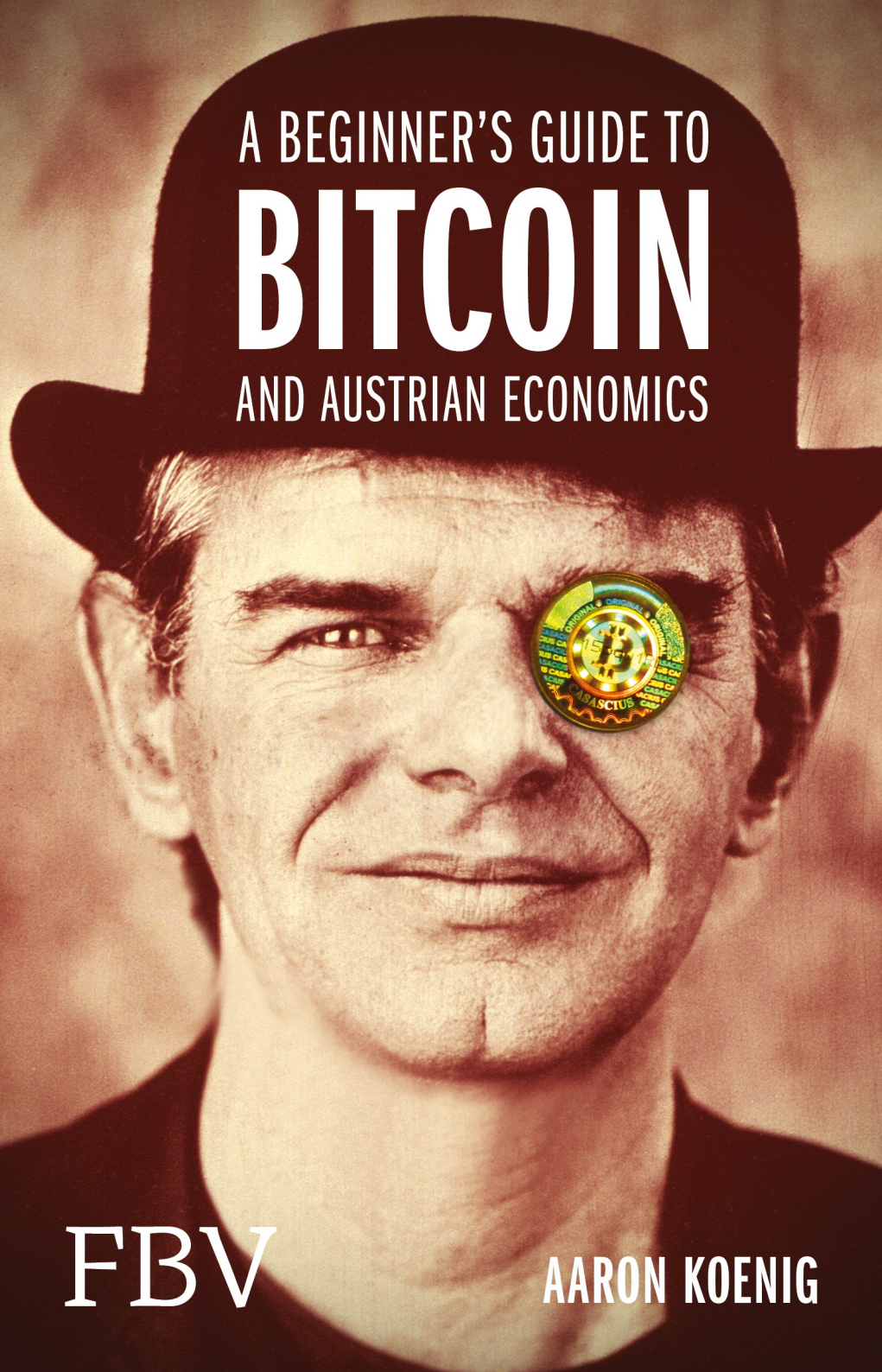
A BEGINNER'S GUIDE TO BITCOIN AND AUSTRIAN ECONOMICS



FBV

AARON KOENIG

A BEGINNER'S GUIDE TO
BITCOIN
AND AUSTRIAN ECONOMICS

Aaron Koenig is an entrepreneur, consultant, writer and film producer, specialised in Bitcoin and Blockchain technology. His company Bitfilm creates short commercial films for clients, most of them Bitcoin and Blockchain start-ups. Find out more at www.bitfilm.com

FBV

English version supported by
coinsilium

The Deutsche Nationalbibliothek
Lists this publication in the Deutsche Nationalbibliographie; detailed bibliographic information is available online at **http://d-nb.de**.

1st edition 2016

an imprint of the Münchner Verlagsgruppe GmbH
Nymphenburger Straße 86
D-80636 München
Tel.: +4989 651285-0
Fax: +4989 652096

The information and opinions have been compiled or arrived at based upon information obtained from sources believed to be reliable and in good faith, but is not guaranteed as being accurate, nor is it a complete statement or summary of the securities, markets or developments referred to.
The information mentioned is not intended to be construed as a solicitation or an offer to buy or sell any securities or related financial instruments.
The details and opinions are provided without any guarantee or warranty and are for information purposes only.

Proofreading: Hella Neukötter
Jacket design: Aaron Koenig
Image on the cover: Marcin Dzieniszewski
Composition: inpunkt[w]o, Haiger
Printing house: Books on Demand GmbH, Norderstedt
Printed in Germany

ISBN Print 978-3-89879-963-8
ISBN E-Book (PDF) 978-3-86248-875-9
ISBN E-Book (EPUB) 978-3-86248-877-3

Further informations are available at

www.finanzbuchverlag.de

Contents

Foreword by Rick Falkvinge

Bitcoin, like file sharing before it, the Internet before it again, BBSes, and indeed computers themselves before that again, has been seen as something unworthy, largely because it was the domain of tinkers, geeks, and makers.

A Beginner's Guide to Bitcoin and Austrian Economics is a good book to start understanding why Bitcoin is as important as the internet, as important as computers, and as important as sharing. If not more important, significantly more. Bitcoin builds on top of all of these, and while computers and the Internet challenged whole classes of industries, no technology before Bitcoin has had the power to challenge nation-state governments as a concept.

Yes, it's that big. This book will outline why and how, in broad strokes of the brush.

In 2006, when it was all about file sharing challenging the copyright industry, I made a prediction in front of

an entrepreneur crowd: Any company that builds its business on the idea of preventing people from sharing interesting things with their friends will not survive. A company that tolerated it would survive. But to really thrive in the coming environment, I explained, a company would need to absolutely depend on people sharing interesting things with their friends, at complete odds with the then-dominant distribution monopoly model.

A mere decade later, Facebook has built a business ten times the value of the record labels by encouraging people to share everything they touch with their friends, and Spotify, Pandora, and Netflix are eating the breakfast, lunch, and dinner of the copyright industry's old model.

Bitcoin's disruption will be far greater. Not just in how it changes behavior and entertainment patterns, like Pandora and Netflix do, but in how it enhances the understanding of the nature of money itself. For the first time, using money will lead you to ask some very pertinent questions about the nature of the money you're using, and all of the answers to those questions are incredibly embarrassing to the old world.

The first obvious question is "where does a Bitcoin come from?". And in order to understand that, you need to juxtapose the answer with the origins of a euro, a dollar, or a yen. That's when you gradually come to understand that banks have had the power and the right

to conjure money out of thin air and lend it out at interest, and are using this power to speculate between them on the value of residences, via mortgages.

If people in general understood this, there would be riots.

In contrast, Bitcoin's value is in its predictability. Nobody can start the printing press and hyperinflate you out of your savings. For as history tells us, a government will always save itself first. Many people cried in Greece and Cyprus as they naively thought that money deposited in the bank were somehow theirs. The lesson learned – that money deposited in a bank is the bank's money, which the government can and will confiscate if it desires – was expensive, dire, and hurting to many.

With Bitcoin, money is completely yours. Not the bank's, not the government's, not the central bank's. It has been issued through a common agreement on what constitutes money, which means a government can't point a gun at somebody and tell them to change the agreement. This, in itself, is profound.

With real ownership of money, there will also inevitably be a better understanding of market economics. If your previous money was subject to planned economics – which was the case with a central bank – and you're now holding market-economy money in your hands, and you

discover that it brings both power and understanding, it's easy to start applying that understanding to other fields of the economy. This book does a good job of introducing those concepts and their place in history; even how Bitcoin conceptually was wished for as a "government-independent, market-driven form of money" by thought leaders of the Austrian economic school, long before it was technically feasible.

The greatest power in society comes from holding the ledger. The accounting master copy. Being able to dictate true from false. Being able to interpret – and change – who owns what. Nation-state governments have not just held this right, but have taken this right by use of force – and applied it by use of force. The Bitcoin technology revokes that contract and brings the ledger back to a common understanding, where no government can change who owns what, no matter the force applied.

In this way, governments stand to lose their major enforcement mechanisms – and also access to their primary revenue streams, as merchants increasingly turn to Bitcoin to circumvent the expensive banking system, for purely commercial reasons.

This is just touching the surface of the changes that Bitcoin will bring. To really understand the power shift underway, one can observe that today's wealth holders are

the heirs of the oil barons of the 1850s. Those wealth holders are directing research and development toward the same things as ever: new transportation lanes, better fossil fuel engines, carbon extraction. When Bitcoin takes off, those who took all the risk and were early into Bitcoin will take the new throne of primary wealth holders, superseding the oil heirs.

What research will be funded by that new class of wealth holders? It won't be a better diesel engine. It won't be a marginally better undersea gas pipeline. More likely, it will be the end of global poverty through Austrian economics, terabit-per-second Internet connections, space exploration, enhancement of the senses, and next-generation power plants of all kinds.

It will be a new frontier entirely.

Rick Falkvinge is the founder of the first Pirate Party and campaigns for sensible information policy. (Image by Anna Troberg)

Introduction

In his 1976 book *The Denationalization of Money*, Nobel Prize laureate Friedrich August von Hayek called for the abolishment of the state monopoly on money and the introduction of freely competing currencies. At the time, such a free money market was virtually unimaginable.

The world has changed significantly since 1976, when only the US military and a few scientists used the Internet. Back then, computers were the size of wardrobes and were rarely used outside of large companies or government agencies. Only a few crazy, free-thinking hippies such as Steve Jobs and Steve Wozniak envisioned a world in which personal computers were a common possession – in fact, Jobs and Wozniak founded Apple the same year Hayek released his revolutionary book.

The Austrian School of Economics, of which Hayek was a member, was nearly forgotten in the mid-70s. Today, this school of thought favoring the free market and rejecting government interference with the economy has gained significant popularity, most notably among young people. The fact that only the Austrians

had predicted both the economic crisis of 1929 and the one of 2007–2008 correctly has surely contributed to this renaissance.

We are now able to harness to power of the Internet, peer-to-peer networks and cryptography in order to realize Hayek's vision of money separated from state. But why does it matter? Why shouldn't we allow states to create money? And how can a stateless monetary system be implemented?

These are the questions I seek to answer within this book, which focuses on what is by far the most popular and successful stateless money project: Bitcoin, a digital payment system and currency. But Bitcoin is just the tip of the iceberg. Satoshi Nakamoto, Bitcoin's inventor, has successfully created the first payment system that works without a central institution. It has no single point of failure and as a result it is impossible for governments to forbid or eliminate its use.

Governments and banks may not like it, but they are powerless in the face of this new financial force. The clever ones among them will try to cope with the changes decentralized money brings, and to exert as much control over the system as possible.

Even if they succeed in this, the genie is out of the bottle. There are already hundreds of decentralized

currencies built upon the same principles introduced by Satoshi Nakamoto. It may not be Bitcoin itself, but one or more of its successors who will win the competition and end the era of centralized monopoly money.

Furthermore, the Blockchain technology upon which Bitcoin is based can be utilized for many purposes beyond payments. It can replace any kind of public register, be it for land ownership, companies or marriages. Whenever humans need to keep records of any kind, they can now do so on the publicly available, immutable Blockchain. Governments are no longer required to act as middlemen and gatekeepers.

This invention has the potential to change the world even more so than the Internet. Many people have yet to recognize this. They still see Bitcoin as a kind of toy money for geeks. You hear the same silly prejudices and handwringing about Bitcoin that you heard about the Internet in the early 90s. If you fell for the media hype back then or were simply too young to jump on the Internet bandwagon, then don't miss the next great technological development and the many opportunities it brings. It pays to know the basics of Bitcoin. And you don't have to understand any cryptographic algorithms to use it – or do you think about the TCP/IP protocol when you surf the net?

This book explains the phenomenon of stateless, decentralized money for people who are more interested in economics and politics than in computer science and mathematics. Its main focus is the relationship between Austrian Economics and digital currencies like Bitcoin. Luckily, you don't have to be an economist or an Austrian to read it – everything will be explained in plain English.

You will find some practical tips in the info boxes. Interviews with Bitcoin insiders provide you with personal insights into the world of digital money.

We will begin by traveling to a country where people are likely more open to Bitcoin than anywhere else in the world, a place that has experienced all the evils of financial tyranny and the struggle that it comes with.

INTERVIEW

ROGER VER

Tokyo

What fascinates you about Bitcoin?

Thanks to Bitcoin, for the first time in the history of the world, anyone can now send and receive any amount of money with anyone else. It doesn't matter where they were born, where they are a citizen, where they live, or what color their skin is. Anyone can participate without requiring permission, and there is nothing, even governments, can do to stop it. Bitcoin is a platform that allows permission-less innovation.

How did you get involved with Bitcoin?

I spent my youth studying economics and using computers. When I heard about Bitcoin on *www.freetalklive.com's* radio show, I fell in love with it as soon as I understood the characteristics.

What are your activities now?

I was the first person to start investing money into Bitcoin related startups. I created the first website (*Bitcoinstore.com*) with a wide range of products, that could be purchased in Bitcoin. From 2011 to 2014 I ran national radio ads promoting Bitcoin, and put up several billboards promoting Bitcoin in Silicon Valley.

I did everything I could to get more people to understand how amazing the Bitcoin technology is. As of January 2015 I am an investor in over a dozen active Bitcoin related startups, so I spend my time helping them and Bitcoin as a whole gain more traction in the world.

What are the most important use cases of Bitcoin as money and payment system?

I'm most excited about seeing Bitcoin used in instances where the state is violently interfering in the peaceful interactions of others.

What has to happen for Bitcoin to gain mainstream adoption?

We are currently seeing all the pieces of the puzzle coming together to bring Bitcoin to the mainstream:

1. Easy to use and secure wallets.
2. Easy to use exchanges, accessible to all.
3. Merchants directly accepting Bitcoin.
4. Businesses paying bills and employees with it.

All of those are happening, but still will require some more time and work.

Where do you see the biggest obstacles for that? How can they be overcome?

The biggest obstacles will be legal issues. Hopefully they can be overcome via education on both economics and morality.

What else can be done with Blockchain technology? Which useful applications can you imagine?

In the short term, I'm excited by distributed apps. Uncensorable versions of social media, and financial platforms will be interesting. Eventually we will see uncensorable computing platforms. It is hard to even imagine what interesting and creative things will be enabled with this.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

Bitcoin and Blockchain tech will create a separation of money and state. This will lead to a vast increase in the world wide rate of economic growth. It will lift billions more out of poverty. It will likely bring an end to wide spread wars because governments will no longer have a way to finance them. In the end, I think it will make the world a much more productive and peaceful place.

How do you imagine the world after Bitcoin and Blockchain technology have gained mainstream adoption?

I envision a world with much less institutionalized coercion. People anywhere on the planet will be able to interact with anyone else, without requiring the permission of any government.

1. La Revolución Bitcoinista

Bitcoin in Argentina

"*Cambio, cambio, cambio*" – you hear it all over the pedestrian area of central Buenos Aires, where money-changers stand at every corner. Buying dollars, euros and other foreign currencies is strictly regulated in Argentina. If Argentinians want to officially change pesos into dollars through their bank, they need to prove that they intend to travel abroad and submit their tax return before completing the exchange. Even after submitting proof, they are only entitled to limited amounts

of foreign currencies. As a result, the black market for dollars and euros is flourishing.

Bitcoin is popular in Argentina

Argentinians don't call this free market *black*, but *blue*, which is Argentina's national color. Although exchanging dollars on the free market is officially illegal, Argentinians do it anyway. The *Blue Dollar's* exchange rate is posted across websites and discussed in the finance pages of major newspapers.

