Good morning.

I am surprised so many of you made it to this **early after-party talk**. Its title sounds a little strange, so some of you are probably here out of curiosity – to see **what kind of talk this is**. Be warned: I will **ruthlessly exploit your curiosity** for some political propaganda.

First of all, there is nothing wrong with the slides. There are none. Instead of enjoying a PowerPoint karaoke show **I have to ask you to listen to me**. I hope no-one is embarrassed by this rather **ancient concept of a lecture**.

It is also somewhat unusual these days to talk about politics at a tech conference. **Politics** – very much like religion – is considered an **offensive topic** by many people. Talking about it is seen as an **invasion into private comfort zones**, a violation of the **code of conduct**.

Why can't our political discussions be **as committed**, even compassionate, as our discussions on software design? What offense can it possibly be to **say what you think**? I for my part will do just that in my talk, even if some are offended by some **harsh words and overstatements** I might use to make a point.

I am giving this lecture here because I believe that **political awareness is important** – especially in the "**our**" domain: technology. Although technology has become a **dominant mediator in societal change** – and therefore is **political by definition** – a lot of people seem to **disclaim** this fact.

But politics is not **quantum mechanics**: It happens even if you **choose to not look at it**. Ignoring it simply means **giving away power to others** that will shape all our future lives as they see fit. I hope **none of you** are willing to surrender the future **this easy** and that **you too** want to actively shape your own life, that of your community and even that of your society.

Because that is **what politics is about**: it is not about **left and right, a political dogma** or something like that – it is about **your** own ideas, **your** action arising from **your** answers to the questions of **power, property, privacy and public interest** – in real life as well as in cyberspace.

For me this was the primary reason to become a hacker some 40 years ago and to join the Chaos Computer Club a few years later. As you probably know, the Chaos Computer Club (CCC) is one of the **largest and oldest hacker communities** on planet Earth.

It was founded in 1981 by people who had been **politically active** in other places before. It was not by chance that the first meeting took place in the newsroom of a leftist newspaper in Berlin, sitting around a table that once belonged to "K1", a politically motivated commune formed during the student revolts in 1967.

It was precisely this **political approach** that distinguished the CCC from the countless other small computer clubs in Germany at the time. To be politically active means to actively engage in the development of a society, so it is always based on **hope, idealism and a vision for the future**.

So, what about politics…?

3/14

In the mid-80s, we had the vision that, instead of an "**information society**", we could create and shape an "**informed society**"; a freer society in which informational self-determination, decentralization, freedom of speech and information are no longer **marginalized demands** of some crazy geeks but **lived reality**.

This kind of hope for what we believe is a better future has been guiding the CCC ever since. But just because something has the **potential** to become reality, it does not mean that there is a **historical necessity** for it to actually realize in the future – or at least not exactly the way you hope for.

When we declared the computer and the emerging networks to be the **new medium for global communication** in the early 80's, we did not foresee that all this would lead to something like **Facebook, Google or Amazon**. Our mistake.

Yes, the computer can be an instrument of **free communication and access to information**, but the society does not necessarily change that way – and not on its own. And we made the mistake to underestimate the **powerful forces of the capitalist system** to appropriate "**our**" technology for **their** purposes.

As a **die-hard, old-school hacker veteran** I have a hard time accepting that the unspoken CCC dogma "**Information sets you free**" will not survive a reality check because **surveillance capitalism profitably uses the anti-thesis as its business model**.

Even though liberated information – commonly referred to as **leaks** – has given us all a deeper insight into the **global political and economic systems** in recent years, it seems to me that the development of our society **hasn't changed much track** the way I would like to see it.

Maybe this sounds a bit frustrated, but I have **not resigned yet**. Some years ago, on one of the **hacker conferences** of the CCC (with tens of thousands of hackers from all around the globe) there was a much debated talk called "**We lost the war**" – a rather bleak report on how we failed **big time** in our fight for a better future.

I don't think we lost the war, but we **lost a lot of battles** even if **did win some** – but the fight for a better future is not over yet. But there are **new battlefields** now. New arenas suddenly appear whenever a new **disruptive technology** emerges out of the blue.

These places are peaceful and creative environments in the beginning, as long as relatively few **like-minded people** are involved or exposed to the technology. This **grace period** will for sure end the day when **other, more established actors in society** appropriate and later advance the technology for **their own purposes**. That is the day the next battle begins…

After the personal computer and the internet, **blockchain technology** is one of these new arenas. It could be helpful for you to learn from the mistakes we as hackers made in the past. Because your grace period is long over and the battle in your arena is already waging, **just in case you haven't noticed it yet**.

Our biggest mistake was the **belief that technology will change the world by itself**. That it is sufficient to create a liberating technology, so that the liberation and self-determination of the people will follow suit as a **necessary consequence** of the mere existence of the technology itself.

But unfortunately that is not the case – never. It is not technology itself that changes societies, it is the **intentional use of technology in the self-interest of societal actors** that does. If you just create technology for its own sake, you have lost already – **more powerful actors** will take over and utilize your technology in their plans for the future.

