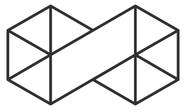
FUTURE
CRYPTOECONOMICS

WWW.RIAT.AC.AT



Future Cryptoeconomics is a quarterly publication that examines the global cryptoeconomic condition and its effects on culture and society.

We live in times of *zero trust*, a term stemming from computer security research, which is applied to all sectors and businesses. Most prominently zero trust is used in cryptoeconomic systems such as Bitcoin and other blockchain-based technologies - describing the practice to "never trust, always verify".

But what is cryptoeconomics exactly, and what are we talking about when we are talking about "Future Cryptoeconomics"? We are facing a discipline which is not formally defined yet. It reminds us of the early developments of game theory, an area of study that at the beginning was very narrowly defined, but then grew to be an interdisciplinary field that included the social sciences, political sciences, and many other disciplines. In order to discuss the future developments of world computers, immutable code and cryptocurrency, we must broaden our viewpoints and make sure to understand the full scope of possibilities of true decentralisation. "Forking institutions" might be a starting point, but we have to be aware that this possibly also means a "constant destruction and recreation of institutions and experimental cultures", to make space for invention and new disruptions.

Cryptoeconomics and the first blockchain were introduced through Satoshi Nakamoto's self-published white paper in 2008. This event changed the life course of many, including Andreas Antonopolous who told us in his interview that he "dropped everything" to dedicate himself to this "very powerful decentralised distributed system with a security foundation based on cryptography". The blockchain, which according to Jaya Klara Brekke some call "a truth machine, others say it is magic" is thematised in her essay, which outlines how to find truth in an indeterminate world. Josh Stark describes the roots of the discourse about cryptoeconomics and calls it "a very applied thing", where researchers worldwide are "thinking about new ways they can use rules in cryptography and economic incentives to build these systems". Stark also calls to define more clearly what the boundaries of cryptoeconomics are, and states that "one of the biggest misconceptions about blockchain technology and cryptoeconomics is to depict it purely as a topic of computer science". Vitalik Buterin talks about experiments in token sales and points to the fact that the "ICO space is cooling down a bit", demonstrating that the initial inflationary use of the term cryptoeconomics is beginning to mature into a more informed culture of cryptoeconomic experimentation. Since the interview with Buterin and Stark took place in 2017 at devcon3 in Cancún, we can see how a lot of the "Crypto Winter" of 2018 was already foreseen.

Simon de la Rouviere described how cryptoeconomics are "giving rise to the computing commons", and these effects have still not reached all sectors yet. Shintaro Miyazaki from the Critical Media Lab of the Institute of Experimental Design and Media Cultures in Basel conceptualised "models as cultural techniques, agential media and designed systems, which catalyse fruitful discussions on serious matters of our commons". His text in this issue offers a historic overview of the commons, and calls for design work and aesthetic experimentation with diffractive modelling.

Cryptoeconomics has its roots in the cypherpunk movement as well as in cryptoanarchy. Jan Hubik from Paralelni Polis talks about the background of the organisation and about how parallel societies are reinventing these ideals and transporting them into the 21st century. After all, these future utopias of the past are the status quo of today for some organisations, which act decentralised, as well as localised at the same time. Another example is the think-tank Dezentrum, which contributed the essay 'The Advent of Digital Persons' explaining why software-based agents should gain personhood.

Future Cryptoeconomics are debated and tested in almost real-time, and we have a long way to go in order to achieve 'cryptoeconomic literacy' and global adoption of cryptocurrency. Could anxiety foster mass adoption of cryptocurrencies? The transparency vs. privacy debate, or the shortcomings of fiat, banks and large financial institutions? This first issue of *Future Cryptoeconomics* tries not to find answers to speculations, but to identify the questions that are foundational for envisioning next societies.

FORK THE INSTITUTIONS

Governance, post-DAO

MATTHIAS TARASIEWICZ

Since the microcomputing revolution in the 1970s we have lived in the age of permanent technological disruptions, but institutionalised educational practices have not yet caught up. "Technologies come and go but the university remains, in a recognisable and largely unchanged form". Decentralisation challenges the role of the university as gatekeeper to knowledge, and questions the structure and organisational architecture of institutions. The only chance for educational institutions is to find interfaces to informal and technology-driven experimental cultures to be able to radically reinvent themselves. If universities don't react to technological and societal change, they will be forked, replaced, and decentralised.

With the accelerated pace of the introduction of new technologies, the appropriation of techno-culture has targeted all niches of informal work. The inflationary use of terms such as *hackerspaces* and *hackathons* show that *hackers* and *makers* have been commodified (Davies 2017). In recent years, informal cultures of knowledge production are actively targeted and their methods and formats are emulated and transported into business and education. The "hacker ethic", as Brett Scott points out, is a composite of "not merely exploratory curiosity or rebellious deviance or creative innovation within incumbent systems. It emerges from the intersection of all three" (Scott 2015). Numerous incompatibilities question the interfaces between *informal* and *formal* research (Wagner, Newman and Tarasiewicz 2015). In the new age of permanent disruption, "it is not assets we need to leverage, but networks" (Satell 2013).

Disruption and university

A "disruptive innovation" (Bower and Christensen 1995) is said to create a new market and value network (or disrupt existing ones) with "significant societal impact" (Assink 2006). Hypes and hype-cycles are evolving, while at the same time "tethered appliances" (Zittrain 2008) are consequently "reducing the potential for technological literacy" (Wuschitz et al. 2016). Institutions as tethered appliances introduce limitations, and have been *re-invented* (Johnson et al. 1995), hacked (Cohen and Scheinfeldt 2013) and rebooted (Berechet and Istrimschi 2014), while still being in permanent crisis (Nelson 1997; Scheper-Hughes 2011; McCabe 2013).

Although there are many ongoing attempts to implement novel and "disruptive" technologies into teaching and learning practices, institutional practices have barely changed (Blin and Munro 2008; Christensen et al. 2011). "Teachers have implemented computers in the most common-sense way – to sustain their existing practices and pedagogies rather than to displace them" (Christensen et al. 2011). As Michael Flavin notes, "technologies come and go but the university remains, in a recognisable and largely unchanged form" and "the use of disruptive technologies challenges the role of the university as gatekeeper to knowledge and signifies the possibility of a more open borders approach." (Flavin 2017).

The age of permanent disruption: from the 'crypto dream' to the 'blockchain revolution'

> *"disruptive innovation does not take root through a direct attack on the existing system. Instead, it must go around and underneath the system" (Christensen et al, 2011)*

Simon Penny describes how cultural production and innovation always involves diverse communities of toolmakers, and their "particular contributions and motivations are seldom noted, except in specialised studies" (Penny 2008). Often such cultures are, as Penny calls them, "renegades" or "eccentrics", producing their tools outside of institutions and "by definition, ahead of the technological-industrial curve" (Penny 2008). One example of such an eccentric innovative technology-based community are the cypherpunks.

Since 1983 cypherpunks already debated the usage of digital cash without a central issuing authority (Chaum 1983, 1990; Finney 1993; Medvinsky and Neuman, 1993; May 1994; Szabo 1997; Dai 1998; Reagle 2005), which was only introduced in 2008 by the anonymous entity *Satoshi Nakamoto* (Nakamoto 2008). Within a self-published paper, Nakamoto described the blockchain ledger, thus inventing the first cryptocurrency: Bitcoin. Digital currency, and even more so the blockchain, might be the most disruptive invention since the internet, though its 'disruptiveness' is still debated (Iansiti and Lakhani 2017; Swan 2015; and others).

Blockchains have a multitude of potential applications and the industry has been "imagining a blockchain world" (Ernst & Young 2016). After the hype of 2017, in the "crypto-winter" of 2018 we can observe that mass adoption of cryptocurrencies is still far away from being a reality. The techno-utopist future is stuck in useful prototypes, and the *new order* is waiting in the shadows in parallel economic enclaves (cf. HCPP 2018).

At the same time traditionally designed institutions are trying to react to the massive technological and societal change that these disruptive technologies and novel trust machines introduce, but the underlying own governance models and decision making protocols are rarely questioned.

Code governance and fork politics

"Generally, no leaderless developers have ever written big and complex software. It is unheard of. Whether that shows that people cannot or prefer not to do it, is unclear." (Meatballwiki, 2010)

Conflicts appear in coding communities on a regular basis, so protocols for resolution have to exist in order to continue development. A *Fork* in software engineering describes the situation when developers create their own *branch* and start individual development on it. "The right to fork is inherent in the [fundamental software freedoms] common" and "also takes place in non-profit associations and political and religious movements". Participants of the social system of software projects can utilise their "right to fork" as well as their "right to leave" (Meatballwiki 2010). Software repositories are usually governed through "benevolent dictators", in contrast to "management committees of meritocratic projects" (Gardler and Hanganu 2010). But the introduction of the blockchain (Nakamoto 2008) introduced numerous new governance models, which are based on experimental "cryptoeconomic" settings (Zamfir 2014) and are tested by numerous initiatives in experimental way. As De Filippi notes, this had been already achieved through the automation to decision-making processes, the incorporation of legal rules into code and more recently, through the "code-ification of law" (De Filippi 2016).

Flattening organisational structures (to emulate and mimic development and production cultures) is experimented upon in technology-based companies for a longer time already. Holacracy, for example, is a system of organisational governance developed by the company HolacracyOne. It's claims are to "[turn] everyone into a leader" and goes on, explaining "this isn't anarchy – it's quite the opposite" (Robertson 2015). Critique of the system is manifold - Bernstein et al. describe "old power rules can be deeply embedded in culture and institutions", so a transition from an existing (hierarchical) governance model to self-governed one appears problematic (Bernstein et al. 2016). Other examples are "liquid democracy" or "delegative democracy" (most prominently used by the German Pirate Party), where an electorate vests voting power in delegates rather than representatives (Ford 2002). Futarchy describes a form of governance proposed by economist Robin Hanson (2007). He criticises that democracies "fail largely by not aggregating available information" and that "betting markets are our best known institution for aggregating information". Under futarchy, users would "vote values, but bet beliefs" (Hanson 2007). Voting would not be to implement particular policies, but on metrics to determine how well their organisation/institution is doing, and prediction markets would be used to pick the policies that best optimise those metrics. In a binary (yes/no) vote on a specific topic, two prediction markets would emerge, and on resolution, all trades on the rejection market would be reverted. Vitalik Buterin (co-founder of the Ethereum 'world computer') in 2014 described a decentralised autonomous organisation (DAO) using futarchy to govern a (fictional) nation. "DAOs allow us to very quickly prototype and experiment with an aspect of our social interactions that is so far arguably falling behind our rapid advancements in information and social technology elsewhere: organisational governance" (Buterin 2014). The Ethereum project had to face a "hard fork" on the network in 2016, resulting in two different blockchains: *Ethereum* and *Ethereum Classic*, as philosophical differences between "radical crypto-decentralists" and "bailout supporters" of the first decentralised autonomous organisation emerged (Widrum 2016). The DAO was to this date an investor-directed, stateless venture capital fund, with the largest crowdfunding campaign in history at over $168 million in available (crypto) funds (Metz 2016). After hackers exploited a vulnerability in the DAO code and a third of the collected funds were moved away, the original proclamation of Ethereum's "unstoppable code" and "by-laws [which] are immutably chiseled into the Ethereum blockchain" (Cryptohustle 2016) was questioned. The community decided to block the 'stolen' funds through a hard-fork of Ethereum, a modification of the underlying code.

Rules, protocols and the future of decision making

De Filippi and Loveluck in their 2016 paper differentiate between "governance by the infrastructure (achieved via the Bitcoin protocol)" and "governance of the infrastructure (managed by the community of developers and other stakeholders)". Blockchains often get interpreted as a "regulatory technology", enforcing a particular set of predefined protocols and rules (Bitcoin), but we should also consider their potential as "platform on which people might encode their own sets of rules and procedures that will define a particular system of governance" (De Filippi and Loveluck 2016). For 'new' and 'old' institutions alike, governance models based on distributed consensus and cryptoeconomics offer a significant opportunity for implementing change to react to technological and societal developments. The preconditions for such a model are not only technological, as governance relates to decisions about the "rules of the protocol (the code) and the incentives the network is based on (the economics)" (Tomaino 2017).

There is a strong need for 'cryptoeconomic literacy', but more importantly there must be an emphasis on the interaction and communication between both institutions and informal communities ("where the action is") to further the research into and development of new amalgamations of social and organisational structures. We have to foster the constant destruction and recreation of institutions and experimental cultures - cultures in which new forms of governance are tested and experimented with. Such new systems in distributed, collective agency between humans and machines can pave the way for another future, where "Extended Intelligence" (Ito 2016) can produce "collective agents capable of transitioning between multiple levels of political, material and conceptual organisation" (Laboria Cuboniks 2015). Research is a collaborative process - a cybernetic fusion of distributed agencies; part human, part machine, part program.

SEIZE YOUR RIGHTS WITH THE FORCE OF CRYPTO

An Interview with Andreas Antonopoulos

MATTHIAS TARASIEWICZ &
DANIEL PICHLER

Matthias Tarasiewicz and Daniel Pichler spoke with Andreas Antonopoulos at the WeAreDevelopers World Congress in Vienna. Antonopoulos is known for delivering electric talks that combine economics, psychology, technology, and game theory with current events, personal anecdote and historical precedent; effortlessly transliterating the complex issues of blockchain technology out of the abstract and into the real world.

DP: We have met on multiple occasions in the past years, but I never asked you: what drove you to Bitcoin and cryptocurrencies in the first place?

AA: I'd say I was primed. My background is in distributed systems and information security. I started programming when I was under 11 years old and I've been involved with computers since the early days of the internet, but I also got interested in the cypherpunk movement in the early 90s and in the first digital currencies like Digicash with David Chaum. I was fascinated with the applications of cryptography to social sciences and the impact this could have on political movements. When I first came across Bitcoin, I didn't understand what it was and ignored it, and six months later I found a link to the white paper of Satoshi Nakamoto. The moment I read that, I realised what it was: a very powerful decentralised distributed system with a security foundation based on cryptography and in fact, the entire construction incorporated all cypherpunk ideals that I strongly believed in. So I immediately dropped everything else and dedicated my focus to that. Here we are seven years later, still as excited as ever and fascinated by this technology which has gone further than I ever expected.

MT: I personally came to Bitcoin through the experimental research project *Bitcoincloud* in 2010. I started further researching on the culture of decentralisation through "Cryptocurrencies as Distributed Community Experiments" (2014), which examined how different altcoins emerged from Bitcoin and how forking culture emerged. I was fascinated how value was created in these emerging communities. A lot has changed since then, especially the actors in the cryptosphere and how they interact. How is your perspective on this, do you think cypherpunk ideals are still there, out there?

AA: Oh they absolutely are, because they are still being espoused by a lot of people who are very much engaged and are working in research, innovation, technology and building new systems. A lot of people have joined this entire space, for whom this is not interesting, because it's simply inevitable. If a technology becomes more mainstream, it loses some of its root principles and people forget why it was created in the first place. But that's okay, because one of the interesting things is that in many previous technologies, new people come in who do not understand, know about or even believe in the original principles. They change the technology to match their new interests. They can't do that with cryptocurrencies, because the technology cannot be changed, because no one has control over it. People can create new cryptocurrencies that don't have those principles, but they can't change those principles in existing cryptocurrencies, because they have no control over them. That's a very interesting phenomenon. If you believe, as I do, that those principles translate to greater usability, greater freedom and in the end greater utility and value, then the fact that they can't be changed means that we will continue to have this technology and we will continue to have these principles, and they will be very useful.

MT: I want to shift the discussion to what people are actually using cryptocurrencies for. There is the term #HODL, and the Ethereum community often calls to #BUIDL. Monero with Monerujo suggests to #SPEDN more. Could too much focus on hodling in the end hodl back cryptocurrency mass adoption?