Inflation and Frozen Accounts

Argentinians have a variety of reasons for their distrustfulness of the ever-devaluing peso, in their government, and in banks. To save money, Argentinians prefer to

buy dollars on the "blue market" and hide them in their house – it would be unthinkable to leave large amounts of money in a bank account.

The memory of the 2001 *Corralito* ("the little corral") is still fresh. During the *Corralito*, bank accounts were frozen for nearly a year and only small amounts of money could be withdrawn. Then, the peso was massively devalued, and as a result people lost significant portions of their personal savings. Similar measurements of capital control were applied in Cyprus 2013 and in Greece 2015. But while Europeans may still consider this to be out-of-the-ordinary, Argentinians have come to expect such behavior from their banks and governments. They have suffered repeatedly through hyperinflation, government defaults and currency devaluations.

In the late 19th and early 20th century, Argentina was one of the richest countries in the world, blessed with natural resources, fertile soils and a rapidly growing immigrant workforce. *"Rico como un Argentino"* ("rich as an Argentinian") was a common Spanish expression. But for decades the country was ruled by socialist politicians who ruthlessly tampered with the economy, and as history is teaching us again and again, even a naturally rich economy can be run down by socialist experiments.

It is no coincidence that the Bitcoin scene in Argentina is one of the most vibrant in the world. Money that

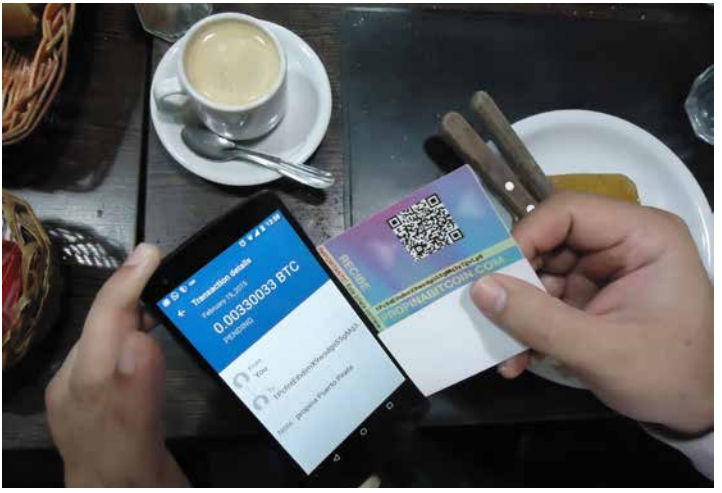
cannot be manipulated by politicians and which works without banks – you don't need to explain to an Argentinian why that is a good thing!

The *Espacio Bitcoin*

The Espacio Bitcoin in the center of Buenos Aires

Not far from the "blue money changers," in a major location of central Buenos Aires lies a four story building with 500 square meters of rentable space: the *Espacio Bitcoin*. Many Bitcoin startups have their offices here, and many meetups and public lectures on digital currencies take place in its meeting hall. On the ground floor there is a pirate-themed restaurant where waiters wear red bandanas and black vests, and where you can pay for your meal in Bitcoin.

"In the US, the restaurant owner would probably change his Bitcoins into dollars right away," says Rodolfo Andragnes, one of the founders of *Espacio Bitcoin*. "But here, he prefers to keep them. The Bitcoin price may go up and down, but with the peso you can be sure it will only lose value."



Paying with Bitcoin at Puerto Pirata

Rodolfo scans a QR code on the screen of the restaurant's POS. One more click and the Bitcoins for a steak with french fries are on their way.

The founders of Bitcoin Argentina at Puerto Pirata

"I pay with Bitcoin wherever I can," says Rodolfo, who had registered the domain name *bitcoins.com* in 1998, ten years before the invention of Bitcoin. In 2012 he sold the domain to Mt. Gox, which at the time was the leading Bitcoin exchange – the deal was made in Bitcoins, of course. Rodolfo is adamant that he has nothing to do with the invention of the digital currency, and that he has never met its creator Satoshi Nakamoto.

But today he is one of the most active evangelists of the digital currency in South America. He is the co-founder

of Bitcoin Argentina, a nonprofit organization that promotes Bitcoin. Rodolfo is also one of the organizers of the Latin American Bitcoin conference, which took place in Buenos Aires in 2013 and in Rio de Janeiro in 2014. The 2015 edition will be in Mexico City.

Public meetup at the Espacio Bitcoin

"I want my kids to grow up in a world without the fear of inflation or frozen bank accounts," he explains. Rodolfo and his co-founders in *Espacio Bitcoin* and *Bitcoin Argentina*, Diego Gutiérrez Zaldivar and Franco Daniel Amati, met in early 2013 at one of the first Bitcoin meetups in Buenos Aires. Only a few months later they organized a top-notch conference with a number of international speakers.

"At *Espacio Bitcoin* many Bitcoin startups work next to each other, so one can exchange ideas and experiences and cooperate on projects," explains Diego, who founded his first Internet company at the age of 16. "We also organize public talks and get-togethers in our event room – and we have great parties and barbecues on our spacious roof terrace."

Franco Daniel Amati and Rodolfo Andragnes at the Espacio Bitcoin

Hot Spot Buenos Aires

Seven Bitcoin companies are currently based within *Espacio Bitcoin*, including the Latin American headquarters of US payment provider Bitpay. With a $30 million investment and more than 50,000 clients, Bitpay is one of the biggest players in the Bitcoin industry. Most of its software is being developed in Argentina, where salaries for highly skilled developers are much lower than in the US or Europe. Buenos Aires is undeniably one of the hot spots for the global Bitcoin economy. While the advantages of Bitcoin are not widely understood in the US or Europe yet, Argentinians know the flaws of the current monetary system from first-hand experience.

"In the times of the *Corralito*, many people lost a lot of money, including my family," says Diego Gutiérrez, who runs an investment fund for digital currencies. "You could feel a great sadness everywhere, and the aftermath is still present. That's why people here are more open to alternatives to banks and government money than in countries where people cannot remember the last national bankruptcy."

Bitcoin growth rates in Argentina are significantly higher than in the US or Europe[1], yet in absolute figures the number of users is still quite low. As always, innovation takes a while to prevail. For Argentinians, dollar bills under the mattress are still the most popular way to

save money. But the more desperately the government tries to prevent illegal dollar trade – even using specially trained dogs to detect cash at border controls and airports – money that can easily be moved across borders becomes more and more attractive to defend yourself against financial tyranny.

Bitcoins for Pesos

The Obelisque in the center of Buenos Aires

In a café close to the *Obelisk*, one of the landmarks of the Argentinian capital, Dante Castiglione meets up with clients who want to change Bitcoins for pesos.

"I started a software company that accepts Bitcoin, and when we tried to sell some, we found out that there is a huge demand," explains Dante. "So we decided to professionally trade Bitcoins, and the business is running really well."

A customer (who wants to stay anonymous) shows up with a typical Argentinian delay. They agree on a price: the current Bitcoin rate on the Slovenian exchange Bitstamp. Using a Bitcoin app on his cell phone, Dante scans a QR code with the customer's Bitcoin address shown on his cell phone screen. A few seconds later, both parties are notified that the Bitcoins are on their way. To be sure that the transaction is irreversible, they would have to wait about ten minutes, the average time of the Bitcoin network to confirm a transaction. But the customer is in a hurry, they know and trust each other, so he counts some used 50 peso bills into Dante's hands and leaves.

"I don't want to miss the train," says Dante, who runs his Bitcoin exchange together with his son and daughter. "The amounts we are trading are still small compared to the classical finance industry – but Bitcoin will be huge, I am sure about that."

Liberty on the Calf

The setting: a bar in the trendy Cañitas district on Tuesday night. The libertarian group *Liberty on the Rocks* meets up here to discuss politics, cryptography and Bitcoin. The overlap between the Bitcoin scene and the libertarian community is big, in Argentina as well as in other places. Libertarians align themselves against governmental interference with the economy and fight for a society that is built on voluntary relations rather than forceful ones. Free market money like Bitcoin fits well into this worldview. Franco Amati from *Bitcoin Argentina* is also a co-founder of the Libertarian Party of Argentina, and he organizes this monthly meetup in the Bar *Röt* (German umlauts are hip and exotic in Buenos Aires), which expectedly accepts Bitcoin.

Most of the participants are male, but instead of shaking hands they kiss each other on the cheek, as is custom in Argentina. Many of the group's members also belong to the Libertarian Party, which ran for local elections for the first time in 2013. After a short talk on the uses of cryptography in daily life, there is a casual discussion about promoting libertarianism in Argentina over mojitos, beers and burgers.

Franco Daniel Amati sporting a "Freedom" tatoo

"We want the government to stop tampering with the private life of the citizens and the economy," says Franco, who used to work as a system administrator, but now lives on his early investment in Bitcoins. "Unfortunately in Argentina the faith in government is still strong, although we should know better."

The Libertarian Party performed OK in their first election, but they did not get enough votes to enter parliament. The hurdles to participate in the national elections are much higher, so it is unlikely they can even take part. But no one in the group is seriously interested in a career in politics anyway.

"We mainly founded the party to make libertarian ideas more popular," says Franco, who has a huge tattoo with the old Sumerian word for liberty on his calf. "But now I find it much more exciting to build up the necessary tools to expand individual liberty for anyone as much as possible. And that includes using a monetary system that works without banks and governments."

Bitcoin is an on-ramp to libertarianism for many young people. A fascination for open source software, cryptography and digital money inspires many to dig deeper into the basics of the monetary system. Sooner or later they discover the groundbreaking works of Austrian economists like Ludwig von Mises and Friedrich August von Hayek.

"I had been interested in using cryptography to protect my privacy for some time," Franco recalls. "When I heard about this new form of money that is based in cryptography, I got curious right away."

Franco had read the classic texts of the Austrian school before he discovered Bitcoin. For many Bitcoiners, it's the other way round. But where does this significant overlap between the Bitcoin scene and Austrian economics stem from? Why are today's digital natives fascinated by thinkers who grew up in the Austrian-Hungarian Empire of the 19th century?

INTERVIEW

STEPHANIE MURPHY

Manchester, New Hampshire

What fascinates you about Bitcoin?

The most fascinating thing about Bitcoin for me is that it's money we can use without permission from anyone else. It's crazy the amount of restrictions that are imposed on bank accounts, PayPal, even cash. You can't deposit or withdraw over certain amounts. Everything you do financially can be tracked and reported to the government. If you have too much cash you are considered suspicious and storing it yourself is viewed as dangerous. You can't send PayPal to dozens of countries from the US. I can't believe it took until within the last decade for the world to have money they can use without these arbitrary controls and restrictions.

How did you get involved with Bitcoin?

In 2011 I was listening to the libertarian radio show Free Talk Live. Gavin Andresen, the lead core developer of

Bitcoin at the time, was a fan of the show also and he convinced the two main hosts, Ian Freeman and Mark Edge, to start using Bitcoin and talking about it on their radio show. Lots of people called in with questions about it and they were hashed out on the air in the following months. Libertarians started using Bitcoin right away because they immediately understood that it was government-free money and got excited. People around where I live in New Hampshire started using Bitcoin to buy and sell things – mostly food – and started using Bitcoin to tip their favorite bloggers and podcasters. I got my first Bitcoins that way, as donations for podcasting. Once I started to use it, I was hooked. I think the first thing I ever bought with Bitcoin was a bacon weave sandwich.

What are your Bitcoin-related activites now?

I host a popular podcast called Let's Talk Bitcoin (*letstalkbitcoin.com*) with Adam B. Levine and Andreas Antonopoulos. In 2014 I traveled to dozens of Bitcoin conferences and interviewed Bitcoin luminaries from all over the world. I also spoke at several conferences about Bitcoin. I always try to carry a little bit of Bitcoin on my phone so I can help someone who wants help to set up a Bitcoin wallet and send them a few dollars worth of Bitcoin. I am a voice actor and I have my own

online business, where I have many clients who pay me for voiceovers with Bitcoin. I always offer those clients a discounted rate because it is so much easier to deal with Bitcoin than with fiat money.

Why do you do this?

Bitcoin makes my life way better and I want to tell other people about it so that they can share in the benefits. Also, I don't want the government to control money. The future is peer to peer and I hope the world is moving away from top-down, centralized control.

What are the most important use cases of Bitcoin as money and payment system?

Being able to send money freely, even to politically unpopular or persecuted recipients. Sending money is a form of speech and speech should be free. Transcending national borders and national currencies. Being able to send money without revealing personal information like credit card details.

What has to happen for Bitcoin to gain mainstream adoption?

It has to be easier to keep secure.

Where do you see the biggest obstacles for that? How can they be overcome?

Security vs. convenience of access is a hard problem to solve in general. I don't really have a good answer. Maybe there has to be somewhat of a cultural shift – in a world where one can cancel a stolen check or reverse a fraudulent credit card charge, people get lax about their financial security. Bitcoin needs to be thought of and protected like cash.

What else can be done with Blockchain technology? Which useful applications can you imagine?

It's useful for keeping historical records of anything.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

Bitcoin already has changed the world. Pandora's box has been opened and it will definitely disrupt the banking and financial system. It has even forced some people to reexamine their ideas about what defines money, for example the idea of "intrinsic value." Honestly though I am really freaked out about the idea of Blockchain technology being combined with, say, the Internet of Things, when big companies like IBM and Google are in charge of that stuff. Imagine if there was a Blockchain

somewhere with records of what temperature your home is and when your lights are on and it fell into the wrong hands and someone robbed you. What if the police could just unlock your door by putting in some code in the Blockchain? What if your self-driving car were redirected from the destination you wanted to go to somewhere else, by a hacker or by the cops, and you couldn't do anything about it? This stuff all scares me and like any technology, Blockchain tech has the potential to be used for amazing good or for scary evil stuff. Which mostly depends on who controls it.

2. The Austrian Way

An Introduction to Austrian Economics

In the late 19th and early 20th century, Vienna had a much higher significance than today. It was the capital of a multi-ethnic empire that comprised the present-day states of Austria, Hungary, the Czech Republic, Slovakia, Slovenia, Croatia, Bosnia-Herzegovina and parts of Italy, Poland, Romania, Serbia, Montenegro and Ukraine. Many great thinkers, scientists and artists lived in the city on the Danube. Some of them made important contributions to modern economics.

The Austrian School of Economics was founded by Carl Menger (1840–1921), who in 1879 became the first professor for political economics at the University of Vienna. His main work was a new theory of prices and values. Equally important was Eugen von Böhm-Bawerk (1851–1914), who served as a minister for the Austrian Empire and taught at several Austrian universities, including the University of Vienna. Böhm-Bawerk became so well-known for his theory on capital and interest that the Austrian 100 Schilling bank note sported his portrait until the Schilling was abandoned for the euro in 2002.

Böhm-Bawerk on the 100 Schilling banknote

Mises and Hayek

The most influential thinker of the Austrian school was undoubtedly Böhm-Bawerk's disciple Ludwig von Mises (1881–1973). He was born in Lemberg (or Lviv),

which today belongs to Ukraine. Mises refined Menger's monetary theory and developed a new theory of business cycles. Unlike his predecessors, he never became a professor at the University of Vienna. This was partly because he was Jewish, as Anti-Semitism befouled Vienna at that time. But even more important was his strong commitment to a free market economy, which contradicted the socialist *zeitgeist* of the 1920s and 30s.

Ludwig von Mises and Friedrich August von Hayek

So he organized a private seminar on economics instead, which was frequented by a number of scholars who later became well-known economists. The most prominent one was Friedrich August von Hayek (1899–1992), who became Mises' partner in the *Austrian Institute for the Research of Business Cycles* in 1927. When the National

Socialists took power in Austria in 1938, Mises escaped, first to Geneva, then in 1940 to the USA. Hayek had already immigrated to England in 1931 to teach at the London School of Economics. In 1950 he subsequently moved to the USA to join the Chicago School of Economics.

As a result of their movements to the US, the Austrian School has become much more popular in the US than in its home country, where it is virtually extinct. Some other important "Austrians" who never lived in Austria are Murray N. Rothbard (1926–1995) and Israel Kirzner (born 1930), both from the USA, and Jesús Huerta de Soto (born 1956) from Spain.

