Trusting the Math and Mistrusting Humans

How Politically Sensitized Engineers of Cryptographic Systems Cope with Ontological Insecurity in the Digitally Augmented Life-World

Nicolai Ruh

> While I pray that public awareness and debate will lead to reform, bear in mind that the policies of men change in time, and even the Constitution is subverted when the appetites of power demand it. In words from history: Let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography.
> Edward Snowden (cited by Greenwald 2014: 24)

Politically aware designers and implementers of cryptographic systems conceive of the internet as the 'nervous system of the 21st century', one that permeates virtually all aspects of the social fabric.[1] This diversified community is united by a shared epistemic perspective on the digitally augmented life-world. This specific approach to the world is informed by their expert knowledge about the internet's technological foundation principles. These constitutive conditions that underlie digitally mediated social relationships are invisible for the common internet user. It is this exclusive knowledge within the tech-community that leads to a collectively shared awareness of trust problems that are idiosyncratic for the way information is being (re-)produced and distributed in a network environment. This chapter pursues the goal of providing new insights into the social functions of mistrust as well as into its relationship with the phenomenon of trust. The chosen field of research is of specific interest

1 | The analogy of the internet being the nervous system of the 21st century was formulated by Cory Doctorow in his article 'The internet is the answer to all the questions of our time'. See: https://www.theguardian.com/technology/2015/jun/15/internet-answer-questions-of-our-time

in this regard, since the builders of cryptographic systems pursue their goal of solving trust problems within the context of a fundamentally mistrustful communication environment. As it turns out, trust and mistrust fulfil interrelated functions in this field. I argue that developers and implementers of cryptographic systems do not fully suspend trust, but source out specific elements of nescience to the sphere of mathematics. My thesis is that by doing so, they create an isolated domain of calculability and provability that allows them to cope with the complexities and fundamental insecurities of an increasingly digitally organized life-world.

The goal of modern cryptographic protocols is to allow communicating parties to communicate securely over a fundamentally insecure channel. Cryptographic protocols therefore make sure that no third party ('man-in-the-middle') has the ability to either impersonate itself as a trusted end-point (reflecting the concept of 'authenticity'), manipulate the data from one point of the communication channel to the other (the concept of 'integrity'), or record the data in transit (the concept of 'confidentiality') (Schneier 2000: 85). The security of asymmetric cryptographic systems rests on the (yet unproven) assumption that mathematical problems exist that are computationally unfeasibly to solve, even for the most sophisticated and technically best equipped attacker (which today most likely is the NSA). The exchange of private keys over an insecure channel (public key cryptography) and the employment of digital signatures to ensure the authenticity and integrity of the communication rest on two assumptions. Firstly, that it is easy for the communication parties to compute a mathematical calculation in one direction and, secondly, that it is computationally infeasible for an attacker knowing the result of the calculation to redo the calculation process in order to break the encryption. System designers develop cryptographic protocols against the assumption of an omnipresent 'man-in-the-middle' who is trying to intercept and manipulate information on its way from sender to receiver (Schneier 2000 ibid). It is this generalized mistrust in the sense of an awareness of the omnipresent potential for an internet user's experience to be manipulated by unknown third parties on the invisible and intangible technical layer that developers of cryptographic tools take as a starting point for the conceptualization of trust models based on the assumed hardness of specific mathematical problems.[2]

In the following, I will examine how politically sensitized developers and implementers of cryptographic tools cope with what I term ontological insecurity. Drawing on the concept of 'ontological security' (Giddens 1990), I will

2 | This generalized mistrust also finds its expression in cryptographers' terminology for anticipated adversaries: 'Eve' stands for any possible eavesdropper and 'Mallory' for any malicious entity which is trying to forge the content of information or to impose itself as a communicating endpoint (see Schneier 2000: 85).

develop the concept of ontological insecurity in order to describe the specific epistemology of the analysed actors towards trust relationships in the digitally augmented life-world. What is revealed is that this way of approaching trust is characterized by a fundamental questioning of the givenness of specific pre-conditions for trust relationships. These problems only become visible underneath the level of the actual communication experience – the level of the networks and protocols that make up the internet.

From a Sociology of Knowledge perspective, I will show that generalized mistrust has a constitutive function for establishing reliability in a life-world that is increasingly inhabited by a multitude of unknown actors with opaque interests. Cryptographic systems are a reaction towards a social environment that is increasingly pervaded by fundamental insecurities and characterized by a lack of acquaintance of its inhabitants with regards to its underlying trust conditions. It will become clear that from the perspective of politically sensitized system developers, the reliance on mathematical assumptions constitutes the last remaining trust anchor for a new social contract that is implied in the introductory quote by Edward Snowden.[3] Snowden's epigraph points to a fundamental erosion of trust assumptions towards human institutions. I will point out that this fundamental mistrust goes as deep as to the ontological layer of our epistemic approach to the world that is increasingly structured by digital technologies. Snowden's urge for a new social contract based on cryptography implies that mathematics contains within itself specific qualities that allow cryptographers to replace trust in human institutions with systems that regulate social behaviour in an unambiguous and tamper-proof manner.

This chapter is structured in the following way: After a brief portrayal of the community of politically sensitized engineers of cryptographic systems, I will contextualize their epistemic perspective of ontological insecurity in the context of the specific characteristics of the digitally augmented life-world. I will then discuss relevant literature on trust and mistrust. Subsequently, I will critically discuss these concepts in their relation to the characteristics of the digitally mediated life-world. Based on these theoretical considerations, I will delineate the approach of generalized mistrust as a strategy of engineers of cryptographic systems to cope with the problem of ontological insecurity and the associated lack of acquaintance with regards to the trust modalities in this new social sphere. In the final part, I will briefly outline a worldview within which mathematics and the associated ideas of transparency and provability be-

3 | In this quote Snowden paraphrases a statement by Thomas Jefferson. Jefferson's original quote goes as follows: 'In questions of power, then, let no more be said of confidence in man, but bind him down from mischief by the chains of the Constitution.' This statement is part to the Kentucky Resolution from 1798.

come the cornerstones of a post-social contract that locates the feasibility of social principles in a sphere beyond the social realm (Knorr Cetina 2001, 2007).

The Community of Politically Sensitized Engineers of Cryptographic Systems

When I talk about the community of politically sensitized engineers of cryptographic systems, I am referring to a highly diversified network of people and institutions. This community is comprised of complex expert systems that include cryptographers from the field of applied mathematics, system developers, coders, and hackers. These technically versed experts work on different parts of cryptographic systems. Mathematicians develop cryptographic primitives that encompass mathematical problems, which build the foundations of cryptographic protocols. Cryptographers develop the protocols that specify the modalities in which communication between parties takes place. System developers draft the applications in which the protocols are embedded and implementers write the code that transfers these concepts into running software. The boundaries between the areas of responsibility are fluent in practice. Many of these experts work on different aspects of cryptographic systems and have a broad understanding of the underlying problems. However, what became apparent during my research was the existence of experts in each of these specific domains whose expertise is decision-relevant for the other community members. This is due to the complexity of the field and the diverse professional knowledge that flows into the design and implementation of cryptographic systems.