So while we as hackers enjoyed ourselves believing that computers and networks are such **technologies of liberation**, they actually became **tools of slavery** in the hands of our adversaries. Big-data assets and machine-learning algorithms **under the auspices** of a capitalistic system **degrade us as humans to a commodity**. Facebook is not a communication platform, Google is not a search engine and Amazon is not a market place – these things are only means for the actual purpose: the **financial and informational exploitation of its users**. The resulting digitized human selfs are sold unrestrained to anyone who pays for them.

I think it is time to call these companies what they really are: **traffickers**. Our ideas of freedom and enlightenment through computers and networks have been **perverted by reality**.

Will this happen to the **blockchain community** too?

It for sure follows the **pattern described above**: Bitcoin was born out of a hacker / nerd / **cypherpunk** environment at a time that was politically very interesting.

It was the aftermath of the banking crisis of 2008 (which we have interpreted somewhat **naively and prematurely** as the **upcoming collapse of the capitalist system**). It was the time of **Occupy, WikiLeaks and Anonymous**.

Many people had the hope, albeit briefly, that they could change the society to something better…

Although the Bitcoin white paper did not mention politics explicitly, it is all but obvious that it was also a **political act**. The mistrust in centralized financial institutions and the self-empowerment of people denied access to the banking system were for sure of relevance to **Satoshi Nakamoto** – whoever he/she/they are. So hackers world-wide embraced the new technology (and its ideology) and started to play around with it.

But even during this grace period of Bitcoin (which lasted no longer than 2012 in my view) **fewer and fewer people** were seriously interested in the political aspects; purely technological questions dominated the discussions and drove the development.

But at the time when outside actors got involved the discussion quickly shifted towards only one question: How to **make money from Bitcoin fast** – the more the better. For these actors the technology itself is completely

irrelevant, as long as it fulfills its purpose (**making profit**), is reasonably safe and works reliable.

And the best of all: it comes for free. You can become a **major player** in this game without having to pay for the **means of production or a workforce**: it is all decentralized for you, so others pay for the hardware that works in your interest.

You might argue that because everyone can pursue his or her self-interest, Bitcoin (or blockchain technology in general) is basically democratic, even **egalitarian**. From my point of view this seems to be a rather **naive conclusion**.

Let us look at the term "decentralization". What does it mean? "**Decentralized Web**" is somewhat the slogan of this conference, so I guess you all have an answer to this question… It it all boils down to: "**What gets decentralized**?"

The answers I usually get at tech conferences are focusing on the technical aspects like network governance, hardware, computing power and soon dive into the depths of protocols, consensus mechanisms and the like. Is that the kind of decentralization the hacker movement **propagandized for in earlier times**?

If we consult the **Hacker Ethics**, the moral guardrail of the CCC from the mid-80's; point 3 of it reads: "**Mistrust authorities – promote decentralization.**

So it is all about the **decentralization of power. Nothing else.**

But what **power is distributed by the blockchain** technology? Just one – the **control over the network**. No single entity should be able to manipulate the blockchain in its own interest. This issue covers a **major part** of the initial Bitcoin white paper, because it is a **decisive point**. And it still is an important issue.

Most people in the blockchain community are confident that the technical design is solid and that is more profitable for miners to **play by the book** than trying to **manipulate** the blockchain. **I agree with them**: In this sense the blockchain is a technology that successfully decentralizes network control into multiple hands.

But is that all the power that **plays out on the blockchain**? Certainly not. Like the internet, that took ten years to develop from a nerd-playground to the beginning of the **surveillance capitalism**, blockchain also took some ten years to show first signs of some kind of **blockchain capitalism**.

Just as other peer-to-peer networks before, for example the Bittorrent network, it is now invaded by "**leechers**" (a more appropriate word for traders and fund managers) – people sucking the juice out of the infrastructure (and other people of course) **without contributing back to the common good**.

The design of other P2P networks like Bittorrent or GNUnet at least has controls to punish **leechers** for example with **lower download bandwidth or limited access** to other network resources, but I see **not the slightest**

technical safe-guard in the design of the blockchain to prevent similar "**misbehavior**". Why not?

Some of you might not even understand **why I ask this question at all**, because you can see no misbehavior in exploiting the technology in self-interest. Blockchain is a liberating technology after all, setting everybody free to make as much money as they can. **It is all about this freedom, isn't it?**

As someone with a different anarchistic mood I can't agree. In this **libertarian interpretation** of "freedom", where everyone is "free" on his or her own, history teaches us that the **worst human traits will prevail**. Greed and selfishness can easily tear the **fabric of society** apart.

It would result in the complete opposite of an **anarchistic society** which strives to eliminate forced social relations by decentralization, and therefore **gradual, eventually factual** elimination of power.

But the blockchain origins are somewhat deeply rooted in this **libertarian ideas** cultivated at the West Coast of the USA, and I don't even dare to ask how many in the blockchain community have read and are inspired by books written by **Ayn Rand**.

So maybe I shouldn't wonder that the design of the blockchain technology does not prevent an **accumulation and concentration of capital** in the **hands of a few**.