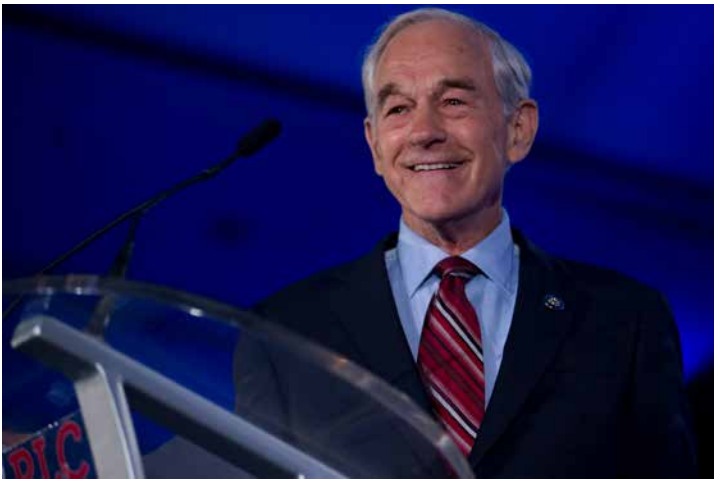
Renaissance of the Austrian School

The early 20th century was dominated by national and international Socialism, and the Austrian School was nearly forgotten. After World War II it regained some ground when Friedrich August von Hayek published his popular book, *The Road to Serfdom*.

Mises and Hayek also co-founded the *Mont Pelerin Society*, which influenced many politicians, among them the German Minister of Economics, Ludwig Erhard. Erhard's courageous free market policy was based upon the insights of the Austrian School. Against heavy

resistance from all German parties he abolished all post-war price and wage controls and unleashed the power of the free market. This lead to the so-called *"Wirtschafts-wunder"* ("German Economic Miracle") of the 1950s.

The economic policies of Margaret Thatcher and Ronald Reagan were also partly inspired by Hayek, although they did not roll back the state as much as he would have preferred. The US politician and "Austrian" Ron Paul, who ran as a presidential candidate for the Republican Party in 2008 and 2012, triggered another major popularity boost for the Austrian School. Although his candidacy was not successful, he attracted a huge base of followers – especially among young people – and inspired them to learn more about Austrian Economics.



The libertarian US politician Ron Paul

Economy and Libertarianism

There are many private institutes and think tanks conserving and promoting the teachings of the Austrian School. The most prominent one is the Ludwig von Mises Institute in Auburn, Alabama. Mises Institutes can now be found in many countries all over the world. Classical Liberalism, which in the US is better known as *Libertarianism* (because "liberal" for some strange reason has become a synonym for "left wing") is deeply connected to the Austrian School. It is important to realize that the Austrian School is not a political ideology, but rather a set of methods to analyze and understand the economy. However, having apprehended the insights of the Austrian School on prices, values, interest, money and business cycle, it is nearly impossible not to favor a free market economy with no government intervention. Even Ludwig von Mises and Friedrich August von Hayek were socialists before they discovered the works of Menger and Böhm-Bawerk!

Human Action

The individual and its actions are at the center of Austrian Economics. Austrians frown upon the habit of economic schools to squeeze human action into abstract mathematical models. Austrians always start at the needs and desires of real people, and do not accept

the concept of a "homo economics," whose behavior is simplified to fit into the artificial models of economists. In contrast, mainstream economists work with abstract terms and formulas, mimicking the precision of natural sciences. But economic processes are much more complex than scientific experiments in a laboratory, which can be repeated at will. In contrast, the economy is influenced by many factors, which work together differently in every situation.

The Austrian School therefore instead focuses on understanding the actions of human beings. It is no coincidence that Ludwig von Mises' magnum opus is called *Human Action*. In its early days, the Austrian School was sometimes referred to as the "Psychological School," because of its human-centered approach. Mises rejected this name, as he did not care about the psychological motives of human behavior, but only about its practical consequences for the economy. He preferred to call his approach *Praxeology*: the science of human action.

Where Do Prices Come From?

A good starting point to understanding Austrian economic thinking is to look at its explanation of how prices arise in a free market. While earlier economists argued the price of a product is mainly derived from the costs of its production, Carl Menger and his successors

claim that prices are solely defined by the subjective value that a user assigns to a product in a specific situation. For this, he coined the term "marginal utility." The marginal utility of a product is the additional benefit you get from consuming an additional unit. This can differ significantly depending on the situation, even for the same good.

Someone who is nearly dying of thirst in the desert would be willing to pay more money for a bottle of water than he would at his hometown supermarket. For him, the value of this life-saving bottle of water is much higher than the 100 dollars a greedy seller would charge. His willingness to pay will be significantly lower for a second bottle, because its marginal utility is much lower after his thirst has been quenched. The seller, on the other hand, will value the 100 dollars higher than the bottle of water – if he disposes of enough water not to die of thirst himself. Otherwise he would not sell his last bottle for any amount of money.

Value is Subjective

We see that the buyer and the seller do not assign the same value to a product. Quite the contrary: a transaction will only take place if for the buyer the product has a higher value than the money he pays for it, while the seller appreciates the money more. Therefore, a

"fair price" or an "intrinsic value" of a product does not exist. Prices always arise from individual decisions in specific situations. If a central authority fixes prices, distortions and unwanted aftereffects will inevitably follow.

The higher price of the *Blue Dollar* in Argentina is a natural consequence of the capital controls by the Argentinian government. Their efforts to prevent Argentinians from buying dollars are in vain. Argentinians need dollars, so they are willing to pay a price that is much higher than the "official" rate as defined by the government. Price controls always lead to "black," or to be precise, free markets. Another example from Argentina: when the government limited the price of beef to maintain its affordability (eating immense amounts of beef at a barbecue is an essential part of Argentinian culture), many cattle ranchers went out of business and started to grow soybeans instead. This lead to a scarcity of beef, eventually forcing the government to suspend the price controls.[2]

The Function of Prices

The Austrian School believes prices are extremely important to the proper functioning of an economy. Prices send signals to which buyers and sellers adapt their behaviors. When resources become scarce in a

free economy, prices rise and buyers will use less of this resource by replacing it with another, less scarce one. They do this without having to know anything about the supply, delivery volume or production costs of that resource; they simply want to save money. Entrepreneurs may then find it pays to tap new resources which were previously economically unviable. Alternatively, entrepreneurs may invent new products that work without using the expensive resource but offer the same benefits. The ecosystem will automatically adapt to the scarcity of that resource, and often this adaption process will lead to innovation and progress.

This natural adjustment cannot happen in a planned economy, where prices do not arise from supply and demand, but are instead fixed by a central institution. Therefore, central planning inevitably leads to a waste of resources and a lack of innovation. A central institution would have to inform all participants of a production process when a resource becomes scarce. But it is mathematically impossible to dispose of all necessary data, let alone to compute them and draw the right conclusions. And how should the central authority convince people to change their behavior? By appealing to their reason and insight? Most likely they will resort to use force.

Market Economy and Socialism

In a free market economy, resources are channeled to where they can be used in the best way via the simple but striking signaling effect of prices. Only a price-driven process of competition in which inferior products are constantly ousted by better ones can lead to an efficient usage of scarce resources – which is what economy is all about.

Ludwig von Mises already proved why Socialism could never work and would lead to impoverishment in the 1920s. At the time, he faced a chorus of outrage, as Socialism was popular and had not yet been discredited. But history has proven Mises right, as one could easily see by comparing the economies of Socialist East Germany and North Korea with their free market counterparts in West Germany and South Korea. Both countries began under the same conditions and shared the same culture, work ethics and natural resources. But whether socialist or free market policies were applied made a huge difference. Currently, Venezuela proves that even the country with the largest oil reserves on earth can be run down through socialist policies.

The Austrian Interest Theory

Interest is another topic the Austrian School has thoroughly examined. The Austrians claim that people value the money at their immediate disposal higher than money for which they need to wait, e.g. when they have lent it to someone else. Carl Menger has coined the term *time preference* for this phenomenon, which became the basis of Eugen von Böhm-Bawerk's theory of interest.

When you lend money to someone else, you might to do this for a close friend or family member without a markup on the return. However, in most other cases you would charge an interest that compensates you for not being able to immediately spend the money yourself. It is also a compensation for the risk that the loan may not be repaid.

Some religions and even some economic schools reject interest and consider it immoral. In contrast, the Austrian School sees it as fair and justified, as long as it results from a voluntary agreement between lender and borrower. Due to time preference, no loans would be given if there were no interest. Indeed even in Islamic banking, which officially bans interest, there are many incentives for a lender. He would receive presents or a profit share, which have similar effects as an interest.

Interest becomes problematic when it is artificially set by a central institution. Austrian economists disapprove of the central bank's power to fix interest rates. It is an intervention in the economy that is as harmful as a central planning authority fixing prices. The free market's advantages in determining the prices for consumer goods should also be used to set the price for money, which is the interest. In a free market, the interest rate would depend on people's willingness to save. If there are many people who save and want to lend money, the interest rate will be low. If the supply of loans is lower, as people are less willing to save and lend, the interest rate will be higher.

Mises' Theory of Business Cycles

In the current monetary system, this natural balance of interest rates is malfunctioning. Loans are not given by people who have gained a surplus and want to invest it, but by banks that have the privilege to create money out of thin air. The interest rate is defined by a central bank, so it does not have any connection to the saving rate and the "natural" interest rate that a free market would produce. This results in misleading incentives for investors. Due to artificially low interest rates, they invest their money into projects that under normal circumstances would not be economically viable. Cheap money can cause a short-termed economic boom, but it is only a

straw fire. In the long run, uneconomic investments will fail and the boom will turn into a recession.

Ludwig von Mises' theory of business cycles does not only deliver a logical proof of this, he also correctly predicted the economic crisis of 1929. According to his theory, the boom of the "Roaring Twenties" was caused by cheap loans issued through the *US Federal Reserve System*, which was founded in 1913. When investors discovered that this boom did not correspond to real value being created, it collapsed.

Also the financial crisis of 2007–2008, which hit many "economic experts" by surprise, was correctly predicted by Austrian economists. The combination of the Federal Reserve's low interest rate policy with the political demand to grant loans to people who do not have the conditions to afford them resulted in the burst of the real estate bubble. Many complicated financial products that were "secured" only by subprime credit became worthless.

From an Austrian perspective, only money that is saved by abstaining from short-term consumption can lead to a sustainable buildup of capital. The current monetary system, which is based on debt and loans created from thin air, does not deserve the name "capitalism," as it does not lead to an accumulation of capital and has nothing to do with a free market economy.

Austrian economists reject a monetary system that is based on a state monopoly. They observe many harmful effects that are the results of governments and central banks acting. The Austrian School has logically proven why a central authority should not fix prices. However, a central institution fixes the price for the most important good of an economy, which is money. That's why the libertarian author Roland Baader calls our current system "money Socialism."[3]

Gold Standard or Competition?

Inside the Austrian School there are different opinions on which is the best alternative to a state monopoly on money. Ludwig von Mises was in favor of a currency backed entirely by gold, which would theoretically prevent government manipulation. Friedrich August von Hayek believed that governments would never allow such a strict gold standard; he therefore favored a free competition of currencies.

In his book *The Denationalization of Money* he suggested that state-issued money should compete with money issued by private companies. In such a free monetary system, he predicted, better currencies would prevail. But why is a state monopoly on money so bad? In order to understand this, we need to explore the nature of money.

INTERVIEW

EDDY TRAVIA

Hong Kong

What fascinates you about Bitcoin?

The simple solution to complex problems and the number of applications Bitcoin can lead to. When I discovered Bitcoin it felt as if a pandora box had just been unlocked. It is dizzying the number of ways Bitcoin can help with society's issues, both as a currency and a distributed ledger.

How did you get involved with Bitcoin?

I was introduced to Bitcoin by Hakim Mamoni, with whom I co-founded Seedcoin. The Cyprus bail-in in Spring 2013 opened my eyes about Bitcoin as a potential solution to monetary and financial crises. In May 2013 Coinbase was raising funds from IDG, a Beijing-based fund I was familiar with and that confirmed my interest in Bitcoin startups.

What are your Bitcoin-related activities now?

Along with my partners I help entrepreneurs building products and services based on Bitcoin and Blockchain technology. I have co-founded a one-stop shop for entrepreneurs called Coinsilium Group comprising an accelerator (Block Chain Space), an investing company (Seedcoin), a corporate advisory (Coinsilium Ltd) and a media & communication division.

I wish to contribute to the development of the crypto-currency and Blockchain ecosystem because we see its potential to transform several areas of the private and public sectors.

What are the most important use cases of Bitcoin as money and payment system?

I believe the most important use cases are the ones providing cross border transfer payment solutions in emerging markets where such transfers are costly and inefficient, and the ones helping the 4bn+ unbanked and underbanked participate to global commerce.

What has to happen for Bitcoin to gain mainstream adoption?

More investment in startups and core development, more education and more relevant solutions.

Where do you see the biggest obstacles for that? How can they be overcome?

Investors need a long-term vision to avoid the short-term focus and disenchantment of the VC industry funding internet startups in the late 90s. Bitcoin and Blockchain can produce great long-term benefits but that means patience and sensible management. This is why the company I have co-founded offers corporate and advisory services to bring professional management practices in fast growing startups. We also contribute to the education of professionals to better understand Bitcoin and Blockchain. Education is a global endeavour, however it is urgently needed for regulators, journalists, politicians, professionals and millenials at a global level. These decision makers and trendsetters can shape the way society embraces or rejetcs new technologies.

What else can be done with Blockchain technology? Which useful applications can you imagine?

Blockchain technology applications include, among others: real time settlements, governance solutions, identity management, real time audit trail, asset ownership authentication, any form of contracts removing the need for third party intermediation.

As new technological advances are made in Internet of Things we should see Blockchain technology as a great tool to power or support these applications.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

Bitcoin and Blockchain technology can bring more transparency to existing centralized systems. It can bring more cost-efficient solutions to existing problems currently solved with centralized databases. Society should benefit from more transparency in general and can stop relying on trusted third parties where human or technical failure can occur at various levels.

The Bitcoin community is a collaborative community, hopefully society will move toward a more collaborative and consensus based framework.

How do you imagine the world after Bitcoin and Blockchain technology have gained mainstream adoption?

There are various scenarii where Bitcoin and Blockchain technology gain mainstream adoption. The one I see more likely to occur is one where Bitcoin does not replace fiat currencies but it is adopted widely enough

as to represent a viable complementary currency and therefore can insulate its users from future financial crises – as it could have helped Greek citizens if Bitcoin infrastructure and ecosystem had been developed enough in Greece.

Which other important question have I forgot to ask? Please answer it.

Maybe a time scale question … I think we are at the early stage of the life cycle of these technologies. Although adoption should be faster than the Internet – because indeed we have the Internet today which reduces new tech adoption cycles – Blockchain is such a leap forward compared to existing systems that its adoption is likely to be slowed down by incumbents and anyone with vested interest in opaque and costly legacy systems. My estimate is that it could take about five years to reach significant adoption.

3. Let There be Money

Why The Money Monopoly is Evil

We are used to money being issued and controlled by the state – but if we look at its history we see that money originates from the free market. Without money, a reasonable division of labor would not be possible. If humans want to trade with each other, bartering is not practical. If I have apples and need eggs, I would need to find a person that wants to trade his eggs for apples at this very moment, which is not too likely. On top of that, we have to agree on a ratio of how many apples have the value of an egg or vice versa.

When humans still lived together in small groups, an informal credit economy developed. You would share goods with your neighbors and keep track of the debt

each had with one another. In the long run, everyone would try to maintain an even balance and to give as much as one would get. If you infringed this unwritten rule by fleecing others, you would quickly become an outsider.

But such a system based on trust and social control no longer worked when humans began to live in bigger societies. To be able to trade with one another, a medium was invented to express the value of goods and services: money. In nomadic societies, the first choice for money was often cattle. This is why the Latin word for money, *pecunia*, was derived from the word for cattle, *pecu*. Throughout history many different goods were used as money, from arrowheads and seashells to cocoa beans and dried tiger tongues.

Tip 1 – What can I buy with Bitcoins?

Pretty much anything, from electronics and flight tickets to pizza and alpaca socks. As of today there are more than 100,000 online shops that accept Bitcoin, and that figure is growing rapidly. You find a good overview at *www.usebitcoins.info*. They also have a map with shops in physical stores that accept Bitcoin. Another good map for Bitcoin-accepting stores is *www.coinmap.org*.

The Qualities of Good Money

Eventually, humans of different regions and countries started to use precious metals as money. They discovered independently of each other that some qualities of gold and silver make them especially useful as a medium of exchange. This is because precious metals are:

- scarce
- easy to transport and to store
- durable
- divisible
- hard to counterfeit
- fungible – which means that one piece is as good as any other one.

The most important quality for money is scarcity. Precious metals are rare and can only be extracted from the earth with significant effort. The scarcer a useful good, the more valuable it becomes. Therefore it is much more practical to use gold than the abundantly available iron – otherwise you would have to go shopping with a heavy pushcart. Another important quality of money is its durability: iron corrodes, gold doesn't. So you can use it not only as a medium of exchange but also as a medium to store value over a long time.