Coming from a qualitative research perspective, I approached the field openly following the snowball principle in arranging interviews. I entered the field by looking at two organizations: the Chaos Computer Club (CCC) in Germany and the Electronic Frontier Foundation (EFF) in San Francisco. Berlin and San Francisco turned out to be two hot spots of tech-activism with strong networks among the respective communities. The CCC is Europe's largest association of hackers and, according to the club's website, it offers 'information about technical and societal issues, such as surveillance, privacy, freedom of information, hacktivism, data security and many other interesting things around technology and hacking issues'.[4] Attending the Chaos Communication Congress in Hamburg in 2014, as well as attending other conferences, provided me with new insights into the existence of strong networks between the CCC and various other projects and organizations like the Tor Project[5], the Free Software

4 | This quote is taken from the club's English website, see: https://ccc.de/en/

5 | Tor is an onion-routing network that allows for anonymous communication online. See: https://www.fsf.org/

Foundation (FSF)[6], and the EFF to name but a few. What unites these institutions is their members' strong believe that cryptography is a key technology for preserving social norms like privacy or freedom of speech.

The EFF is the most prominent civil rights organization focusing on digital rights issues in the United States. The organization employs lawyers, activists, and IT-experts. Aside from litigation work, EFF's tech staff is working on technical solutions for surveillance issues. The 'Let's Encrypt' project for example was realized by the EFF in cooperation with the Mozilla Foundation.[7] During my research I conducted interviews with people from various crypto-related projects that I encountered in the immediate surroundings of these organizations. What unites these people is the commonly shared awareness that their work as system engineers has strong political and moral implications. A commonly shared attitude within the community is the idea that technological design decisions have regulatory effects on a societal level. Lawrence Lessig – a legal scholar and former member of the EFF's Board of Directors – made famous this notion with the concept of 'Code is Law' (see Lessig 2006). One system implementer I talked to in San Francisco argued that a lot of people within the community would tie normative assumptions to this notion of code having similar regulatory effects as legislature. He further stated that many community members would adhere to specific idealizations of how the internet should be. The following quote by Bruce Schneier, a prominent figure within the politically sensitized cryptographic community, exemplifies a self-conception that I encountered quite frequently within the community: the self-understanding that there is a moral responsibility facing system developers: to design the internet according to specific social norms. In the wake of the publication of the NSA's and GCHQ's secret surveillance programs, Schneier addressed the engineering community with the words:

> Government and industry have betrayed the internet, and us. By subverting the internet at every level to make it a vast, multi-layered and robust surveillance platform, the NSA has undermined a fundamental social contract. The companies that build and manage our internet infrastructure, the companies that create and sell us our hardware and software, or the companies that host our data: we can no longer trust them to be ethical

6 | The Free Software Foundation (FSF) promotes user freedom. It is a non-profit organization whose developers publish free and open software under the GNU Public License, see: https://www.torproject.org/

7 | For further information about the EFF see the organizations website, available online under the URL: https://www.eff.org/. For further information about 'Let's Encrypt', see: https://letsencrypt.org/

internet stewards. This is not the internet the world needs, or the internet its creators envisioned. We need to take it back.[8]

In this moral wake-up call Schneier is referring to the fact that US-companies like Google and Facebook, who, either voluntarily or under legal pressure, cooperated with intelligence agencies by sharing user data. Framing this cooperation as the breaching of a global social contract is characteristic for the idealization of this technology. In fact, many of these morally sensitized tech-experts grew up with the pre-commercialized internet of the 1980s and early 1990s and still uphold the promises, hopes and expectations that a lot of internet pioneers invested in the technology in its early days. One commonly shared idealization of the internet is the idea that digital networks enable the free flow of knowledge and thereby prevent censorship and increase individual autonomy.[9] Tied to this assumption is the promise that computers can improve humanity's understanding of the world. This idea became an important pillar of the 'hacker ethics' that was formulated by Steven Levy in his 1984 book 'Hackers: Heroes of the Computer Revolution' (Levy 2010) and has since been circulated within the politically sensitized engineering community.

Before I proceed with a discussion of the concepts of trust and mistrust as different strategies of coping with uncertainty, I will delineate the problem of what I term ontological insecurity. I argue that politically sensitized developers of cryptographic systems perceive the current IT-infrastructure to be characterized by radical uncertainty with regards to the actual properties of trust relationships. I will show that their systems approach this problem of uncertainty in a specific way.

The Problem of Ontological Insecurity in the Digitally Augmented Life-world

Digital information technologies increasingly affect virtually all spheres of the contemporary life-word. Especially proprietary internet services like Facebook, Twitter, and Google have become natural tools for sharing personal information and gathering information about what is going on in the world. However, the fact that internet users produce more and more data means their utterances

8 | Schneiers' article 'The US government has betrayed the internet. We need to take it back' was published in the Guardian on September 5th 2013, see: http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

9 | This idea was famously formulated by John Gilmore – one of the early cypherpunks – in his statement 'the Net interprets censorship as damage and routes around it'. See: http://www.toad.com/gnu/

of life become more traceable and subject to further scrutiny by a variety of social actors like governments, private corporations or criminals. A large part of these manifestations of life is being emitted unwittingly in the form of so called metadata. Metadata is a by-product of computation and provides information about when, where and with whom communication took place. The looming 'Internet of Things' – the meshing up of everyday 'smart' objects with the internet and the algorithmic evaluation of personal data – has added a new quality of how knowledge is generated and how it takes effect in contemporary life. According to Couldry and Hepp this data driven stock of knowledge shapes the 'ontology of everyday interaction' in a way that social actors often are unaware of and do not have control over (Couldry and Hepp 2017: 126). I argue that the temporally and spatially decontextualized procession of our utterances of life by globally dispersed unknown entities increasingly restructures our system of orientation in the world in ways intangible for the networked individual (Ruh forthcoming).

Bruce Schneier refers to this imperceptible, spatially and temporally unbounded social dimension of the life-world in his blog post 'Data Is a Toxic Asset'.[10] He argues that personal data is being emitted over insecure networks, stored on vulnerable infrastructure and analysed by entities that the individual is unaware of. The equation of data emission with environmental pollution that resonates in the title of Schneier's blog post is a common interpretation scheme among crypto-advocates. In that vein, one San Francisco based system developer I spoke to argued that he considers data to be something 'that can possibly harm you in the future.' Like radioactive contamination, it would take effect underneath the level of an individual's experience with its disastrous consequences surfacing only in the future. One year prior to the leaking of the 'Five Eyes' surveillance programs by Edward Snowden, Julian Assange highlighted the physical delimitation of our utterances of life and the invisible social dimension of the current internet infrastructure:

> When you communicate over the internet, when you communicate using mobile phones, which are now meshed to the internet, your communications are being intercepted by military intelligence organizations. It's like having a tank in your bedroom. It's a soldier between you and your wife as you're SMSing. We are all living under martial law as far as our communications are concerned, we just can't see the tanks – but they are there (Assange 2012: 33).

