yet: disintermediation can bring a larger piece of the pie to the producers, multiple user-controller personas on blockchain could help users protect their privacy by selective revealing their data and monetize it directly, reducing fraud by having better publisher identification options *etc*.

Governing Openly with Unknown Entities

Since **Distributed Autonomous Organizations** are created and ***run*** *in the open* (otherwise they would look like a suspicious black-box for its potential users) and their ***members*** *could be* ***unknown*** (probably only their public addresses on the blockchain are known), there are some interesting ***consequences*** and ***potentials*** they offer.

- **Transparency** – The structure, all functions and privileges of a DAO are written in smart contracts, whose source code is public and can be examined at any time. Any changes to the deployed contract are unequivocally seen in the open. All actions a DAO makes, are visible on the blockchain. Nothing is hidden. Applied to governments, a *decentralized autonomous governmental agency* ("DAGA", the term from Tori Adams) would bring transparency in public spending to a whole new level.

- **Anonymity** – All actions that happen in a DAO, are visible as transactions on the blockchain, initiated by pseudonymous peers on the network. Members are known only by their addresses. No personal identity is shown (if so desired). In the future, we might see some KYC requirements implemented, depending on how regulation will evolve. Some networks already impose such onramping.

Responsible Actions

If there is a possibility for a real-life organization to decide on an action in secret or to obscure its structures so holding any person responsible becomes very hard, this is fundamentally different within a DAO.

- **Accountability** – Commitments to stakeholders and abiding by them is defined by the rules in smart contracts, making little room for doubt or ambiguity. With such transparency, there is little chance to hide corruptive actions or denying responsibility. Could Wall Street loose so much reputation if bad actors would be visible instantly and publicly *(but would they ever operate publicly?)*? Under a DAGA, persons authorizing each spending of the national budget would be automatically and indisputably held accountable. There is definitely some room to improvement from this perspective.

- **Liability** – Special care needs to be taken here, as a question who is liable, for instance, for software errors and bugs, is a challenge to regulators. There are basically a couple of possible answers: developers, creators, participants or the DAO itself. Formalized verification of smart contracts will help to some degree, but we must still expect future bugs in the software. Due to the usual pseudo-anonymity of participants, some fallback mechanisms will probably needed to be designed so as to minimize possibilities of scams (like Vitalik Buterin's proposal for DAICO).
  - A thought experiment … Under what jurisdictions do decentralized smart contracts operate? We need to consider who maintains them, who is offering them … but pseudo-anonymous users might never be identified. It's worse than that: what about full nodes, that *store* these contracts and *relay* them forward, could they be held liable?

Governmentality of DAOs

- *Governmentality* can be thought of as practices or actions through which subjects are governed (a term by French philosopher Michel Foucault). The meaning is not limited to enacting governance of a state, but it applies generally to „the conduct of conduct“, from self-control to managing a household.

- In relation to algorithmic governance, a **governmentality perspective** suggests that a governance in a DAO is more than just keeping participants together when there is no legal hierarchical structure and keeping them in-order with its rules. It **uncovers a much wider set of actions and mechanisms that constitute the workings of DAOs**.

- *What can participants do?, how can they change the DAO? - what are the implications of correcting mistakes by rolling back transactions, what are the rules of making a fork? etc.*

- Questions like these are pesky if you try to answer them. All of a sudden, the decentralization dissolves, unstoppable code becomes stoppable, cheap transactions become expensive … and opposing groups of people engage in conflicts.

“Governance crisis”