Divisibility is another reason why cattle did not prevail as money: two halves of a cow simply won't have the same value as a whole one. Diamonds also lose a lot of their value if you smash them into small pieces. Gold, however, can be divided without losing any of its value. By using gold, people have more ways to settle on a trade, even if they only have something less valuable to offer than a whole cow. Because of these special qualities, gold has served as the best form of money for thousands of years. As J.P. Morgan, one of the most successful bankers of the early 20th century, pronounced, "Only Gold is money, everything else is credit."[4]

Gold has been used as money for more than 5,000 years

Manipulation of Money

As long as money exists, kings and rulers have tried to manipulate it for their own benefits. They determined that gold could only be used in the form of special coins, usually ones carrying the king's image. It became the state's duty to guarantee the correct value and content of gold, so one did not have to weigh it. A popular way to manipulate coins was to file of a bit off the edges. In fact, the decorative edge patterns we see on coins today were originally introduced to prevent fraudsters from using shaved coins. Another way to cheat was to dilute gold or silver with less valuable metals. Often, the rulers themselves used these tricks to secretly steal citizens' property. But their possibilities to manipulate money increased by magnitudes when a new practical invention appeared: paper money.

Paper Money and Fractional Reserve

Originally, banknotes were nothing else than receipts for gold or silver that were stored safely in a bank vault. Carrying heavy coins was not very practical and quite unsafe, as street robbers could easily assault you. As a result, many people preferred to keep their gold in banks. For practical reasons, people started to use the receipt they received from the bank for the stored money as a means of payment. When buyer and seller were

clients at the same bank, the gold did not even have to be moved when its owner changed. If they had accounts at different banks, the bankers were responsible for the gold's secure transport. In both cases, the bank subtracted the amount of gold from one client's account and added it to another one. One had to trust the bankers that they did this without cheating, but many saw this as the lesser evil than running the risk of being robbed. It also made international trade much easier.

Some smart bankers found out a new way to make money: they simply gave out more receipts than they had gold in their vaults, as it was very unlikely that all their customers would come to withdraw their funds at the same time. This enabled them to issue loans and charge interest for money that did not belong to them. In normal life this would be called deceit. In the financial world it is called "fractional reserve banking." Governments legalized the fraudulent behavior of the bankers, and banks were granted the right to only keep a small part of their deposits and to speculate with the rest. In return, banks funded government wars.

But what to do if too many clients withdraw their money at the same time and the swindle gets debunked? To avoid such a "bank run," a central bank was created as the "lender of last resort." Its main function was to provide enough money to banks that got into trouble.

The Gold Standard

As paper money led to some financial bubbles and bankruptcies in the 18th and 19th century, Peel's law of 1844 demanded that in Britain all bank notes had to be entirely backed by gold.[5] Unfortunately, this applied only to physical banknotes, not to sight deposits on bank accounts, so the fractional reserve fraud could carry on.

Anyhow, due to the relatively strict rules for British banks and the dominance of the British Empire in world trade, many nations followed the British example and adopted a gold standard. Most national currencies had a fixed exchange rate to gold and therefore to each other.

The late 19th and early 20th century were periods of immense economic growth. International trade increased. Prices remained stable, in the USA they even dropped. Wealth in the developed world grew steadily, partially as a result of the international gold standard.

But when the First World War started in 1914, all warring nations abolished the obligation of their central banks to redeem gold for bank notes – otherwise, the war would have lasted for only a few weeks. Central banks could then print unrestricted amounts of money

to cover the high costs of warfare. Had the gold standard been in place, their gold reserves would have expired in no time.

German hyperinflation 1923

Hyperinflation and World Economic Crises

The citizens paid for the huge bills resulting from the war. In Germany and many other countries hyperinflation decimated people's savings. By November 1923, one US dollar was equivalent to the insane price of 4,210,500,000,000 German Marks.

Some nations tried to return to a common gold standard, but their attempts failed. In 1924 Britain reintroduced

the gold standard, but the British currency was overvalued due to the increase of paper money during the war. This became a high burden for the British economy and caused an economic crisis in Britain. This crisis was, however, dwarfed by the global economic crisis, which began on October 24th, 1929, or "Black Thursday."

This crisis is a classic example of Ludwig von Mises' theory of business cycles, which states that a boom caused by cheap loans will inevitably be followed by a bust. When investors can borrow money for an interest rate below the natural rate as defined in a free market, they will invest into ventures that are not really lucrative. Sooner or later this will show and must be adjusted, sometimes painfully.

According to Mises, the boom of the "Roaring Twenties" was the result of the US Federal Reserve Bank and its policy of easy credit. When it became obvious that the economic boom was built on sand, the economy crumbled. Unfortunately, the view of the Austrian School – which identified centralized intervention as the root of the crisis – did not prevail at the time. Instead, the theory of British economist John Maynard Keynes guided popular opinion and governmental response. According to Keynes, increased government intervention is necessary during times of economic crisis. He claimed that governments should fund economic stimulus plans by creating debts.

Keynes and the "New Deal"

Politicians embraced Keynes' theory as it gave them scientific justification to increase governmental power. Throughout the 1930s, state intervention in the economy became the rule. This was especially damaging in the Soviet Union and in National Socialist Germany, but even in the USA economic freedom was severely reduced.

Owning gold was made illegal for US citizens in 1933. President Franklin D. Roosevelt's policy of state intervention stood in stark contrast to the free market policies of former US administrations. In accordance with Keynes' theory, he spent huge amounts of money to "stimulate the economy." These measures gained him short-term popularity among voters, but it expanded the state apparatus to a size that became harmful to individual liberty. In fact, Roosevelt's so-called *New Deal* did not end the crisis, but prolonged it, as Austrian economist Murray N. Rothbard demonstrated in his book *America's Great Depression*.

Bretton Woods and the End of the Gold Standard

At the Bretton Woods conference in July 1944, the USA and its war allies created the post-war financial order. The US dollar became the anchor currency for the

world, with the US government guaranteed other central banks that they could sell their US dollar reserves for gold at a fixed rate. Thus, the Bretton Woods system established an indirect worldwide gold standard.

This system worked well for a while, but when the US started to print more and more dollars to fund the Vietnam war, its weakness became obvious. The USA did not have enough gold to redeem for all the dollars circulating in the world. When several governments, especially the French, exchanged increasing amounts of their dollars for gold, the US gold reserves began to shrink to alarmingly low levels. On August 15th, 1971, President Nixon abolished the gold backing of the dollar. That was the beginning of the end for the Bretton Woods system, which was formally canceled in 1973.

Since then, currencies are no longer backed by anything. Unbacked currencies are called *Fiat*, which has nothing to do with the Italian car brand, but is derived from the Latin expression for "let there be." Fiat currencies only exist because the state proclaims them to be "legal tender." Without a government forcing people to accept it, no one would work for a piece of paper.

Fiat currencies have been the worldwide norm since 1971. In a fiat money system, money can be created in two ways. It can be issued by a central bank, which has the exclusive right to print banknotes and mint

coins. The central bank then lends money to commercial banks for an interest rate it defines itself. Money can also be created by commercial banks. The state has granted them the privilege to generate new money each time they issue credit.

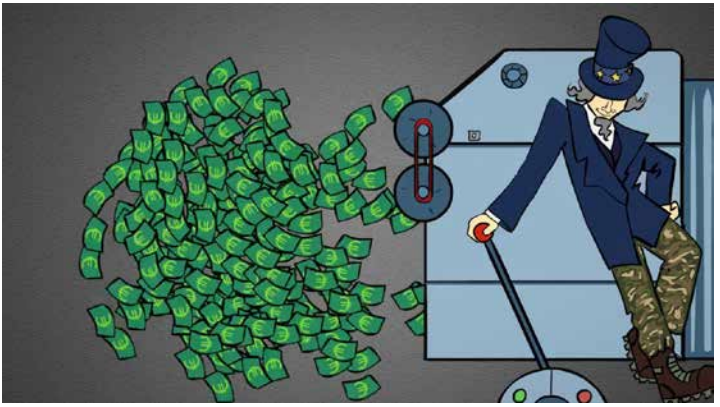
Loans from Nowhere

In the age of gold- and silver-backed money, a loan could only be given if someone had saved enough money to issue one. The lendee would ask a bank to act as a middleman in a transaction between him and someone else in return for interest. Today, a loan can be given without being backed by anyone's savings. When a bank lends money to someone, it is newly created money. The bank only has to deposit a small fraction of each loan (in the US it is around 3%) as a security at the central bank.

This system is so absurd that most people would not believe it: while a borrower needs to work hard to pay back his loan and the interests on it, a bank can create new money out of thin air by the push of a button. A borrower may lose the house he has bought for a mortgage if he defaults. A bank can simply write a bad loan off. If it runs into financial problems, it is usually bailed out with taxpayers' money. When new money comes into the world, new debt arises with it, which has to be paid back

with an interest. This vicious circle leads to ever-growing piles of debt. Only the wealthy and the banks benefit from this system. For everybody else, saving money or accumulating a fortune becomes increasingly difficult.

Inflation



The state prints money at willingness

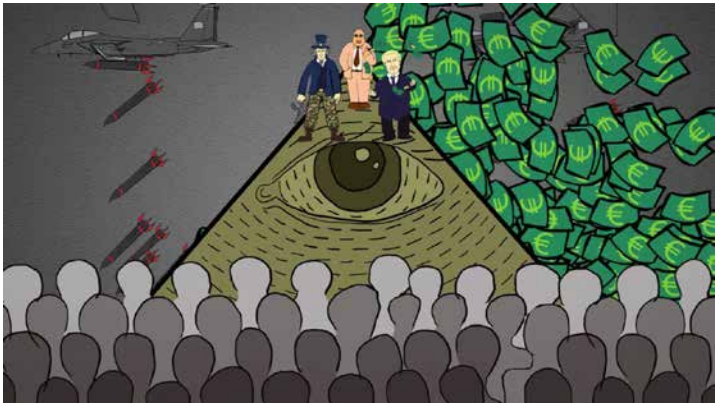
Inflation is defined as the increase of the money supply in an economy. It derives from the Latin word *inflare*, meaning, "to blow up." When the money supply grows faster than the amount of goods and services in an economy, prices usually increase. We tend to call this price increase inflation, but economically this is incorrect. When news programs report on the "inflation rate," what they are really referring to is a price index measured by a rather arbitrarily compiled basket of

goods. Due to increased productivity and global division of labor, the prices of consumer goods in this basket should have fallen. Instead, the effect of monetary inflation keeps prices the same or only causes moderate increases. You can see the price-raising effect of monetary inflation in the ever-increasing prices of real estate and shares, which are not part of the basket, and therefore not recorded by the so-called "inflation rate." You will hardly ever hear about real inflation, which is the growth of the money supply. For example, in the USA the money supply has grown from about 500 billion dollars in 1971 to nearly 12,000 billion dollars in 2015.[6]

The Cantillon Effect

Inflation leads to growing social inequality. This is caused by the Cantillon effect, named after the economist Richard Cantillon. He demonstrated that those close to the source of the newly created money – governments, banks and big companies that are well connected to government institutions – have a huge advantage to those who receive the money later. The privileged ones can buy goods and services at the old prices before inflation takes effect. When the money trickles down to those who earn salaries or live on pensions, prices have already increased, they can buy less for their income. Additionally, their savings lose value, as the central bank maintains interest at artificially low rates. Today, the interest

on savings is even lower than the official "inflation rate," let alone the real one. Only few people benefit from a system like this, and it is at the expense of many others. The Cantillon effect has resulted in an ever-growing gap between the super-rich and the average citizen.



Inflation means: restribution of wealth from the bottom to the top

The growing divide between the "1%" and the rest of us is not capitalism's fault, as people with little of knowledge of economics claim. Quite the contrary, it is caused by our monetary system, which has nothing to do with capitalism or a free market economy. You will find the idea of a centralized monopoly on money and a state-run central bank in the Communist Manifesto by Karl Marx and Friedrich Engels. As most Marxist ideas, it has done a lot of damage. Allowing a central authority to control money and define its price makes as much sense as letting a central planning institution

fix the prices for consumer goods. The Austrian School has proven that the free market should determine the price of every good, including money.

Government Debts

Since the dollar is no longer backed by gold, the purchasing powers of all major currencies have plummeted. Today it would cost 15 dollars to purchase the same amount of goods as you could buy with a single dollar in 1971.[7] At the same time, governments' debts have skyrocketed. The US debt has grown from about $400 billion dollars in 1971 to more than $20,000 billion dollars in 2015.[8]

This is no coincidence. Borrowing fiat money is much easier for politicians than borrowing real money backed by gold or silver. The state issues bonds, which are backed by nothing other than the government's ability to tax people. These bonds are either sold to the central bank for freshly created money, or to wealthy people who consider them a relatively safe investment. By debasing the currency or by lowering the interest rate, the central bank can easily reduce the burden of interest on the government's budget. In extreme cases the debt can be wiped out by a hyperinflation or a currency reform, as it happened in Germany after its lost wars.

But normally, more and more debt is piled up, which will probably never be paid back. Interest rates are being paid by tax revenues or even by taking up new loans. Every company with this kind of fiscal policy would be sued because of a delayed filing of insolvency. But rules for politicians are different. They are not accountable for the debt they cause, they simply saddle the next generation with it.

The End of the Fiat Money System

It is much easier for politicians to fund their promises towards their voters and sponsors by incurring debt and using the hidden tax of inflation than to risk unpopularity by officially raising taxes. But the long-term damages this causes to a society are substantial. A fiat money system inevitably leads to a distribution of wealth from the bottom to the top. Taxpayers and savers are gradually expropriated for the benefit of those who already have money and power.

The system of unbacked, debt-based money that has ruled the world since 1971 is harmful and evil. It is the main cause for financial crises, growing government debts and the increasing gap between rich and poor. It should be abolished immediately. But that is not so easy. Very powerful institutions, such as banks and governments, have a vested interested to keep it alive.

There is a superior option to fighting against this system: building a new one. This new system needs to be so much better than the existing one that more and more people start using it, until one day the old system becomes obsolete. That is what Bitcoin is all about.

INTERVIEW

JULIA TOURIANSKI

Toronto

What fascinates you about Bitcoin?

I love Bitcoin because it's inclusive. It doesn't matter if you are born into a family of lawyers in New York City, it doesn't matter if you're a hacker living in a squat in Barcelona. Not only can you use Bitcoin, but you can develop the technology itself, and no third party can tell you otherwise. I love Bitcoin because it's a way out. You no longer need a bank account to accept payments from anyone in the world. Now people from the poorest countries can skip this step of financial infrastructure and be directly empowered by cryptocurrency. All you need is a smartphone to participate. The Blockchain does not discriminate.

How did you get involved with Bitcoin?

I first heard of Bitcoin when I may or may not have been looking to purchase a substance on the Silk Road.

I understood the economics of Bitcoin after I began writing for Mises Canada. I understood the politics of Bitcoin after I met Amir Taaki. I understood the humanity of Bitcoin after I met Andreas Antonopoulos.

What are your Bitcoin-related activities now?

I am an anti-state propagandist. I run a YouTube channel and a website called *Brave The World*. Recently I've been helping Ross Ulbricht, the founder of Silk Road, covering his trial. I don't want the Government involved in my life, and that includes my financial business. Hopefully with Blockchain tech we can evolve and decentralize most other systems as well.

What are the most important use cases of Bitcoin as money and payment system?

The ones that are kept private.

What has to happen for Bitcoin to gain mainstream adoption?

First off, I don't care for the term "adoption." What the mainstream does and what real people everywhere do are two different things. So I'll speak of the latter.

I think everything has happened. People just need to look and listen. But I guess another Cyprus wouldn't hurt. One thing to note, there's a reason Russian folks have been using BTC with vigor. We had 72 years of communist oppression only to now have a Putin dictatorship. We know governments are evil at their core, we are a naturally distrustful people. We aren't allowed to have financial freedom but we don't give a fuck and don't wait for permission, yet Americans seem to. Maybe it's because they at one point did have a taste of "freedom" and are now stuck in the remembrance of decadence. The largest Bitcoin black market is without question operated by Ruskis (in Russia, Canada and America). Comparatively the West has not been that harsh with Bitcoin restrictions, yet not as many people embrace it.

What else can be done with Blockchain technology? Which useful applications can you imagine?

