Infrastructures of trust and distrust. The politics and ethics of emerging cryptographic technologies

Maja Hojer Bruun, Astrid Oberborbeck Andersen & Adrienne Mannov

Maja Hojer Bruun is associate professor at the Department of Educational Anthropology of Aarhus University. Her research interests include science and technology, organisational and economic anthropology, and interventionist and experimental ethnographic methods.
Astrid Oberborbeck Andersen is assistant professor in Techno-Anthropology at the Department of Culture and Learning at Aalborg University. Her research focuses on human- environment relations, technology development, and interdisciplinary and collaborative methodologies.
Adrienne Mannov is a postdoc at the Techno- Anthropology department of Aalborg University. Her research focuses on notions and practices of security, the relationship between rights and technology development, and interdisciplinary research within and beyond academia.
They may be reached via mhbruun@edu.au.dk.

Abstract
The authors of this article are engaged in anthropological research on the links between the growing interest in privacy and data security as a technical field and how notions of trust, security and accountability are practised in and beyond technical fields of cryptography, specifically a field called multi-party computation (MPC). They pursue the relationship between trust in different forms of cryptography – academic and activist – and notions of trust as they are articulated in relation to data security and the protection of citizens' data. There is a tension between the concerns raised in public debates about data security and the promises of emerging cryptographic protocols. In political speeches and public debates, citizens' trust that governments and tech companies will protect their data is framed as important and essential. In the environments of emerging cryptographic technologies, such as blockchains, bitcoin and MPC, a promise to provide 'trustless trust' and abandon the need for trusted intermediaries, authorities and institutions is articulated.

The continued increase in data flows, data collection and the aggregation of data from personal devices, sensors, social networks and commercial and public databases carries promises of ever more efficient services and 'smart' uses of the world's resources, but also heightens the need for secure and privacy-preserving communication. In popular debates around data privacy, a particular understanding of 'privacy' has come to dominate, one that privileges the idea of the individual and individual privacy, perhaps because 'privacy' brings to mind 'private property' and the private as opposed to the public. Yet, data privacy, or data protection, is a public concern. It not only serves to protect individual citizens against the state, but to protect all kinds of information and communication against more powerful organizations, be they states or global companies.

In this article, we approach the debate about data protection from an alternative angle, engaging the concept of trust, particularly in relation to cryptographic technologies. When privacy is related to public responsibility and accountability, trust, as a concept and phenomenon – who and what is to be trusted, and questions of what trust *is* – emerges in public debates about data protection and among cryptographers and technologists. In the context of data privacy, trust is a matter of what institutions, functions or mechanisms are entrusted, or should ideally be entrusted, to protect citizens against the misuse of data and the abuse of power connected to data that is collected.

We sketch out two discourses of trust that circulate in relation to data protection: the first is found in political speeches and public debates about data privacy and security, especially in Scandinavia. Here, governments and the business world emphasize the need for people to trust in data systems in order to create a well-functioning digital society. In this discourse, trust is generally described as the 'glue' of society. Perhaps 'lubricant' is a more apt metaphor, because trust is believed to make a digitalized society run more smoothly. The second discourse is found in the research and development environments of emerging cryptographic technologies, such as blockchains, bitcoin and multi-party computation (MPC). In contrast to political speeches and public debates, these communities promise to provide 'trustless trust' and abandon the need for trusted intermediaries, authorities and institutions.

As we will show, MPC claims to enable encrypted communication and data privacy, circumventing the need for an outside trusted institution. All involved parties are distrusted as potential adversaries, and distrust is thus promoted as a useful framing. At first sight, distrust appears to be the opposite of trust, but distrust does not always work against trusted institutions. Distrust can be a formal way of withholding trust in any one party in a situation of risk, uncertainty or mistrust, and can play a part in building social order and establishing collaboration – for instance in political systems of checks and balances. Mistrust, in comparison, means a lack of confidence in a person or thing, often based on instincts or gut feelings.