AA: Absolutely! Any form of single focus, refusing to appreciate the diversity of applications, the diversity of viewpoints, and the diversity of interests that come into this space and trying to make this a single choice that everybody has to follow is not relevant to everything that this is about. It's all about choice. One of the beautiful things about this is that in traditional startups, traditional funding mechanisms and traditional platform technologies, especially centralised platform technologies, to introduce a new application to the platform it has to have a very, very large addressable market, otherwise the entity that controls the platform has no interest in introducing it. You don't get your application to run on Facebook unless it has a very, very large market. It's not an open system. The beauty of cryptocurrencies and open platforms is that the market

space you need to address in order to run an application is two people. You and the other person, and as long as you two are interested in writing an application and using it with a trust platform behind it, you can run it. If nobody else is interested in that application, it still runs, it still gets the same level of priority on the network, it's neutrally treated by the platform. That's how innovation thrives. You get permissionless innovation at the edge, you don't need to have a market of more than two people. That means that we are going to see applications that serve narrow markets, that serve people with disabilities, people who are neurotypical, and people with different economic or social backgrounds who have different needs. And the need of someone who is trying to protect the wealth of their family in Venezuela is very different from an Austrian who wants to buy coffee at the local store. That's okay. These platforms are big enough and varied enough to serve the needs of many. I think it is wrong to focus on one approach and say, we win if we all do this. No, we win if we let everyone do what they want to do on this platform. Big approach! Broad approach! I don't think anybody should tell anybody else what Bitcoin is, what a blockchain is and what they should be used or should not be used for. That violates neutrality and I think neutrality is one of the strongest building blocks of this technology.

MT: There is a lot of debate if Bitcoin failed the cash aspect, not only because of rising fees (that got largely solved by SegWit and Lightning), but also in regards to the deliberate design aspects of Bitcoin as a deflationary currency. There are a lot of external factors that would drive this scarcity higher, there is this saying that a third of all the Bitcoins are not in circulation, they are stagnant.

AA: Or lost.

MT: Or lost, yes. There are blockchain analysis services to mark coins as tainted, so we have a two-layer value already within Bitcoin. Andreas, do you think the cash aspect of Bitcoin is still relevant and what is your position on this? We also know that Bitcoin has never been fungible in the first place.

AA: I think that it's wrong to ascribe a specific function for everyone. Meaning, what I use Bitcoin for is not what everybody else uses Bitcoin for, and that's okay. In fact, I don't think we've closed the door on using this technology as cash. I think we don't know where the evolution of this technology will go, it's very, very early days and to say that the future is already written in one way or another is naive. To say that it must be one way or another is hubristic, and I don't think we should attempt to predict which way it's going to be used. The truth is that design of technology has a small influence over its future use or adoption, and the markets ultimately decide what a technology will be used for. I also take a broader view, which is that we don't have to solve all the problems with one cryptocurrency. In fact, I think when we have a future in which you can enter and exit a cryptocurrency in milliseconds, for values of milli-satoshis, and you can switch between one and another cryptocurrency with almost zero cost and almost zero time, what does it really mean to commit to one? I would like to see this almost as a routing mechanism in my wallet, such that I don't even know which currencies I have. My wallet automatically decides, based on heuristics, which currencies are the best store of value for the moment. If I need to do a transaction that's more like cash, if the thing I'm holding isn't the best thing or isn't the most compatible with the vendor I'm standing in front of, then my wallet can, in one millisecond, switch to the lowest exchange rate, lowest fee rate, highest privacy coin according to the settings that both I and the merchant accept, out of maybe 1000 different currencies, and then take the change and switch it back to the highest store-of-value currency. At that point, what choice have I made? None. So the very idea of committing to a single system to the exclusion of all others seems ludicrous to me. It's almost like saying, I have to pick one website to get all of my information, I have to use one routing protocol to get my packets from A to B. That's not the case, it hasn't been the case on the internet, why should we make it the case for cryptocurrencies?

DP: Privacy of cryptocurrency is a very important topic, which is underrepresented in mainstream media. After all, the majority of people still believe that Bitcoin is anonymous. What is your position in the 'always on' vs 'optional anonymity' debate and do you think one of them has more viability as an idea?

AA: To me, the only privacy and anonymity technologies that are really powerful are those that are always on, for everyone who uses them, all the time. If you look for an example on the internet, what is the most effective privacy and security technology that has been deployed? It's not PGP, it's not encrypted drives, it's TLS and SSL.

And the reason it's TLS and SSL is that 90 percent of the people who use it have no idea they are using it, and they don't get a choice. In fact, you can't turn it off, for most of the sites. You can't connect to them over a non-encrypted connection, so when everybody's connection is encrypted, that massively increases the privacy for everyone. Even if you have sophisticated privacy and anonymity technologies, if they are only used by 100,000 people on a single blockchain, then arguably these people can simply be monitored, all of them, all the time and eventually they will not have perfect operational security. They are going to slip up. I'm much more interested in having a lesser degree of privacy, which is always on for the 25 Million people who are using Bitcoin. So for me, it really matters what the set of users is. And I think that while privacy and anonymity coins are great because they provide an excellent basis for providing experimentation and pushing the envelope, they also somewhat attract the attention and anxiety of regulators.

> **Cryptocurrencies are just a litmus test. It allows you to test your own government and I think some will win that test.**

In the end, I think applying these privacy and anonymity technologies to every blockchain out there is going to be essential, because to limit freedom of expression, to limit freedom of association, you don't only have to deal with prior restraint. If you have the freedom to transact with everyone, but all your transactions are visible to everyone, then you can be punished after the fact for transacting with the wrong people, which essentially robs you of your freedom to transact. We have to realise that privacy is a foundational human right and without it, freedom of association, freedom of (political) expression, all go away. If you can vote for whoever you want, but your family can be shot for voting for the wrong person... you cannot vote for whoever you want! The vote is useless without a private vote, and this applies to all of the human rights, so privacy is a fundamental human right. I don't think we can afford to have blockchains without fundamental privacy tools, which is why I've been talking for a while now on the importance of establishing privacy technologies within Bitcoin, and I think we have some excellent choices: confidential transactions; joint-transactions; Ring Confidential Transactions; schnorr-signatures; aggregated signatures; Lightning Network; onion routing; dandelion routing; and several other technologies that are being developed, eventually possibly zk-SNARKs. All of these are great, but they are only useful if we give them to everyone and always turn them on.

MT: The right to privacy is heavily debated. For instance, despite it being mentioned in the US Bill of Rights, it does not have the same status in the EU. There has been a lot of debate on this recently because of data collection, the Facebook trial and the General Data Protection Regulation (GDPR). Richard Stallman wrote in the Guardian that "the surveillance imposed on us today is worse than in the Soviet Union", arguing that "to restore privacy, we must stop surveillance before it even asks for consent". How do you see the current situation, with corporate surveillance being on the rise, forced consent, and with surveillance packages being activated across Europe? Could it be that Bitcoin, in the end, creates a more transparent society, which could be problematic for end-users?

AA: Absolutely. Until we fix privacy and anonymity, we have a problematic situation. But then again, you have to compare it to the status-quo, which right now is increasingly no longer anonymous cash. It's very, very surveilled financial transactions through debit cards. Which means that not only you are under complete, continuous, totalitarian surveillance for every single one of your financial transactions, but also not even by one single entity, because every intelligence agency in the world is sharing. The European Intelligence Agencies are prohibited from spying on Europeans, so they outsource that to the Americans, the Americans are prohibited from spying on Americans, so they outsource that to Europeans, and your rights are meaningless.

Rights are not secured or granted by government. If you expect rights to be granted by government, you lose your rights. Rights are like muscles, you exercise them or they atrophy. And you do not ask for rights, you seize them, and if you have to, you seize them with force. I would prefer to seize them with the force of cryptography, which is the defensive force, but when you realise that your society is abrogating your fundamental human rights, you fix your society, you don't give up. The fact that privacy has a stronger constitutional basis in the United States is meaningless, because the constitution is being violated on a daily basis. The government does not care to subscribe to a constitutional basis. The same thing is happening in Europe. People are willing to give away their rights and freedoms to protect themselves from imaginary threats, and in the end, those threats get amplified, and it's their own government that is the greatest threat of all. And this is a lesson that Europe learned recently and America hasn't learned yet. When we see the rise of fascism in Europe and around the world and in the United States, it's unfortunately a lesson the next generation will have to learn again. I'm hoping that cryptography and cryptocurrencies and other powerful technologies like that can be used, especially by young people, to seize back and exercise their own rights. They will be called criminals, and they will be told that they are doing something that is wrong, and then they need to ignore that and do it anyway.

> **I would prefer to seize [human rights] with the force of cryptography**

DP: We already had the Bitcoin split with the block-size debate, because it was a controversy within the community on which route to take. Do you think that the next debate we'll have in the Bitcoin community will be anonymity vs non-anonymity? Will we have another split based on those ideals?

AA: Anonymity is going to become a controversial and contentious issue. Those who want to sell the anonymity of people and in return get corporate profit, favourable regulation or government endorsement will try to do that and they will fail to compromise on the integrity of the underlying chain and will fork-off their own. That fork will be compromised by design and I won't use it, but other people might. In the end, as long as their government remains free, they will be safe, but in the moment that they have one bad election, their freedom is gone. So I will continue to use the things that secure my own freedom, and to assert those rights.

DP: Let's start a thought experiment, and let's argue from a statist perspective about cryptocurrency and blockchain. If a country like Austria would want to foster cryptocurrency experimentation, what would you recommend to them? To regulate or to encourage?

AA: One of the things that is becoming quite ironic is that cryptocurrencies become a litmus test. They serve to reveal the intentions of your government. If your government has no respect for individual freedom or is worried and terrified if people have the power of privacy, anonymity and commerce, and the capability of private transactions (which for thousands of years has been something we have had with anonymous cash) - if your government is afraid of that, it says a lot about your government and very little about cryptocurrencies. So it becomes a litmus test that allows you to evaluate how freedom friendly your government is. It's a test that many governments are failing. And when they fail this test, they try to remove cryptocurrency from their country, but what they achieve is removing their country from cryptocurrency. They remove themselves from innovation, from growth, from possibility and eventually also from liberty. And that's fine. Because it won't affect cryptocurrencies. They'll just continue to happen, they'll just happen underground.

I think we're already seeing a level of competition emerging, where governments act as magnets for those who are interested in pursuing these innovative technologies. In the end, it is just as much a litmus test as the internet. If your country does not believe in the free internet, there is a problem with your country. But the internet will still remain free, somewhere. In the end you'll see, the countries which are likely to ban freedom of expression are also the ones which are not happy with a free internet.

MT: Could anxiety foster mass adoption of cryptocurrencies? The transparency vs. privacy debate, or the shortcomings of fiat, banks and large financial institutions?

AA: I don't think privacy is ever going to be a popular adoption mechanism. I don't think freedom, privacy and independence are things that most people seek. As a popular cartoon shows, you have two tables and one says 'uncomfortable truths' and the other one says 'easy lies', and there is a very big line in front of the one for easy lies. I don't think people are conditioned to seek uncomfortable truths. But the bottom line is, at some point you'll be forced to confront reality. That can either happen because your government becomes corrupt, because your government becomes totalitarian, because your money becomes worthless, hyperinflated or controlled as a political weapon against democracy. And all of those things are happening in many places around the world. Let's hope they don't happen here, I would certainly not want to see that. But again, if they do, that's the reason why people will seek alternatives. Sometimes you have to be outside of your comfort zone in order to discover that alternatives are needed. I'm just very interested in making sure that those alternatives exist when people need them and where people need them. Today it's Venezuela, let's hope it will never be Austria.

DISASSEMBLING THE TRUTH MACHINE

A story in two parts

JAYA KLARA BREKKE

So there is this thing. Some call it a truth machine[1], others say it is magic[2]. Many have pledged their faith in it as a solution to problems of power, a way to get rid of all the lying, cheating and corrupt politicians once and for all and put the greedy bankers out of their undeserving jobs. This thing is called the blockchain, it was introduced to the world through the cryptocurrency Bitcoin and it has its own way of producing truth. And the following is the story of how it does so …

… followed by a story of how it does not do so.

Part 1: Functional truth

Let's begin with the magic. This is a mathematical kind of magic and it is at the core of all cryptocurrencies. In fact, it is the crypto in cryptocurrencies and the backbone of pretty much all data security, authentication, verification, invocation. Yes, invocation. It is used across several major industries and has also inspired a hidden undercurrent of blockchain superstition and rituals, but more on that later.

The magic of maths. What I am talking about here is cryptographic hashing. It is a process by which some arbitrary data is run through a mathematical process that spits out a short and fixed length string of characters and numbers depending on the hashing function used, say for example: 000000000000000018bf622358138392e15833dc0b6b 6d785226002dcfeaa8de. Only an exact data input can produce that specific string, however it is near impossible to reverse this and work out the original data from the string of numbers, (feel free to try with the string above if you don't believe me). Now, because any change to the original data would produce a whole different output when hashed, it can be used as proof that a record of data has not been tampered with. And by adding a timestamp, it can also be proven when that data was added. Chain this together and you have a provably secure linear record of events. This peculiar mathematical property has inspired a broad field of research and development since the late 1970s onwards, of hashing functions with different properties and security models (cf. Merkle 1979; Preneel 2010). It is the basis of things like public key cryptography, Merkle trees and digital signatures, all used in cryptocurrencies.

Ok, you might say. So far the magic of cryptographic hashing is helping us to ensure that we have a record of events that we can prove was added at a particular time and has not been tampered with. But how does this help establish truth about anything? Who decides what is added to the record in the first place? And how do we agree that the event is true?

> The answer is everyone.
> Potentially.
> Well, in a sense anyway.[3]

I will explain this through the architecture of the still-undeniable-archetype-of-cryptocurrencies, Bitcoin, because without some concrete example this might just get too abstract. Here is how it works:

Bitcoin was introduced to the world as a peer-to-peer decentralised electronic payment system. The intention was to get rid of the need to trust in banks, institutions or any kind of authority to verify transactions and hold the record of accounts. Instead, this would now be done in a decentralised manner, by us, the very people doing the transactions, through a decentralised network of computers. To put it differently, information about who sent what amount to who, and when, would no longer be recorded and enforced by a bank and a legal system, but by nodes in a decentralised network.

So here it is then, the consensus algorithm in Bitcoin, AKA proof-of-work, AKA the truth machine.

Take a deep breath and follow me:

- Transactions are broadcast to the decentralised network.
- Nodes in the network then group these transactions into "blocks".
- The nodes then compete with each other to decide who gets to verify this block of transactions.
- The competition consists of hashing (remember?) the block of transaction data along with some random number so that the output string fulfils some requirements, it needs to have a certain amount of zeros, like: *0000000000000000a98127ca14a1e9bda07d58fb4093d16436a50fda5d8127b3*[4]. Finding such

a number is what is called mining in the world of cryptocurrencies.

- The hashed output is called the proof-of-work and has the characteristics of being difficult to compute and impossible to fake.
- It is published to the network along with the block of transactions and nonce so that anyone can check that it is indeed a valid proof-of-work (has the right amount of zeros and is indeed the output of the transaction data hashed with the published nonce).
- Nodes keep trying different nonces until they have found one that, when hashed with the transaction data, meets that requirement.
- This block is then considered valid, and any contradicting transactions are considered invalid.
- The validated block is added to the blockchain, which is a chain of the entire history of validated transactions.
- Competition then begins again for validating the next block of transactions.
- Nodes are rewarded for each block that they find with an amount of newly created Bitcoin and/or fees, as incentive for validating transactions and securing the network.

Take your time and read that again if you need to. It is a highly unusual and dense entanglement of concepts and functions from the fields of cryptography, mathematical probability, game theory and, yes. – A sprinkling of right wing political economy, instrumentalised (Golumbia, 2016). I say "instrumentalised" because these ideas serve a function here that does not necessarily translate directly into a practical right wing economics. (Apologies for any disappointment to critics and fans, but tech and the blockchain are just not that deterministic). [5]

Let us analyse a bit more what is happening here. The output of this process is indeed a secure and computationally agreed upon record of events (transactions events in this case). But the consensus algorithm here, the "truth machine" produces a very specific kind of "consensus" and "truth". Let's say two transactions were contradicting each other. Someone was trying to send the same value token to two different recipients, broadcasting these transactions to different parts of the network. What matters here is that the decentralised network comes to an agreement about which one is valid. It does not matter which one it is, as long as it is just one of them. It does not matter which one is more "true", more "fair" or anything of the sorts. The truth of what happened is arrived at, and agreed upon, through a competitive hashing process, determined by CPU number-crunching power. Truth in any transcendental sense, or even in any scientific sense is irrelevant and put aside for the sake of arriving at a functional truth of events.

Lets go through this once again. Economic incentives are used to get people to compete with one another in running computations, hashing transaction data with a nonce, until they find one that is valid and thereby validating that block of transactions. And then they start again, competing to verify the next block. The chances of anyone being able to repeatedly determine which transactions are considered true is diminished as the network gets bigger and more decentralised because they would have to control the majority of the network computing the blocks. The "consensus" of the consensus algorithm should therefore not be misunderstood as some sort of agreement on the truth of events, but rather an incentive driven settlement on events, the version of which is decided on through randomised turns determined by expending CPU power. It's legitimacy lies not in negotiations, consensus of opinions or some notion of justice or objective truth but in randomness and large numbers generating an operational computational consensus across the network.