- In 2016, Primavera De Filippi and Benjamin Loveluck published a paper that said what nobody wanted to say: there is no running away from the human factor, even in an environment of purely technical protocols and algorithms – as much as Bitcoin stands for decentralization, it faces significant political pressures.
- The paper has a telling title: “The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure” and it is recommended to read, despite perhaps a little bias, but you can try to find some counter-arguments.
- To summarize the paper with regards to Bitcoin:
  - Bitcoin aims to be self-governing and self-sustaining → market-driven approach to social trust and coordination.
  - However, the development of the protocol is concentrated in a group of developers (an open group, but still).
  - Thus, we can observe a polarization of “governance by the infrastructure” (Bitcoin protocol) vs. “governance of the infrastructure” (developers).
- Ethereum is very different in this aspect:
  - The Ethereum Foundation is recognized in the community and with many signed agreements with various institutions, we could argue it is accountable and legitimate.
  - Funding of developers is much more organized, there are grants, bounties, rewards etc., but more importantly, a very large amount of its currency was pre-allocated to fund ongoing development.
  - However, despite there being more developers and groups, there is one developer with a higher status, the author, Vitalik Buterin. It’s a bit like if Satoshi Nakamoto was still around in Bitcoin. Still, if Vitalik would do something out of the “ordinary”, it would raise suspicions and the community could easily reject him.

“Governance crisis” (Cont.)

- Further on, the paper addresses 3 entwined challenges of online peer-production communities, such as Bitcoin:
- **community borders** – are *open* for the infrastructure due to PoW, but the development discussions are open up until changes need to be made in code and that’s when the developers draw a line of what design will be implemented and what not, the BIP process is an example of that;
- **incentives for participation** – are clear for the infrastructure with mining rewards, but for developers, it is more indirect, in a way that it is about social reputation with the technical expertise or charisma;
- **pacification of conflicts** – is straightforward for the infrastructure as the protocol resolves any issues by its own technological means, but for the developers it is a big challenge, that can lead to deadlocks and personal fights, as we have seen how divisive was the implementation of SegWit.

- In conclusion, the paper states that: *“… socio-technical systems cannot – by virtue of their embeddedness into a social and cultural context – ensure their own self-governance and self-sustainability through technology alone. Any technology will eventually fall prey to the social, cultural and political pressures of the context in which it operates …”*

“Governance crisis” (Cont.)

- So, should “technocratic power structure” be replaced by “institutional framework”, as De Filippi and Loveluck suggest?
- While we can easily see the benefits of standardized governance, coordination among actors, there are some good reasons why we would instead want to preserve incoordination*:
  - we want an **immutable** blockchain (is this the whole point?),
  - we need **dependable** functionality (upgrading software for hard forks is cumbersome and dangerous),
  - incoordination enables **uniform access** (permissonless use, that is constrained only by the internal rules of the protocol and by no means limited by something external to the system, like social status, IP address, blacklists…).

- Having loose governance does mean a certain degree of technological stagnation and that is both a tradeoff and a guarantee for immutability.

*Thaddeus Dryja, Decentralization and Incoordination, 2017

Resolving Conflicts

Conflict Resolution

- In this session we will be discussing ways in which incompatible or conflicting differences are likely to be resolved in an environment that was supposed to have solved consensus.
- As notable examples we will be referring to:
  1. **The Bitcoin scaling conflict**:
     - **Intro:** this was a conflict of how to scale the Bitcoin network without compromising on decentralization (scaling vs. decentralization trade-off)
     - **Observation:** These conflicts brought to the foreground the ways in which such protocols are managed in decentralized environment, at the same time raising questions with regards to the actors that can influence a protocol's governance.
  2. **The DAO exploit**
     - **Intro:** "The DAO" was proposed as a first attempt at developing a Decentralized Autonomous Organization (DAO) that would be controlled purely by smart contracts, beyond human control. A hacker exploited part of the contract code to siphon off large amounts of Ethereum cryptocurrency, ether, causing the Ethereum Foundation to enact what is called a 'fork' in the code.
     - **Observation:** This caused significant debate about the purpose of decentralized systems and the promise of trustlessness – totally against the immutability of blockchains philosophy?

Controversies unveiling Bitcoin governance

- The proposition with Blockchains is that there is a level of algorithmic determination in governance – a decentralized, autonomous and neutral way of negotiating and resolving differences.
- However, there is a political question that remains unanswered:

  "Who is responsible for making the decision on how to make decisions?"