Where mistrust exists, formal systems of distrust can be put in place. However, as we will show, the problem with distrust or 'trustless trust' in MPC is that political accountability can be difficult. Because of MPC's algorithmic protocols, it is not easy to make connections between the final analysis and the original data points. We end the article with some reflections on the possible implications of new forms of (dis)trust that come with the intensified development of cryptographic technologies in datafied societies. Do new forms of cryptographic trust compete with established forms of public trust? May they inhibit public trust or perhaps even undermine existing relations of trust among people, and among citizens towards social institutions?

The authors of this article are involved in an interdisciplinary research project[1] with mathematicians and engineers working in the fast-evolving field of cryptography, called secure multi-party computation, or simply MPC. MPC was formally introduced in 1982 by the Chinese computer scientist Andrew Yao, and in recent years, some universities, research institutions and spin-off start-ups have worked together to develop practical tools for the application of MPC, e.g. for the benchmarking and data analysis of sensitive data (Lapets et al. 2018). We conduct fieldwork among researchers and developers of MPC at a number of international universities, research institutions and start-ups to achieve a basic understanding of the cryptographic logics and technologies, and how key themes such as security, privacy and trust are articulated in these workspaces. These fieldwork activities include participation in international conferences, seminars and industry fairs. We also participate in public events where digitalization, data privacy and security are debated from a policy and citizen perspective.

Cryptography – the kind of computer algorithms and data encryption standards that secure the flow of digital communication and data, including our activities on the Internet, email, ecommerce and all kinds of electronic identity authentication – is part of our ubiquitous, yet invisible, digital infrastructure and a cornerstone in data protection and privacy. We use it every day, but very few of us understand how cryptography actually works. Cryptographic systems and methods largely escape public attention, but scandals such as Edward Snowden's 2013 disclosure of the US National Security Agency's backdoor into cryptographic security systems and thereby into the telecommunication data of millions of people reveal that data infrastructures and cryptographic systems are not just technical but also social and political forms.

Cryptography thus emerges as a privileged site for examining broader political and ideological issues, such as the relationship and power balance between citizens, the state, technology, technology developers and companies and different notions of and visions for society, often expressed through the idiom of trust. Different cryptographic technologies – academic and activist – that constitute and mobilize different versions of trust, distrust and so on, are also complex social projects, with histories and futures, specific characteristics, and their own ethos and morality, and anthropologists are equipped to disentangle and render such processes and relations visible. A short history of cryptography and an introduction to the activist and academic crypto-community and its central political and ethical debates may be helpful in mapping this out. But first, we turn to the concept of trust in the social sciences and anthropology and show, ethnographically, how trust is articulated as a social, political and economic resource at public debates in Denmark.

Trust as rational choice and affect

In different social science approaches to trust, one dividing line is between scholarship that takes trust as a strategy – as a deliberate, conscious and rational choice – and scholarship that sees trust as an attitude or affect, a rather

indefinable social phenomenon that serves a diversity of unpredictable psychological and social purposes (cf. Carey 2017). Sociologists, political scientists, legal scholars and economists have long seen trust as modern society's glue, the basis for social order and cohesion, serving the legitimacy of modern states and the functioning of market transactions (e.g. Gambetta 1988; Misztal 1996). Trust as a strategy can also be seen as a rational choice in situations of uncertainty or *not knowing*, e.g. due to limited technical or scientific knowledge, but where it appears to be functional and prudent to trust in social, political or scientific institutions.

Corsín Jiménez (2011) describes public trust as a 'political epistemology of neoliberal society' where transparency and audit regimes create the preconditions for trust and make trust measurable and capable of audit. This is also how trust is conceptualized by politicians and opinion makers in the context of our fieldwork. They praise trust as a resource and a virtue that needs to be nurtured in our digital age, to compensate for the general public's lack of technical understanding, to avoid political crisis and to secure the continued functioning of data flows, digital infrastructures and public institutions.