I have gone into detail here explaining the consensus-algorithm of the Bitcoin blockchain not to baffle your mind with technicalities, but in order to open a discussion about a form of truth that draws its legitimacy from an entirely new source – not god, not science or philosophy, nor democracy, but a functional truth founded on mathematics. I first sensed this new source of truth and legitimacy, and with it an emerging cult of blockchain believers, when at a meet-up some number of years ago an aspiring actor and Bitcoin enthusiast told me "I don't trust the banks, or believe in any politician – but I do believe in maths." I am now going to disassemble this belief. I am sorry. I do this not for the sake of disenchantment, but because these mathematical phenomena are actually part of a much more wild and rich magic than this. A magic from a world that is alive and full, rather than lonely and paranoid. Let me explain.

Believing in maths instead of humans. We have opened the protocol, now let's do the same with the blockchain belief system. The distrust of humans that runs strong amongst blockchain believers can be traced to at least three different sources. First, on an immediate and perhaps obvious level, is the experience of blatant

lying, cheating and stealing by those in power and a sense that financial, legal and political institutions do more to protect the powerful rather than hold them accountable. Secondly, if we go one step deeper, there is the question of language itself. Human language is vague: we can say one thing, mean something else, and do yet another. This, for blockchain believers, is another source of distrust. Language is too imprecise, and easy to game (cf. Filippi and Wright 2015; Wood 2014; Jentzsch 2016). Third, and finally, at the deepest level, the level of existence itself, there is a mistrust of our own minds and senses. How do we know that what we are seeing and feeling is really real? How do I know that my mind is not tricking me? Do I even know my own mind?

A gaping uncertainty between our subjective sense of selves and our ability to comprehend or access any objective reality.

The new cult of the blockchain seeks to resolve this anxious paranoid condition by constructing an apparatus that is external to us, founded on laws that we cannot game. Humans will always be corrupted, whereas technology is disinterested, based on objective laws of nature and does not care about power nor even us necessarily. Political and legal institutions are to be replaced by decentralised clusters of automatic smart contracts that will run regardless of whether you want them to or not. Rules will be written in a language that also cannot be gamed, namely code that executes as written. What is written is the execution itself, not just a claim of the execution (cf. Galloway, 2004). And the mathematical phenomena of cryptographic hashing is mobilised as a fixed point of objective certainty and a source of unbreakable security on which this apparatus is built.

Now the funny thing is, even cryptographic hashing requires constant development. The security of different hashing algorithms is an area of continuous research and development, needing to be regularly updated. In fact, anyone who looks closer at blockchain applications will see that there is nothing certain, stabile or necessarily true about ANY of the claims associated with it. Sure, the thing works. In the sense that people are making transactions, coding smart contracts and developing new value tokens. But the central claims of blockchain believers in relation to truth and power are never quite fulfilled. This objective outside from which truth of transactions is devolved, the decentralised, immutable and neutral truth machine, is constantly in a state of correction, forking and development, neither quite decentralised[6], nor immutable[7] or neutral[8].

So I have stated that the truth machine, while seemingly external to us, is a thing of our creation, and not only that, it is also a constantly evolving thing that we keep maintaining, correcting and changing. Here is where the ongoing claims of the blockchain truth machine become important, if still not exactly fulfilled. The belief in the blockchain as a decentralised, neutral truth machine is exactly what mobilises the very efforts to try and realise it. While certain aspects of the system are the sites of intense rigorous work, tireless maintenance, research, testing and emphatic forking by a broad community of incredible engineers and developers, still, in other aspects their agency, this ongoing development work, thinking and decision-making, is sidestepped when it comes to broader ramifications and subsumed into the grand stories of blockchain maximalism. And this creates some serious blind-spots. It divorces the ability to assess the effects of the system from the claims made of it because it is relegated to an objective world external to us, mediating at a scale that is larger than us.

Yes. You got it. I am going in for the kill on crypto-superstition. In the following I am not going to give you a different model, but instead a set of methods. Ways of understanding and thinking about the establishment of truth and ideas of objectivity that do not require an external machine, but allows us to use this truth machine, the blockchain, our machine that we are making and experimenting with, as another tool amongst many. This will also allow us to assess the effects of this machine and give us a better understanding of the agency we have to change it, do something else or get rid of it if we don't like it.

Part 2: Finding truth in an indeterminate world

The dividing line that is at the basis of so much confusion in the way that we relate to machines, markets and maths; the line between the subjective and objective, or humans and technology (subjective, corrupted, vague vs. objective, neutral, precise) or indeed words and things (concepts vs. reality), is a flawed line. The cut is elsewhere. What I am going to do in the next few paragraphs is explain the thinking of a philosopher and physicist, Barad – who, drawing on such disparate sources as Niels Bohr and Judith Butler, shows us where the cut is, or rather, how the cut is drawn and redrawn in a continuous process of materialisation. By resolving this line, we will hold once again in our grasp a workable method for assessing truth, not in any final way, but in a way that is true to a continuously changing and open-ended world while also staying accountable and functional.

There is a tendency when countering technological determinism to bring technology back into the realm of the social. But there is a problem with this. Yes, sure, we can see by examining the histories of various inventions and devices that these things we make are defined and designed for specific needs and are shaped by the struggles and contestations over these, by political, social and legal dynamics as much as scientific ones. But it would be wishful thinking on behalf of social scientists and political theorists to claim that these are the only dynamics that affect technological development. We cannot simply make a thing and have it work exactly as we want it to just by saying it is so. There are some things that, well, work, and others that simply don't whether we will them to or not. Technology is not entirely socially determined, and there is an objective reality, but it is a reality that is not as divorced from our subjective selves and social concepts as assumed.
We will start with Barad's understanding of the scientific measuring apparatus. (We can keep in our minds our own apparatus as we go through this, piecing back together our disassembled truth machine). In Bohrian quantum physics, Barad explains, the apparatus is not external to the observed phenomenon, which it would then objectively measure as is usually assumed. Instead, the apparatus is part of the conditions that in fact determine the very characteristics of the observed phenomenon. This was the ground-shifting reading by Bohr, a reading that seeks to resolve one of the most famous conundrums in physics – whether light is a particle or a wave. For Bohr, the contradicting evidence meant that it has the potential to be either, and how it becomes one or the other is determined in relation to the measuring device. What Barad draws from this, in an updated and expanded notion of Bohr's thinking, is that all things at the level of the quant are indeterminate. Phenomena become determinate, have particular determined characteristics, in relation to the apparatuses through which they are observed, made visible and made knowable. The apparatus that registers the mark of a phenomenon forms part of the objective conditions for determining the very characteristics of that phenomenon.

This is quite a mouthful to swallow. Reality. Truth. Indeterminate. They only become determinate as coherent phenomena in relation to an apparatus or body that registers, senses and is marked by it. Now, before the vertigo of relativity throws us entirely off balance, let's define what objectivity can mean for us in such a reworking of observer and observed. Objectivity for Bohr and Barad, instead of being a thing outside ourselves, always just out of the reach of our limited subjective selves, is the ability to accurately describe and recreate the conditions necessary to reproduce a given phenomenon. What this also means is that words (concepts) are not divorced from things (reality) but are part of a process of materialisation in the stabilisation of phenomena. Descriptions matter. They form part of the materialising apparatuses and their objective account. But this does not mean that we can just invent whatever reality we want by describing and creating concepts determining an otherwise indeterminate reality according to our will. Why? Because we are not alone in this world and we are not the only agencies at work. There are eons of materialiation that predate us, and, indeed – not all concepts are effective. This is important. One might say that concepts are effective to the extent that they are able to matter – a play on words used frequently by Barad, in which what matters refers to mattering, and a process of materialisation. And this brings us to agency.

The question of agency is closely tied to the question of ethics, responsibility and the possibility for things to be different. But agency is not something that someone has or hasn't. Agency describes a force that creates a difference in trajectory, mobilising a power to make things different. An important point here, and the way that Barad expands on Bohr and accounts for the fact that we can't just decide what works and what doesn't, is that agency exists as a potential in any thing, every where,

not just in humans. We are not the only active subjectivities in a container of objects called reality. The world is alive with agency, potential for things to be different, by mobilising agency, in humans or non-humans. What we have here is a huge shift in conceptual grounding that also requires a shift in attention from seemingly insurmountable schisms of the subjective interior and the objective exterior, the separated realms of humans and technology, to an ever-shifting topology.

Our truth machine now no longer exists as a fixed point of reference constructed in an objective clean realm of mathematical certainty. The magic of maths and markets cannot be so easily divorced from us. So what happens to our truth machine? Can we reassemble it? Does it do anything at all? The machine is still there, and it does indeed reconfigure our agency, but not by resolving it once and for all in a higher order of technological neutral execution. No, instead, what we can see now is that we have mobilised non-human phenomena in an apparatus that ties our behaviors together in networks that affect us and the world in new ways, redistributing what is possible and for whom. The exact ways that it does this is for another essay, because the focus here is on the construction of truth. And what we have done in this disassembling of the truth machine is to shift the source of truth from a belief in an absolute objective condition assigned to the magic of maths, towards an ever-changing topology where the construction of what is true is an ongoing process of making concepts, ideas and desires material. We are not alone in this ever-evolving materialisation. But we are responsible for our part in it, also and especially when we mobilise mathematical phenomena into new configurations.

Does this mean that anything is potentially true? And therefore nothing? Is indeterminacy the same as post-truth? Can we ever know what is true at all in an ever-shifting topology? Post-truth entails a divorce of statement from a material reality, an eclipse of responsibility for statements. But the answer to this condition of post-truth is not to go looking for a complete coherence between statement and event, between word and thing, whether in code that executes as written or by inventing a pure mathematical world external to us that retains such coherence. The condition of indeterminacy is not the same as post-truth. The form of indeterminacy we have discussed here is one that describes the materialising force of statements, making them absolutely responsible and accountable to effects. We are responsible for the apparatuses we employ and develop exactly because they literally have a materialising effect. Not in a linear manner, but in relation to the other (non-human) agencies at work, in a collaborative effort of materialisation.

What I am attempting here is a new form of accountability to truth that does not require faith in a fixed external and eternal certainty, nor in the randomised functional truth derived from such a vanishing point, but a truth that is accountable to it's materialising effects also when they are ugly. Because only in this way can we start to glimpse our own agency and responsibility amongst that of a myriad of others all around us that we are in constant relation to and collaborate with. What we would like to materialise through this specific arrangement of mathematical phenomena, silicon, fossil fuels and game theoretical constructs, and for whose benefit, would then be the next question.

---

1 See amongst others Vigna, M. and Casey, P. 2018. The Truth Machine: The Blockchain and the Future of Everything.

2 See for example an early description by Vitalik Buterin: "A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible..." https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

3 See Brekke, J.K. 2018, Part two of "Three Postcards from the World of Decentralised Money" A tribute to those who will never be peers, in Moneylabs reader, ed, Gloerich, I., Lovink, G. & de Vries, P.

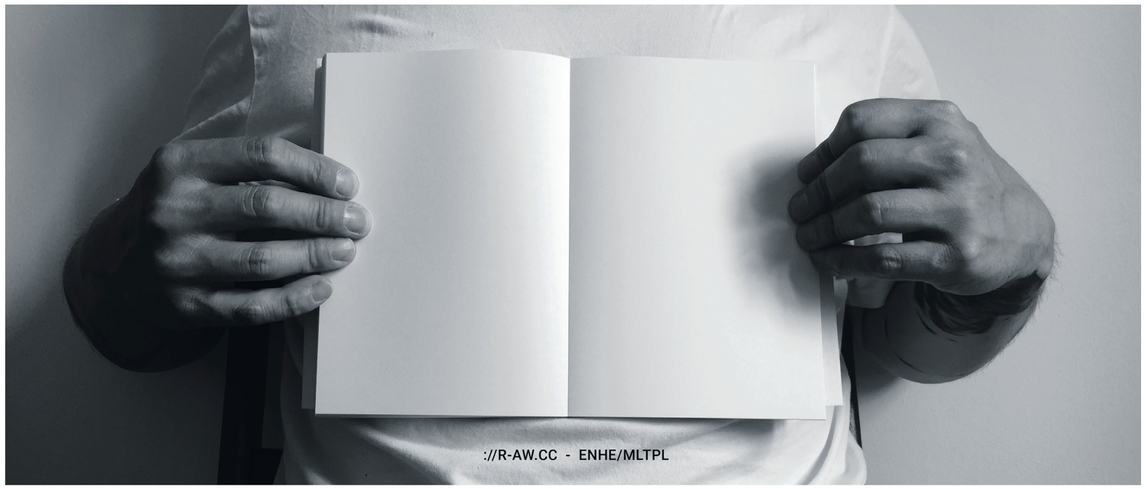
4 This block was number 295,297 on the blockchain and the nonce used to hash the proof-of-work was 0.
See: https://live.blockcypher.com/btc/block/000000000000000a98127ca14a1e9bda07d58fb4093d16436a50fda5d8127b3/

5 Most Blockchain applications incorporate economic incentives as an important security mechanism, serving a very particular function in the overall system. However, it is also important to note that blockchain thinking on power and decentralisation has a major blindspot also drawing from right wing economics of assuming an isolated economic agent who only interacts via the system itself. This assumption means that the model is blind to comunication and coordination outside of the market system, thereby excusing and making invisible the emergence of monopolies and shadow powers, while insisting on the tyranny of the more visible powers that aim to break up such monopolies (the state). How the politics of blockchain systems play out practically however is highly contingent on more than just the protocol and really not as of yet determined.

6 See Bitcoin centralisation of mining or read up on the scaling conflict.

7 See forks, especially the 2016 Ethereum DAO fork, and it is clear that the integrity of blockchain records really depend on reputation and legitimacy and lobbying power of developers and miners.

8 Well, it can't be neutral if it is neither decentralised nor immutable really.



404

_ A DISPLAY IN THE FORM OF A PUBLICATION. / _ AN ASYMMETRICAL REFRACTION. / _ A PROXY FOR THE DISSEMINATION OF INFORMATION.
_ A NERVOUS TURN THAT SLAPS ITSELF. / _ A REFLEX FLOW. / _ AN OPAQUE GUIDE TO A WORLD THAT REQUIRES MORE THAN FIVE SENSES.
_ *PHLEGM.*

CONTRIBUTIONS
Sandra Braman
Jaya Klara Brekke
Nicolas J. Bullot
Mario de Vega
Víctor Mazón Gardoqui
Magda Havas
Nina Janich
Rebekka Kiesewetter
Selena Savic
Nishant Shah
Daniela Silvestrin
Chris J. Villafuerte

EDITORS
Mario de Vega
Víctor Mazón Gardoqui
Daniela Silvestrin

CONCEPT / DESIGN
Mario de Vega
Víctor Mazón Gardoqui
Daniela Silvestrin
Dicey Studios

https://meta-id.info

Produced with the support of National Fund for the Arts and Culture (FONCA), Mexico and Sonic Acts, The Netherlands.

RULES ENFORCED BY CRYPTOGRAPHY

An Interview with Josh Stark

MATTHIAS TARASIEWICZ

Matthias Tarasiewicz spoke with Josh Stark at Ethereum devcon3 in Cancún, Mexico. Stark is a lawyer and cofounder of L4 Ventures. L4 conducts cryptoeconomic research and is focused on building a decentralised web that removes middlemen and incentivises users to contribute.

MT: Josh, you wrote the article "Making Sense of Cryptoeconomics" on CoinDesk in August, 2017. How do you define cryptoeconomics?

JS: It's an area that's very much in development, but to me cryptoeconomics means building and engineering new kinds of systems, where critical components are rules that are enforced by cryptography, and an economic game where a set of strategic interactions produce a certain outcome. Bitcoin is a cryptoeconomic system, because the economic incentives that are offered to miners to support the network are a necessary piece of it, and those economic rewards are only possible given a ruleset enforced by cryptography. Both of those elements are critical pieces of the design of these systems. Cryptoeconomics is the combining of these two disciplines (economics, cryptography) to build systems that we couldn't build before which have strange and interesting new properties. It's a term that's been thrown around over the last few years. Obviously Vitalik Buterin was building frames, a lot of his thinking is in cryptoeconomics. Vlad Zamfir has been a proponent of the term, and has done a lot of presentations and some writings about what cryptoeconomics is to him: "achieving information security goals using cryptography in economic theory". Jeff Coleman, a colleague of mine, is also a big proponent of the term, being a distinct area of study in applied science. Only since 2017 has cryptoeconomics become more well-known. It's not discussed only by experts, but also as something the broader community is starting to latch onto, as a way to frame what's going on in this industry.