Law, charity, management, proof of publication, more trustless systems, and history. I think the Blockchain will harbor unalterable historical documentation. We won't need revisionism anymore.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

I'm not sure anymore, with the way things are going. Bitcoin seems to be moving towards absorption into our current system. But its mere existence may create fertile grounds for a larger movement away from central governing, financial controls and censorable information systems. My naive hope is that it will bring forth a choice for true individual independence in all facets of life.

4. As Good as Gold

The Basics of Bitcoin

On October 31st, 2008 someone calling himself Satoshi Nakamoto published a whitepaper for a decentralized payment system called Bitcoin via a cryptography mailing list.[9] Shortly afterwards, he shared his software code so other developers could freely contribute to the project.

Nobody knows who hides behind this Japanese name as common as "John Smith." It is not even clear whether it is an individual or a team. Satoshi frequently communicated with other developers by email and forum

posts, but nobody ever saw his face or heard his voice. In December 2010, Satoshi Nakamoto completely withdrew from the project, without ever having revealed his identity.

On January 3rd, 2009, he generated the Genesis Block and the first 50 Bitcoins. As a proof of that date, he included the daily headline of the London-based newspaper *The Times*, which read *"Chancellor on Brink of Second Bailout for Banks."* One can understand this as a political message: with Bitcoin, the age of bank bailouts is over.

On January 9th, Satoshi published the first compiled version of the Bitcoin software, which is useful not only for software developers, but for anyone interested in Bitcoin. By using this software, one can be part of the Bitcoin network, check transactions and be rewarded with new Bitcoins. This procedure is called *mining* (we will explain it in detail in chapter 5).

Three days later the first real transaction took place. Satoshi transferred 10 Bitcoins to software developer Hal Finney, who had been contributing to the Bitcoin source code for some time. These "digital coins" had no value yet. In the first two years of its existence, very few people were engaged in Bitcoin. They were mostly computer scientists and cryptography experts who became fascinated by Satoshi's idea and wanted to support him in further developing the software.

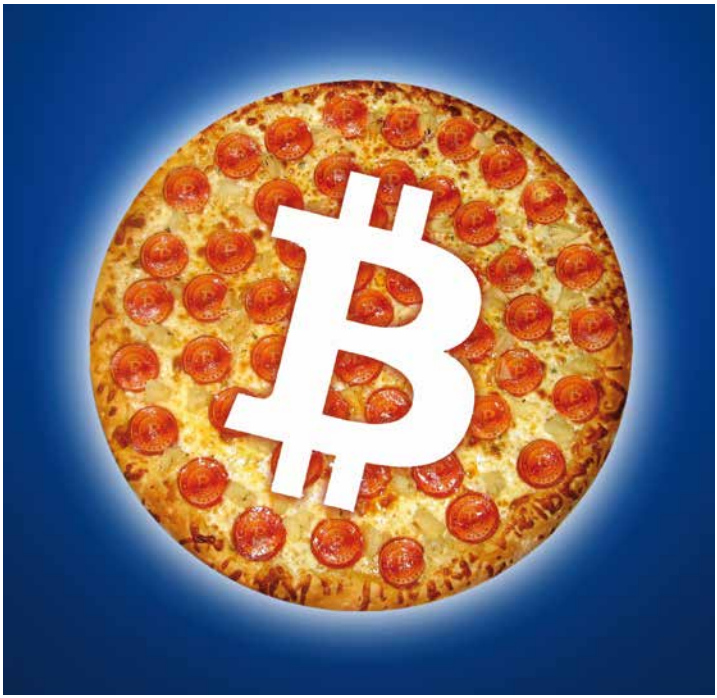
In computer terms, Bitcoin is a protocol. That is a set of rules that defines how computers communicate with each other. Without knowing it, we use protocols whenever we surf the Internet. The TCP/IP protocol defines how computers exchange data. The HTTP protocol, which is based upon it, defines how websites and links work. The Bitcoin protocol defines a way to transfer value in a data network.

While in the World Wide Web there is a clear distinction between servers and normal users' computers, Satoshi decided to build the Bitcoin network on the peer-to-peer principle. In a peer-to-peer network there are no central servers. Computers in the network have equal standing; they act as both senders and receivers. Such a distributed network is much more robust than a centralized one. If a centralized system's main server malfunctions, the whole network collapses. In a decentralized peer-to-peer network everything will work as long as there are at least two computers communicating with each other. It can therefore hardly be shut down. One can compare it to the hydra of Greek legends. If one of their heads is cut off, many new heads will appear.

The Most Expensive Pizza of All Times

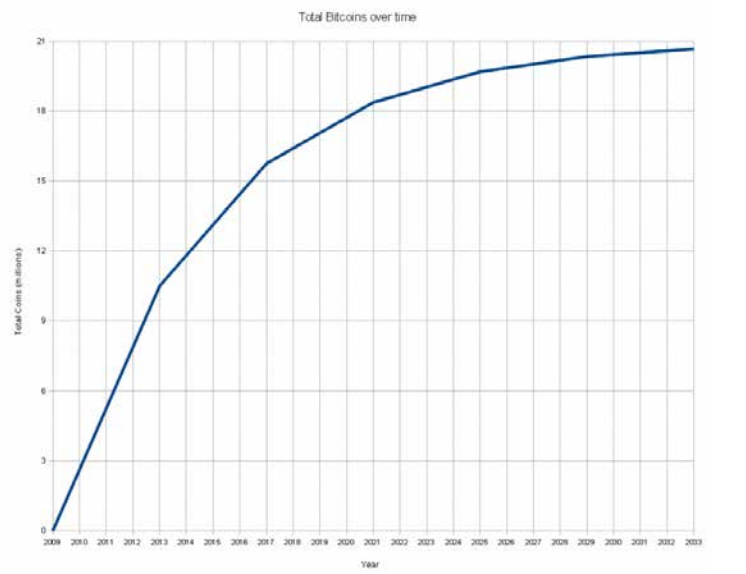
On May 21st, 2010, software developer and Bitcoin enthusiast Laszlo Hanyecz from Florida posted an offer

on the Bitcoin forum: he would pay 10,000 Bitcoins for two pizzas. Today (September 2015) this would be worth more than $2.5 million US dollars! He received the pizzas the next day, transferred the coins and entered the history books as the first human to buy a tangible product for Bitcoins. Laszlo probably mined the Bitcoins himself and considered it cool to pay for his pizza in Bitcoin. The idea that money you can create yourself in your computer has a real value was still strange to the Bitcoin pioneers of the early days.



3 million dollars for two pizzas

In October 2009 the exchange rate for one Bitcoin was defined as 0.000763924 US dollars, based on the costs of electricity to generate one Bitcoin at that time. In July 2010, the Mt. Gox exchange began operating. It soon became the most trafficked site to exchange Bitcoins for fiat money. The price of one Bitcoin climbed to one cent and continued to rise. In February 2011, the Bitcoin on Mt. Gox reached parity to the dollar, and some proclaimed this to be a speculative bubble. How can a digital coin that you can generate on your own computer have the same value as a real dollar issued by the powerful US government?



Growth of the Bitcoin money supply

This question sounds difficult, but from an Austrian economic perspective, it is surprisingly easy to answer. Any good that is useful and scarce has a value.

Why Do Bitcoins Have Value?

Bitcoins are scarce because the Bitcoin protocol defines it so. It limits the absolute amount of Bitcoins that can ever exist to 21 million. These are issued in fixed intervals and in packages. The size of the packages decreases over the years. In the first four years, 50 new Bitcoins entered the market every ten minutes. In 2013 the amount of new Bitcoins was reduced to 25. In 2016 it will be halved again to 12.5, and so on. Halving of the new Bitcoin supply happens about every four years. So, over time, the growth of the money supply converges to zero.

What about the usefulness of Bitcoin? When it was only a toy for crypto nerds, it had no use and therefore no value. But the more online shops, brick-and-mortar stores, companies and freelancers accept Bitcoin, the more valuable it becomes. The Austrian School defines value as deriving from the subjective decision of a user. Only if something is useful to me, I will assign a value to it. There is no such thing as an "objective" or "intrinsic" value. Obviously many people consider Bitcoin valuable, as they are willing to accept it and trade their time,

goods or fiat money for it. So, Bitcoins undeniable carry value. But why do people find Bitcoins useful?

Tip 2 – Where can I get Bitcoins?

There are many exchanges on the Internet where you can change dollars, euros or other currencies into Bitcoins. You find a good list of them here: *www.teambitcoin.com/bitcoin-exchange-list*
Exchanges usually ask for a proof of identity and the data of your bank account. If you prefer to meet up in person and change Bitcoins for cash, you can arrange a meeting with a trader through the platform *www.localbitcoins.com*. In many cities there are regular meetups in public places where you can get information about Bitcoin, and often there are also people who would buy and sell Bitcoins. Many of these meet-ups can be found at *www.meetup.com*.

Bitcoin's Main Attributes

The word Bitcoin stands for two things: a worldwide payment system and the digital token that you need to participate. The ingeniousness of Bitcoin stems from the design of its payment system: it is much faster, cheaper and more secure than any other that has ever existed. If we look at Bitcoin as a currency, we see that it has the same qualities that made gold the preferred money of mankind for thousands of years.

1. Bitcoins are scarce, even scarcer than gold. New gold sources could be discovered; we could even imagine a huge asteroid made of pure gold could land on earth. While very unlikely, it is possible. The Bitcoin protocol, however, strictly limits the total amount of Bitcoins that can ever exist to 21 million.

2. Bitcoins can easily be divided into smaller units without losing any value. Compared to gold, which can only be partitioned to a certain physical limit (as it is made up of atoms), Bitcoin can be divided in much finer parts. At the moment the smallest possible unit is 0.00000001 Bitcoins, or a hundredth of a millionth of a Bitcoin. If needed, this smallest unit can be divided again.

3. Bitcoins are durable and cannot decay. Bitcoins do need the Internet, computers and electricity to exist, but that is true for our whole modern civilization. If the Internet ceases to function, we will have much bigger problems than the loss of Bitcoins. But even in this scenario, one can prevent the loss of Bitcoins by storing them on paper (see info box 4) and feed them into a future computer network.

4. Bitcoins cannot be falsified. In contrast, gold needs to be thoroughly examined for evidence of fraud. It is a common practice to dilute it or to hide metals like Wolfram within the bars. Such fraud is impossible with Bitcoin, whose authenticity is mathematically proven in every single transaction.

Bitcoin payments are additionally very convenient in comparison to gold payments, which are rather impractical for everyday transactions. Bitcoin is like gold that can be sent around the world at the speed and the cost of an email.

Was Satoshi an "Austrian"?

Satoshi quite obviously mimicked the qualities of gold with his creation. Bitcoin's built-in scarcity illustrates this point rather well. A follower of the monetarist school of Milton Friedman would certainly not have set an absolute limit to the money supply, as Friedman teaches that the money supply should grow with the economy. Instead, Satoshi followed the Austrian approach and made his creation as scarce as a precious metal.

Bitcoin in Hayek's tradition

It is no coincidence that one of Bitcoins theoretical predecessors was called *Bit Gold*, which was created by computer scientist, legal scholar and cryptographer Nick Szabo in 1998. Many people suspect Szabo is the man behind the pseudonym Satoshi Nakamoto, a charge Szabo adamantly denies. In any case, we can assume that Satoshi knew Nick Szabo's work and attempted to put his ideas into motion.

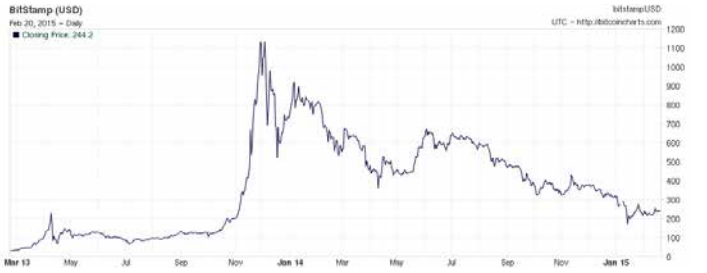
Bitcoin and Mises' Regression Theorem

Ludwig von Mises explains why money has value by his *Regression Theorem*. It states that the value of money can be derived from its value in the past.[10] People accept money because they know they could buy something for it the day before. Yesterday's acceptance results of the purchasing power the money had the day before yesterday, and so on. This chain of thought can be followed until the very moment a good was used as money for the first time.

Before gold became the universal medium of exchange, it already had a value, because it was used for creating jewelry and cult objects. Bank notes, which were originally just receipts for gold, still derive their value from gold. When the gold backing of currencies came to an end, the value of all currencies decreased, but their

subjective value can still be traced back to their original gold backing.

This remains true for Bitcoin. Unlike gold, Bitcoin possesses no benefits aside from being a medium of exchange. So, if no other form of money had existed before Bitcoin, it would have been impossible to assign a value to it. But that is not the case. We live in a world with numerous currencies that all derive their value regressively from gold. When people voluntarily change their euros, dollars or yuan for Bitcoins, that value is consequently assigned to Bitcoin.



The Bitcoin price in 2013/2014

The Up and Down of the Bitcoin Price

How is the Bitcoin price calculated? This happens at the many Bitcoin exchanges, which are open 24 hours a day, seven days a week. The law of supply and demand

commands the Bitcoin price. The more people who want to buy Bitcoin, the higher the price. Sometimes the prices on the different exchanges vary, but the activities of arbitrage traders seeking to profit from price differences cause the prices to converge. In the past, the Bitcoin price was extremely volatile, but when viewed in the long term, the market trend is clearly upwards. This is logical; Bitcoin's supply is strictly limited while the demand is constantly rising.

The curve of the Bitcoin exchange rate over the last few years feels like a roller coaster ride – it's surely nothing for people with weak nerves. The first media blitz around Bitcoin was in spring 2011, when a wave of articles in the mainstream press drove the price to the seemingly crazy height of $31.91 on June 8th, 2011. This sudden peak was followed by a long descent. In December 2011, the Bitcoin price was down to $2 dollars. Many believed Bitcoin was a straw fire. Wired Magazine even published an article titled *The Rise and Fall of Bitcoin*[11]. But Bitcoin slowly revived through 2012 and rose to about $15 in January 2013.

Then, Bitcoin's price soared to unprecedented heights. In March 2013, when Cypriotes experienced a wave of frozen bank accounts and confiscation of savings, many people discovered the world's first non-confiscatable and unfreezable currency.

Bitcoin is big in China

In March 2013 Bitcoin exceeded $100, bounced up to $260, then suddenly crashed to $50. Mt. Gox, the dominating Bitcoin exchange at that time, could not cope with the amount of traffic and had to cease operations for several days. This unsettled many investors. The price recovered from this severe crash and for some months hovered around $100 before it started another price rally in October 2013, which made the "bubble" of April 2013 look like a mere pimple.

In November 2013 Bitcoin jumped above the $1,000 threshold for the first time. On November 17th, a single Bitcoin traded at $1,242, more than the price of an ounce of gold. This time, it was the Chinese driving the price upwards. A Bitcoin gold rush was underway in the

world's second largest economy. Turnovers at Chinese Bitcoin exchanges skyrocketed, more and more important Chinese online shops started to accept Bitcoin, and state-owned media aired positive reports about Bitcoin. The Chinese national currency is not freely tradable, and as a result Bitcoin investments were a desirable way for the Chinese to invest in an internationally accepted and tradable currency. But when the Chinese government started to regulate Bitcoin, the price experienced a deep plunge.

2014 saw a repeat of 2011's long, downward movement. In the beginning of 2015 the price dropped below $200. This was certainly frustrating for people who began investing in Bitcoin at its peak in November 2013. But from a long-term perspective, Bitcoin was a good investment: its current price of about $230 (September 2015) is still about a hundred times higher than in late 2011 and more than 10 times higher than in early 2013.

Tip 3 – Which Bitcoin wallet shall I use?

In order to send and receive Bitcoins, you need a piece of free software that is called a *wallet*. There are many different wallets for all devices and operating systems. Here is a good overview: *bitcoin.org/en/choose-your-wallet*
You may download wallets for computers from the websites of the developing companies. Wallets for smartphones or tablets are available at the Google Play Store (for Android) and at Apple's AppStore (for iPhones).

There are wallets that download the whole Blockchain and others which connect to a server that holds it. This is more practical in daily life, as downloading and updating the Blockchain can be quite time-consuming.
You should avoid so-called *web wallets*, which store your private keys on the provider's server. If that server is hacked, your Bitcoins are gone and the wallet provider will usually not pay them back. You can recognize web wallets as you will not download a piece of software but only register with a username and password to a service – better don't! Always control your Bitcoins yourself!