10 | The post is accessible on Schneier's blog 'Schneier on Security', see: https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html

This risk awareness is characteristic for 'reflexive modernity' in that the sources of the underlying problem are framed as being invisible and its possible effects to be locally as well as temporally unbounded (see Beck 1992). The imperceptible, locally and temporally unbounded dimension of the life-world is one feature of what I term ontological insecurity. However, ontological insecurity – as I deploy the concept – has a further dimension that is characterized by a general suspicion towards the truthfulness of digitally mediated information and a generalized mistrust towards social institutions.

The publication of the Snowden material not only demonstrated the extent to which intelligence agencies are tracking global internet traffic in a passive manner but also gave insights into how these well-funded arcane institutions actively undermine the current IT-infrastructure in order to set up covert false-flag operations and corrode trust within oppositional communities. For instance, it turned out that one of GCHQ's strategies to damage a target person's reputation is to hack their social network and email accounts in order to send fabricated information to friends, colleagues and neighbours. These strategies of deception are explicitly aimed at 'using online techniques to make something happen in the real or cyber world'.[11] In addition to the exploitation of the internet's current infrastructure, the very providers of the underlying technology are frequently criticized for their opaque algorithms and their attempts to manipulate the way internet users experience social reality. One famous example of the manipulation of internet users' perception is Facebook's secret psychological mood experiment on nearly 700,000 users in 2012. The social network hid specific emotional words from peoples' news feeds in order to analyse the influence of emotional expressions for users' behaviour to 'like' and distribute posts (Kramer et al. 2014).

The suspicion of the deliberate distortion and algorithmic manipulation of digitally mediated representations of reality by diverse social actors has become a recurring topic over the recent years (van Dijck 2014). The most current debate over the manipulation of internet users' perception and experience is centred around accusations made by US-intelligence agencies against the Kremlin and President Putin regarding the influencing of the US-election campaign in 2016 by ordering the leaking of confidential material from the Democratic National Convention and influencing public opinion in favour of Donald Trump

11 | This quote is taken from the publication of a GHCQ document entitled 'The Art of Deception: Training for Online Covert Operations'. In his article 'How covert agents infiltrate the internet to manipulate, deceive, and destroy reputations', published on the website The Intercept, investigative journalist Glenn Greenwald analysed the document and came to the conclusion 'that these agencies are attempting to control, infiltrate, manipulate, and warp online discourse, and in doing so, are compromising the integrity of the internet itself.' See: https://theintercept.com/2014/02/24/jtrig-manipulation/

with the help of 'fake news' distributed by automated social-bots. What makes these allegations critical is the problem of evidentialization of authorship, the challenge of providing proof for the manipulation of information in an online environment.[12] One consequence of the problem of providing proof for the authorship of a hacker attack is that it is easy for state actors to instrumentalize these attacks for political ends.

The omnipresent potential of the manipulation of internet users' experience of trust relationships is another feature of ontological insecurity. This involves the technical ability to distort the perception of digitally mediated representations of reality. I use the concept to refer to a specific attitude towards the world that informs a generalized mistrust against social entities of all kinds. The concept is, in some sense, related to Anthony Giddens's notion of ontological security. For Giddens, ontological security is closely connected to the concept of trust (Giddens 1990: 92). He defines ontological security as the 'confidence that most human beings have in the continuity of their self-identity and in the constancy in the surrounding social and material environment of action' (ibid: 92). Giddens conceptualizes ontological security as a psychological phenomenon in the sense of an unconscious emotional state of mind that brackets out reasonable feelings of insecurity in an increasingly complex life-world that is characterized by existential threats.

He distinguishes two types of actors that exclude ontological security in their way of looking at the world: philosophers and schizophrenics. These two categories of actors who take over a perspective of ontological insecurity differ in what Schutz and Luckmann call the 'specific epochē' that characterizes their cognitive style of approaching reality (Schutz and Luckmann 1973: 27). In the mental sphere of scientific reasoning, the philosopher renders problematic ontological assumptions about the world whereas in his everyday attitude these problems are being excluded. For the schizophrenic however, doubts about the givenness of ontological security pervade what Schutz and Luckmann (with reference to Edmund Husserl) call the 'natural attitude of everyday life' (ibid: 3). As a consequence, the schizophrenic ties a relevance of action to his problematization of the world. Giddens points out that the anxieties of the schizophrenic are 'hardly expressive of a mental lack' but are 'more the result of emotional supersensitivity than irrationality' (Giddens 1990: 93). Against this background, I argue that the attitude of generalized mistrust shown by system engineers is the result of a specific approach to the world that is informed by their perception of ontological insecurity. This perception of ontological insecurity is not really an emotional gut feeling; rather it stems from their expert knowledge

12 | For an in depth discussion about the political and technical problems of evidentialization see Bruce Schneier's blog on the DNC hack: https://www.schneier.com/blog/archives/2017/01/attributing_the_1.html

about the foundational principles of the digitally augmented life-world. In this regard, it is telling that a lot of activists who were referred to as 'tin-foil-hats' by community outsiders saw their deepest fears about the manipulation and surveillance of global internet communication vindicated in the wake of the Snowden publications.

In the following, I will look at the prevalent literature on trust and mistrust in order to contextualize my observations. I argue that mistrust is a functional equivalent of trust in that it allows the reduction of complexity against the background of uncertainty. Furthermore, I contend that in the case of engineers of cryptographic systems the specific function of mistrust is to enable them to establish a context of action that is characterized by calculability. Extreme negative expectation allows them to suspend ambiguity with regards to the anticipated intentions of the mistrusted entity. As we will see, in the case at hand, this strategy of suspending ambivalence is supplemented by a flanking strategy of 'trusting the math' and thereby transferring the element of nescience to an isolated province of meaning.

Trust and Mistrust as Attitudes to Deal with Uncertainty

Social scientists have paid scarce attention to the phenomenon of mistrust. When we look at definitions of mistrust, we can find some common positions in the existing literature. First of all, mistrust is commonly characterized as a subjective attitude that is grounded in a specific mode of experiencing the world. This is also one main feature that is commonly assigned to trust. Martin Endress locates mistrust on the extreme negative end of a scale that describes an individual's inner attitude towards the experience of the latent fragility of social reality. According to Endress, mistrust is the result of a juggling act emerging from having to deal with aspects of the life-world that are taken for granted and aspects of the life-world that have become problematic and make necessary new strategies for action and sense-making (Endress 2002: 8). In this characterization, we find a characteristic that can also be found in Luhmann's approach towards trust as well as mistrust. Luhmann argues that trust and mistrust both presuppose a certain degree of acquaintance or familiarity with aspects of the life-world. Only if we have a certain degree of knowledge about the constitutive conditions of social situations, we can develop an attitude that is characterized either by trust or mistrust. According to Luhmann, acquaintance is a precondition for the development of expectations of a specific type (Luhmann 1973: 83). Simmel also emphasizes the importance of knowledge as a precondition for trust. He argues that trust takes place in a state of uncertainty between knowledge and nescience (Simmel 1992: 383). Guido Möllering digs deeper into the

space between knowledge and nescience characterizing it as a 'leap of faith'. He thereby focuses on the irrational element of trust, arguing that 'trust combines weak inductive knowledge with some mysterious, unaccountable faith' (Möllering 2001: 413). Udo Thiedeke also emphasizes the irrational element of trust by stating that trust – due to the lack of knowledge – makes reasonable calculation impossible (Thiedeke 2007: 175).