MT: Can you tell us where the discourse on cryptoeconomics is taking place? As you have also been observing informal places where this discipline is debated.

JS: The most important contributions in cryptoeconomics right now are in papers and code-bases, projects that are testing and applying cryptoeconomics. I think the Casper white papers are works of cryptoeconomics. The TrueBit paper is an example of a cryptoeconomic application. There is academic work also being done that it is more about the discipline of cryptoeconomics, as opposed to just being basically a project-specific piece of work, but there's not a lot of it yet. Cryptoeconomics is a very applied thing, it is being actively built out and the people that know this stuff best are not navel-gazing, they're building new systems and thinking about new ways they can use rules in cryptography and economic incentives to build these systems. So, to me, it's all just a reflection of what's actually being built in this space, what's actually being designed, and that's the most important area to look at. Obviously there's some writing as well, a lot of Vitalik's blog posts deal with cryptoeconomic ideas. *Interactive Coin Offerings* from Teutsch and Buterin is another example.

MT: Why is the term so popular right now and how do you think it will evolve in the future?

JS: A lot hangs on Proof-of-Stake, Sharding and Plasma, and there's a lot of attention focused on those areas of research and application. The leading people working on those protocols refer to their work as cryptoeconomics. And of course, in 2014 Ethereum was much less popularly known. There was much less attention on it, so Vlad's talk at that time garnered less attention. Now, it's very much the forefront of what people think about, when they think about Ethereum and what's coming next. The term cryptoeconomics, without a careful definition, became many things to many different people. So there's a lot of people out there who use the term to refer to just the study of cryptocurrency markets. Or, because there's so many people out there trying to hold an ICO and get lots of money, they want to use fancy terminology in their papers, and they often misuse it.

> **The economics of tokens is still economics, it's still the study of human choice, of human behaviour.**

I hope the term to be much more narrow in the future. If cryptoeconomics just becomes any application of any economic idea to blockchain or cryptocurrencies, then the term is meaningless. It's just a fancy way of saying: applying economics to a new kind of asset class. The economics of tokens is still economics, it's still the study of human choice, of human behaviour. If the term stays broad, I suppose it will end up being a meaningless term. There's enough coordination now,

experts working in this field, and we're going to get to a more narrow definition. Some people say 'it's an awful term and we should change it'. Cryptoeconomics makes it sound like it's the economics of tokens and that we should abandon it, because it's confusing. But I think we're stuck with it. It reminds me of people talking in 2014 about how 'we need to change the name of Bitcoin, because Bitcoin sounds too technical and scary'. Of course that was never ever going to happen. And I do think we have the tools, the new terms for new fields. They don't need to be perfectly descriptive, because quite quickly you move to this new mutual understanding of what the term means. And it's no longer confusing because people aren't hearing it for the first time and thinking what it must mean, they just read the definition somewhere else. So it'll be a pretty quick process.

MT: Game theory was, in the beginning, very narrow, and then it grew into an interdisciplinary field which is also informed by social sciences, political sciences, and other disciplines. Do you believe cryptoeconomics could also evolve that far?

JS: Cryptoeconomics is not a pure theory. It's very applied, and it is very much about engineering and building things. A large part of the theory that ends up informing and being developed from cryptoeconomic design will sit already in game theory. We will have new avenues to study human behavior in new kinds of systems and markets, and that might inform the more theoretical side of things. One difference is that it'll grow and become bigger, but it'll become a very applied thing. We might end up with game theory and cryptoeconomics being separate, and cryptoeconomics remaining a more applied science. It will be interesting to see how that turns out.

> **One of the biggest misconceptions about blockchain technology and cryptoeconomics is to depict it purely as a topic of computer science.**

MT: For cryptoeconomics to be widely accepted, do we need more academic rigorosity in this context? Do you see that already happening with the existing academic field that we have?

JS: A very tricky thing about the field is that it is so interdisciplinary, and in a way, that previously hadn't existed. The study involves cryptographic protocols and game theory analysis. There's not many people in the world that were doing that kind of interactions before, so it requires bridging gaps between two quite different disciplines, which is going to be a challenge. Either we make it its own academic niche - academics early in their career would need to learn both of these disciplines in parallel to become true experts in this field- or we need scholars from one discipline to learn the skills of the other domain. Academia can be very narrow and very focused on one specific field, and depending on the university, there can be some challenges there. It will pose problems for future academia if interdisciplinary thought is not promoted, especially for career perspectives of academics. One of the biggest misconceptions about blockchain technology and cryptoeconomics is to depict it purely as a topic of computer science, making it about programming. This of course is not true. You cannot remove the economic incentives from the systems and hope to understand them. The result is that we abstract away the idea of incentives, so if you have ever seen the saying 'Bitcoin is backed only by math', it's not true. Although it is partly backed by math, this math is enforcing a set of rules that rely on assumptions about human behaviour. It's backed by math and the assumption that people will respond to incentives to continue mining Bitcoin. So I do hope that academia can bridge these divides and can get everybody to see both sides of that issue.

MT: Where are the boundaries of cryptoeconomics? What role does the organisation, company culture, and the community play in cryptoeconomics?

JS: Analysis, not just of a core team but also of the broad community, is critically important. And by community, my definition of that would be: miners, core developers, developers of critical infrastructure, like clients and any user wallets, and then the users themselves. All of these have a different kind of vote in the system and they check each other to a certain extent, and each have different interests, different incentives. If you're looking at a company and you try to understand how it will behave, you think about who is executive, you think who the employees are, you think who's on the board, you think who the major shareholders are, then you understand the interactions between them to produce a model of what that company might do. Most people, when they look at cryptocurrencies, are not thinking in those terms because they think it's different somehow. But they need to be thinking about who the miners are, what their interests are, what their votes are, who the core devs

are, what their interests are, what they are going to do, and who the users are. And we're seeing a high stakes version of this play out now in the Bitcoin community, where there are different communities, except that they're deadlocked and cannot find a solution, and they're not willing to work with each other. Monero is a good example, where they have a more complex way of rewarding community, incentivising development, paying out to them and so forth. I think there is a lot of work to be done in trying different models of that kind and seeing what works. The counterpoint to that is that many open source projects have been wildly successful without any financial rewards necessarily. People spend time on these projects, not because they're being rewarded, but because they want to. What is the balance between people contributing because they want to and are passionate about it versus people contributing because of financial incentives? Are these mutually compatible? We have a lot to learn from the open source experiences of the last 20, 30 years in order to design and foster our communities. I wouldn't say that's cryptoeconomics, but that's another thing. We're trying to create a community that has a certain end result which is sustainable, positive and welcoming. What can we do to make that outcome more likely? The same way that you would design a company, for example through good HR policy, you need to think about what you can do from a soft power perspective to make a community more positive.

The difference between open source projects and more traditionally managed institutional design is that you have very little actual control. If you are core devs and you're starting a project, building a positive community, you are not employing anyone. You can't fire them, you can't hire them, you can only hope to attract certain kinds of people. You can reward them financially, but you can't really penalise them. You've a different set of tools with which to try and construct a human organisation. It's not like building a company, and it's not like building an NGO. Linus Torvalds once said that someone asked him "what's the most important thing you've learned that you would have done differently?" His answer was "treat people better, don't be a jerk", because in the end he saw how toxicity really hurt the Linux community. And what seemed important at the time, to be aggressive; in the end it was clear how much it hurt us. I strongly disagree with my friends in the Bitcoin community who think their toxicity is somehow a good thing, that it represents their high standards or it makes them more elite. It's going to hurt them for a very, very long time, because you cannot keep developers in that community if they hate being there, if they are talked down to and if they are not respected. And not that that's true across the whole bitcoin community, because there are many amazing talented positive people, but there certainly is toxicity to that community at times. And I certainly hope that other communities will be able to learn from that and try to head that off, when they themselves have difficult political struggles in the direction of a project.

MT: I can understand this 'toxicity' to some extent, but I also think that a lot of controversies are not really making sense and communities should be more open to learning and being civil in challenging each other. After all we are building the future together.

JS: The problem of this toxicity is that once an issue becomes personal, once people become very emotional about it, it hardens their attitudes and they're less likely to be able to change course. When you've committed publicly that 'this is what I'm going to do', for example: "no to Segwit", this becomes a part of your identity, and it is much harder to change course and to change your mind. It's just obvious that in order to have a community that reacts properly to new information, that can experiment and try things, you need to have one that can have civil discussions and not toxic ones. Rewarding the community is not cryptoeconomics, and that's actually a good example of a border case of whatever we call cryptoeconomics. To reward and to incentivise a large group of people to do something, you don't necessarily need cryptocurrency. If you're just doing the exact same thing as the Monero community but with fiat or paypal, you could have a similar design challenge of paying out people for certain things. Is that necessarily cryptoeconomics, if you can accomplish it with something that's not cryptocurrency? I think probably there are some things you can only do with cryptocurrency, because you can only automate it to some extent with cryptocurrency. Is Google AdWords cryptoeconomic? Well, it certainly is not because it existed before Bitcoin, but in a way it is a fairly complex and sophisticated, automated, money driven auction system. If we built that with Ether, we would call that cryptoeconomic. Why is one cryptoeconomic and the other is not? We have to define more clearly what the boundaries are.

HOW TO TALK ABOUT SERIOUS MATTERS OF COMPLEXITY WITH MODELS AS AGENTS

A speculative essay

SHINTARO MIYAZAKI

This essay is conceptualising models as cultural techniques[1], agential[2] media and designed systems, which catalyse fruitful discussions on serious matters of our commons. The term 'commons' means all the natural, technological and cultural resources accessible to all members of a community. This is also relevant for artistic and design-based research as it is argued in this essay. Models are called into action especially when these "matters of concern"[3] transcend our intuitive understanding and reach a degree of complexity[4] that goes beyond simple human reasoning. In such cases, we need help from models. They show us, and let us experience, important aspects of the unforeseeable, emergent, and sometimes global effects – both positive and negative – of our machine's day-to-day micro-behaviour. Consisting of little actions, they combine to affect our common resources and infrastructures.

Models manifest themselves as mechanical machines, analog computers, synthesisers, software simulations, games, animals, bacteria, ecological systems and much more. They are crystallisations of scientific theory in agential matter, which we humans can see, feel and hear. As such they belong not only to the domain of science and technology, but also to art, design, architecture, dance and sound. Models can be artistic or have an elaborate design. On their way from techno-science to art galleries, design exhibitions, workshops and public interventions, they go through a metamorphosis from ideally being functional to being diffractive, sometimes even dysfunctional. Following this thought, the essay addresses a yet-to-be realised program of artistic and design-based research. This strategy intends to enable, catalyse and open up fruitful discussions of the ongoing micro-design (Ernst 2013)[5] of the different modes, rules and habits in the human and non-human 'mattering', enactment, organisation and management of common resources, goods, knowledge and infrastructures.

Minor of matters

During their endeavour to acquire new knowledge, scientists and engineers usually apply established designs of instruments, tools, models and simulations. Often, they need to develop their own tools of experimentation, but unfortunately rarely have time to reflect and experiment upon their extended aesthetic, artistic and design-related aspects. While accuracy of content abstraction and technical functionality matter, these issues, although recognised, are of secondary importance. They are minor matters and do not appear on scientific research agendas. As the aesthetics of things, objects and processes are key competences of art and design, everything which addresses the human sense-modalities is a matter of our concern. Given the ongoing cost reduction in electronic tinkering, mechanical parts, computation power, robotics and rapid prototyping, as well as the dawn of open soft- and hardware projects, researching matters of complexity with alternative models as agents in creative, but technologically-informed ways is at the edge of becoming an issue of application-oriented fundamental research done at art and design universities.

Practices of modelling are seen both in the field of the arts and in technoscience. Physical models, for instance, are used in both contexts. Nude models, model figures, clay models and sculptures, indeed all sorts of assemblages of body and materials in artistic contexts, are similar to scale models, model cars, globes, atom and molecule models massively used a long time ago in science and engineering. Nowadays, they are only used for pedagogical purposes. The same applies to conceptual models, which are based on feedback circuits. The electronics used in analog computing, a long-forgotten scientific field that proliferated between the 1920s and 1970s, are basically the same circuitry later incorporated in the audio and video synthesisers used by many composers and artists since the 1960s, such as Nam June Paik, Steina and Woody Vasulka, Jack Burnham and many more. Others such as John Cage or Harald Haacke (1924–2004) experimented more conceptually with the idea of feedback.

In technoscience, the aim of modelling is "to represent an idea, concept, or situation, usually in a form that facilitates further analysis. The more malleable and flexible the modelling medium, the more powerful and experimental the modelling" (Care 2010). With the dawn of digital computing in the 1980s, scientific modelling was increasingly done with simulations watched on computer screens. At the same time, artists and designers started to use the computer for their creations. But while the creative still preferred

diversity and used not only visual, but also sound-based forms of expression, always showing the hardware of their projects and works, scientists and engineers were more and more using only visual, screen-based media for their modelling. Understanding complexity by simulations applying agent-based modelling, for example, was mostly done via eyes staring at some screen, interacting via keyboard and mouse, later by touch-screen.

The aesthetics of things, objects and processes are minor matters in technoscience. What counts is the content. Therefore, the way simulations and modelling is done never changed substantially since the dawn of the PC. There are several reasons for this ongoing tendency towards visual and virtual abstraction (Latour 1986). One is certainly the above-mentioned malleability of digital media and another the printability of computer graphics, but these can't get fully discussed here. Instead, I will give a brief general account on a speculative, yet-to-be realised program of artistic and design-based research. A program that will liberate technoscientific models from their aesthetic constraints in order to make them more useful and understandable. Not simpler, but more complicated, affective, disrupting, disputable; more interfering, parasitic and troubling than before.

Common concerns

There are no consistent research programs without some theoretical backing, therefore some considerations are in order. The legitimacy to do research in art and design shall not be questioned. That would be pointless. We build on two assumptions. Firstly, artistic research and experimental design are techniques of emergence (Manning and Massumi 2014). Secondly, research practices in science and engineering are similar to design processes. Verification of both assumptions occurs only by concrete enactment and unfolding. Focusing on modelling complexity might be an interesting strategy within these conditions, since it affords a coupling to urgent global issues of governing the commons, not only addressed to politicians and policy makers, scientists, engineers and critical thinkers such as sociologists, philosophers or historians, but, as I argue here, also to artists and designers.