Anthropologists tend to study trust in social interactions in specific lifeworlds, an approach that avoids reducing trust to political functionality (e.g. Broch-Due & Ystanes 2016). Here, trust is often described as a disposition or an ability to act, as a qualitative sense of confidence that people place in particular relations and institutions within their surroundings. Based on their collection of ethnographic studies, Broch-Due and Ystanes define trust as 'a disposition, a powerful affect, a stance towards the world expressed in a confident reaching out to others. It is a social orientation towards the future nurtured by the gradual accumulation of positive experience and sometimes revealed in a leap of faith' (2016: 1).

Only a few anthropologists have explored how trust is configured in social interactions mediated by digital devices and digital data, and to our knowledge, none have addressed notions of trust in cryptographic systems underlying digital infrastructures. Pink et al. (2018) have studied how everyday producers and users of digital data in Spain and Australia experience data storage techniques and overcome the anxiety of losing data, or it being misused by others. In their study, trust is defined as 'a feeling that specifically appears to the ability to be able to move on and do something in the immediate future' (2018: 3).

They show how living with data means living in a world of uncertainty and mess, and how their research participants pushed aside their anxieties and devised ways of managing data that they trusted were 'safe enough', e.g. using cloud storage or hardware backups, but which did not comply with the data security procedures offered by software designers. In our present research on data protection, we do not focus on the everyday experiences of any particular groups of users of cryptographic technologies – as said, this category encompasses all. Instead, we zoom in on the ways in which trust is perceived by policy makers and those designing cryptographic systems.

Trustless trust

These *is* a growing branch of literature on trust in the digital age, but this is carried out by legal and business scholars and journalists who argue that new forms of trust are pivotal in emerging digital technologies and infrastructures. This literature focuses especially on the so-called sharing economy and bitcoin, a cryptocurrency building on blockchain technology and cryptographic protocols (e.g. Botsman 2017; Nelms et al. 2018; Werbach 2018). In the sharing economy, e.g. in Uber or Airbnb transactions, users' trust in the platforms and each other, often described as peer-to-peer or P2P trust, appears as 'credibility', 'reputation' or 'loyalty'. In blockchain transactions, 'trustless trust' or 'blockchain trust', trust is based in the network of participants/peers and in the underlying algorithms, without necessarily being placed in any of the individual participants or any outside authority (Werbach 2018). Although blockchain and MPC are not the same, they both operate with distributed, decentralized networks and trust models where no participants or components are trusted as individual entities. Unlike prevalent cryptographic protocols that require a trusted third party to facilitate data computations (Fig. 1), MPC protocols enable several parties to jointly compute functions without relying on a trusted third party and without revealing their own information to anyone (Fig. 2).

Leading figures in the Internet and blockchain movements, most notably the person or collective behind bitcoin, Satoshi Nakamoto (Nakamoto 2008), picture a world in which trust in powerful authorities, or in fact in any mediating entities, be it banks or nation states and their intelligence agencies, can be substituted by cryptographic protocols and the laws of mathematics. Trustless trust may be a paradoxical term, but the fact that the concept of trust is not discarded, testifies to the power of the discourse around trust and the functions that cryptographic trust is believed to perform. Even though the intention is to eliminate trusted institutions, in trustless trust, the concept of trust is iconized and takes on multiple meanings.[2]

We will return to cryptography and MPC shortly, but the following notes from the tech festival Internet Week Denmark (2018) illustrate how trust in public debates is articulated as a necessary resource in a well-functioning and competitive digital society.

Trust as a resource

At an event in May 2018 called 'Digital optimism? Denmark towards new digital horizons' at the public library in Denmark's second largest city, Aarhus, a panel of invited politicians and business people discussed 'Denmark's digital future'. The audience, including the authors of this paper, were invited to ask questions via Slido, a digital audience interaction tool. The moderator from the Confederation of Danish Industry Enterprises started out by asking 'What is your digital dream–' He asked us to imagine being in the year 2025, looking back at 2018. One of the moderator's recurrent themes was the issue of trust and how to secure trust in a digital era. 'Back in 2018 there was also mistrust', he said, citing the Cambridge Analytica scandal and the debates of its aftermath.