The Oil of the 21st Century

It seems as though the Bitcoin price curve follows a certain pattern that repeats itself over time. For some time it remains relatively constant, then it suddenly skyrockets to an unprecedented level and rapidly plunges, before experiencing a longer, stable period settling higher than the pre-rally price. There is no guarantee that this pattern, which can be observed at least four times, will continue. But given the scarcity of Bitcoin and its continuously rising demand, many people expect the Bitcoin price to continue increasing in the long run.

Such high volatility is a phenomenon typical of new products. In the 19th century, when oil started to gain importance, its price showed similar movements. From 1861 to 1863 it increased tenfold, then dropped to a

third of its peak value until 1868, before once again rising.[12] A new market usually has a low volume, and therefore relatively small amounts of trade can cause huge price movements. This was true for oil in the late 19th century as well as for Bitcoin today. When a market grows and matures, this tends to even itself out.

Although the price of a Bitcoin plunged in the last year, other important parameters rose. The number of Bitcoin transactions doubled from July 2014 to July 2015. The trading volume on exchanges increased more than 50% from 2013 to 2014. And most importantly: investments in Bitcoin startups rose from $96 million in 2013 to $335 million in 2014 – significantly more than the $250 million that were invested into dotcom companies in 1995, the first year of the Internet boom.[13] This means that many companies now have the funds to build useful applications that make Bitcoin more practical and user-friendly, which is a key component to its future success. Venture capitalists consider Bitcoin as one of the hottest investments of our era. Their main interest, however, does not lie in the currency, but in the technology that Bitcoin rests on: the Blockchain.

INTERVIEW

MAREK PALATINUS

Prague

What fascinates you about Bitcoin?

Bitcoin is first of all a social experiment of an unprecedented magnitude. I think a lot of people tend to forget that, most of the wider audience more or less considers Bitcoin to be a payment system or a fiat money alternative, but there's way more behind the concept.

How did you get involved with Bitcoin?

I first noticed Bitcoin in 2010 on a mailing list I recieved from my colleague. I dismissed the idea very quickly as some nonsensical "novelty." Only later that year I stumbled upon Bitcoin once again and realized there might be potential in it. Then I started mining just to find that mining alone isn't sustainably going to be profitable and that gave birth to the idea of pooled mining and the Slush Pool.

What are your Bitcoin-related activities now?

I am one of the three founders of SatoshiLabs, a parent company for our Bitcoin-related projects. The major one being TREZOR, a Bitcoin safe, device that let's you store and send your Bitcoins securely out of the reach from hackers and viruses on your computer.

The second one is the Slush Mining Pool. And the last of our current activities is a website called *CoinMap.org*. Because there are so many places accepting Bitcoin scattered all around the world, it is logical to have a directory or in this case a map that let's you browse them and perhaps see what's in your neighborhood. Besides these three projects our members actively participate in the Czech Bitcoin community, attend local meetups and give talks.

What are the most important use cases of Bitcoin as money and payment system?

The immediate problem Bitcoin can solve is high cost and low speed of global transactions, in other words remittance markets, business to business transactions, international salaries and more. These can benefit from Bitcoin's network to save on costs and become more effective straight away. Then there are the possible services Bitcoin could open up. For instance recently I've

seen a sketch for project combining torrent data transfers with Bitcoin micropayments, imagine something like this replacing huge centralized media distributors and bringing the profit directly to the authors of content.

What has to happen for Bitcoin to gain mainstream adoption?

The Bitcoin ecosystem has to undergo a thorough shift of its infrastructure. We need to move on from the phase of basement-dweller startups to the phase of intuitive friendly interfaces and finished, stable products. In many ways this is already happening, but there's still a long way to go for the average user to benefit from it.

Where do you see the biggest obstacles for that? How can they be overcome?

Regulatory uncertainity doesn't make it particularly easy for people to start new businesses in Bitcoin. Overall security level of Bitcoin services must be on much higher level than it is now. The onramps and offramps to fiat money should be not only easy to use but also cost effective. If you imagine there were 0% fee exchanges everywhere, money could float frictionlessly around the world and provide liquidity where necessary.

What else can be done with Blockchain technology? Which useful applications can you imagine?

For the first time in history we're able to actually record digital information and store it in a way that everyone sees it but no one can alter it. There's a good connection between the Internet of Things and Bitcoin. Imagine things like interconnected smart power grid, shuffling the electrical energy across countries with the highest efficiency and settling the expenses in Bitcoin, in decentralized manner. Your house could have its own wallet and manage its energy financing or even generate you profits and you could manage all of that from your smartphone.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

I imagine a borderless economy where the cultural and political friction slowly dissolves as we get united in our goals thanks to this natural will to trade. We have finite resources on this planet so the chase for efficiency is completely justifiable. So in the end, as the wildest utopian dream, this could be the first step for humankind to establish worldwide peace. I know it is quite far fetched, idealistic and perhaps naive, but I keep hoping that at the end of this experiment will be a better place for living for everyone.

How do you imagine the world after Bitcoin and Blockchain technology have gained mainstream adoption?

We will hopefully have less advertisement in front of our eyes. Registering a car or house ownership will no longer be a nightmare. Our governments will start to care about us more, as there will be more incentives to motivate citizens to actually pay taxes and they'll use these resources more effectively too. Tax havens might cease to exist. Criminalists will once again have to seek and fight actual crimes and not just constantly check balance sheets and bank account links.

5. The Ledger Lives On

The Blockchain – Satoshi's Disruptive Invention

In creating Bitcoin, Satoshi Nakamoto's foremost goal was to design a payment system capable of functions without needing to rely on third parties, like banks or governments.[14] Institutions are vulnerable to human corruption: bank employees could potentially tamper with a customer's account. This is why these institutions are subject to heavy regulation.

The problem with regulation is that the governments who design regulatory structures have their own vested

interests. More often than not, these regulations are advantageous to institutions rather than citizens. Governments benefit from low interest rates and steady inflation – namely that they are able to borrow cheaply at the expense of savers and taxpayers. A system that relies on trust in banks and governments is prone to abuse, as the numerous financial crises of the last decades have proven. But what does a trustless system look like?

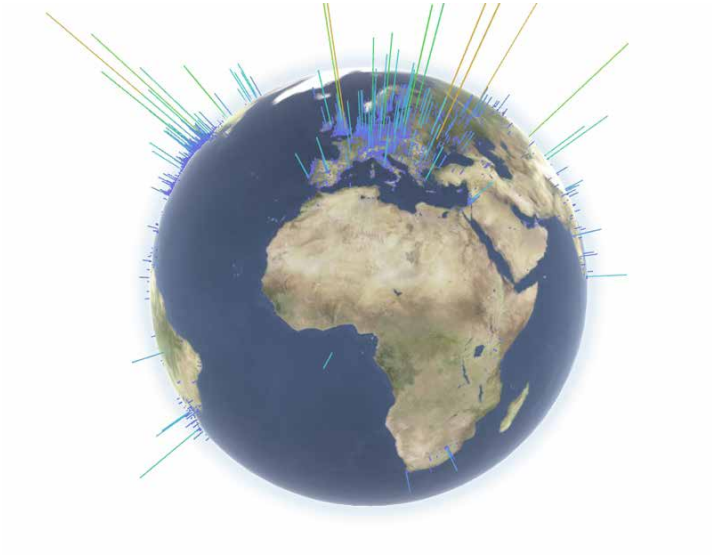
Encrypted Cash

In order for a digital payment system to function, two issues must first be resolved:

1. How can someone prove ownership of money if it only exists digitally?

2. How can this property be transferred to a new owner?

Both questions have been answered for quite some time. In the 1980s, software developer and cryptographer David Chaum created a system called *E-Cash* based upon encryption technology, just like Bitcoin. Each "coin" carries a digital signature, readable by everyone. However, only the owner of the coin can create such a signature using a unique private key.



Globe with active nodes of the Bitcoin networks

Encrypting cash is similar to encrypting emails. In both cases you need a pair of keys: a public key, which anyone may know, and a private key, which is known only to the receiver. If I want to receive an encrypted email from someone, I can easily send him my public key through an insecure channel like the Internet. Anyone can use this public key to encrypt an email and send it to me – but only with my matching private key I can decrypt and read the email.

These paired keys have a similar function for digital cash. The public key serves as a kind of "bank account number." Everyone who knows it can send money to it.

But in order to access and spend this money, one needs the corresponding private key, which is comparable to a bank account's PIN code (but much more secure).

Tip 4 – Secure Storage (I): Paper Wallets

It may sound absurd, but one of the most secure ways to store Bitcoin is on paper. You print your private key several times and store the copies in different places, e.g. in a safe. None of these printouts should get into the hands of anyone but you, as the private key is what you need to access the Bitcoins. Paper wallets are good for storing money that you do not need for a longer time. If you want to access the money you need to import the private key into your wallet software by scanning it as a QR code.

Take good care of your private key!

The Double Spending Problem

By using established encryption technology, Satoshi Nakamoto could build on predecessors like E-Cash and utilize their experiences. But another issue still needed to be resolved: How can you prevent someone from spending a single digital coin multiple times? In the digital world, a copy is as good as the original. While this is practical for copying music and video files, having the ability to copy digital cash as often as you like would render the currency useless.

Before Bitcoin, the only way to avoid double spending was to establish a central institution that would verify that someone sending money indeed possessed the named funds and then deducted the money from his account before adding it to the account of the receiver. E-Cash had a central server that performed these tasks. But again, you would have to trust the company that runs this server. It can be hacked or shut down, and the company that owns the service must be strictly regulated to prevent fraud.

Accountants in a Gold Rush

Satoshi Nakamoto's ingenious solution was to render central institutions obsolete by replacing them with a publicly auditable and immutable ledger: the Blockchain.[15]

Technically, it is a distributed database, stored on thousands of independent computers, which can be accessed and downloaded by anyone. A single person acting alone cannot write something into this database. The whole network, following a set of universal and transparent rules, must make any updates. Anyone who has installed the Bitcoin software on his or her computer can take part in this process. Through the use of sophisticated mathematical methods, the software verifies that a transaction conforms with the protocol. Does the sender have enough money at his disposal? Is his digital signature valid? Is the receiver address correct?

Bitcoin mining is hard work

This process is called *mining*, because it also generates new Bitcoins. The people and their computers who

form the network are called *miners*. They could have been called *accountants* or *auditors*, but it would seem Satoshi preferred a name with a bit more mystique. Maybe he enjoyed the image of tough guys with pick axes and shovels, digging for gold – isn't it much cooler to be a miner than an accountant?

Each miner checks the newest transactions and writes them on a new "page" of the ledger, or in Bitcoin lingo, into a new "block." A block is basically a list of transactions; on average, it contains a few hundred of them.

Miners try to generate a new block by solving a complicated mathematical puzzle. The first one to solve the puzzle adds his block to the block chain and receives a reward to compensate his efforts. At the moment, this reward is 25 Bitcoins. As soon as a new block has been found, all the other miners accept it, update their Blockchain and begin working on the next block. This procedure guarantees that all miners agree on the same version of the Blockchain. By the very architecture of the Blockchain, it is technically impossible to alter entries after they have been recorded.

The Mining Arms Race

This race for the next block takes about ten minutes on average. So about every ten minutes, 25 new Bitcoins

are created and transferred to the miner who has found the new block. This block reward is halved about every four years. The exact moment is defined not by time, but by the number of blocks. The next halving to 12.5 Bitcoins will probably happen in late 2016.

The more computational power a miner contributes to the Bitcoin network, the higher are his chances to solve the mathematical puzzle and gain new Bitcoins. Therefore he has a financial incentive to let his computer do the intensive work of checking the transactions' validity. The technical infrastructure (which in the legacy banking system is run by banks in gigantic data centers) is provided by the thousands of people who form the Bitcoin network.

The Bitcoin network is already the most powerful computer network on this planet. The more computational power the network has, the more difficult it becomes to solve the mathematical puzzles and to earn Bitcoins. This is due to a factor that Satoshi called *difficulty*. It is adjusted every two weeks to suit the capacity of the network. In the last several years, the computational power of miners and subsequently the difficulty have increased by magnitudes. So today you need a much more powerful computer to mine the same amount of Bitcoins than you did only a year ago.

In the early days, one could mine new Bitcoins with a normal desktop computer. Today, doing so would waste more electricity than you would ever earn in Bitcoin. Participating in the Bitcoin network requires you to invest in special computers equipped with ASIC chips. These chips are specially designed to solve the mathematical tasks that the Bitcoin protocol defines, so they are a lot faster than normal computer chips. It also means that they cannot be used for anything else than mining Bitcoins.

Tip 5 – Secure Storage (II): Armory

A secure method to store your Bitcoins while still being able to access them whenever you need them is the *Armory* wallet. It is a very safe way to store Bitcoins, but it requires some extra hardware and is not easy to use. You need two computers: one is connected to the Internet and one that will always be offline. Its only function is to store the private keys and to sign transactions, so the offline computer can be an old laptop that you no longer use. The online computer requires a significant amount of RAM, because Armory downloads the whole Blockchain. This computer only runs a limited version of the wallet. You can see your account and initiate transactions, but to finish them and to send money you need the offline computer. This process is described here: *bitcoinarmory.com/tutorials*.

How to Send Bitcoins to China

What exactly happens when I send some Bitcoins to a friend, let's say in China? First, we both need a piece of software called a Bitcoin wallet, which will enable us to send, receive and store Bitcoins.

Everyone can download a wallet for free. You do not have to ask for permission or disclose any personal data to own a wallet. There are many wallets on the market differing in detail but all working by the rules of the Bitcoin protocol. It does not matter which one you use; you can send Bitcoins from any wallet to any other one. It's just like sending an email: you don't have to care whether the recipient uses Gmail, Thunderbird or Hotmail.

My Chinese friend – let's call her Li Ming – has to give me a Bitcoin address to which I should send the Bitcoins. Her wallet can generate endless numbers of these addresses, which consist of many different numbers and letters in upper and lower case. She can easily send this to me via email, as there is no technical risk if the address leaks. To access the money associated with it, you would need the matching private key, which only Li Ming knows. Or to be precise: her wallet knows the key. Normally she will not need to see this long string of numbers and letters.

However, if Li Ming does not want the Chinese government to know that someone from Germany sends her money, she should rather encrypt the email containing her Bitcoin address. One has to understand that sending Bitcoins is not anonymous, quite the contrary: every transaction is recorded in the publicly accessible Blockchain. The Chinese secret service only has to find out that the address 1BXXJ4PaN9u9NMyvYD-49voySUynAWnKwAe belongs to my friend Li Ming and they will know that someone has just sent her 0.1 Bitcoins. So she should better not publish her name and her Bitcoin address together. It also makes sense for her to use a new Bitcoin address for every transaction. Her Bitcoin wallet can easily do this, as there is no lack of these addresses.

Around the World in Ten Minutes

Now I choose the *Send* function of my Bitcoin Wallet, copy and paste Li Ming's Bitcoin address into the correct line and add the amount of Bitcoins I want to transfer. I may add a small transaction fee of about 0.0001 Bitcoins, which will go to the miner who successfully writes my transaction into a block. The fee is not obligatory, but it will reduce the time my transaction needs to be confirmed, as miners prefer transactions with a fee. When I click the *Send* button, the following information is used to create a transaction:

1. Li Ming's public key

2. The amount of Bitcoin that I transfer to her

3. A signature from my private key that proves that I can spend this amount of Bitcoins (the private key is not part of the transaction, but it is needed to authorize it).

The wallet then broadcasts the transaction to the worldwide Bitcoin network, where thousands of miners verify the submission. If it is verified, they try to integrate it into the next block of the chain.

After a few seconds, Li Ming's wallet will show her that the money is being sent.

On average it takes about ten minutes to receive a confirmation that your transaction has been recorded in the Blockchain. For a higher amount of Bitcoins, it is recommended to err on the side of caution and wait for six to seven confirmations. This is because the Blockchain sometimes splits into two separate forks, meaning two blocks are discovered at approximately the same time. Such a "soft fork," which causes some confirmed transactions to become invalid again, does not usually last for long. The network agrees on which path to follow as soon as the next block is found. The invalid

transactions have to be reconfirmed, which takes some extra time.

Neither Li Ming nor I will see any of the complicated computations on thousands of computers necessary to the success of our transaction. Like you don't need to have any idea of the SMTP, POP3 or IMAP protocol to send an email, you don't need to know the cryptographic algorithms that make Bitcoin work.