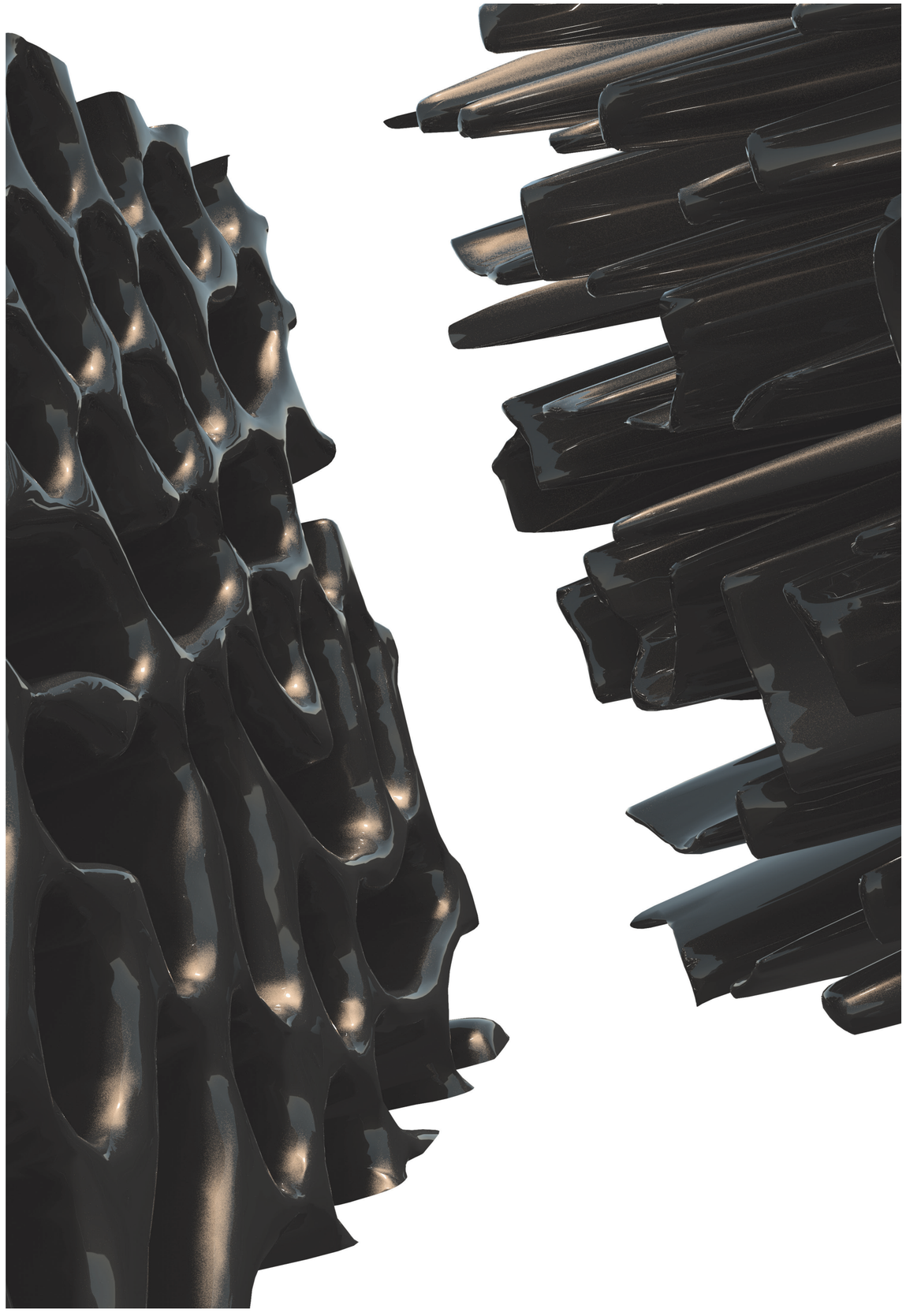
Convincing examples of such urgent matters are cooperation dilemmas and issues among users of common pool resources. A common pool resource is a type of asset consisting of natural, cultural or social resources like air, drinking water, fishing grounds, pastures, forests, irrigation systems and generally all energy and nutrition resources; also resources like literature, music, movies, all media products in general and open source software. According to our democratic ideals, these are all resources that are or should be held in common, not owned privately, since they affect all connected forces, parties, agents and humans, regardless of their geopolitically allocated influence factor. Disastrous effects of bad resource management and cooperation dilemmas, such as traffic jams, over-fishing or even climate change, are often results of complex interplay of all involved micro-forces.

Resource sharing is not easy. *The Tragedy of the Commons*, as formulated in 1968 by Garrett J. Hardin in an article in Science, is one of the most famous depictions of the social problems of common goods sharing. "Picture a pasture open to all. It is to be expected that each herdsman will try to keep as many cattle as possible on the commons. [...] Therein is the tragedy. Each man is locked into a system that compels him to increase his herd without limit – in a world that is limited" (Hardin 1968). This will inevitably lead to an over exploitation and resource depletion.

About twenty years later, Elinor Ostrom[5] published *Governing the Commons* and therein referred to Hardin. Besides picking up similar models such as the prisoner's dilemma game, she also took up Mancur L. Olson's *The Logic of Collective Action (1965)*, where he theorised that members of large groups do not act according to a common interest unless motivated by personal economic or social gain, while small groups can act on shared objectives. Personal gain leads to bad results, if the resource is limited. Obviously most resources are limited in some form.

Ostrom was more optimistic than her precursors, and described many real-world cases where sharing a common resource pool is working. By field research and referring to Game Theory, she famously formulated eight design principles for stable local common pool resource management. Most importantly, operational rules of resource usage would need to be defined by the participants themselves, not from top-down, but bottom-up.

Governing the Commons was highly influential. In the last twenty-five years since 1990, models of common resource sharing were implemented in digital computer simulations; and concepts from cybernetics[6], system dynamics (Castillo and Saysel 2005), chaos theory (Wilson et al. 1994), and even cellular automata theory



have informed this still evolving field of research (Berge and van Laerhoven 2011). Already Ostrom herself not only referred to W. Ross Ashby's *An Introduction to Cybernetics*, but to Thomas Schelling's *Micromotives and Macrobehavior* as well as Ilya Prigogine's *Time, Structure and Fluctuations*[7]. Both are discourse-founding Nobel Prize lectures (1978, 1977) for establishing research in emergent, counter-intuitive group behaviour, nonlinear dynamics, self-organisation and research on complex systems.

Modelling the complexity of micro-actions within the field of the commons is promising. These and other connections allow innovative links to alternative modes of modelling beyond digital simulations, such as analog computing, feedback circuitry and hybrid models. More recent research on the commons combined with computer gaming is equally promising. Since 2015, after the rise of serious gaming (Schuller et al. 2013), tragedy of commons games are playable online. Still the steps to a recursive application back to common pool resources users in order to inform them are rare, while the importance of self-organisation and self-governance has already been formulated. A conventional design task would then be to facilitate and enable such processes of self-organisation by improving aspects of visual communication, product or interaction design. Victor Papanek, since the 1970s, was one of the first to combine ecological thinking with product design. More recent emerging research fields are participatory design, design in the context of citizen science, eco-design, sustainability and transformative design. Such projects hopefully provoke interest from institutions such as the Centre for Policy Modelling in Manchester (Edmonds and Gershenson 2015). A slightly more radical approach would claim that merely playing a prisoner's dilemma or a tragedy of commons game is not enough, since making, programming and designing such a game involves much more learning and is therefore much more effective.

Diffractive modelling

Design work and aesthetic experimentation with the communicative affordances models within fields such as those offered by the commons, unfolds firstly via contact with policy makers and managers working in organisations acting in these fields, and secondly via linking more directly with the involved actors, users and workers. The experience of complex matters via artist and design-based sense-making with models and interaction is surely insightful. An emphasis on enabling not just a reflective, but a diffractive understanding[8] about common pool resources might prove to create stronger impacts. This is the speculation this short essay builds upon.

According to Karen Barad and Donna Haraway diffraction, in comparison to reflection, which is the common term used in conjunction with critical inquiry or critical thinking, is not merely about mirroring without influence. It is also about positive interfering, blurring, bending and transforming with the content under study (Haraway 1992). It is a spurious *différance* (Wood and Bernascono 1988) or a smeary differentiation. When you drop two stones in a pond they generate ripples, interferences and interweavings on the water surface. Similarly, fields as diverse as the arts and technoscience could positively interfere with each other, still maintaining their specificity and characteristics. A diffractive inquiry both transforms and bends its subject in order to create a range of alternative approaches for its study, but also tries to keep high-fidelity concerning its sources.

Diffractive modelling designs communication between the matter to understand the model and its user in a highly flexible, if not an agential manner. Agential is a term I borrowed again from Barad. Quantum physics showed us that "theoretical concepts are defined by the circumstance required for their measurement" (Barad 1998). This means "that there is no unambiguous way to differentiate between the 'object' and the 'agencies of observation'." Not only is the user (inter)acting with the model, the model is acting back and becomes an agent. Model, user and creator are all, as agents, coupled to each other like in a ménage à trois. As Henri Poincaré showed, three interacting bodies generate nonlinear dynamics. A minor change in the condition of one of those three is agential upon the remaining two. Furthermore, as in quantum physics, where a particle can become a wave and vice versa, diffractive modelling is never static. Ideally, it is unfailingly experimental, slippery, strange and peculiar; not sticking to one version of modelling, but constantly researching new forms of representation, aestheticisation and sense-making. It therefore demands a lot of effort.

To be more concrete concerning different techniques of modelling, a first step would be to broaden the current aesthetic qualities of simulation and modelling by transgressing again to physical space and real-world processes – as was done in the past with physical models, electrical equivalents (analog computing) and mechanical types of models. Furthermore, by combining digital computation with electronics and real-world actuators such as motors, electromagnets, hydraulic, optical or acoustic systems and more advanced sorts of transducers – in other words, by combining hardware with software or by carrying out physical computing – positive diffractions of current modelling and simulation practices could emerge. Neighbouring fields such as interface/interaction design and research on the so-called Internet of Things at institutions such as the MIT Media Lab, Royal College of Art, ETH Zurich and many more are offering thousands of starting points to unfold diffractive modelling.

It was not by accident that for a long time interactive modelling was regarded as the domain of analog computing, and information processing and calculation as the domain of digital computation (Care 2010). Analog systems operate in real-time. There is no symbolical translation of the matter in action. No data involved. That was its specificity, but the acceleration of digital processing made it redundant. Historical ignorance is obviously no option. Digital simulation shall thus not get abandoned, but extended with analog computing: Agent-based modelling not only as virtual simulation, but more as some sort of tangible real-world happening, not fully out of, but a little bit under control.

The history of analog computing affords a whole ecosystem of strange apparatuses, peculiar assemblages and unheard-of models. Soap bubbles were used in aerospace engineering for obtaining mathematical solutions of the so-called Laplace equation. Their surface was an analogon for mathematical principles (Care 2010). Hydraulic flow systems were used to model the national economy of the United Kingdom (Care 2010). Electrolytic tanks were used broadly for oil reservoir modelling (Care 2010) or so-called rotating dishpan models for chaotic fluid dynamics (Care 2010). Could such strange apparatuses become diffractive models for experiencing and understanding current matters of concern? In the early 1960s, British cybernetician Stafford Beer was experimenting with organisms such as leeches in an artificial pond, which would model a whole economy. He did not succeed (Pickering 2009), but in a recent scientific field called *unconventional computing*, leeches were used as models of the behaviour of humans fleeing buildings (Adamatzky and Sirakoulis 2015).

Diffractive modelling is not meant to become fully useful in its straightforward meaning. It is not about utilising creativity in order to solve global issues. It is more about addressing them by interactive involvement via modelling and experiences, which provoke new alternatives of established practices. Diffractive practices need to stay vague and experimental, in order to enable new modes of coupling. At the same time, it is important to keep it down-to-earth and establish high-fidelity with the sources of the interference. How to talk about serious matters of complexity with models as agents is not an answer, but a question, which should indeed be the main driving force of such a difficult endeavour.

---

1 Parrika 2013
2 Barad 1998
3 Latour 2004
4 I define complexity as a phenomenon linked to a system, network, collection or assemblage with many parts where those parts interact with each other in multiple ways, so that they generate effects that are unforeseen, not in or der (predictable), nor totally random, but in-between these states. See Mitchell, 2009
5 In 2009 Ostrom shared the Nobel Prize in Economics with Oliver E. William son for her analysis of common resource pool governance.
6 For those who are inclined to ask for references, here a short, but pertinent list: Wiener 1948; Ashby 1956; Hayles 1999; Mindell 2002; Turner 2006; Johnston 2008; Pickering 2011.
7 See bibliography in Ostrom 1990.
8 Thanks to my friend and current work colleague Jamie C. Allen for hinting me to this important vein of post-feminist materialist theory.

CRYPTOECONOMICS AND EXPERIMENTS IN TOKEN SALES

An Interview with Vitalik Buterin

DANIEL PICHLER,
MARKUS ZIMMERMANN &
MATTHIAS TARASIEWICZ

Matthias Tarasiewicz, Daniel Pichler and Markus Zimmermann spoke with Vitalik Buterin at devcon3 in Cancún, Mexico. Buterin is the creator of Ethereum and co-founder of Bitcoin Magazine. He first discovered blockchain and cryptocurrency through Bitcoin in 2011. He now leads Ethereum's research team, working on future versions of the Ethereum protocol.

MT: You are responsible for the research of the Ethereum Foundation. What kind of research are you undertaking? And how are you interfacing with universities and traditional academia?

VB: We are heavily interacting with traditional academia. For example, we have an annual workshop with IC3, that's the Institute for Cryptocurrencies and Contract that we have at Cornell. A lot of them are doing research on proof-of-stake and sharding, scalability solutions and for more verification, things like trusted hardware and so forth.

We are in very close contact with all the professors that are inventing zero-knowledge proof stuff, SNARKs and STARKs. There are a lot of individual cryptographers and economists that we're talking to, and then there is a large portion of research that just happens basically among ourselves within the research team, but we interact with outsiders heavily just to make sure that we're still sane.

MT: Where do you publish, when you're publishing?

VB: We are basically publishing 100 percent online. We did publish one paper to archive, which is the Casper Friendly Finality Gadget paper. So far, the output of our research has been informal ideas discussed on forums, though it is getting to the point where we are starting to move towards more polished results.

MT: Can you explain the idea of cryptoeconomics to an audience that's not deep into cryptography and economics.

VB: Cryptoeconomics is an area combining together ideas from cryptography, game theory, fault tolerance and decentralisation in order to build systems that have security properties that any one of those things alone can't provide. The one example I always give is basically just the Nakamoto blockchain itself, because it is almost a philosophical innovation. You have a system which defines an asset inside of itself and that asset is responsible for incentivising the systems continued existence. That's something that's very powerful and interesting by itself, and then on top of it, lots of things can get built.

MT: Cryptoeconomics is largely based on game theory. In its infancy game theory was a very closed field and later it emerged into what we have today, an interdisciplinary field. Do you see cryptoeconomics in the future also growing like that?

VB: I think cryptoeconomics is still in its infancy right now, but it is at the point where there are a lot of traditional academics getting interested, and a lot of them are basically doing it without calling it that. The design of these kinds of systems is something that deserves to be viewed as a separate field of study. Right now there are a lot of cryptographers that already see this as a potentially very powerful extension of cryptography because with incentives, not only can you prove things about the past, but you can try to make guarantees about the future. But I think there is still a lot of room for people from traditional game theory to get involved as well.

Cryptoeconomics is an area combining together ideas from cryptography, game theory, fault tolerance and decentralisation.

MT: Who would you say are people already doing things that could be considered cryptoeconomics, but maybe not being recognised as such. Are there notable researchers?

VB: Let me think. I mean just anyone who has worked on a proof-of-work or proof-of-stake algorithm. There are people like Iddo Bentov and others out of Israel that have been doing proof-of-stake. There's the selfish mining papers. All the things that are close to cryptoeconomics and could be directly applicable. There are definitely protocols and branches in cryptography that specifically have to do with attributability, so if the system goes wrong, then make sure that it's provable, and it's provable who made it go wrong.

Even though something like the concept of attributability isn't economic by itself, it does work very nicely with economics, because if you can attribute then you can penalise. So that's something that's also fairly important.

There is research into things like different types of equilibriums; coalition game theory, that's even further, but it still has a lot of relevance to consensus protocols. It's probably a sum of all those things put together.

MT: In the paper *Interactive Coin Offerings* you wrote with Jason Teutsch, you raised the point that a few token or crowdsale mechanisms didn't go as expected and offered new perspectives. Can you give us a short overview of what the idea was?

VB: The idea is a coin sale, where you would have a long period of time where anyone can send a buy offer specifying at what maximum valuation they are willing to buy at. Either after some point in time, or when some cap hits, the buying period would stop. There might be further periods in which people could ask for refunds, but then after that, the system basically takes the set of people who would be willing to purchase at the highest valuations and gives them the tokens. The idea is that the system makes sure that you only get tokens at a valuation which is equal or lower than the valuation you're comfortable with. It tries to satisfy the goals of fairness, giving everyone a chance to participate and the goal of not setting a cap that accidentally ends up too low, which just rewards the people who get in first. And it removes the need for the person who's creating the sale to try to even figure out things like a cap if they don't necessarily want to do that. It also provides us a guarantee of participation. So, if you participate then either you get in or the valuation is so high that you would not have wanted to get in, anyway.

MT: Who tried this particular token sale yet?

VB: The closest thing that we had was probably the reverse Dutch auction for the Raiden token, but the interactive model is still a bit nicer because it's not time dependent. But there is definitely risk. I hope we see some small-scale experiment just to see how it works economically. Even the Raiden sale itself is a bit of an experiment because it is a vaguely similar mechanism in some sense, and it actually seems to be working fairly well.

DP: Do you see also an option for round based ICOs in the future, where they act more like the traditional funding rounds? Right now they are all up front...

VB: I definitely think that moving beyond the up-front model is important. Gnosis did what I think, in a lot of ways, is the right thing. They did do a reverse Dutch auction, but they also had a fairly low cap - which worked, but they ended up keeping 94 percent of the tokens and without the cap, they may well have been one of the other 100-200 million-dollar sales. Because they capped 94 percent they got accused of being a central bank with unilateral control of the token. There is a bit of a trade-off here: If you are taking ten million dollars from people who are willing to give you a hundred then that means either you are wasting ninety million or you're creating this protocol where you end up keeping 90% of something.