One panellist, a politician from the Social Democratic Party and spokesperson for information technology in the Danish parliament, stated that Denmark is the one country in the world that knows most about its citizens, due to its Civil Registration System, a high degree of digitization, and 'a high degree of trust'. This, she argued, means that foreign tech companies want to invest in Denmark. She went on to depict trust as a kind of resource that the national economy can harness, an asset reminiscent of Robert Putnam's notion of social capital that can be measured, quantified and compared across countries and communities. According to the European Union's (EU) Digital Economy and Society Index, Denmark is the most digital country in the EU, citing indicators such as broadband connectivity, use of the Internet, online trade and digital public services.

The country's Digital Strategy for 2016-2020 sets out goals for the collaboration of the public sector with the business community and for stakeholder organizations to speed up digitalization. In the strategy's introduction, the population's 'great trust and confidence in each other and in the public sector' is presented as the first reason why Denmark is in a good position to 'embrace the digital future' (Danish Government 2016). Another panellist, an associate from a consultancy, objected that trust is a 'double-edged sword'; it used to be local, but in these years, when trust is 'taken into globalized digital communities, we can suddenly find ourselves in the clutches of some Chinese platform'.

During this and other political events and public debates about digitalization (e.g. the People's Democratic Festival, Figs 3 & 4), the Danish population's trust is portrayed as a valuable resource, an asset and a 'competitive advantage'. As in other Scandinavian countries, trust is taken to be a basic premise for a well-functioning society in general and in the case of the digitization of societal functions, it is emphasized as a vital part of the Danish digital infrastructure. Such trust also produces certain vulnerabilities, and the fear is that trust could be misused by foreign or commercial interests. This is one version of trust we have identified (so far) that partially overlaps with and in other ways is very different from trust as it is articulated and constructed within the field of cryptography.

Privacy and trust in cryptography

Cryptography is a branch of mathematics and computer science that develops techniques to *encrypt* communication and prevent others from capturing it by the use of code or cipher and to *decrypt* the secret communication of others through cryptanalysis. Encrypted military communications date back to ancient Egypt, Greece, Persia and Arabia, and

numerous war victories are attributed to cryptographers' codebreaking. Perhaps most well known today, is the British cryptanalytic effort at Bletchley Park during the Second World War that broke the German Enigma machines (Fig. 5) and allowed Britain and its allies to intercept Enigma-encoded messages.[3]

During the cold war, cryptographic techniques were classified as 'munition' by most governments. Since the 1970s, the spread of personal computers and the development of the Internet have constituted a challenge for defence systems' control over encrypted communication. In 1978, mathematicians and computer scientists Ron Rivest, Adi Shamir and Leonard Adleman stated: 'The era of "electronic mail" may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are private, and (b) messages can be signed' (cited in Hellegren 2017: 292). They developed public key cryptography and the RSA (Rivest-Shamir-Adleman) algorithm that built these two capabilities into email systems. These developments have been fundamental for encryption and authentication in today's Internet. Encryption could no longer be seen as solely an issue of *security* and the protection of sovereign states' secrets and interests, but was also used to protect citizens' *privacy* and freedom from state and other interference. This change ushered in a new work ethos for cryptographers. The proliferation of the Internet extended security issues to private companies' business secrets and the protection of citizens' private data in all kinds of electronic communication.