- This question became ***more evident for blockchains over the course of major conflicts*** about protocol changes in both Bitcoin and Ethereum.
  - For Bitcoin:
    - Not meant to be controlled by any central authority
    - Monetary policy is shaped and defined by the protocol
    - Block size and block frequency are defined and controlled by the protocol
    - Source code is maintained in an open environment
    - The generation of Bitcoins is based on a computationally intensive process
  - In reality though and to the "assumed consensus argument" there have been several incidents of events that took place to the Bitcoin network that questioned this argument and led to widespread public debates on different governance dimensions.
  - We will be investigating some notable Bitcoin events that enacted mechanisms of governance about Bitcoin's resolution mechanisms.

Bitcoin glitch - “involuntary fork

- March 2013’s “involuntary fork”
  - a miner running version 0.8 of the Bitcoin software created a large invalid block (i.e., incompatible with earlier versions of the software)
  - this resulted to an unintended “fork” in the Bitcoin blockchain, since nodes running the most recent version of the client at the time (v0.8) accepted the invalid block and continued to build on the diverging chain, whereas older client versions rejected it and continued building on the original chain without the offending block.
  - This split resulted in two separate transaction logs being formed without clear consensus or even knowledge of the other event happening, which allowed for the same funds to be spent twice on each chain.
  - ***Miners resolved the split by downgrading to version 0.7, putting them back on track with the canonical chain. User funds largely remained unaffected and were available when network consensus was restored.***
  - This interesting glitch of the network raises several questions with regards to the network governance. The resolution of the issues was the result of technical, politician and social elements required to be undertaken by the community. However,…
    - Who was responsible for the resolution of the split? How did the network reach consensus? Who were the actors involved and in which sequence of events?

The Bitcoin scaling conflict

- A long-standing question in Bitcoin is around scalability, with several proposals to increasing transaction throughput e.g., increase the block size or block rate
- In 2017 there were two Bitcoin supporters: those that supported large blocks and those who preferred small blocks.
- This scaling conflict resulted in network “forking” in August 2017 – splitting the network into two chains (Bitcoin Core and Bitcoin Cash) that grow in parallel, each with its own Bitcoin client software and network hashing power.
- Challenges to the assumed consensus in the network turned what were otherwise perceived as purely technical issues into “political” debates and raised questions of what holds blockchain pieces together and how they come apart when differences and incompatibility turns out to be unresolvable.

Resolving Conflicts

- These events are of particular interest as they reveal how the Bitcoin community, from core developers to miners, to users have responded to a moment of crisis deeply embedded in the technical architecture, for which both a technical response and a “political” consensus on the solution needed to be developed.
- According to the conditions of the community, the incentives and the influences even deep technical issues are turned into political debates that are materialized in different mediums.
- The Bitcoin scaling conflict has resulted into a “fork” which was proposed as a conflict resolution mechanism through which incompatible proposals are resolved.
- From the other hand ”The DAO” hack challenged the idea of autonomous governance and forced a reassessment of understanding the non-human determinacy. In general, it opened the way of algorithmic “on-chain governance” with collective human knowledge or wisdom of the crowds.
- In Bitcoin and Ethereum, the concept of ‘decentralization’ was mobilized and operationalized alongside cryptography in order to determine and enforce consensus without resorting to authorities, and yet, decentralization is in itself articulated and materialized in and through different mediums (networks, assemblies, chats or otherwise) and can be encoded in different ways.

„The DAO“ story

- The year 2016 was perhaps marked the most by the shocking initial success of a DAO called „The DAO“, that later tragically ended due to a security hole. The DAO was made by company Slock.it that focuses on Internet-of-Things (IoT) solutions, and it was an attempt to decentralize as many things as possible, even the mother company that would fund IoT products.

- The idea was that as crowdfunding made investing for smaller players easier, it was also more dangerous, not the least because of lack of risk management done by smaller investors, and that this could be solved by transparent, automated smart contracts.

- The DAO contract would accept investments in Ether and exchange them for DAO tokens, that investors would use for voting on offered project proposals.

- **Its legal status was undefined,** and it remains unclear even now. Since The DAO was not a legal entity in any jurisdiction, any litigation or tax liabilities were problematic. It stood as „code is law“ (the disclaimer explicitly mentioned that the code has priority over anything else), therefore any disputes were supposed to be resolved by interacting with the smart contract itself, through the functionalities that it provided.