If trust and mistrust both refer to specific attitudes that stem from an uncertainty with regards to specific aspects of the life-world, then the question remains: what are the qualitative differences between those two attitudes and what are their functionalities? It is a common argument in the literature that trust is an attitude characterized by the suspension of doubt. According to Luhmann, trust is characterized by the acceptance of risk with the goal to reduce social complexity (Luhmann 1973). He points out that mistrust is not the flipside of trust but its functional equivalent. Following Luhmann, trust and mistrust both reduce social complexity. He argues that the attitude of mistrust is characterized by a maximum negative expectation. This radical negative expectation would then rule out specific types of action and allow for instrumentally rational behaviour (ibid: 78).

On the basis of these considerations, I argue that in a life-world that is increasingly characterized by ontological insecurity, instrumental rationality, provability and calculability can become highly desirable features.[13] This argument will become more evident when we take a closer look at how crypto-advocates contextualize their work in the bigger picture.

Generalized Mistrust as a Constitutive Element for the Preconditions of Trust

In the following, I will delineate the productive dimensions of generalized mistrust for the construction of cryptographic solutions for trust problems in the digital age. It will be shown that generalized mistrust indeed reduces social complexity. In the case of the developers of cryptographic tools, the premise of a fundamentally hostile communication environment functions as a starting point for developing protocols that provide the 'integrity', 'confidentiality', and 'authenticity' of communication as a precondition for trust. Within this perspective, the concept of trust still plays a crucial role in that the designers of

13 | One counter strategy in dealing with ontological insecurity can be identified in the fundamental abandonment of the expectation of truthful behaviour. This attitude is characterized by the acceptance of the lie as a persuasion strategy. It finds its political expression in the often-quoted term of 'post-factuality' that was elected 'Word of the Year' in Germany in 2016.

cryptographic tools externalize trust towards specific assumptions about the mathematical features of their protocols. We will see that the 'leap of faith' that, according to Möllering, is characteristic for dealing with uncertainties, is still a relevant feature within crypto-activists approach to the world.

However, I argue that generalized mistrust towards any possible intermediary in the communication process creates an isolated sphere of predictability and provability. This isolated domain allows designers of cryptographic protocols to develop technical tools that substitute acquaintance towards the constitutive principles of the life-world with reliance on specific features of its underlying technical infrastructure. These features of 'confidentiality', 'integrity', and 'authenticity' are aimed at providing the preconditions for the accurate experience of trust relationships in the digitally augmented life-world in that they force humans towards trustworthy behaviour. In this regard, mistrust allows cryptographers to shift from trust to reliance in that the features of their protocols claim to be mathematically provable in an objective sense.

In order to get a clearer picture of how system engineers conceptualize trust problems in an increasingly digitalized life-world, we need to take a closer look at how crypto-advocates locate their work in a bigger societal context:

> People are used to a world where most of the time they can just assume that their trust relationships are functional. They assume that you can walk into a hospital, that there is a person sitting at the desk, that that person (...) is authorized to take your information. You give them your information and you assume that it will be communicated with the doc. (...) In the world we come from (...) trust and fraud, malice is the cost of making business. We institute some level of procedure to make sure that that's happening. We are now transitioning to a world where (...) operating on a level of assumed trust is no longer viable. (...) It costs you personally and the people that you interact with and society at large too much to just simply assume trust. Verifying trust manually is also too expensive. We cannot possibly do that. So what we need is our machines to verify the trust for us. (...) We need a machine that you trust to simply go in and check all of these relationships. And just do it quickly, seamlessly and only tell you if something is a mess and do that in a reliable way (...). So what the fundamental nature of cryptography is, is to embed in systems trust relationships and then verify that those trust relationships are correct before proceeding through mathematics. That's the fundamental goal. (Interview with founder of Silicon Valley start-up, Skuchain. June 2015, Mountain View, California.)

This quote is part of an interview I conducted with the founder of the Silicon Valley start-up Skuchain. The initial idea behind Skuchain was to make it possible for end consumers to trace the supply chain of consumer products via digital signatures that mathematically proof the origin of the single components

of a particular good.[14] It therefore utilizes the Blockchain technology, which is at the heart of the crypto-currency Bitcoin.

This interview snippet embeds the work of politically motivated cryptographers and designers of cryptographic systems in the context of a fundamental cultural paradigm shift with regards to the functioning of trust relationships in the digitalized world. It captures and condenses the bigger societal picture of their endeavour: to build cryptographic tools in order to restore the functionality of trust relationships in a world where 'operating on a level of assumed trust is no longer viable.' This brief extract describes the fundamental problem facing designers of cryptographic tools. According to this argumentation, the risks underlying trust assumptions have increased in a digitalized world to a level that makes the suspension of doubt as an irrational element of trust impracticable. Therefore, my interview partner argues for a solution where 'our machines verify the trust for us' in a 'reliable way', since 'verifying trust manually' would be too expensive.

Following his argumentation, trust in the analogue world of physical encounters is an implicit phenomenon that is characterized by mutually shared implicit knowledge about the nature and contexts of social relationships. In this world of physical encounters, relationships characterized by trust rely on the ability of individuals to know the social entities that are engaged in a specific context of action. In the quotation above, this would be the receptionist who communicates medical information to the doctor. The founder of Skuchain considers this acquaintance with regards to typified role expectations (Goffman 1959) as a prerequisite for an attitude of trust. He further specifies the function of cryptographic systems. They basically fulfil two purposes: they (1) 'embed in systems trust relationships and then (2) verify that those trust relationships are correct before proceeding through mathematics'. The interviewee further points out, that cryptographic protocols undertake this task underneath the level of the actual communication experience in that these technologies inform the communicating parties only if 'something is a mess'. In the first approach, we can characterize this process as the substitution of human cognitive processes based on acquaintance or familiarity towards the life-world with erecting and enforcing mathematically provable protocol sequences. We will see that most cryptographic tools do not make trust dispensable but rather provide the pre-conditions for trust that are becoming fundamentally problematic in a communication environment that does not guarantee the properties of 'authenticity', 'integrity', and 'confidentiality' in any tangible way.