Tip 6 – Secure Storage (III): Hardware Wallets

An alternative that combines high security with better usability is a *hardware wallet*. This is a small device that stores your private keys. Its only function is to sign transactions. The most well-known hardware wallet is *Trezor*. With its small black-and-white screen and two buttons, it calls to mind an old-fashioned MP3 player. You connect it to the USB port of your computer, and all functions of the wallet are provided by the website *mywallet.trezor.com*. As the private keys are not stored on the web server but on your Trezor device, there is no risk of losing your keys through a hack. You could even use the computers in an Internet café for Bitcoin transactions. A PIN protects Trezor against theft. In case you lose your Trezor, the first thing you do before you start using it is to print out its so-called *seed key* and hide it in a safe place. If your Trezor device gets lost, you can buy a new one and restore the private keys from the seed key.

Paying with QR Code

QR codes simplify Bitcoin payments

If I pay for a cappuccino with Bitcoin at Café Floor's in Berlin-Kreuzberg, the process is similar. I would probably prefer to use a wallet that runs on my smartphone rather than one on my computer, which I don't carry all the time. Instead of receiving a Bitcoin address by email, the waitress shows me a QR code on her tablet computer. This black and white pixel code is just a computer-generated visualization of a Bitcoin address, so there is no need for copying and pasting. In this case the QR code even contains the amount I have to pay. So, I only have to scan the QR code with my smartphone, click *Confirm* and the money is on its way. As the value of a cappuccino is quite low, the café owner

will not wait for ten minutes (one confirmation) or one hour (six to seven confirmations) before she lets me go, but just accept the low risk that I would somehow find a way to double spend my money before the transaction is confirmed by the network. If they sold me their entire café, they certainly wouldn't be quite so cavalier.

The Security of Very Big Numbers

The long, number-and-letter packed Bitcoin addresses may look a bit scary at first, but they guarantee Bitcoin's security. The probability that any of these addresses are used twice is virtually zero. One could spend several lifetimes generating new Bitcoin addresses without ever receiving the same number twice.

This is an important security measure as Bitcoins do not exist as physical objects and are also not stored on my computer or cell phone, as one might assume. In fact, Bitcoins exist as nothing more than entries in the worldwide distributed ledger, the Blockchain. All that Bitcoin owners need is a public and the corresponding private key that allows access to their funds. Therefore, it is crucial that these key pairs cannot be guessed or computed.

Services like Netki make the rather awkward looking Bitcoin addresses easy to use for normal people. Instead

of having to copy monstrously long strings of numbers and letters, you can now use a wallet address like *wallet.aaronkoenig.com*. The service produces a new Bitcoin address for each transaction, but all you need to know is the name of the wallet.

Bitcoins behave like cash in many regards. You do not need to trust a third party like a bank to make a transaction. They cannot be blocked and frozen. They give you a certain amount of anonymity as long you take care not to connect your Bitcoin addresses to your identity. In contrast to cash, you can make backup copies of your Bitcoins, or to be precise, of the private keys. You can save them on a USB stick or print them out on paper and store the hard copies in secure places, like a safe or even a bank vault. Every copy of the private keys gives you access to your coins on the Blockchain, which is stored on thousands of computers. If your computer or cell phone gets lost or the printout gets burnt or flooded, the Bitcoins still exist. You can always access your funds, providing that you keep one backup copy and nobody has stolen your keys.

Just as you would be with cash, as a Bitcoin user you are responsible for your money. If someone steals your private key and moves the coins to his account, it is like losing your physical wallet filled with cash. There is no

emergency number that you could call to claim a charge-back, and no way to have the money returned. This is why proper education on private key storage is important. In info boxes 4 to 7 we present several methods for proper and secure storage. It might sound a bit difficult in the beginning, but these tools are becoming increasingly simple to use.

Tip 7 – What is Multisig?

Multisig is an abbreviation of "multiple signature transaction." For a normal Bitcoin transaction you need one person to sign it. But it is also possible to define transactions that need to be signed by several people with their private keys. You can create a transaction that will only be performed if two out of three sign it. A practical use case would be an online purchase. If the seller and the buyer agree, the pair will sign the transaction. But if there is a dispute, e.g. if the buyer is not happy with the quality of the product, a neutral person can hold the third key and act as an arbitrator who decides if the money is transferred or not. Other combinations such as "five out of six" or "eight out of eight" are also possible. Besides its function to make contract partners agree, multisigs increase security. If a thief steals only one private key, he cannot access the money; he would need to steal them all. Multisig wallets such as *bitgo.com* or *copay.com* make it easy to use multisig transactions.

The Blockchain Principle

Encryption methods and cryptographic algorithms pre-existed Satoshi's work. The distributed public ledger, the Blockchain, is Satoshi's real innovation. The idea to create a public, immutable, distributed database and to incentivize cooperation by issuing currency is a new and ingenious invention. There is unlimited potential in this innovation. It can be used in any situation in which humans must come to consensus without having to trust each other, as the system cannot be cheated. It enables people who do not know each other to cooperate and find consensus.

This opens up a variety of new and exciting methods of interaction. Throughout human history, only very small groups were capable of reaching consensus without a central institution, without hierarchies, and without power or coercion. Blockchain technology can end the age of command and control and finally allow humans to cooperate in ways previously unknown. Therefore, Blockchain technology has many more implications than being "just" a new currency and global payment system.

Before we take a closer look to the possibilities of Blockchain technology, let's debunk some of the most common prejudices and misconceptions about Bitcoin.

INTERVIEW

MORAN SHAKED

Tel Aviv

What fascinates you about Bitcoin?

Being a non technological person, the first time I have heard about Bitcoin, I didn't know exactly what it was, but I did understand the concept of it. I am a big believer in Bitcoin, first as technology more than a currency, and I do believe it is going to change the way we will be handling money in the near future. It's one of these things that once it happens, people start saying: how did we ever managed without it, just like it happened with cell phones. Can you truly imagine your life without it nowadays?

How did you get involved with Bitcoin?

My first real encounter with Bitcoin was in a Bitcoin Hackathon, the first one in Tel Aviv. Being the only woman and non tech one on top of it, I felt I must come up with an amazing idea to this Hackathon, my

ever first one. My idea won, and this is how I got my first two Bitcoins. This had opened the gate for me, to the amazing local Bitcoin community, and I started to get more and more involved, being part of the Tel Aviv Bitcoin Embassy and finally founding Miss Bitcoin Ltd.

What are your Bitcoin-related activities now?

I'm working on Miss Bitcoin, which is about bringing more women into the new digital finance world. More than 80% of the decision in a household are made by women, so we have decided to focus on them. Miss Bitcoin will show them the way to all things like digital finance and finance management in order to maximize their engagement with it. Miss Bitcoin focuses on developing educational products in order to encourage more women make that transaction.

What are the most important use cases of Bitcoin as money and payment system?

Transacting money internationally. If you ever tried to wire money from the US to Europe for example, it is unbelievable that the system still works this way today. It is long, complicated and ridiculously expensive.

What has to happen for Bitcoin to gain mainstream adoption?

Women must get into the game. As users and as consumers.

Why women?

Since they are the ones who are mainly in charge of running the household expenses. A household management is the smallest unit where all financial things happen, and it's crossing countries, religion and culture. A true change starts from these small basic financial units, billions of small financial cells. It must start from the small basic day to day financial decisions, and this is the home field of women, dominated almost exclusively by them.

Where do you see the biggest obstacles for that? How can they be overcome?

It is not user-friendly enough. Education and awareness are usually the answer when it comes to mass market change of habits and behaviors, as you could see in the education to the use of condoms to prevent Aids from spreading in Africa, recycling in western countries and

more. Once people understand how and why they need to change a certain behavior, we can start progress to the next level like offering them different products and services.

What else can be done with Blockchain technology? Which useful applications can you imagine?

I think the Blockchain technology will make lots of things in different fields decentralised. Whether it's the Internet or whether it's social networks and structures – it can go as high as governmental institutions.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

The main and first change is in the state of mind of people. The realisation and understanding of things being decentralised, and the real effect on one's life, is very powerful. It is like you have tasted something and now you can't imagine your life without it. Once the world will go Blockchain, we will not look back again.

How do you imagine the world after Bitcoin and Blockchain technology have gained mainstream adoption?

I think it will change and even destroy many old, irrelevant unchangeable structures. People are claiming their power back. Once the "small citizen" puts himself in the center and knows it is within his power to choose, then a competition starts. And competition always works for the benefit of us, as citizens and as consumers. Once everything is opened to competition, once old myths are being broken, once people's trust is not to be taken as obvious, everything is open and new rules and game will be applied. I think we will witness major changes especially in political and financial structures, e.g. decentralised regional governments.

6. Bitcoin CEO Bans China

Popular Falsehoods about Bitcoin

If people have heard of Bitcoin at all, it is usually by way of the mainstream media. Unfortunately, these sources hardly provide accurate, well-researched coverage. The mainstream media usually only report about Bitcoin when something dramatic happens, often focusing on bad news like exchange hacks, sudden drops in price, or the shutdown of a drug purchasing platform that accept Bitcoins as payment. You will rarely find relevant news about the growing number of Bitcoin-friendly merchants or innovative services and business models.

It is in the nature of mainstream media to perpetuate mistakes, misconceptions and misunderstandings. Journalists writing about complex topics generally lack the knowledge and time to gain a deep understanding of the issues they cover. The exception proves the rule. And this isn't just the case with Bitcoin – you will notice it every time you have intricate knowledge of a particular subject.

If you really want to inform yourself about Bitcoin, you need to follow specialized media and attend Bitcoin conferences. Of course, very few people actually do this. As a result, in most people's heads you will find a bizarre mélange of half-truths, fake reports and prejudices. There is no need to be worried about that. Mainstream media also portrayed the early Internet as a dangerous place full of terrorists, lunatics and porn addicts. It has obviously not stopped its worldwide success. And just as with the Internet, most preconceptions about Bitcoin can be clarified quite easily.

So here you go: the most popular falsehoods about Bitcoin and what to tell the people who still believe in them.

1. Bitcoins Are Only Good for Buying Drugs

You can buy pretty much everything you want for Bitcoins today, from pizza and consumer electronics to airplane tickets and alpaca socks. According to a study by payment provider Bitpay, there were about 100,000 online shops accepting Bitcoins at the end of 2014.[16] Given the high growth rate, this number has probably already significantly increased by the time you read this.

It is true that a handful of online shops were shut down because they sold substances that were forbidden under certain jurisdictions. The most prominent of these was the online marketplace *Silk Road*, where you could buy all kinds of drugs for Bitcoin. Nevertheless, one can assume that the vast majority of drug trades still take place in fiat currencies. It is actually a bad idea to use Bitcoin for illegal activities. Every Bitcoin transaction is recorded in the Blockchain forever, making them accessible to law enforcement. Although there is no direct connection to the name of the sender or receiver, many things can be revealed by data analysis. Criminals must be extremely careful to never use any information revealing their identities or locations. So, it is actually much safer to use cash for any illicit activities.

2. You Cannot Touch Bitcoins, So They Are Not Real

The vast majority of money no longer exists in physical form, but as digits in a bank's computer system. Paper banknotes and physical coins are becoming less and less important. In this regard, there is little difference between Bitcoin and state-issued currencies. In contrast to fiat money, which can be created from nothing, the creation of new Bitcoins is strictly regulated and limited. This makes dollars, euros and yuan much more "virtual" than Bitcoin, which mimick the rarity of precious metals. In our digital age, many valuable things are no longer physical. If you spend money for credit on your cell phone, Google search terms or magic swords in a computer game, you should have no problem to accepting Bitcoins as real.

3. Bitcoin is a Speculative Bubble

In a typical bubble the price of an asset rises dramatically before crashing and stagnating at a low value. A popular example is the Tulip Bubble of the Netherlands in the 1630s, when speculation drove the prices for some tulip bulbs to insane heights. For a short time, the prices of certain tulip bulbs were higher than the prices of a house in Amsterdam. When people realized that there's no sense in paying exuberant amounts of money for such a short-lived good, prices plummeted and never

recovered. There were also sharp rises and drops of the Bitcoin price, so it may look similar to a bubble if you look at only a small part of its curve. But in contrast to a typical bubble, those sharp rises and sudden drops have happened several times. The Bitcoin price always stayed on a much higher level than before the rally – and its price rose to an even higher level in the next round. In retrospect, the alleged "bubble" looks like a small pimple on the face of the curve. Despite sudden drops and long periods of decrease, the long-term trend of the Bitcoin price has been upwards. One has to understand that Bitcoin is not an object of speculation, but a new technology with a high disruptive potential. A global payment network with high security and low costs undoubtedly has a sustainable value. As you can only take part in it if you own the digital token Bitcoin, its growing price is justified.

4. Bitcoin is a Ponzi Scheme

A *Ponzi Scheme* is a fraudulent business model promising high profits to its participants, but then pays the profits using the investments of latecomers. Such a scheme can only work as long as people are continuously joining. Ponzi schemes inevitably collapse, and late investors subsequently lose their money. Only the investors at the top of the pyramid benefit – and they do so at the expense of others. A famous example is Bernard Madoff,

who was convicted for fraud in December 2008. Another, less well-known Ponzi scheme is the German pension system, which pays out pensions for senior citizens from the contributions of working people. They can be sure never to get their money back, as the population shrinks and ages, which will inevitably lead to a system collapse.

Bitcoin has nothing in common with this fraudulent investment model. It does not rely on a steady growth of new investors, and there is no "Bitcoin company" that could benefit from new clients. It's true that some people who invested in Bitcoin when it was worth only a few cents are rich now, but not at the expense of others. They simply made a bet on a promising technology when hardly anyone was aware of its existence. This was risky, as their investment could have easily become worthless. You can compare them to people who invested in companies like Apple or Google in a very early stage: these early birds were rewarded for the risk they took by extraordinarily high profits. But in contrast to a Ponzi scheme you can still make money on these shares, as the companies still generate substantial values, even if you wouldn't make as much as an early stage investor.

There have been fraudulent activities based on the Ponzi principle in the Bitcoin world, just as there have been elsewhere. In the case of Bitcoin, the most famous Ponzi scheme was the sale of shares in mining farms that

did not actually exist. The alleged mining payouts were taken from the deposits of later investors.[17] Wherever money can be made, criminal activities will be found. This is regrettable, but has nothing to do with Bitcoin itself.

5. Bitcoin Has Been Hacked

Although many hackers have tried, the Bitcoin software itself has never been compromised.[18] The security measures based on established cryptographic algorithms that Bitcoin relies on seem to work extremely well. Not a single Bitcoin has ever been counterfeited.

What *have* been hacked are some exchanges and web wallets that did not invest in appropriate IT security. The most spectacular case happened in early 2014, when about 650,000 BTC were stolen from Mt. Gox, which at that time was one of the leading Bitcoin exchanges. The prevailing theory is that the theft insiders who had access to the core system were responsible, so it was probably not really a hack.[19]

One has to keep in mind that in the early days of Bitcoin, Bitcoins held very little value. Bitcoin enthusiasts built exchanges or other applications mostly for the fun of it. IT security was not their highest priority. In the early days, Bitcoin was seen more as an experiment than

as a serious business. But when the Bitcoin price skyrocketed, criminals were naturally attracted. They could easily overcome the sloppy safety precautions of first generation Bitcoin players.

Modern exchanges have a much higher level of security than Mt. Gox, which was originally a trading platform for phantasy cards. The biggest issues seem to happen when people do not respect the main principle of Bitcoin: never trust a third party. If you entrust the private keys to your coins to the company who runs a web wallet or an exchange, you should not be surprised if those Bitcoins get stolen. Always take care of your private keys yourself! An increasing number of companies are working to improve Bitcoin security, mostly by using hardware wallets (see info box 6) or multiple signatures (see info box 7).

Users and enterprises are learning how to avoid becoming the victim of targeted attacks. The "Wild West" days of Bitcoin with its frauds and hacker attacks will soon be history.

6. Bitcoin Has a Deflation Problem

Economists define inflation as the increase of the money supply. Deflation is its opposite: a money supply that shrinks. A classic example of a deflation is the

monetary reform of post-war Germany in 1948, when the German Reichsmark became invalid and all bank deposits were exchanged at a rate of 1:10 to the new Deutsche Mark. This radical reduction of the money supply (which was heavily inflated by the National Socialists to fund their war) and the abolishment of all wage and price controls resulted in the "German Economic Miracle" of the 1950s.

Today, the word deflation is often incorrectly used to describe a decrease in prices. According to the strict definition of deflation, Bitcoin is not a deflationary currency, as its money supply currently grows at about 9% a year. If we look at the prices of goods, we can see that when denominated in Bitcoin they have fallen sharply. Remember the two pizzas that were sold for 10,000 Bitcoins in May 2010? At the time of writing (September 2015), they would hardly cost more than 0.08 Bitcoins.