In the end it is quite possible that the fate of the blockchain technology is to be an **instrument of concentration and consolidation of power**, and not that of the promised decentralization of power.

The new market mechanics of Bitcoin already make it nearly impossible for people without access to the banking system to get involved. And the **established high finance actors**, who's authority and control the original Bitcoin design strives to overcome, are **emerging as the winners** – and not the losers.

With these new players comes a **new spirit** to the blockchain community that is not just concerned with the **use of the existing** technology, but also **exercises influence** on future developments. These new actors have the means and the will to tailor the technology to their **particulate needs and beliefs**.

For me the most striking evidence for such an **ideological shift** happens in the **distributed consensus protocol** discussions. An obvious place because that is where the rules of **network governance** play out – a power play so to say.

I understand that the "Proof-of-Work" approach has its disadvantages the way it is implemented: It is wasting precious energy, while doing nothing useful. And of course it is not egalitarian, because your chances to win a block are directly related to your **existing financial and technical resources**.

Why can't someone come up with a "Proof-of-Work" concept that also **does something useful for the common good** like folding DNA molecules for medical research or searching for extraterrestrial signals in radio telescope data?

This way at least the miners would start to **contribute back to society**, while still making reasonable profit. But the times when miners were the **most profitable** group on the blockchain are coming to an end anyway; revenues are more and more generated by speculation and high-frequency trading.

So it appears even logical that network governance moves away from the "Proof-of-Work" towards the "**Proof-of-Stake**" approach. It seems to be the more natural fit for this changing environment, where the relevance of **running the system** becomes subordinate to **exploiting it**.

Whenever stake is expressed in something that can be **transferred and therefore monetized**, I can understand why it is so highly appreciated by the **apologists of blockchain capitalism**. It mirrors a belief deeply rooted in **classical industrial and financial capitalism**, that it is a law of nature for money to recreate.

I can see no way that this will not lead to higher concentration of power. It is **history repeating**: big money is making profit, small money is **fair game** and the "**have-not**"s? Who cares…

And in case the scheme **blows up again**, we can be sure that the losses will be **socialized**.

For those of you who help to develop and advance the blockchain technology and who share my **discontent with the way things evolve** in this arena, I have some final thoughts. We need to ask ourselves to what extent we are **complicit in this development**?

As technophile nerds, we tend to think too little about the possible negative consequences of the things we create in software and hardware. Especially a **pure fascination** with the technical possibilities will make us the **bailiffs** of those we deeply disprize by heart. Unfortunately, there are plenty of good examples for this mishap:

The scientist who developed the algorithm to reconstruct the five **OCEAN personality traits of a person** from just a few Facebook likes was not thrilled that his work was used by Cambridge Analytica to **influence voters** in the 2016 US presidential election campaign.

He was probably not thrilled that his next algorithm, which can classify the **sexual orientation of a person** from just a few different photos, will probably be first used in Saudi Arabia. I myself was not thrilled when I learned in the mid-90s that my research on computer viruses had being used by the German intelligence service for espionage and sabotage on East Block mainframe computers.

Sometimes we simply forget to ask ourselves the question, "**What vision of a better world drives me to create this technology**? And how will the technology help to realize that vision?"

But maybe this question is too personal to be helpful. We certainly will **not agree on a common vision** for a better society – and that is a good thing because it allows for **vivid discussions**. But we could ask ourselves questions of a more fundamental nature, which could be a common starting point.

The **political question** is first of all a **question of power**, and in our technological world computer technology is a **system-relevant** instrument of power. For every development, for every algorithm, we have to ask, **"Whom empowers this technology - and whom can (or even should) it incapacitate?"**.

At least the second question is for sure controversial: Should we **even consider** creating a technology that incapacitates people? Isn't that a 180° turn from our ideas of a **liberating technology**?

Many in the **Free Software** community suffer great pain, when they see photos from **drone command centers** of the US Army. Many of the displays show that they are running **GNU/Linux**. But the Free Software License does not – and probably **even can not** – restrict the use of free software in the killing of people.

So can or should a blockchain technology be different? **Yes, it can**. And from my point of view it **also should**. I imagine even Satoshi Nakamoto would agree.

Just remember that Bitcoin was designed with such a **restriction as its foundation**: Its decentralized approach **incapacitates** people that want to

censor or take over the network. Their **freedom** to do what they want gets limited by t**echnical safe-guards**. I would love to see projects in the blockchain community working to extend this basic principle to higher levels of the stack.

We **need to move** from the technical question "**Who controls the network**?" to the socio-political question "**Who controls what is happening on the network?**". I think it should be us to have an influence on the answer – and we have **the capabilities and the means** to make it happen. "**War is over if you want it**"…

Am I talking about **censorship** here – as a hacker? No, I am talking about the **extension** of our ideas on network governance into the realms of society. It is our right – no, it is our **obligation** to define the consensual rules we want to be enforced in our society and be implemented in software. Remember: "**Code is Law**".

Don't repeat the biggest mistake we as hackers made in the past; to believe that technology itself will change the world to the better. It will not. As long as we are distracted by the technical details and don't ask the political question, others will set the rules of our society on their terms. Don't let it happen…