14 | Over the course of my field work the start-up's focus shifted towards the deployment of financial products (Brackets) that are aimed at facilitating B2B Trade and Supply Chain Finance. See https://www.skuchain.com/

For a better understanding of how this substitution process works we have to take a closer look at how designers of cryptographic tools translate mistrust from a social into a technical problem. Politically sensitized IT-experts treat increasing tendencies of centralization and intermediation of the global communication infrastructure to be fundamentally problematic, since this trend facilitates the surveillance and manipulation of information flows on a mass scale. These experts know about the general insecurity of software applications and the specific vulnerability of centralized systems. The incomprehensibility of the multitude of possible malicious actors that try to attack and undermine centralized systems on a global scale leads to a commonly shared threat model among cryptographers and system developers. This threat model is characterized by a general mistrust towards any known and unknown entity with the ability to successfully attack a communication network. One activist put it the following way:

> Any entity that sits between (or next to) the user and the endpoint they're communicating with represents a potential threat. The list of threatening actors includes institutions of all sorts (businesses, universities, etc.), governments, internet service providers, malevolent network administrators, and random hackers (Slepak 2014: 13).

This incomprehensibility of possible attackers makes necessary specific strategies for anticipating and preventing possible attacks, since the anticipation of the motivation of each single attacker is impossible. One strategy of cryptographers and system developers is to transfer this generalized mistrust from the social sphere to the level of the technical infrastructure. In a talk held at the Chaos Communication Congress 2014 in Hamburg, Seth Schoen – Senior Staff Technologist at the Electronic Frontier Foundation – called upon the hacker community to develop a broader understanding of the fundamental technical insecurity that the digitally augmented life world is based upon. He stated:

> We need a much stronger vision that the things around us are communications networks that are actually attacking us all the time on a large scale, routinely. That these networks are untrustworthy and that we need to protect our communications against them, for many reasons, for many threat models, against many attackers, in many different situations. And there isn't just one reason for that. There is a whole panoply of reasons why we ought to think of networks as untrustworthy and why we ought to think of network protocols as needing to protect communication against the networks. (...) The network operator, everyone along the path has the full ability to spy on everything that you do, and to modify it and to inject things.[15]

15 | This quote is part of a transcription of Schoens' talk on 'Let's Encrypt' held on the Chaos Communication Congress 2014. See: https://media.ccc.de/v/31c3_-_6397_-_en_-_saal_6_-_201412301400_-_let_s_encrypt_-_seth_schoen#video&t=209

Schoen characterizes the digitally augmented life world as being permeated by an omnipresent network infrastructure that is attacking trust relationships between end users permanently and routinely on a large scale. In this technical portrayal of the life-world, human adversaries and their motivations fade into the background and the infrastructure itself becomes the source of ontological insecurity. It is this fundamentally unsafe technology that allows for fraudulent and malicious behaviour and therefore reinforces a generalized mistrust towards any entity that potentially sits between the communicating parties.

Blinding out the motivations of an attacker reduces social complexity and has tremendous implications for conceptualizing a trustworthy network infrastructure on a global level. First of all, treating all possible nodes of a network as untrustworthy imposes the same rules on everybody. Secondly, transferring mistrust from the social to the technical sphere creates an isolated domain, in which trust problems become calculable. It is crucial to understand cryptographer's reference to the extra social realm of mathematics and physics in this regard. Without going into the theoretical and technical details of modern cryptographic protocols, it is important to understand the equalizing role that cryptographers assign to mathematics when developing solutions for trust problems on a global level.

Trusting the Math to Create an Isolated Domain of Provability

As mentioned in the introduction, the goal of cryptographic protocols is to safeguard the principles of 'authenticity', 'integrity', and 'confidentiality' of digitally mediated communication against the assumption of the hardness of specific mathematical problems. These mathematical problems are embedded in the cryptographic primitives that form the basis on which cryptographic systems are built upon. Developers and implementers of cryptographic systems usually utilize established cryptographic primitives that are listed in so-called 'cipher suites' according to particular areas of application.[16] Politically aware system developers deduce an empowering aspiration from these assumptions. Jacob Appelbaum, a former developer of the Tor Project, put this capacitating and equalizing quality of mathematics the following way: 'One must acknowledge with cryptography no amount of coercive force will ever solve a math problem' (Assange 2012: 61).

It is important to understand these dimensions of 'empowerment' and 'provability' as interrelated elements for crypto-activists' goal of providing

16 | One such cipher suite that is recommended by the NSA is called 'NSA Suite B Cryptography'. See: https://www.nsa.gov/what-we-do/information-assurance/

'authenticity', 'integrity', and 'confidentiality' as a precondition for trust. The equalizing quality of cryptography not only rests on the assumed hardness of specific math problems, but also on Kerckhoffs' principle. It states that the security of a cryptographic system is reliant on the secrecy of the private key and on the disclosure of the cryptographic algorithm (Kerckhoffs 1983). Only cryptographic systems that can be studied in public and that withstood attacks over time are believed to be secure. As a consequence, the same cryptographic primitives are being deployed on a global scale. Politically motivated system developers see this as equal fighting chances for everyone. Many crypto-advocates therefore characterize cryptographic systems as bipartisan technologies. One spokesperson of the Chaos Computer Club put it the following way during a debate in Berlin:

> There is an inherent refusal [among state officials] to accept the fact that math does not care about your intentions. And computers most of the time do not. They are unable to differentiate whether what they are currently doing is good or bad.[17]

This statement is a reaction towards state officials' demand for the regulation of strong cryptography in the context of fighting organized crime and terrorism. Cryptographers argue that undermining the cryptographic standards would weaken the overall global IT-security and pose a threat to the global communication infrastructure.[18] In addition to these empowering and equalizing qualities that activists assign to mathematics, relying on mathematics creates an isolated sphere of clarity and calculability that allows cryptographers to shift from trust to certainty. Within the academic cryptographic community, there has been a strong tendency towards the promotion of formal security definitions. It is a common narrative within the academic community that modern cryptography has shifted from an 'art' to a 'science' and that one crucial condition for this scientific turn is the creation of highly contextualized formal security definitions. Koblitz et al (2001) define a 'security proof' or a 'reductionist security argument' the following way:

---

17 | Linus Neumann, one of CCC's spokespersons, made this statement at the 'Open Debate on the Politics of Encryption', a podium discussion held in Berlin in July 2016. See: https://cdn.netzpolitik.org/wp-upload/2016-07-20_Open-Debate-on-the-Politics-of-Encryption.mp3

18 | As a reaction to US- and British government officials' claim to restrict the use of strong cryptography after the attacks on the French satirical magazine Charlie Hebdo in January 2015, leading cryptographers published an expert assessment with regards to the feasibility of these proposals. The experts concluded, that weakening the cryptographic standards would pose a threat to the overall IT-security. See: https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf

> What a 'security proof' – or, as we prefer to say – a reductionist security argument [57] – actually does is show that an adversary cannot succeed in mounting a certain category of attack unless a certain underlying mathematical problem is traceable. (Koblitz et al. 2011: 20)

This form of generalized mistrust as a scientific epistemology reduces social complexity in that it brackets out the motivation of an attacker by creating an isolated domain of definition. Security proofs only take into consideration clearly defined categories of attacks as well as assumptions about the computational capacities of an attacker and his or hers sophistication in solving particular mathematical problems.[19] At this point it is important to note that the formalization of security proofs is part of a discourse within the academic community that aims at locating cryptography in the field of the natural sciences. This community only partially overlaps with the politically sensitized community of system developers and implementers. The latter is more concerned with 'real world problems' than with formal definitions (Rogaway 2015). However, I argue that the basic idea of the provability of specific security parameters against a generalized attacker still is an important aspect of their mind-set. In the wake of the publication of the Snowden documents, Bruce Schneier addressed the engineering community with the words 'Trust the math. Encryption is your friend.' He argued that properly implemented, cryptography would remain the last tool to protect the internet user even against the most potent adversary.[20] One system implementer I spoke to in San Francisco told me that this notion of trusting the math was taken over by the engineering community as 'a gospel'.