„The DAO“ story

- **Surprising investments:** in May 2016, The DAO raised equivalent of $160 million (14% of all ether issued by then), by far the highest crowdfunding in the history and 300x more than was the campaign target.
- Its smart contracts were reviewed both internally and by a security audit company, that only found a potential, minor rounding bug. Later, a research [1] from Dino Mark, Vlad Zamfir and Emin Gün Sirer detected several possible attacks, some quite severe, thus urging them to ask for a moratorium on The DAO.
- In June 2016, The DAO went live and within days **another security hole was found that could drain the funds in the DAO contract** (it was a recursive call bug in one of the contract‘s functions). The fix was developed and awaited approval.
- At the same time, other members of the IC3 group reported on the bugs in The DAO that they found during scanning the Ethereum blockchain [2].

[1] https://docs.google.com/document/d/10kTyCmGPhvZy94F7VWyS-dQ4IsBacR2dUgGTtV98C40/edit

[2] http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/

„The DAO“ story, attacks

- The DAO’s code was “exploited” by an unknown individual. This exploit used unintended behavior of the code’s logic to rapidly drain the fund
- Unfortunately, the creators didn‘t realize the severity of the bug and even if they did, the time was against them as **the attacker engaged only 1 day after the IC3 report, siphoning over $50 million in ether.** The investors and Ethereum community in large tried many ways of stopping the attack, from trying to slow it down by spamming the network, to several attempts at white-hat counter-attacks.

- Nonetheless, it came down to a **hard fork of Ethereum blockchain as the last emergency resort**, by which the attack was reverted, and all investors made whole.
  - By doing so, the ***immutability*** of the blockchain was put into question and a minority of users did not accept such fork – they stayed on the old blockchain, which is nowadays called Ethereum Classic.

„The DAO“ story, aftermath

- The whole incident would not receive such attention, if The DAO‘s funding would be less substantial, in which case the bug would probably be fixed before drawing the attention of attackers.

- It became obvious that there is a tremendous interest in this technology, investors are eager to participate. The DAO was a good lesson, a very hard one and it will eventually lead to better code.

- Radically new technologies are initially prone to widest error sets imaginable – they are essentially exploring things that are complete unknowns and by focusing on this task, nearly everything else is put on sidelines. Smart contract programming is one such novelty. **The DAO story showed, unfortunately very painfully, that best-practice guides for all critical areas must be followed.**

Sine scientia ars nihil est (without knowledge, skill is nothing).

Best-practices that are now being popularized:

- Ethereum Smart Contract Security Best Practices, which also comes with a list of security tools
- Onward with Ethereum Smart Contract Security, library and knowledge base for secure smart contracts
- Build Secure Smart Contracts with OpenZeppelin Contracts, with the use of well-tested libraries of smart contracts for Ethereum and other blockchains.
- The Initiative for CryptoCurrencies & Contracts (IC3), also their blog is a good source

Post-merge Ethereum: consequences of switching to a new consensus mechanism?

- **The Merge**
  - Ethereum mainnet to transition to a PoS consensus mechanism, removing the energy inefficient PoW mining.
  - Ethereum miners will be replaced by validators (aka stakers)
- **How are communities reacting to this transition?**
  - This move has caused various conflicting views within Ethereum's ecosystem
  - Miners are unwilling to give up their investments and revenue stream
- **Ethereum PoW fork, What does it mean for the miners?**
  - the Merge suggests a cut to the the revenue stream of PoW miners
    - What choices do they have?
- **Conflict resolution proposal?**
  - proposed forking Ethereum or starting to mine other blockchains

Other Ideas

Blockchain and the Gonverence with AI and IoT

- Several propositions from the literature suggest that blockchains can resolve problems of authority and political power through a decentralized system.
- Anticipating the combinations of blockchain with AI there is a control layer that is removed from humans. Instead, this control layer is assigned to systems with forms of reasoning that are non-human (e.g., computational agents).
- Think of a system where smart contracts, transactions, agreements and various other actions and reasoning can take place between digital entities, or physical things (IoT) that have been granted digital identities.
- Several considerations to think of here:
  - We need a control layer to resolve disputes
  - We need a control layer to determine whether a task is most fit to be executed by an algorithmic agent (a machine) or a human
  - What is a reasonable degree of algorithmic authority? How much algorithmic freedom? How much algorithmic centralization?
  - What would be a reasonable governance layer that will diffuse the dynamics implied from a “singularity” event?