In the decades that followed, a battlefield, including the so-called 'crypto wars', opened between governments and intelligence agencies who wanted to restrict civilian use of cryptography and maintain their back doors into encrypted communication. A rising civilian movement of Internet rights activists, hackers (Levy 1984) and cypherpunks (Hellegren 2017) saw the development and spread of encryption software as a way to safeguard the human right to freedom of opinion and expression (Fig. 6). In May 1992, the cypherpunk movement started with a mailing list and the declaration of 'A cypherpunks manifesto'. It has since developed into new initiatives, such as the whistle-blower organization WikiLeaks and hacktivist groups such as Anonymous (Fig. 7) (Coleman 2013). Common for these groups is that they do not trust state institutions, but see the Internet itself as a tool for accountability and transparency.

Even though the cypherpunk movement's technical tools can be traced back to the work of academic cryptographers, our interlocutors in the present project generally do not see their research as *political*. Most academic cryptographers see themselves as scientists, trained in the fields of mathematics, electrical engineering, physics or computer science, and, like many other scientists, they claim to be immersed in scientific problems that are framed as technical, not political.[4] They fear that political and ethical concerns will inhibit their scientific endeavours or impede scientific curiosity, arguing that uses and abuses of new technologies cannot be foreseen.

There are exceptions, and in the years after Edward Snowden's revelations, some cryptographers made public statements or expressed their ethical and political concerns in the crypto community.[5] In 2013, Arvind Narayanan, in a paper entitled 'What happened to the crypto dream?', bemoaned cryptographers' work on 'crypto-for-security' – the kind of cryptography that benefits commercial interests, e.g. to enable ecommerce – rather than on 'crypto-for-privacy' serving public ends, e.g. the kind of cryptography that is used for encrypted messaging and anonymous transaction systems (Narayanan 2013).

In 2015, Phillip Rogaway held the International Association for Cryptologic Research Distinguished Lecture with the title 'The moral character of cryptographic work'. As the invited keynote, it was expected that he would give a technical paper, but he had another errand. He warned the research community of becoming too inward-looking, and claimed that the biggest problem for cryptographers is neither working on 'crypto-for-security' nor on 'crypto-for-privacy', but on 'crypto-for-crypto'. He reminded the audience of the social responsibilities that scientists carry, such as those laid out in the Russell-Einstein manifesto and the Pugwash movement. He addressed a range of ethical issues, such as the question of military funding, a call to work for cryptographic commons and neutralizing the impression of cryptographic protocols through cute visualization (Rogaway 2015).

In proof we trust

The concepts, metaphors and visuals used in cryptography to explain different functions, protocols and algorithms are typically couched in warfare terms, which can be attributed to the discipline's military genesis. An entity that attempts to listen into encrypted communication or disturb it is called an 'adversary' or 'malicious party', often depicted as a little devil with horns and a pitchfork. Cryptographic protocols generally assume hostile disturbance and they are founded on mutual distrust.

In today's most widespread cryptographic systems, 'trust' is established in so-called trusted third parties, e.g. for the authorization of cryptographic keys and authentication of identities in the Internet. Rogaway describes the 'trust models' of these cryptographic systems as authoritarian and hierarchic, because powerful agents such as 'state-level adversaries' (e.g. intelligence agencies) can easily force access or build back doors into such systems.

MPC systems do not rely on trusted third parties. Instead, the information is fragmented or scrambled, then distributed among the protocol participants and finally computed upon. The data itself is never sent. For this reason, MPC is also called 'computation in the dark'. Not even powerful parties, such as nation states or cloud service providers, can gain access to the full data (Lapets et al. 2018). Adversaries, visualized as little red devils, are not kept *outside* the interaction by creating trusted third parties, but incorporated *in* the interaction itself (Fig. 8). Mathematical proof, not trust, forms the basis of privacy-preserving computations and communication.