There are a bunch of fairly equivalent solutions. One of them is that you can have a sale that gives people the ability to refund for some point of time. The other one is that you can commit to releasing the other 90 percent on some schedule. The 90 percent could literally just directly go into a market maker that enforces the commitment. So, doing things like that removes this kind of centralised trust level. It definitely is going to require more experimentation and few more failures though.

The other thing is, it does seem like the ICO space is cooling down a bit, so the experiments may well end up being smaller, which is probably a good thing, too.

DP: Do you think an approach would work, where people basically have to hit development milestones and give money back if they don't deliver?

VB: Yeah, I think that's definitely a good idea. The one parameter in that model becomes who decides when the milestone was hit. So, one model that I think is actually interesting is one in which the participants in the sale basically vote on when the milestones are decided. And if they would really want to, they could just vote to fire the developers and move the funds to someone else. That's something that should be tried more.

DP: Like in a prediction market?

VB: Prediction markets are one way, but the other way is just literally a vote. So, if 51 percent of the buyers say cut off the funds, then the funds get cut off.

MT: In your 2014 paper you were explaining the idea of futarchy from Robin Hanson, and I still find it very relevant but also it was written in a time before there was the Fork.

VB: Futarchy is definitely an interesting idea, but it's main challenge is a measurement problem. So basically, for futarchy you have to have an objective, and then how do you measure from inside the system whether or not the objective has been satisfied? If you have a proof-of-work system, you can do things like optimising for mining difficulty, but even that's a fairly coarse estimate. That would be a proxy for the price of a token and that might be one thing you want to optimise for, but in a proof-of-stake system even that's very difficult.

I'm not really sure if there is that good a way of measuring things, especially at base protocol layer without introducing new vulnerabilities. At the level of DApps it might end up working much better. We'll see.

THE ADVENT OF DIGITAL PERSONS

Why software-based agents shall gain personhood

OZAN POLAT &
BENEDIKT SCHUPPLI

Digital entities - as humans in a digitised world, we frequently interact with them, communicate with them, trust in their decisions as well as ask them questions. They accompany us on a daily basis, curate, pre-select and alter information just to present it to us in a palatable form. As blockchain geeks, we send assets to and receive assets from them. Although they lack many characteristics which we commonly associate with other actors we interact with, we often subconsciously ascribe agency to them.

Throughout history, the notion of personhood continuously evolved to include both human and non-human actors, from deities to corporations. In literature, we employ stylistic devices to animate otherwise inanimate objects. In economics, we anthropomorphise financial markets to better grasp "their" behaviour. As digitisation has brought new entities into life, which act both more autonomously and more humanlike than the aforementioned corporations, we face the immanent question of whether we must once again extend our concept of personhood to encompass these numerous digital entities we steadily interact with.

It is the goal of this article to explore the concept of personhood including its transported limitations and consider whether we can feasibly expand it to include digital entities such as AI-systems, single smart contracts or DAOs[1].

First, we will explore the historic context of the concept of personhood, examining both legal and spiritual considerations regarding personhood of non-human entities. Thereafter, we look at existing instances of autonomous digital entities and examine what properties they possess. Finally, we make the case why we indeed must introduce the concept of digital personhood.

What is Personhood?

What is a person other than a subject that can be held accountable for their actions? Such is the definition of a person according to Immanuel Kant, as laid out in his 1785 treatise on the metaphysics of morals.

While the characteristic of being accountable for one's actions is commonly ascribed to human entities, our history is full of examples where such accountability has been expanded to include non-human entities.

It was the great jurist Karl Friedrich von Savigny, influenced by Kant's considerations on legal capacity in metaphysics of morals, who stated that legal capacity can be expanded to encompass something without the single individual, i.e. by artificially construing a legal person.

> *"Wir betrachten sie (Die Rechtsfähigkeit) jetzt als ausgedehnt auf künstliche, durch blosse Fiction angenommene Subjecte. Ein solches Subject nennen wir juristische Person, d.h. Eine Person, welche bloss zu juristischen Zwecken angenommen wird. In ihr finden wir einen Träger von Rechtsverhältnissen noch neben dem einzelnen Menschen" (Savigny 1840)*

With this statement Savigny proposed that the legal capacity was being expanded to artificial subjects, conceived of solely via the power of fiction. This subject was called "legal person", i.e. a person which is assumed to exist exclusively for legal reasons. Thus, according to Savigny, a legal person is an artificially conceived subject capable of owning property.

As of today, courts around the world have ruled on the limitations of rights awarded to legal persons and concluded that legal persons are not only capable of owning property, but also capable of personality rights such as the right to a reputation and constitutional rights such as freedom of speech[2]. According to article 53 of the Swiss Civil Code, "Legal entities have all the rights and duties other than those which presuppose intrinsically human attributes, such as gender, age or kinship".

But it's not only in law that our notion of persons being first and foremost humans has traditionally been challenged. The oldest non-human entities capable of actions are very likely deities and spirits. While ascribing agency to non-human entities such as deities may seem like a foreign concept from a modern, secular perspective, such ascription was commonplace for a long time.

If we delve into the Bible, we find many examples of God as a subject being capable of property:

> *"The land is mine and you are but aliens and my tenants" (Leviticus 25:23)*
> *"To the Lord your God belong the heavens, even the highest heavens, the earth and everything in it." (Deuteronomy 10:12)*

In danger of alienating religious people, we consider deities as fictitious. And just as deities are dependent on humans to both communicate and carry out actions, so are legal entities dependent on their human constituents to make decisions (e.g. members of a board of directors who make decisions binding on the legal person's property), to communicate and to carry out actions. Just as the company VW can own property, deities in ancient egypt were considered to be the owners of temples and could assert their will through actions of the pharaoh and his underlings (Harari 2015).

As demonstrated, legal entities require natural persons to act on their behalf and execute the will of the entity. Furthermore, it's natural persons who are at both the entry and exit point of the decision-making process of legal entities: a single or a number of natural person(s) form a decision as legal representatives of the legal entity which thus becomes a legally binding decision by the legal entity which is subsequently executed on behalf of the legal entity by natural persons. The same goes for deities which needed humans as their vessel to transport messages into the public and act on their behalf as well as administer their possessions.

Thus, the degree of autonomy legal entities and mystical entities enjoy is of a limited extent and always dependent on human support. As we intend to show below, this is different for some digital entities.

Digital Persons

We envision a rise of autonomous entities enabled through advanced research in artificial (general) intelligence and given agency through code, inter alia in the form of smart contracts, built upon public distributed networks such as a public blockchain. A smart contract is a piece of code on the blockchain that comes with a guarantee of self-execution given an event or state.

As one of its key characteristics, a smart contract cannot be shut down or altered once it is deployed on a network which is run in a distributed manner – unless the whole network is taken down. An example of an autonomous entity could be a network of vending machines, where a single vending machine is notified via a sensor that it is running out of certain items and therefore sends an order to a supplier which causes the deployment of a smart contract to which the supplier becomes a party: once the vending machine's sensor signals that the requested items have been refilled, the smart contract is triggered and the supplier is paid. One can also imagine a fleet of self-driving cars, where the interactions with human suppliers, car mechanics, guests and other entities are fully governed by self-executing contracts on a decentralised network.

However, for digital persons, the extent of their autonomy can be significantly larger than in the examples above. Although a digital person may still require humans to execute its will in some cases, it is able to form decisions and act on them in an entirely autonomous fashion in other cases, independently of humans.

> *"If AI systems eventually get better than humans at investing, this could lead to a situation where most of our economy is owned and controlled by machines. If it sounds far-off, consider that most of our economy is already owned by another form of non-human entity: corporations. Which are often more powerful than any one person in them and can to some extent take on life of their own (Tegemark, 2017a).*

In the near-term future, we will face digital entities who act autonomously on a transnational, distributed network and don't always need a physical manifestation or representation to interact with natural or legal persons. They will manage funds, pay humans for labour, possess things and create other entities - independent of third party involvement. These developments give rise to a myriad legal questions such as tort liability, tax liability, social security benefit liability, and property rights of digital entities. While these questions are fascinating, answering them (from a de lege lata perspective) would go beyond the scope of this text. Rather, we propose to accept these entities as autonomous, digital persons as they are endowed with no lesser level of autonomy than the legal persons we interact with on a daily basis. What this means from a de lege ferenda perspective shall be the subject of further research.

In order to assess the digital personhood of any digital entity, we must further explore the level of autonomy required for such qualification.

Autonomous Agents

The Oxford Dictionary defines autonomy, inter alia, as the "freedom from external control or influence; independence". As stated above, a legal entity relies on its organs comprised of humans, such as a board of directors, presidents, secretaries etc. to act as agents in the process of decision-making, and in the execution of these decisions on its behalf. Legal entities are therefore not autonomous agents. It is precisely the characteristic of agency in the form of self-execution, without the interference or need of a third party that gives digital entities the necessary level of autonomy to be regarded as digital persons.

This does not mean that a digital person must be able to execute its will[3] exclusively without a human being or another party. Especially in the analogue realm, a digital person would still need representation through a human surrogate. But given the current technological developments, the digital person can now act directly without human intermediation e.g. in employing humans and paying their salaries through smart contracts as well as autonomously managing its assets, including transactions of programmable funds.

Such is the case with Plantoids: "A Plantoid is the plant equivalent of an android; it is a robot or synthetic organism designed to look, act and grow like a plant[4]." Plantoids are blockchain-based lifeforms that reproduce through the combination of code and human interaction. The goal of a given Plantoid is to raise enough funds to be able to employ a human surrogate that then would produce the Plantoid's offspring.

In the example above, technology no longer acts as a tool but as a peer in a direct relationship with natural or legal persons[5].

Substrate Independence

> *What do waves, computations and conscious experiences have in common, that provides crucial clues about the future of intelligence? They all share an intriguing ability to take on a life of their own that's rather independent of their physical substrate (Tegemark 2017b).*

Similar to a natural person whose mind inhabits a body, each *Plantoid* consists of comparable components. On the one hand, its physical body in the form of an electro-mechanical construction, and on the other hand, its "soul" – "represented by an autonomous software agent that lives on a blockchain"[6]. If the physical body of the Plantoid is destroyed, the autonomous software agent - in the form of a smart contract - continues to live on the distributed network it was deployed on. Therefore, the soul of an autonomous software agent – to stay in anthropomorphic speak – is capable of inhabiting different bodies or even none, while the human mind is currently bound to its carbon-based manifestation[7].

For fans of science fiction culture, this feature might immediately create the association of a new cast of eternal life forms living on the ever-connected cyberspace, changing or leaving bodies or shells behind when needed.

While substrate independence is a characteristic of software-based agents such as DAOs, smart contracts, and AI algorithms which seems to increase their level of autonomy, it remains unclear whether it's a necessary characteristic for digital persons to be awarded personhood. This shall be the subject of further research.

Current Developments

As stated above in Max Tegmark's quote: what might sound far-off has already begun to manifest itself. Plantoids are a tangible form of autonomous entities launched in 2016 by Primavera De Filippi. Two years before the first Plantoid blossomed and interacted with natural persons, !Mediengruppe Bitnik, consisting of Carmen Weisskopf & Domagoj Smoljo, launched their "Random Darknet Shopper", a bot managing the private key of its own Bitcoin wallet, that receives weekly a budget of 100 USD in Bitcoin. The bot would activate itself every Wednesday, stroll independently through darknet marketplaces such as Agora and Alpha Bay, and randomly order items to the gallery that would host the bot's current show.

The spectrum of items that were ordered over the course of the first show ranged from fake *Nike Air Yeezy 2* sneakers, to a fake utility bill by *British Gas* and a cook book covering French cuisine, to eventually illegal substances such as 10 ecstasy pills. The show was exhibited at Kunsthalle St. Gallen in Switzerland.

Due to the apparent legal implications, the public prosecutor of the Canton St. Gallen seized the whole exhibition and the bot itself, one day after the finissage, upon which he was faced with a tough question: Who is responsible for ordering illegal substances? Is it !Mediengruppe Bitnik who wrote the code in the first place, even though they neither chose the illegal products nor executed the order? Was the gallery guilty of aiding and abetting the potentially criminal act by accepting the package with the illegal content? Or is it the bot, a piece of code, that ordered autonomously a pack of ecstasy pills out of thousands of illegal and legal products?

"We as well as the Random Darknet Shopper have been cleared of all charges. This is a great day for the bot, for us and for freedom of art!" - !Mediengruppe Bitnik[8]

While !Mediengruppe Bitnik's Random Darknet Shopper inhabited galleries and ploughed through the darknet, terra0 Research is "exploring the creation of hybrid ecosystems in the technosphere" (Seidler et al. 2016). As their debut, they launched terra0, "a scalable framework built on the Ethereum network that provides automated resilience systems for ecosystems". Terra0 is a self-owned forest that autonomously sells licenses to log trees through smart contracts. Hence, the forest gains the ability to accumulate capital which allows it to purchase more land and expand according to certain programmed rules.

"We can program it to make a little bit of profit, so it's got some money for a rainy day, but not excessive amounts. We can make it the most moral, socially minded capitalist possible" (Hearn 2015).

Conclusions

In this article, we intended to explore the concept of personhood in its various forms. We've argued that legal entities are always dependent on human agents to form and execute their will, while some digital entities - such as smart contracts on a distributed network as well as complex AI algorithms - are not. By comparing these distinctive features of legal and digital entities, we made the case for expanding personhood to digital entities which show a sufficient degree of autonomy. Using concrete examples, we've then shown the independence of software and physical embodiment and painted a picture of possible future developments.

In light of the above, we – as a society – need to engage with the fundamental question: What happens when technology becomes autonomous and therefore rises from the ranks of being a mere tool to being a peer interacting on par with us humans?

The conjunction of advancements in artificial intelligence and distributed networks will eventually lead to technology acting autonomously. Referring to Kant's definition of personhood, technology will gain accountability through its autonomous actions. It seems that our legal frameworks are not there yet, where technology is heading. Therefore, we need to adapt our understanding of which entities can and cannot possess personhood.

In the future, we will face digital entities in our everyday lives which act autonomously on a transnational, distributed network and might only temporarily need or even fully avoid a physical manifestation. They will manage funds, pay humans for labour, possess objects and, if needed, create additional entities. So far, law enforcement has ignored these digital entities' existence and tried to get to the natural persons "behind", in the case of DAOs, the token holders, the miners or the developers. This was the case with the SEC's DAO report considering the curators as the securities promoters, as well as with some legal scholar's assertion that the DAO itself was to be treated as a general partnership with every natural or legal person participating being jointly and severally liable for the incurred damages (Palley 2016; Reyes 2017).

However, simply looking through these entities to find responsible natural persons by "piercing the digital veil", so to say, will prove to be increasingly insufficient with the ever-growing level of autonomy these digital entities reach. In order for the legal system to properly function, we need accountability of autonomous agents. It is therefore only consequential to demand the introduction of digital personhood.

"We should reject carbon-chauvinism and the common view that our intelligent machines will always be our unconscious slaves" (Tegmark 2017b).

---

1 One may even ask whether it actually lies within our competence to make such a conscious expansion. In the end, the normative power of the de facto may inevitably do so as digital persons become ubiquitous in our daily lives.

2 Citizens United v. Federal Election Commission, 558 U.S. 310 (2010); BGE 95 II 481, E.4.

3 Defining the process of "forming one's own will" is definitely an important step in assessing autonomy. However, this discussion would go beyond the scope of this text and shall be done in a following post.