Koblitz et al (2001) however, notice that in practice, cryptography still has a strong subjective element in that intuition plays a crucial role in conceptualizing cryptographic systems. This intuitive element stems from the fact that applied cryptography is a future oriented endeavour that has to take into consideration possible computational developments or mathematical breakthroughs. Cryptographers thus have to take into account the temporal aspect of the digi-

19 | It is important to note that basic research in cryptography takes place in a highly opaque research environment. Aside from public academic research there exists a highly arcane cryptographic community within the intelligence community that has a longstanding tradition, which predates public research for decades. It is assumed that this highly funded arcane community might be ahead of the game with regards to specific mathematical breakthroughs or in the field of applied quantum computing. Breakthroughs in the latter field of research would render most of the current cryptographic primitives unusable.

20 | Schneier's article is called 'NSA Surveillance: a Guide to Staying Secure', see: https://www.schneier.com/essays/archives/2013/09/nsa_surveillance_a_g.html

tally augmented life-world.[21] Koblitz et al (2001) therefore characterize cryptography as a highly speculative field of research:

> Part of the reason why cryptography has such a strong subjective element is that speculation is central to the field. When deciding on the basic type of cryptography to use (RSA or ECC, for example), when choosing the type of a protocol for a given application (e.g., whether or not to use identity based encryption), and when selecting parameters (for instance, random generation versus enhanced efficiency), one has to make a guess about future developments in order to evaluate the fundamental issue of safety of the system. One has to ask: what types of adversaries are we likely to encounter, and what will be their most likely avenue of attack? Will there be any breakthroughs in bringing down the asymptotic running time to solve any of the supposedly intractable mathematical problems? Will quantum computing (...) ever become practical? What new 'side channel' attacks (...) might be devised? (Koblitz et al. 2011: 32)

This contrasting of the ideal model of cryptography as a highly formalized discipline that is characterized by mathematical clarity on the one hand, and the rather 'fuzzy' practice of cryptographic work, which takes place in a complex, contingent and dynamic environment is an observation that is not addressed in academic work that aims at reductionist definitions (Goldreich 1999; Katz and Lindell 2008).

I argue that the problematizations in Koblitz et al (2001) indicate a field of tension that people working in the field of applied cryptography have to cope with: the necessity of reducing the complexity of the 'real world' against the background of ontological insecurity and yet still having to take into consideration contingent aspects of future developments that are not theoretically graspable. One San Francisco-based system implementer told me that, over the years, awareness has grown within the community that the reliance on predictions that are based on the assumption of calculable regularities (e.g. Moore's Law that describes how computation power will increase over a longer period of time) has turned out to be highly problematic. He explained to me that this insight would be the result of system developers increasingly having to cope with 'once-solved problems' that are a consequence of lock-in phenomenon and false speculations made against the backdrop of a highly complex and contingent environment. Furthermore, the community of system implementers has to struggle with the fact that transferring mathematical problems into executable code carries with it the risk of human failure. In fact, programming errors in the form of 'bugs' turned out to be the most frequent causes when cryptographic systems fail in practice.

---

21 | Practically speaking they have to take into consideration that the NSA is storing encrypted data in order to decrypt it when it has the possibilities in the future.

It is important to note that there are strategies within the engineering community to cope with the problem of intended and unintended human decisions and their unpredictable consequences. For example, the community is working on concepts like 'machine provable computation' and 'machine provable compiling' (MacKenzie 2001). These reductionist strategies aim at bridging the 'semantic gap' between 'pure math' and software as a 'social construct' by 'getting rid of or at least detecting human idiosyncrasies' as the system developer put it. This mathematization of the translation process – as I would term this strategy – is informed by the idea to create an isolated domain of calculability in a complex and contingent environment. Developers and implementers of cryptographic systems thereby pursue the goal of eradicating the 'leap of faith' – the gap of knowledge – that is characteristic for trust and switch to a position of transparency and calculability.

However, the strategy of mathematically purifying applied cryptography at least currently seems to have its limitations. Confronting him with Schneier's appeal to 'trust the math' against this set of problems, the system implementer replied: 'It is such a contingent claim, that I don't believe it anymore, even though I depend on it.' It is telling that a lot of cryptographic systems that have found widespread application, were designed within an activist community that is not directly associated with the academic world. The papers that describe these protocols often lack the formalized 'security proofs' that have become a standard within the academic world.[22]

I interpret this lack of security proofs as the suspension of doubt that underlies the call to 'trust the math'. I argue that this 'leap of faith' fulfils specific social functions. It strikes me as fundamentally relevant for understanding their perspective that many politically sensitized system builders, while reflecting its flaws, continue to adhere to this notion of math being the last remaining anchor for trust. I argue that this suspension of doubt – the exclusion of the problems behind assumptions about the reliability of the underlying math – enables activists to reduce the complexities associated with having to deal with unpredictably potent adversaries while at the same time still being able to uphold

22 | In his paper 'The Moral Character of Cryptographic Work' that he addressed at the academic crypto-community in the wake of the Snowden publications, Phillip Rogaway criticized the academic community for not taking into consideration real world problems when formalizing security proofs. Rogaway, who himself is part of the academic world, pointed to his observation that the politicized community would develop practicably usable systems that do not come with security proofs. In his paper, which was positively received within the political community, he called on the academic world to cooperate with the practitioners and provide them with proofs for their models. He argued that, although lacking formal security proofs, these systems would work in practice and that security proofs could be stated ex ante (see Rogaway 2015).

the concept of a generalized attacker. This reduction of complexity also allows developers of practical applications to focus on specific features that address problems of the digitally augmented life-world. Furthermore – and probably – most importantly, it allows them to hold on to the empowering qualities that they assign to mathematics.

As a last point, I will illustrate how politically motivated designers of cryptographic systems develop trustworthy alternatives for centralized systems that take into consideration the temporal dimensions of the digitally augmented life-world that I described at the outset. I will portray the features of Perfect Forward Secrecy and Plausible Deniability in order to show how these actors transfer a generalized mistrust towards any social entity into protocols that aim at establishing the foundations for a post-social contract that makes trusting institutions dispensable.

'Perfect Forward Secrecy' and 'Plausible Deniability' as Features of a Post-social Contract

What unites the projects aiming at rebuilding the internet is removing the necessity of having to trust any centralized institution or any specific node in the network. In this vein, one Berlin-based system developer told me that he does not want to have to trust anybody anymore. The projects try to achieve that goal by developing decentralized, distributed systems that supplement trusted third parties with cryptographic systems that allow the verification and proof that certain trust assumptions are correct. Digital signatures, for example, allow the receiver of a message to use a secret signing key to compute a mathematical value out of a sender's message and public key. This allows the receiver of the message to verify the authorship of the sender.