Discuss in the forums!

Conclusions

Conclusions

- In this session, we have discussed yet another potential, enabled by blockchain and smart contracts – an alternative organization structure with decentralized governance.
- While blockchain systems and smart contracts themselves raise many legal and regulatory questions, creating whole corporations on top of them is even more unclear. Questions about their legal status when no legal entity exists, or no member is personally identified remain to be answered. Or maybe a certain level of identification will turn out to be a necessity, imposed by governments.
- We observed a remarkable interest from the community investing into first Distributed Autonomous Organizations and difficulties when dealing with autonomously running code that gets exploited.
- As new experiences are gained, new projects can mitigate the risks that pestered them in the past, especially in expecting that smart contracts will be attacked also in the future and adequate mechanisms need to be put in place for emergency hot fixes.
- Vitalik Buterin shared his opinion about governance in the decentralized space of blockchains, noting social **norms** just like we have in physical life, also referencing cryptoeconomics as a comparatively easy and reliable way of predicting behavior: When New Tech and Dated Policies Collide a Conversation with Vitalik Buterin

Glossary

Glossary

Distributed Autonomous Organizations (DAOs): is an organization that is completely defined online, with all its management rules written in smart contracts.
Autonomous Agents: more or less sophisticated devices or software, that adjusts its own actions in order to achieve its goals and can be owned by nobody but themselves
Distributed Autonomous Enterprises: the most complex model, in which members participate through smart contracts to seek common goal, where actions are not triggered only by humans, but by anything that can interact with blockchain
Oracle: A blockchain oracle is a (third-party) computational elements meant to connect a blockchain-based application with external (i.e., out-of-blockchain) resources (typically, information sources).

Self-Assessment Exercises and Further Readings

Self-Assessment Exercises

- Consider profiling of users through the ranking of search results, or news funneled through online social platforms. They usually have a known owner, a central entity that manages the algorithms that shape our daily lives. What would change if there was a DAO that governs services like that?

You are welcome to share your thoughts on the forums!

Further Reading

Bootstrapping A Decentralized Autonomous Corporation, Vitalik Buterin, 2013

- https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274
- https://bitcoinmagazine.com/articles/bootstrapping-an-autonomous-decentralized-corporation-part-2-interacting-with-the-world-1379808279
- https://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-3-identity-corp-1380073003

(A series of „old“, but thought-provoking articles from the founder of Ethereum about automating the management of a corporation: part 1 is about how this can be achieved, part 2 is about solving the challenge of obtaining external data from the real world, part 3 is about added value of decentralized corporations.)

Decentralized Blockchain Technology and the Rise of Lex Cryptographia, Aaron Wright & Primavera De Filippi, 2015

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664
(Read section F about Distributed Real-time Governance for further details about how blockchain enables alternative ways of governing)

Blockchain Governance: Programming Our Future, Fred Ehrsam, 2017

https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74
(A comprehensive post on the importance of governing schemes in the blockchain space, highly recommend if you want to explore this space more.)

Further Reading (Cont.)

- [Hazard, 2017] Hazard, James, and Helena Haapio. "Wise contracts: smart contracts that work for people and machines." In Trends and communities of legal informatics. Proceedings of the 20th international legal informatics symposium IRIS, pp. 425-432. 2017.

- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284.

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: @mscdigital
Instructor's Email: christodoulou.kl@unic.ac.cy

Course Support:
Mark Wigmans - wigmans.m@unic.ac.cy
Marios Touloupos - touloupos.m@unic.ac.cy

IT & live session support: dl.it@unic.ac.cy