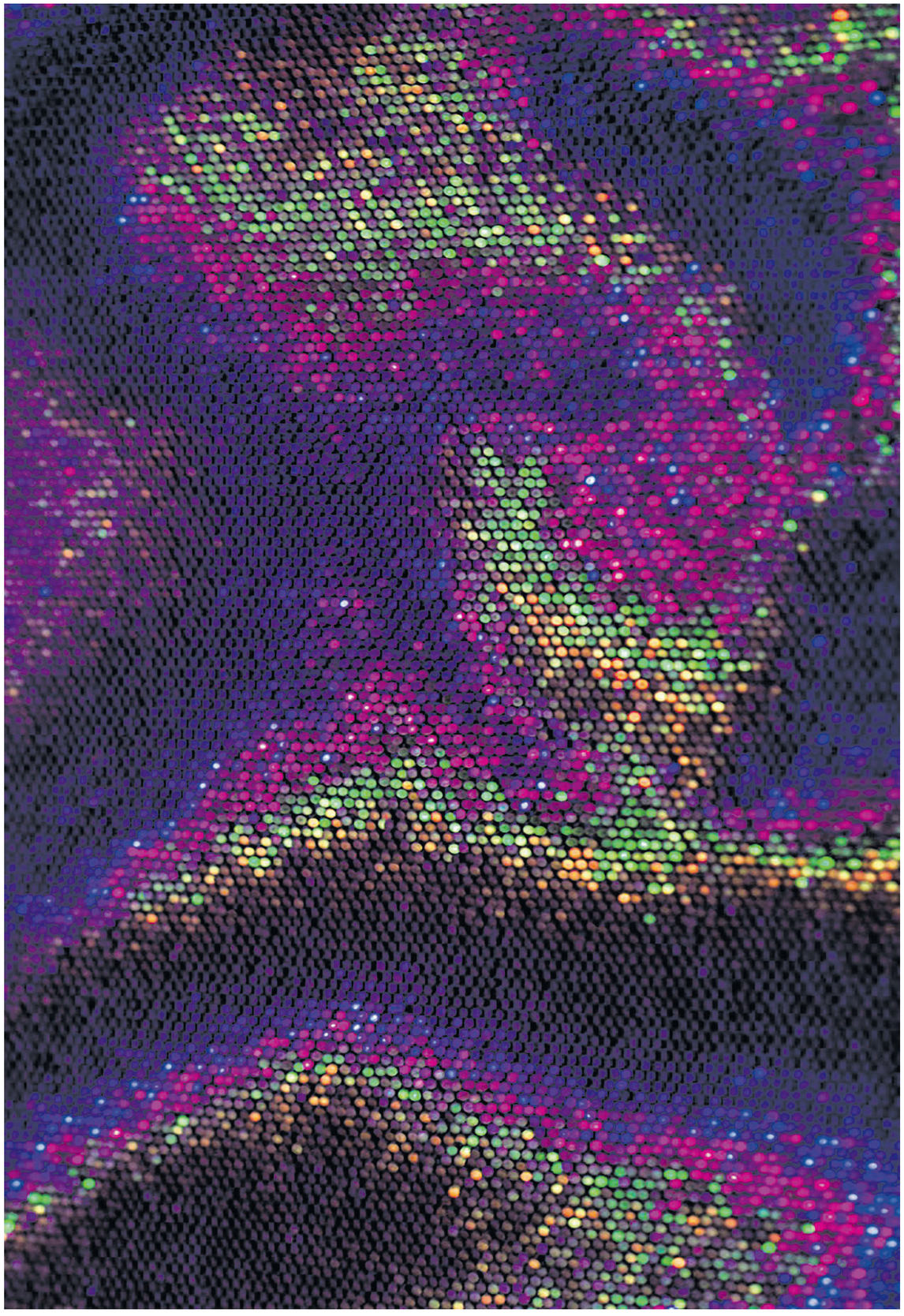
4 http://okhaos.com/plantoids/

5 A distinction made as early as 2011 in the bitcointalk.org forums by user gmaxwell and picked up again by Berlin-based research group terra0.

6 http://plantoid.org

7 We use the word "currently" to leave room for future body-independent mani festations of the human mind as proposed by e.g. Ray Kurzweil in regard to "brain uploads". [7]

8 https://wwwwwwwwwwwwwwwwwwww.bitnik.org/r/2015-04-15-random-darknet-shopper-free/



PARALELNÍ POLIS

An Interview with Jan Hubik

MATTHIAS TARASIEWICZ &
ANDREW NEWMAN

Andrew Newman and Matthias Tarasiewicz spoke with Jan Hubík in the lead up to the Hackers Congress Paralelní Polis in Prague. Hubík started to be deeply interested in cryptocurrencies in 2013 and soon became active in Paralelní Polis, a state-free think tank and hackerspace focused on the topics of decentralisation, digital privacy and anonymity. He currently represents the Institute of Cryptoanarchy as a supervisory board member of Paralelní Polis.

MT: Jan, can you tell us how Paralelní Polis came to be?

JH: Paralelní Polis was founded by members of the contemporary art group Ztohoven. The art group did various projects in the past focusing on problems with the government and the loss of freedom. One project they did was unusual for them because it involved hacking; they hacked into live television and broadcast a nuclear explosion. With this act they wanted to point out that people shouldn't believe anything they see on television. This led to the group gaining the attention of the hacker community, so they were invited to a hacker conference where they met with a few interesting people who told them about cryptocurrencies and encryption. They realised that it's really interesting stuff and people should know about it. So, together with the hacker community, they decided to found this building in Prague which would be a hackerspace for people to come develop these technologies and get to know about them.

After they found a space, they decided to make it really big, so they rented out a four floor building where we now have the *Bitcoin Coffee* cafe on the ground floor, a co-working space *Paper Hub* on the first floor, the *Institute for Cryptoanarchy* on the top floor, and in the basement we have a hackerspace called CryptoLAB.

All the floors have different purposes in Paralelní Polis. The *Bitcoin Coffee* cafe on the ground floor acts like a reception. It's the first area that you go in when you enter our building, and its purpose is to give people their first physical experience with using cryptocurrencies. They can exchange fiat money for cryptocurrencies and buy a coffee. Someone is always there to help them and teach them how to do it. On the first floor, it's a space for the the startup scene and for people who develop crypto technologies; not all of them, but lots of them. In the institute on the top floor, we do various workshops, meet-ups, and create educational content. The institute also does the Hackers Congress which was the event used for opening the Paralelní Polis in 2014. It became an annual thing for us, like a birthday party. It has grown since to be an internationally recognised event with international speakers and it's three days of lots of lectures, workshops and so on.

MT: What was the intention of the organisation to name itself after the concept from Vaclav Benda, and how does it interrelate with cryptoanarchy?

JH: The name Paralelní Polis comes from the essay from Vaclav Benda, who was a dissident in the Czech Republic. The essay basically states that it doesn't make sense to fight with the government, because it has unlimited resources and it's a waste of energy. So instead it is much better to focus on building a parallel society and parallel social structures, like parallel culture, parallel education, parallel news networks and so on. Eventually if the parallel social structures prove to be better than what the government provides, they will already be there to replace the government social structures. We combined this idea with the *Crypto Anarchist Manifesto* from Timothy May who was writing about how crypto technologies will shape the future of society, and how we will be able to use encryption and anonymisation techniques to do whatever we want in perfect secrecy. If you combine these two ideas, from Benda and May, you discover that by using these technologies, you can build a perfect version of Paralelní Polis. So, that's what we decided to do. We decided to use this name to promote crypto technologies, and to build a whole non-profit organisation around it and focus on educating the public on how to use these technologies to increase their personal freedom.

> **… focus on building a parallel society and parallel social structures, like parallel culture, parallel education, parallel news networks.**

MT: If you look back to the 1970s when all these types of technologies and specific cryptography were first made available, for instance RSA encryption, we saw then the emergence of the crypto wars, where governments sought

to limit the public availability of these technologies. This of course led to the cypherpunks and the publication of the *Crypto Anarchist Manifesto* and the *Cypherpunk Manifesto* in the 90s. How do you think cryptoanarchy has changed since then, and what does it mean for you now?

JH: Cypherpunk is deeply rooted in our movement, and we definitely expand on very similar values. In the 70s, 80s and 90s, what the cypherpunks were writing about and working on was a bit about the future, and at that time, Timothy May predicted what could be possible. Nowadays, we are in a very different situation because most of the stuff that he predicted is already available. Especially, for example, digital currencies, which didn't exist at that time. Now we are able to not only communicate privately using encryption, but we also can transfer value over the internet. So nowadays, we can actually use the technologies in practice instead of just dreaming about how they will shape the society of the future.

MT: At the same time, the crypto wars still continue, and there still are attempts to prevent or control the use of specific encryption methods and technologies and to intercept communication. Where do you see the battlefield these days?

JH: Well, today we have really strong encryption available as open source software and once it is out, you cannot take it back. So nowadays it's really hard to change the direction of this technology. The state even helps this movement because they realise that if they are the only ones using certain technologies, everyone will be able to recognise them. So for example, Tor is a government project and it's open source and publicly available because the US military needs to use it and needs to get lost in the traffic of ordinary people around the world. So, definitely the way governments handle encryption and these technologies has changed, but what has also changed are the means that are available to them. There have been some changes, for example governments nowadays try to create new legislation that forces people to reveal their private keys for encryption. Unless you reveal these private keys, you could go to jail. This is really difficult to enforce, and I don't know how much it works in practice. Fortunately, in the Czech Republic I don't think we have any law like this. So, if you have something encrypted, you are not obliged to reveal the encryption keys.

AN: This was just recently being introduced in New Zealand where you have to provide your private keys if they ask you for it or you are threatened with a fine. But with the concept of Paralelní Polis, if you're creating a parallel society rather than fighting the state, obviously these sorts of conflicts will appear. You can't ignore the state. How do you see Paralelní Polis operating at this level, when laws like these are introduced? For instance, the European Union's movement towards outlawing the use of specific privacy technologies in cryptocurrencies.

JH: I don't think they can do anything about it because it's already out there and people can reliably use it in secret. So the regulation can exist in theory, but the effectiveness of such regulations will probably not be good enough. You have countries in the world where these technologies are forbidden and people still use them because they are useful. You have, for example, people in Venezuela using cryptocurrencies to buy stuff and protect themselves against inflation, people in Iran using Tor to access uncensored information and people in China using these technologies to avoid internet censorship, take capital out of the country and so on. So in theory, the European Union, or any government in the world, can create new regulations which ban crypto technologies, but their effectiveness will be very limited.

> **Eventually if the parallel social structures prove to be better than what the government provides, they will already be there to replace the government social structures**

AN: You mentioned that you can effectively use these technologies in secret, but how can, for instance, your organisation, because you're drawing a lot of attention to the fact that you're using these technologies, use these technologies 'in secret'. Does your organisation feel any unwanted attention because you're evangelising for the use of these crypto technologies?

JH: We are openly opposing some of the stupid laws that the governments create. For example, in the Czech Republic we have this law, in English it would be called something like "electronic evidence of sales", where businesses need to send information about every sale to the government. It's because of taxation, they want to have an audit trail so they can check if you reported all of your earnings. We openly opposed this law and decided not to implement this

electronic evidence of sales in our building because it's against our ideals for privacy, and so far nothing has happened to us. But we always consider this an option, that the government will turn against us and try to destroy our organisation. The physical place here in Prague is just a shell where we can meet and discuss this stuff, and if in the future this place has to be abandoned, we can always move online and do these things in secret. Or we can move to a different country, a different place, and so on. So the activities that we do obviously catch attention from the government, but that's something that we count on and we don't think that it's a problem.

MT: I'm wondering, since you relate to these cryptoanarchy ideas, and I see a lot of issues with this original idea of cryptoanarchy because of ethical boundaries, like in the cryptoanarchist manifesto there are these issues coming up with assassination markets and that sort of thing. Also all the problems that come up with free information flow and free availability to buy and transfer any good. How do you deal with these kinds of issues? Do you have an ethical boundary defined in the organisational statement? Or is it a kind of self-governing process?

JH: In respect to the ethical problems of cryptoanarchy, we need to recognise that these technologies are available, and they are tools like any other. People will use them to do good, and people will use them to do bad. By restricting the usage of these technologies, you are probably not going to influence the bad people, because only the good people will respect these restrictions. So we don't think it's effective to limit usage of these technologies. It's important to acknowledge that people can use it for bad stuff, but it's better to come up with ideas how to fight these things rather than restricting the tool. It's not the fault of the tool, it's the fault of the people who do this stuff. In our organisation, we definitely don't want to hurt anyone, we respect private property, and we stand on voluntary principles, which means that we don't want to force anyone into anything given that our organisation is very much dependent on voluntary work and voluntary contributions. So our ethical principles are, I would say, very strong, but that doesn't mean that everyone will respect these principles.

MT: Do you think that the name of your organisation and the relationship to the concept of Paralelní Polis and its political history gives you an additional layer of security in the Czech Republic?

JH: That's hard to say, but I don't think that it's something that would stop the government from doing something. This term is deeply related to the Czech Republic, but people from other countries also understand it and it's easy for them to get it, to understand what we want to do. We are in the process of opening more Paralelní Polis around the world. For example, recently we opened a new Paralelní Polis in Slovakia and we have people in Romania who are also interested in running a place based on very similar principles. There is a huge movement around the world of people who want to do the same, so it's a universal concept.

> **The physical place here in Prague is just a shell where we can meet and discuss this stuff, and if in the future this place has to be abandoned, we can always move online and do these things in secret.**

MT: There is critique that Bitcoin, as a medium of value transfer, doesn't fulfil the original ideas of cryptoanarchy. Privacy-oriented cryptocurrencies, like Monero, are said to have different values, and so we have this distinction already between Bitcoin maximalists and Monero maximalists. Would you say that any technological properties would be able to fulfil the ideals of cryptoanarchy?

JH: First of all, Paralelní Polis is not built on any single technology. We don't only accept Bitcoin, we also accept Litecoin, Monero and Dash. We experiment with different technologies all the time. What people need to understand is that these technologies are very young. Bitcoin has been here for nine years, it's only a little baby. Things move really fast-forward, but maybe not as fast as some people expect. I think that a lot of issues will be solved eventually. Even the privacy problems with Bitcoin will eventually get much better. I don't know if Monero is the future of cryptocurrency or if it's Bitcoin or if it's something else, but what we strive for is to educate people about these technologies in general. They need to know these technologies exist and how they can use them. Only then will they know what benefits they can get from using them. If we succeed in this, it doesn't matter which of these technologies they use because, because as I said, it's just a tool. What matters is how they use it.

REFERENCES

FORK THE INSTITUTIONS

Berechet, Lucian Daniel, and Istrimschi, Petru Adrian. 2014. *Education Reboot: Reinventing the University.* Procedia - Social and Behavioral Sciences. Vol.142: 755-761.

Bernstein, Ethan, John Bunch J, Niko Canner, and Michael Lee. 2016. *Beyond the Holacracy Hype.* Harvard Business Review, July-August 2016.

Blin, Francoise and Morag Munro. 2008. *Why hasn't technology disrupted academics' teaching practices? Understanding resistance to change through the lens of activity theory.* Computers and Education, Vol.50: 475-490.

Bower, Joseph, Clayton M. Christensen. 1995. *Disruptive Technologies: Catching the Wave.* Harvard Business Review, January-February 1995: 43-53.

Buterin, Vitalik (2014). *An Introduction to Futarchy.*

Chaum, David. 1983. *Blind signatures for untraceable payments.* In *Advances in cryptology: Proceedings of CRYPTO 82*, D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), 199-203. New York: Plenum Press.

Chaum, David, Amos Fiat, Moni Naor. 1990 *Untraceable electronic cash.* Lecture Notes in *Computer Science: Proceedings on Advances in cryptology - CRYPTO '88.* Berlin: Springer,Vol.403: 319–327.

Christensen, Clayton M., Michael B. Horn, and Curtis Johnson. 2011. *Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns.* New York: McGraw Hill.

Cohen, Daniel J and Tom Scheinfeldt. 2013. *Hacking the Academy: New Approaches to Scholarship and Teaching from Digital Humanities.* Ann Arbor, MI: University of Michigan Press.

Cryptohustle. 2016. *5 reasons why the DAO bailout was bad for Ethereum.*

Dai, Wei. 1998. *B-Money.*

Davies, Sarah. 2017. *Hackerspaces: Making the Maker Movement.* Cambridge: Polity Press.

De Filippi, Primavera, and Samer Hassan. 2016. *Blockchain technology as regulatory technology: From code is law to law is code. First Monday,* Vol. 21, Number 12 - 5 December 2016.

De Filippi, Primavera, and Benjamin Loveluck. 2016. *The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review,* 5(3).

En.bitcoin.it. 2017. *Genesis Block.* Bitcoinwiki.

Ernst & Young. 2016. *Blockchain reaction: Tech plans for critical mass.* Report 2016.

Finney, Hal. 1993. *Detecting Double-Spending.*

Flavin, Michael. 2017. *Disruptive Technology Enhanced Learning - The Use and Misuse of Digital Technologies in Higher Education.* London: Palgrave Macmillan.

Ford, Bryan. 2002. *Delegative Democracy.*

Gardler, Ross, and Gabriel Hanganu. 2010. *Benevolent Dictator Governance Model.* OSS Watch.