In recent years, politically motivated designers of cryptographic ciphers developed sophisticated versions of digital signatures that especially take into account the above mentioned temporal aspect of the digitally augmented life-world. The developers of the OTR-protocol (Off-the-Record), for example, introduced two features that found widespread application: Perfect Forward Secrecy and Plausible Deniability (Borisov et al. 2004).[23] Perfect Forward Secrecy describes a feature of the protocol that prevents an attacker who intercepted a long-term private key from getting access to the stored encrypted data of end users by introducing session keys that expire after the communication took place. After it had become known to the public that the NSA is storing vast amounts of encrypted communication with the goal of analysing it retroactively

23 | In the initial paper on OTR, the authors use the term reputability when referring to Plausible Deniability.

after the encryption had been reversed, this feature became highly supported by the politically sensitive engineering community.

Plausible Deniability is a communication feature that was developed against the background of protecting dissidents against coercion. It allows communicating parties to mathematically authenticate their communication parties during the communication but to make it impossible for any of the parties to verify to a third party that communication took place. This feature is one example of the constitutive quality of mistrust that arises both from the implications of the digital communication infrastructure and from assumptions about mistrustful behaviour of social actors. One activist put this the following way: 'If laws and courts were rational and just, and governments responsible and ethical, plausible deniability would not be a necessary, or even a desirable feature' (Slepak 2014: 4). This line of argumentation is common within the cypherpunk community[24] – the idea that human institutions are fundamentally untrustworthy and that cryptography is a tool that forces these institutions to act in a trustworthy manner.

A prominent theme within the politicized community is the differentiation between the laws of physics and the laws of men. One San Francisco-based activist told me that 'if the laws of men fail then the laws of physics still work'. The probably most famous example of the idea to use cryptographic protocols in order to force institutions towards trustworthy behaviour is the functional principle of WikiLeaks' dropbox for whistleblowers. It exemplifies how fundamental mistrust towards any social entity and the outsourcing of trust to the sphere of mathematics is mobilized with the goal to establish a political environment where trusting institutions is replaced by the idea of making their behaviour verifiable. WikiLeaks' dropbox utilizes a set of cryptographic procedures (OpenSSL, Tor among others) that allow sources to anonymously upload information that they perceive to be in the public interest. It is the architecture itself that takes fundamental mistrust into human institutions as a starting point. In that the communication between the dropbox and the uploading party is cryptographically anonymized, it incorporates the feature of Plausible Deniability and it stops any third party, including WikiLeaks, from identifying the source.

---

24 | Cypherpunks are a globally dispersed community of activists who seek to achieve social change through the proactive use of privacy-enhancing cryptographic technologies. The movement dates back to the late 1980s. Cypherpunks initially communicated their ideas with the help of electronic mailing lists. Their fundamental ideas are captured in 'The Crypto Anarchist Manifesto' by Timothy C. May and the 'Cypherpunk's Manifesto' by Eric Hughes. Modern cypherpunks include Julian Assange, the founder of WikiLeaks. For May's Manifesto see: https://www.activism.net/cypherpunk/crypto-anarchy.html and for Hughes' Manifesto see: https://www.activism.net/cypherpunk/manifesto.html

The idea of embedding social relationships in a framework of mathematical clarity and thereby restoring fundamental human rights in a world that is perceived to be increasingly governed by opaque interests is what is at the heart of crypto-activist ideas of a new social contract. Edward Snowden's call for a social contract based on cryptography has to be understood against this background. This argumentation about the unreliability and contingency of human institutions, which are prone to manipulation by interests of power is a theme that I encountered quite often during research. One system developer I talked to in the Bay Area argued that he is not too much interested in questions of the US-Constitution, which he considers to be an important but also a contingent historical outcome. Instead, he was interested in asking 'what does the physics say in a five hundred year sense'. He is thereby referring to the dynamic interplay between cryptography and cryptanalysis (the breaking of cryptographic ciphers) that is driven by mathematical breakthroughs. Against the background of this perspective, the validity of social norms like privacy is not reliant on a public consensus or any other form of exercise of power but on the question whether these social norms proof to be universally executable in a scientific sense.

This outsourcing of the practicability of social norms into the realm of mathematics and physics leaves unanswered questions of consensus. It disguises the concrete motivation of the designers of these protocols as well as their political agenda. Lawrence Lessig pointed out early on that cryptography would be a Janus-faced technology, since it would allow for systems that enforce anonymity and systems that allow for the unambiguous identification of individuals (Lessig 2006: 52). The answer to the question of whether there is a global public agreement on the desirability of decentralized systems is also far from unambiguous. Cryptographic systems that work on the premise of generalized mistrust and that replace trust in human institutions with trust in mathematically enforced protocols also blind out questions of accountability.

A current example of the problem of accountability in so-called 'trustless systems' is the case of the DAO hack. It was still heavily discussed in the tech-community during my last fieldtrip to the Bay Area in December 2016. The DAO (decentralized autonomous organization) was an extreme example of a libertarian cypherpunk technology that completely replaces trust in human institutions with a technological system that enforces contracts on the basis of mathematical verifiability. The DAO was a stateless decentralized autonomous organization based on the Blockchain technology. The organization was crowd-funded and only existed in the form of software code which has been made available open-source by its anonymous backers. The company was autonomous in the sense that there existed no Board of Directors or any other human institution that had any legal authority or executive control over its businesses. Richard Waters of the Financial Times described the company as

'a form of investor-directed venture capital fund' since its designated business was to invest in other businesses. The idea behind the company was to get rid of any interference by a third party that might take money for favouring the investment into a particular business.[25] The decisions about specific investments were supposed to be made by the companies' stakeholders based on a consensus model. Stakeholder rights to vote were tied to their shares that were expressed in the form of 'Eth', a crypto-currency based on the Ethereum Blockchain. [26] The consensus model as well as the enforcement of decisions was governed by so-called 'smart contracts' that were also part of the Ethereum Blockchain. However, in June 2016, unknown hackers exploited a vulnerability within DAO's source code and directed one third of the funds to an anonymous account. This led to panic among the company's stakeholders who had altogether raised an equivalent of 120 million USD. The DAO hack raised an intense dispute within the Blockchain community that centred on questions of accountability. It was heavily discussed what social entity could be held liable for the financial loss of DAO stakeholders given that contracts in the DAO environment are being established anonymously and enforced through software code.