MPC resembles bitcoin and blockchain systems in that it renders trusted intermediaries superfluous. We see these technologies as disruptive, with not just technical but also social consequences. Bitcoin is described as 'an electronic payment system based on cryptographic truth instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party' (Nakamoto 2008: 1). Instead of trusted authorities, both bitcoin and MPC rely on a network structure of peers who may remain anonymous and who do not have to trust each other. Regarding blockchain networks, Werbach notes, 'nothing is assumed to be trustworthy … except the output of the network itself' and '[w]hat makes a transaction valid are cryptographic proofs that the other party can verify mathematically. Hence the common saying, "in proof we trust"' (Werbach 2018: 29). Here we can see how the discourse of trust is not eclipsed, but new concepts of trust are coined, e.g. 'trust in numbers', 'trust in math', and 'trust in code' (Nelms et al. 2017: 21). Trust, or the role of trust in enabling privacy-preserving communication, is imagined to take place without trusted institutions. Instead, data privacy is believed to be guaranteed through algorithms that hide and scramble data in an environment of distrust, without any easy way to make the operations and flows of data transparent to the public or political institutions.

Final thoughts

MPC is not (yet) widespread, and unlike bitcoin, there are no evangelists or mystic founders that promote the technology and its underlying techno-libertarian revolutionary ideals. As one of our interlocutors regretted, MPC has not produced a 'killer application as blockchain technology has with bitcoin'. Even though MPC is a hot topic at cryptographic conferences and an emerging technology for start-ups, it is difficult to assess if MPC protocols, in their further developed forms, will become part of vital data infrastructures in the future. MPC has a lot of promise: if no one can see all the data in the system, then no one else can own it, control it, abuse it or make money off it, as the comment about 'some Chinese platform' in the Internet Week's debate warned. But if we use MPC protocols to keep our data safe and thus do not know whose data fragments belong to whom or to what data set, it is difficult to detect errors and to know who may be held responsible for mistakes or abuses. If no entity or institution can ever get a complete overview, then who can be held accountable?

So far, we have detected a disparity between political claims that public trust in data infrastructures is a necessary basis for their functioning and the trust models reflected in emerging cryptographic technologies based on distrust. The question is how the data infrastructures and cryptographic systems that underlie more and more of our communication and management of sensitive information produce new social and political relationships. If MPC is used to protect citizens' sensitive data, then which institutions can be held accountable – and how? Will globalized

data environments erode trust and the legitimacy of trusted, democratic institutions? Will cryptographic, these indeed *cryptic*, technologies afford and produce distrust? Cryptographic systems are imbued with undigested assumptions about social relations, society and societal institutions, including trust, that escape public attention and rarely interest cryptographers. By studying cryptography, its debates and uses as strategic fieldsites, anthropologists can disentangle and contextualize these assumptions and feed them into wider public and political debates about what data privacy, security and accountability could mean in a digital age. □

Footnotes

1. We wish to thank our collaborators in the SECURE (Secure Estimation and Control Using Recursion and Encryption) project at Aalborg University and at the Alexandra Institute in Aarhus for vigorous discussions and a thorough reading of and comments on an earlier draft of this article. All errors remain ours.

2. The discussion whether trust *can* in fact be eliminated is beyond the scope of this article. Such an idea may be naïve, which is already apparent in the widespread use of cryptocurrencies: even though they do not depend on banks, users often rely on cryptocurrency *wallets*, which are services that authenticate users, store their public and/or private keys, etc. – and thus have replaced other trusted third parties.

3. For other highlights in this colourful history of cryptography read Kahn (1996) or Singh (1999).

4. This, of course, depends on the notion of the political, and many cryptographers use and produce open source software and could be said to be part of the Free, Libre and Open Source Software (FLOSS) movement (Kelty 2008).

5. The 'crypto-community' is an emic term used by many cryptographers referring to the academics who meet regularly at the International Association for Cryptologic Research (IACR)'s conferences, the most important of which are Crypto, Eurocrypt and Asiacrypt.

References

Botsman, R. 2017. *Who can you trust? How technology brought us together – and why it could drive us apart*. London: Portfolio Penguin.

Broch-Due, V. & M. Ystanes (eds) 2016. *Trusting and its tribulations: Interdisciplinary engagements with intimacy, sociality and trust*. Oxford: Berghahn Books.

Carey, M. 2017. *Mistrust: An ethnographic theory*. Chicago: Hau Books.