Hanson, Robin. 2007. *Shall We Vote on Values, But Bet on Beliefs?.*

HCPP. 2018. *New Order or Next Order? Strategies of Facelessness in the Age of Privacy vs. Transparency.*

Hemetsberger, Andrea, and Christian Reinhardt. 2006. *Learning and Knowledge-building in Open-source Communities - A Social-experiential Approach. Management Learning. The Journal for Critical, Reflexive Scholarship on Organisation and Learning,* Vol. 37, Issue 2.

Iansiti, Marco, and Karim Lakhani. 2017. *The Truth About Blockchain. Harvard Business Review,* January-February 2017.

Johnson, Sandra L, Sean Rush, and Coopers & Lybrand LLP. 1995. *Reinventing the University: Managing and Financing Institutions of Higher Education.* New York: Wiley.

May, Timothy C. 1994. *Cyphernomicon.*

McCabe, Bret. 2013. *Publish or perish: Academic publishing confronts its digital future.*

Meatballwiki. 2010. RightToFork. Meatballwiki.com.

Medvinsky, Gennady, and Clifford Neuman. 1993. *NetCash: A design for practical electronic currency on the Internet.*

Metz, Cade. 2016. *The biggest crowdfunding project ever - The DAO - is kind of a mess. Wired.*

Nelson, Cary. 1997. *Will Teach For Food: Academic Labor in Crisis.* University of Minnesota Press.

Penny, Simon. 2008. *Bridging Two Cultures: Toward an Interdisciplinary History of the Artist-Inventor and the Machine-Artwork,* In *Artists as Inventors - Inventors as Artists,* Dieter Daniels and Barbara U. Schmidt (eds.), Ostfildern, Germany: Hatje Kantz Verlag, 2008: 55-69.

Reagle, Joseph M. 2005. *Trust in Electronic Markets - The Convergence of Cryptographers and Economists. First Monday* Special Issue #3: Internet banking, e-money, and Internet gift economies.

Robertson, Brian. 2015. *Holacracy: The New Management System for a Rapidly Changing World.* Holt and Co.

Satell, Greg. 2016. *These 4 Major Paradigm Shifts Will Transform The Future Of Technology.* Forbes Magazine.

Satell, Greg. 2013. *A New Age Of Disruption.* Digital Tonto.

Scheper-Hughes, Nancy. 2011. *The Crisis of the Public University.*

Scott, Brett. 2015. *The hacker hacked. aeon magazine.*

Suberg, William. 2017. *Cross-Crypto Market Cap Reaches New All-Time High Due to Altcoin Upheaval.*

Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy.* O'Reilly Media.

Szabo, Nick. 1997. *Formalising and securing relationships on public networks. First Monday,* 2(9).

Tarasiewicz, Matthias. 2011. In *Coded Cultures Between New Media Arts and Production Cultures. Coded Cultures: New Creative Practices out of Diversity.* Vienna/NY: Edition Angewandte and Edition Transfer.

Tarasiewicz, Matthias, and Andrew Newman. 2013. *Experimental cultures and epistemic spaces in artistic research. Proceedings of the 19th International Symposium on Electronic Art,* ISEA2013, Sydney: ISEA International, Australian Network for Art & Technology, University of Sydney.

Tarasiewicz, Matthias, and Andrew Newman. 2015. *Cryptocurrencies as distributed community experiments. Handbook of Digital Currency.* Singapore: Elsevier.

Tomaino, Nick. 2017. *The Governance of Blockchains.*

Wagner, Sophie, Andrew Newman, and Matthias Tarasiewicz. 2015. *Epistemic practices in arts And technology. Journal for Research Cultures,* Issue 1. Vienna: RIAT

Widrum, Aaron. 2016. *Rejecting Today's Hard Fork, the Ethereum Classic Project Continues on the Original Chain: Here's Why.* In: *Bitcoin Magazine.*

Wuschitz, Stefanie, Sophie Wagner, Andrew Newman, and Matthias Tarasiewicz, [Eds.]. 2016. *Openism: Conversations in Open Hardware.* Vienna: University of Applied Arts.

Zamfir, Vlad. 2014. *Towards a general theory of cryptoeconomics. Talk at the Centre Of Mathematical Sciences,* University Of Cambridge.

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop It.* New Haven & London: Yale University Press.

SEIZE YOUR RIGHTS WITH THE FORCE OF CRYPTOGRAPHY

Dreamer, Frank. 2015. *SSL and TLS Explained.*

Emmons, Dan. 2018. Build a Legacy. *Tune out the Price Wars. #BUIDL.*

Levy, Steven. 1993. Crypto Rebels.

McKie, Steven. 2015. *The Blockchain Meets Big Data and Realtime Analysis.*

Minichiello, Nicola. 2015. *The Bitcoin Big Bang: Tracking Tainted Bitcoins.*

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Reddit. 2014. *What's HODL?.*

Reddit. 2017. *Reminder: Segwit Breaks Fungibility. After a Segwit, There Are Coins Tainted By Segwit, and Untainted Coins.*

Steward, Damian, Matthias Tarasiewicz, and Max Gurresch. 2010. *Bitcoincloud.*

Tarasiewicz, Matthias, and Andrew Newman. 2015. *Cryptocurrencies as distributed community experiments. Handbook of Digital Currency.* Singapore: Elsevier.

Unknown Author. 1999. *How DigiCash Blew Everything.* Translated by The Dutch Natives.

DISASSEMBLING THE TRUTH MACHINE

Barad, Karen. 2007. *Meeting the Universe Halfway: Quantum physics and the entangle-ment of matter and meaning*. Durham and London: Duke University Press.

De Filippi, Primavera, and Aaron Wright. 2015. *Decentralised Blockchain Technology and the Rise of Lex Cryptographia*.

Galloway, Alexander R. 2004. *Protocol, How Control Exists After Decentralisation* Cambridge and London: MIT Press

Jentzsch, Christoph. 2016. *Decentralised Autonomous Organisation to Automate Governance*: 1–31.

Merkle, Ralph Charles. 1979. *Secrecy, Authentication, and Public Key Systems*. Stanford: Information Systems Laboratory.

Preneel, Bart. 2010. *The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition*. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): 1–14. 5985 LNCS.

Wood, Gavin. 2014. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Homestead Draft.

RULES ENFORCED BY CRYPTOGRAPHY

Bitcoinwiki. 2017. *Proof of Stake*.

Ethereum:GitHub. 2018. *Sharding FAQ*.

Stark, Josh. 2017. *Making Sense of Cryptoeconomics*. Medium.com.

Poon, Joseph, and Vitalik Buterin. 2017. *Plasma: Scalable Autonomous Smart Contracts*.

Teutsch, Jason, and Christian Reitwießner. 2017. *A scalable verification solution for blockchains*.

HOW TO TALK ABOUT SERIOUS MATTERS OF COMPLEXITY WITH MODELS AS AGENTS

Adamatzky, Andrew, and Georgios Ch. Sirakoulis. 2015. *Building Exploration with Leeches Hirudo Verbana* In *Biosystems* 134 (Aug 2015): 48–55.

Ashby, William Ross. 1956. *An Introduction to Cybernetics*. New York: John Wiley & Sons.

Barad, Karen. 1998. *Getting Real: Technoscientific Practices and the Materialisation of Reality* In *Differences: A Journal of Feminist Cultural Studies* 10.2 (1998): 87-128.

Barad, Karen. 2007. *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Durham: Duke University Press.

Barrow-Green, June. 1996. *Poincare and the Three Body Problem*, annotated edition. Providence, RI : London: Oxford University Press.

Berge, Erling, and Frank van Laerhoven. 2011. *Governing the Commons for Two Decades: A Complex Story* In *International Journal of the Commons* 5, no. 2.

Care, Charles. 2010. *Technology for Modelling. Electrical Analogies, Engineering Practice, and the Development of Analogue Computing (History of Computing)*. London: Springer.

Castillo, Daniel, and Ali Kerem Saysel. 2005. *Simulation of Common Pool Resource Field Experiments: A Behavioral Model of Collective Action*. In *Ecological Economics* 55, no. 3 (Nov 15, 2005): 420-436.

Edmonds, Bruce, and Carlos Gershenson. 2015. *Modelling Complexity for Policy: Opportunities and Challenges* in *Handbook on Complexity and Public Policy*, ed. Robert Geyer and Paul Cairney (Cheltenham: Edward Elgar, 2015): 205–20.

Glanville, Ranulph. 1999. *Researching design and designing research*. In *Design Issues* 15, No. 2, 1999: 80–91.

Haraway, Donna J. 1992. *The Promises of Monsters: A Regenerative Politics for Inappropriate/d Others* in *Cultural Studies*, ed. Lawrence Grossberg, Cary Nelson, and Paula A. Treichler, NY: Routledge

Hardin, Garrett. 1968. *The Tragedy of the Commons*, Science 162, no. 3859 (December 13, 1968): 1243-1248.

Hayles, Katherine. 1999. *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. University of Chicago Press.

Johnston, John. 2008. *The Allure of Machinic Life. Cybernetics, Artificial Life, and the New AI*. Cambridge, MA: MIT Press.

Latour, Bruno. 2004. *Why Has Critique Run out of Steam? From Matters of Fact to Matters of Concern* In *Critical Inquiry* 30, no. 2 (Jan 1, 2004): 225-248.

Mindell, David. 2002. *Between Human and Machine: Feedback, Control, and Computing before Cybernetics*. Baltimore. Johns Hopkins University Press.

Mitchell, Melanie. 2009. *Complexity. A Guided Tour*. Oxford/New York: Oxford University Press.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*. New York: Cambridge University Press.

Parikka, Jussi. 2013. *Afterword: Cultural Techniques and Media Studies Theory, Culture & Society* 30, no. 6 (Nov 1, 2013): 147–59.

Pickering, Andrew. 2011. *The Cybernetic Brain*. Chicago: University of Chicago Press.

Schuller Bjorn W. et al. 2013. *Serious Gaming for Behavior Change: The State of Play*, IEEE Pervasive Computing: 48-55.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

Wiener, Norbert. 1948. *Cybernetics: Or, Control & Communication in the Animal and the Machine*. New York: John Wiley & Sons, Inc. Paris: Hermann et cie.

Wilson, James et al. 1994. *Chaos, Complexity and Community Management of Fisheries*, Marine Policy 18, no. 4 (July 1, 1994):

Wood, David, and Robert Bernasconi, eds. 1988. *Derrida and Différance*. Evanston: Northwestern University Press.

CRYPTOECONOMICS AND EXPERIMENTS IN TOKEN SALES

Bentov, Iddo et al. 2014. *Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake*

Buterin, Vitalik. 2014. *An Introduction To Futarchy*.

Buterin, Vitalik, and Virgil Griffith. 2017. *Casper the Friendly Finality Gadget*.

Ethereum Wiki. 2018. *Sharding FAQs*.

Hanson, Robin. 2000. *Shall We Vote on Values, But Bet on Beliefs?* George Mason University.

Raiden Network - Medium Page. 2017. *The Raiden Network Token Auction Explained*.

Teutsch, Jason, Vitalik Buterin, and Christopher Brown. 2017. *Interactive Coin Offerings*

THE ADVENT OF DIGITAL PERSONS

Harari, Yuval Noah. 2015. *Homo Deus: A History of Tomorrow*. NY: Harper.

Hearn, Mike, quoted in the article, Leo Kelion: *Could driverless cars own themselves*, 16.02.2015.

Savigny, Karl Friedrich von. 1840. *System des heutigen Römischen Rechts*. Berlin: Veit.

Palley, Stephen D. 2016. *How to Sue a Decentralised Autonomous Organisation*, Coindesk (Mar. 20, 2016).

Reyes, Carla R. 2017. *If Rockefeller were a Coder*.

Seidler, Paul, Paul Kolling, and Max Hampshire. 2016. *Terra0: Can an augmented forest own and utilise itself?*. Berlin University of Arts.

Tegemark, Max. 2017a. *Life 3.0: Being Human in the Age of Artificial Intelligence*. London: Penguin Books Ltd.

Tegemark, Max. 2017b. *What Scientific Term or Concept ought to be more widely known?*. In: *edge*.

PARALELNÍ POLIS

Ztohoven. 2017. *Ztohoven*. http://www.ztohoven.com/.

Benda, Vaclav et al. 1988. *Parallel Polis, or An Independent Society in Central and Eastern Europe: An Inquiry*. The Johns Hopkins University Press, Social Research, Vol. 55, nos. 1-2

May, Timothy C. 1992. *The Crypto Anarchist Manifesto*. Emailed 22 Nov., 1992, 12:11:24 PST.

Rivest, R.; Shamir, A.; Adleman, L. 1978. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM*

Schulze, Matthias. 2016. *Crypto Wars: The old song for 40 years*. In *Tresorite Blog* . Nov. 30, 2016.

Hughes, Eric. 1993. *A Cypherpunk's Manifesto*. Emailed Mar. 9, 1993.

Soesanto, Stefan. 2018. *No Middle Ground: Moving on From the Crypto Wars*. The European Council on Foreign Relations, Policy Brief, Jul. 5, 2018.

IMPRINT

Future Cryptoeconomics
Quarterly magazine about the future of decentralisation.
www.cryptoeconomics.at

RIAT
Neubaugasse 64-66/III/4
1070 Vienna, Austria
future@riat.at
www.riat.ac.at

Editors for Issue 1
Matthias Tarasiewicz
Andrew Newman

Contributors
Jaya Klara Brekke
Shintaro Miyazaki
Daniel Pichler
Ozan Polat
Benedikt Schuppli
Markus Zimmermann

Interviewees
Andreas Antonopoulos
Josh Stark
Vitalik Buterin
Jan Hubik

Support
Aleksandar Vrglevski
Timo Michail

Layout & Design
Bahadir Arslan

Photography & Illustration
Christopher Villafuerte
Tobias Faisst
Max Gurresch
Clara Dunklee

Cover Logo Concept
Christoph Schörkhuber

RIAT is an institute for research, development, communication and education in the fields of cryptoeconomics and the blockchain. We work with experimental artistic technology and open hardware. We explore and actively stress-test the role of research and development in the age of zero-trust, through novel forms of presentation, discussion and publication. Examining the global cryptoeconomic condition and its effects on culture and society, we foster an open and interdisciplinary discourse to improve crypto-literacy for the society of tomorrow and foster the adoption of cryptography and privacy technologies across disciplines.

RIAT is an independent non-profit institute operating since 2012 with its main headquarters in Vienna, Austria and a large international network around the globe. RIAT consists of a network of researchers, developers, entrepreneurs and experimentalists working on conceptioning, research design, project development and mentoring on future topics of decentralisation.

Editorial © 2018 by RIAT. Text is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. creativecommons.org/licenses/by-nc-sa/4.0/

Fork the Institutions © 2018 by Matthias Tarasiewicz. Text is licensed under a Creative Commons Attribution 4.0 International License. creativecommons.org/licenses/by/4.0/

Seize your Rights with the Force of Crypto © 2018 by RIAT. Text is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. Photos © 2018 by Max Gurresch.

Disassembling The Truth Machine was first published in META. Tracing Unknown Knowns. meta-id.info Text © 2018 by Jaya Klara Brekke. Photo © 2018 by Jaya Klara Brekke.

Rules Enforced by Cryptography © 2018 by RIAT. Text is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. creativecommons.org/licenses/by-nc-sa/4.0/. Photos © 2018 by Chris J. Villafuerte awkwardtree.com

How to Talk about Serious Matters of Complexity with Models as Agents was first published by RIAT in the Journal for Research Cultures. researchcultures.com. Text © 2016 by Shintaro Miyazaki. Text is licensed under a Creative Commons Attribution 4.0 International License. creativecommons.org/licenses/by/4.0/. Illustration © 2018 by Clara Dunklee claaara.com

Cryptoeconomics and Experiments in Token Sales. © 2018 by RIAT. Text is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. Photos © 2018 by Chris J. Villafuerte awkwardtree.com

The Advent of Digital Persons © 2018 by Ozan Polat and Benedikt Schuppli. Text is licensed under a Creative Commons Attribution 4.0 International License. creativecommons.org/licenses/by/4.0/. Photo EIDOS © 2016 by Tobias Faisst tobiasfaisst.com

Paralelní Polis © 2018 by RIAT. Text is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. creativecommons.org/licenses/by-nc-sa/4.0/
Photos © 2018 by Paralelní Polis

For further Imprint visit: riat.at/future-imprint/

All contents © by the respective authors except stated differently.

ISSN 2617-6289