Conclusion

The goal of the chapter was to examine how politically aware designers and implementers of cryptographic systems cope with ontological insecurity in the digitally augmented life-world. What we find is that this digitalized social sphere is characterized by its temporal and spatial delimitation. Furthermore, this vastly complex environment is characterized by a lack of acquaintance of its inhabitants with regards to the concrete nature of social relationships that unfold within this physically intangible sphere that is occupied by a diverse set of unknown actors with unpredictable intentions. In this social realm, trust becomes fundamentally problematic since it presupposes some sort of familiarity with the constitutive conditions of social relationships. I pointed out that the politically aware community of developers and implementers of cryptographic systems is tied together by a commonly shared epistemic perspective that is informed by their in depth knowledge about the technological underpinnings of this social sphere. This specific epistemology informs a shared problem aware-

25 | For Waters article 'Automated company raises equivalent of $120M in digital currency' see: http://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html

26 | Ethereum is a crypto-currency based on the Blockchain, but has slightly different functionalities than Bitcoin.

ness within this 'community of communities': these actors share knowledge about the omnipresent possibility of the manipulation of trust relationships between end users by unknown third parties. This knowledge creates a generalized mistrust towards any possible intermediary with the ability to undermine these trust relationships.

Furthermore, it became clear that this perspective of generalized mistrust has a productive quality for dealing with trust problems on a global scale. Translating generalized mistrust into a technical problem allows this community to establish an isolated domain of calculability. Creating this clearly circumscribed sphere that presupposes a generalized and omnipresent attacker allows these experts to make social trust problems calculable and to reduce social complexity. Within this realm of provability and calculability, system designers and implementers ostensibly suspend the irrational 'leap of faith' that according to Möllering is characteristic for trust. However, it also became clear that the unpredictable, erratic element of trust is still efficacious. The builders of cryptographic tools transfer the element of doubt from the social sphere towards trusting the empowering quality and the hardness of mathematical problems. As it turned out, questions about the hardness of mathematical problems cannot be answered unambiguously in a complex and unforeseeable real world environment. Not only do these questions depend on incalculable future breakthroughs in the field of mathematics, but also on highly contingent 'human idiosyncrasies'. Nevertheless, outsourcing the element of trust to the mathematical domain fulfils specific social functions that probably have not been covered exhaustively in this article. Here, I focused on the observation that 'trusting the math' allows the builders of cryptographic systems to shift from an attitude of mistrust to a perspective of unambiguity when implementing the concepts of 'integrity', 'authenticity', and 'confidentiality' as the preconditions for trust on a protocol level.

Another interesting unanswered theoretical question is the one of a possible threshold between trust and certainty. Providing the 'integrity', 'authenticity', and 'confidentiality' of an encrypted email still allows Alice to subvert the expectations of Bob. She could unintentionally send him false information or tell him a lie. Smart contracts however, enforce a predefined agreement without leaving the agreeing parties any room for deviant behaviour within the logic of the protocol.[27] Here, it might be interesting to take a closer look at specific cryptographic technologies in order to analyse the junction between trust and certainty. The idea to establish a social contract that is characterized by mathematical unambiguity can be found in its most pronounced manifestation in cryptographic systems developed within the cypherpunk community. These

27 | Note that the DAO hack was a software hack that utilized a weak spot in the code, not in the protocol itself.

systems fundamentally aim at replacing the necessity for trusting human behaviour by mathematically enforcing and disabling specific behaviour that the systems' designers deem to be (un-)desirable. As the example of the DAO hack showed, transferring authority from human institutions to mathematics leads to questions of responsibility and accountability that have not yet been answered.

References

Assange, Julian. 2012. *Cypherpunks: Freedom and the Future of the Internet*. New York: OR Books.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: Sage.

Borisov, Nikita, Ian Goldberg and Eric Brewer. 2004. 'Off-the-record communication, or, why not to use PGP', *Proceedings of the 2004 ACM Workshop on Privacy in the electronic society*. Washington DC: ACM.

Couldry, Nick and Andreas Hepp. 2017. *The Mediated Construction of Reality*, Cambridge: Polity Press.

Endress, Martin. 2002. *Vertrauen*. Bielefeld: transcript.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Stanford: Polity Press.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. New York: Anchor Books.

Goldreich, Oded. 1999. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Berlin, Heidelberg: Springer-Verlag.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S Surveillance State*. New York: Metropolitan Books.

Katz, Jonathan and Yehuda Lindell. 2008. *Introduction to Modern Cryptography*. Boca Raton: Chapman & Hall/CRC.

Kerckhoffs, Auguste. 1883. 'La Cryptographie Militaire', *Journal des Sciences Militaires* 9: 5-38.

Knorr Cetina, Karin. 2001. 'Postsocial Relations: Theorizing Sociality in a Postsocial Environment', in George Ritzer (ed.), *Handbook of Social Theory*. London: Sage, pp. 520-537.

____. 2007. 'Postsoziale Beziehungen', in T. Bonacker and A. Reckwitz (eds), *Kulturen der Moderne. Soziologische Perspektiven der Gegenwart*. Frankfurt am Main: Campus-Verlag, pp. 267-299.

Koblitz, Neal, Alfred Menezes and Ann Koblitz. 2011. 'Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift', *Journal of Number Theory* 131: 781-814.

Kramer, Adam D., Jamie E. Guillory and Jeffrey Hancock. 2014. 'Experimental Evidence of Massive-scale Emotional Contagion through Social Networks', *PNAS* 111 (24): 8788-8790.

Lessig, Lawrence. 2006. *Code Version 2.0*. New York: Basic Books.

Levy, Steven. 2010. *Hackers: Heroes of the Computer Revolution*. Cambridge, O'Reilly.

Luhmann, Niklas. 1973. *Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität*. Stuttgart: Ferdinand Enke Verlag.

Mackenzie, Donald A. 2001. *Mechanizing Proof. Computing, Risk, and Trust*. Cambridge, MA: MIT Press.

Möllering, Guido. 2001. 'The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension', *Sociology* 35 (2): 403-420.

Rogaway, Phillip. 2015. *The Moral Character of Cryptographic Work*, retrieved Jan 2017 from http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf

Ruh, Nicolai. forthcoming. '"The Universe Believes in Encryption" – Implementing Math into the Ontological Layer of the Digitally Augmented Life-World', in J. Dreher (ed.), *Mathesis universalis – die aktuelle Relevanz der "Strukturen der Lebenswelt"*. Berlin: Springer.

Schneier, Bruce. 2000. *Secrets & Lies. Digital Security in a Networked World*. Indianapolis: Wiley Publishing.

Schutz, Alfred and Thomas Luckmann. 1973. *The Structures of the Life-World*. London: Heinemann.

Simmel, Georg. 1992. *Soziologie. Untersuchungen über die Formen der Vergesellschaftung*. Frankfurt am Main: Suhrkamp.

Slepak, Greg. 2014. *DNSChain + okTurtles. Easy to use, state of the art security, for existing online communications*, retrieved 28 July 2017 from https://okturtles.com/other/dnschain_okturtles_overview.pdf

Thiedeke, Udo. 2007. *Trust, but test! Das Vertrauen in virtuellen Gemeinschaften*. Konstanz: UVK.

van Dijck, José. 2014. 'Datafication, Dataism and Dataveillance. Big Data between Scientific Paradigm and Ideology', *Surveillance & Society* 12 (2): 197-208.