Coleman, G.E. 2013. *Coding freedom: The ethics and aesthetics of hacking*. Princeton: Princeton University Press.

Corsín Jiménez, A. 2011. Trust in anthropology. *Anthropological Theory* 11(2): 177-196.

Danish Government 2016. *A stronger and more secure digital Denmark*. Copenhagen: The Ministry of Finance, Local Government Denmark and Danish Regions.

Gambetta, D. 1988. *Trust: Making and breaking cooperative relations*. Oxford: Basil Blackwell.

Hellegren, Z.I. 2017. A history of crypto-discourse: Encryption as a site of struggles to define Internet freedom. *Internet Histories* 1(4): 285-311.

Kahn, D. 1996. *The codebreakers: The comprehensive history of secret communication from ancient times to the Internet*. New York: Scribner.

Kelty, C.M. 2008. *Two bits: The cultural significance of free software*. Durham: Duke University Press.

Lapets, A. et al. 2018. Accessible privacy-preserving web-based data analysis for assessing and addressing economic inequalities. *Proceedings of COMPASS '18,* Menlo Park and San Jose, CA, USA.

Levy, S. 1984. *Hackers, heroes of the computer revolution*. New York: Anchor Press/Doubleday.

May, T. 1992. The crypto anarchist manifesto. Activism: Cypherpunks, 22 November. https://www.activism.net/cypherpunk/crypto-anarchy.html.

Misztal, B.A. 1996. *Trust in modern societies: The search for a base of social order*. Cambridge: Polity Press.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org, 31 October https://bitcoin.org/bitcoin.pdf.

Narayanan, A. 2013. What happened to the crypto dream? Part 1. *IEEE Security and Privacy Magazine* 11(2): 75-76.

Nelms, T.C. et al. 2018. Social payments: Innovation, trust, bitcoin, and the sharing economy. *Theory, Culture & Society* 35(3): 13-33.

Pink, S. et al. 2018. Data anxieties: Finding trust in everyday digital mess. *Big Data & Society* 5(1): 1-14.

Rogaway, P. 2015 The moral character of cryptographic work. Cryptology ePrint Archive, Report 2015/1162.

Singh, S. 1999. *The code book: The science of secrecy from ancient Egypt to quantum cryptograph.* New York: Anchor Books.

Werbach, K. 2018. *The blockchain and the new architecture of trust*. Cambridge, Mass: MIT Press.

Figures

Fig. 1. *Cryptographic protocol with a trusted third party. Trusted third parties are often visualized as angels, judges or weighing scales, the symbol of justice. Credit: Ignacio Cascudo Pueyo.*

Fig. 2. *Cryptographic protocol using MPC where all participants are connected to each other in a distributed system.' Credit: Ignacio Cascudo Pueyo.*

Fig. 3. *"Trust" (Tillid). At the Danish political festival called the People's Democratic Festival [Folkemødet] on the island of Bornholm, the trade union for the area of law, economic, politics and administration (Djøf) had set up a "trust booth". Credit: Astrid Oberborbeck Andersen.*

Fig. 4. *At the trust booth passers-by could finish the sentence "Trust in society will increase if we..." and then post their message in the trust mailbox. Credit: Astrid Oberborbeck Andersen.*

Fig. 5. *The original Enigma machine used by the Germans during WWII. Credit: School of Mathematics - University of Manchester/Flickr (Creative Commons).*

Fig. 6. *"Information wants to be free". Internet rights activists' slogan, often credited to Steven Brand saying it at a hackers conference in 1984. Credit: Pierre Selim/Flickr (Creative Commons).*

Fig. 7. *Guy Fawkes masks have become a symbol for the hacktivist group Anonymous. Credit: Pierre Selim/Flickr (Creative Commons).*

Fig. 8. *Cryptographic protocol using MPC with little red devils symbolizing dishonest parties. Credit: Ignacio Cascudo Pueyo.*