Followers of the economic theory of John Maynard Keynes ("Keynesians") claim that falling prices are bad for the economy and would make people postpone any purchase, as they would wait for the prices to fall even further. Keynesians do not seem to bother that such a behavior cannot be observed in real life. Prices of computers and mobile phones fall year by year. Still, people buy them when they need them – although they know very well that they could buy a device with the same qualities much cheaper in several months.

Unlike economists, normal people are happy about falling prices since they can buy more for their money. Every rational being would prefer a currency that rises in value to one that constantly loses purchasing power.

The ones who portray deflation – or, to be precise, a decrease in prices – as dangerous and harmful usually have a vested interest in inflation and rising prices. Governments love inflation, as it is a practical tool for them to secretly steal people's savings and devalue their debts. That is why they claim that deflation and falling prices are bad. So whenever a so-called "expert" who is on a government pay roll warns against the "deflation monster," you should remember why, and better read a good book written by an Austrian Economist about it.

7. Bitcoin Has Been Banned in China

In December 2013 the Chinese government introduced new rules for the Bitcoin industry. They forbade banks to trade Bitcoins, but they did not ban its usage in general. Quite the opposite: three Chinese Bitcoin exchanges (BTC China, Huobi and OKCoin) are the biggest in the world. A majority of Bitcoin trades are made in the Chinese currency yuan, and most mining computers are produced and hosted in China. The Chinese government even subsidizes Bitcoin startups.[20]

Like all governments, the Chinese regime is facing a dilemma. On the one hand, they fear the loss of power and control that Bitcoin inevitably means for them. On the other hand, they cannot afford to miss the chances that an innovative technology like Bitcoin brings. A new, blossoming industry creates new jobs and therefore new taxpayers, so some governments have positioned themselves as "Bitcoin-friendly." Among them are the UK, Switzerland and Singapore, who have already succeeded in attracting Bitcoin companies with their policies. Some governments and central banks have issued warnings against the risks of Bitcoin, which has not stopped their citizens from using Bitcoin. Some mainstream media misinterpreted these warnings as bans, which in most cases was not true. So far there are only two countries in the world that have explicitly banned Bitcoins: Bolivia and Bangladesh.

Most governments try to regulate the Bitcoin economy just enough – but not too much, as they do not want Bitcoin companies to move to another jurisdiction. Serious venture capital is being invested in Bitcoin startups, and a bevy of big companies like Microsoft, Dell or Overstock have started accepting Bitcoin. A Bitcoin ban in economically relevant countries is therefore highly unlikely.

8. The CEO of Bitcoin Committed Suicide

On February 28th, 2014, US citizen Autumn Radtke was found dead in her apartment in Singapore. Suicide was her official cause of death. Autumn was the CEO of the exchange *First Meta*, through which one could trade in-game currencies from popular computer games. Bitcoins played only a minor role in the company's strategy. Nevertheless, some media called her the *"Bitcoin CEO,"* as if she ran a company called Bitcoin, Inc.[21] Her suicide was even associated with the bankruptcy of the exchange Mt. Gox, which had happened only a few days earlier. This is mere speculation without any evidence – typical for the sloppy nature of many mainstream media.

Of course, Atumn Radtke was not the "CEO of Bitcoin." Firstly, she did not have much to do with Bitcoin and most importantly, there is no company called "Bitcoin" who owns or runs the payment system and currency with this name. Bitcoin is just a protocol that defines how computers communicate with each other to transfer value. The Bitcoin software is completely open source, which means that it does not belong to anybody and can be used by everyone. Based on this public protocol, an ecosystem of commercial companies is flourishing. This can be compared to companies like Google, Facebook or Amazon, who have built their business models on top of the public and open Internet

protocol. Its open and decentralized character is an important strength of Bitcoin, as it offers no single point of failure. Tyrannical governments may shut down Bitcoin companies, arrest their CEOs or even make them commit suicide. But Bitcoin as a whole is unstoppable.

The Bitcoin news service *Coindesk* satirized the media's gaffes rather cleverly. On April Fool's Day in 2014, they ran an article titled "CEO of Bitcoin Officially Bans China."[22] Despite the headline's nonsense, it does contain a grain of truth. Bitcoin does not have to fear the state. It is the state that will be shaken to its very foundations by decentralized technology.

Tip 8 – How can I find out more about Bitcoin?

Bitcoin is developing rapidly. If you want to stay up-to-date, there are many websites and blogs you may follow. Good starting points are the website *www.bitcoin.org*, which is available in more than 25 languages, and *www.weusecoins.com*. News websites such as *www.coindesk.com*, *www.cointelegraph.com* and *www.bitcoinist.com* report on current developments and trends. If you want to know more, you should visit one of the many Bitcoin meetups and conferences that happen all around the world. There you can listen to talks, participate in discussions and meet other people who are interested in Bitcoin. You can find a good overview here: *bitcoin.org/en/events*.

INTERVIEW

DAVID JOHNSTON

Austin, Texas

What fascinates you about Bitcoin?

The fact that the Bitcoin network has become a global movement without the traditional structure of a CEO, a sales force, or a paid development team. That really amazes me and got me thinking about how Satoshi had set in place the fundamentals of open source, a digital token, a fully peer-to-peer system and secured it with the proof of work mechanism. I've been thinking and working toward building projects using that model ever since.

How did you get involved with Bitcoin?

In 2012 I was talking with a software engineer friend of mine about decentralized systems and he mentioned that Bitcoins had reached a price of $10 recently. I hadn't heard of the Bitcoin network before that and when he described it as a stateless currency controlled by mathematics I was immediately hooked and began intensely

researching it. Within a few weeks I made the decision to convert my wealth from fiat to crypto, a process which ended up taking four months time.

What are your Bitcoin-related activities now?

Today, I run a venture capital company that buys digital tokens in the Bitcoin system, but also in all of the technologies being developed on top of the Bitcoin network. So think of it as buying tokens that let you access the Internet and then wanting to buy tokens that access all of the cool website built on top of the Internet. These tokens have a value because as they provide value to people they demand more and more of these services.

What are the most important use cases of Bitcoin as money and payment system?

Right now I believe the most compelling use cases for Bitcoin is as a long-term savings/store of value, and in the developing world for use by the unbanked and those without access to financial services.

What has to happen for Bitcoin to gain mainstream adoption?

In order for Bitcoin as a currency/payment network to gain mainstream adoption, the ways of hedging or

eliminating the currency price risk for the average user must be improved. Projects such as Coinapult's "Locks," HopeGoldCoin's tie to gold reserves, Digital Tangible's tie to physical precious metal coins and Tether's link to USD are all big steps forward. By giving the average user confidence that their buying power isn't going to radically change in the near term, we will reach the same level of confidence we have achieved with merchants via services such as GoCoin, Coinbase, and Bitpay.

Where do you see the biggest obstacles for that? How can they be overcome?

The single largest obstacle in the way of this move toward stable value is the counter party risk inherent in someone else (a vault service) holding assets on the behalf of another person. It will be up to these projects to prove they can achieve real time auditing and transparent processes leveraging the capabilities of the Blockchain to do so.

What else can be done with Blockchain technology? Which useful applications can you imagine?

The applications of Blockchain technology are limitless. Its similar to asking what applications can we use the Internet for? While the Internet is built on information transfer protocols, the Blockchain is built on the

immutable recording of information secured by a vast distributed network. So any record or data set worth securing forever will end up connected to the Blockchain sooner or later. Examples include the obvious high value records of ownership for stocks, bonds, land titles, medical records, but also game tokens, computer files and documents. *Factom.org* in particular is making these applications possible through its general purpose data layer for the Blockchain.

How can Bitcoin and Blockchain technology change the way we live? What are the implications for society?

I believe the most important shift this technology will bring in our lives is that of increasing the level of honesty in our interactions and the behavior of large institutions. Gone will be the days where a bank or large institution can change or alter records, hide behind a barrier of non transparent information.

How do you imagine the world after Bitcoin and Blockchain technology have gained mainstream adoption?

Our buying power will not be constantly eroded away by inflation of the money supply. I can't emphasize how much this single change will improve the lives of

the vast majority of the world's population, who today must run on a constant tread mill just to keep up with this invisible transfer of wealth from themselves to the financial institutions running the monetary systems.

Which other important question have I forgotten to ask? Please answer it.

The question of how people can get involved in this movement. I'd say that this is an amazing time to add your skills and intelligence to this cause for which the time has come. It's still the very early days, perhaps analogous to the early 1990s and the development of the Internet. Now is the time to make your own mark on this young industry.

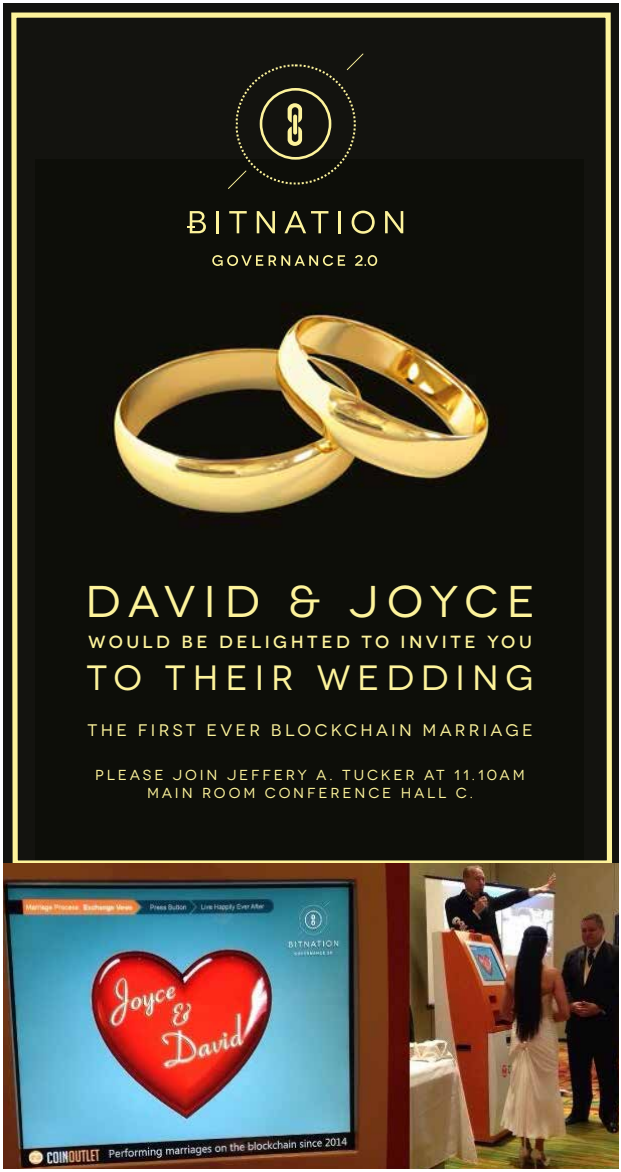
7. Blockchainification

Decentralizing All Aspects of Life

Disney World Florida, October 5th, 2014. During the Bitcoin conference *Coins in the Kingdom*, the world's first "Blockchain wedding" takes place. Joyce Bayo and David Mandrus are married today, and they do not need a marriage registrar, not even a ship captain or a justice of the peace to do so. Their wedding vows are added in this line of text in a Bitcoin transaction: *"For better or worse, 'til death do us part, because the Blockchain is forever."* After signing the transaction with their private keys, it

becomes registered onto the Blockchain for eternity, for everyone to see. The wedding ceremony is streamed live by the libertarian web platform *liberty.me*. Its founder Jeffrey Tucker acts as the master of ceremony, dressed in an elegant suit and bow tie, as always.

"We believe that like the Blockchain, our love and marriage are forever and that our relationship is not defined by governments or the church," explains David Mandrus, the groom.[23] Joyce and David want their marriage to be publicly documented and auditable for everyone, as you would expect it from any marriage. In the pre-Blockchain age one would need a trustworthy institution to maintain a central wedding register. This could be consulted in cases of doubt, like an assumed marriage swindle. But it is no longer necessary. In the decentralized age you need neither a bank to transfer money nor a central register to get married. The Blockchain cannot be manipulated by anyone and all entries are publicly accessible. What else do you need for a document that proves a marriage, the closing of a contract or the transfer of property? There is no reason why documents stored in the Blockchain should not be legally acknowledged. They are at least as trustworthy as those with an official seal.



The first Blockchain wedding

Blockchain, Not Bakshish

All documents that need to be registered in some kind of central register – like birth certificates, land deeds or company registries – can be stored just as permanently and securely, but more quickly and cheaply, on the Blockchain. The immense administration effort that is spent on these undoubtedly useful things can be minimized significantly. If you buy a house today, you need to change its ownership in the land registry. This incurs hefty fees from the notary and the registrar, and it takes surprisingly long. On the Blockchain, it costs a few cents and can be settled in ten minutes. Furthermore, it would be much harder for governments to justify and collect a tax on the transfer of private property if the state is no longer involved.

Bitcoin entrepreneurs in Botswana

Getting the state out of this business also means that a typical point of attack for corruption can be avoided. In many countries you have to pay both the legal fees to get the right stamp from some government official and a bribe to really get things done. Sometimes, you will not even find trustworthy land or company registries, so it is hard to prove that you own a piece of land or a company. This makes buying real estate and founding companies difficult, time consuming and expensive. The more freedom entrepreneurs have to build their businesses and create jobs without being hindered by red tape, the better off the people are. The wealth of a country depends to a high degree on its legal system and how well it protects private property. Countries with an inefficient and corrupt bureaucracy are among the poorest, least well-developed ones. In contrast, successful economies are usually characterized by a slim, efficient and corruption free administration.

A Leap Ahead for the Developing World

Blockchain technology may enable countries in Africa, Latin America and parts of Asia, which are plagued by inefficient and corrupt bureaucracies, to move to a higher level of civilization. A similar development may happen as in the telecommunications industry. For many years, people in those countries would not have access

to telephones, as the land lines operated by state-owned telephone companies were very expensive or simply not available. One would have to wait for years to get one, if at all. Today, a high percentage of people in developing countries own and use cell phones. They are easy to get and cheap, since cell phone operators are private companies that have to survive in highly competitive markets. In a similar way, people in the developing world may leapfrog inefficient state bureaucracy and directly use intelligent, decentralized solutions for all kinds of services that are now provided by the governments.

The first user of a Blockchain ID

The Blockchain wedding described above was organized by the collaborative platform *Bitnation*. Its goal is

to offer all services that so far were offered by governments in a voluntary, decentralized manner. They want to see the state monopoly replaced by a competition between private service providers. With Bitnation, not only can you get married, but you can also issue your own Blockchain-based identity card, register land, organize insurance and much more. While Bitnation is decidedly anti-government, the company *Factom* from Texas offers Blockchain-based services to governments to make them work more efficiently. They are currently assisting the Honduran government with the setup of a Blockchain-based land registry.

Coins With a Color

Not all new services that are based on Blockchain technology are of such a political nature. *Colored Coins* uses the Bitcoin Blockchain to make all kinds of assets easily tradable, be it shares, bonds or commodities. A colored coin is a small fraction of a Bitcoin, which is marked with an additional piece of code. This code makes it represent a specific asset. In order to make this easier for humans to imagine, the software mark is called a "color". A Bitcoin fraction marked "red" may represent a share, a "golden" colored one a gold bar. By transferring these colored coins not only its small Bitcoin value changes the owner, but most importantly the asset that

is associated with it. This is supposed to simplify trading financial assets and making it accessible to many people.

Colored coins

Decentralized Apps

Another important utilization of Blockchain technology are so-called *Decentralized Applications*. Like Bitcoin they are built on the peer-to-peer principle and work without a central server. If you want to use such a service you need to own special tokens – as you need to own *Bitcoins* (the digital currency) to take part in the global payment system *Bitcoin*.

One example is a service called *Maidsafe*, which allows computer users to rent out unused parts of their hard

drives. It works similar to cloud storage services like Dropbox or Google Drive, but it does not need huge server farms. Instead it distributes the data on the available hard drive sections of its users. All data are encrypted so that only the owners can use them. So far such a service would not have been economically feasible, but Blockchain technology permits it. The providers of hard drive space are paid in *Safecoin*, a digital currency that in many respects resembles Bitcoin, but it only works inside the Maidsafe system. Later there will be exchanges on which you can change your Safecoins into other currencies such as Bitcoin, dollars or euros. Instead of giving out shares of the company for venture capital, Maidsafe organized a crowd sale and sold a part of its internal currency to investors. Obviously many made a bet that Maidsafe becomes a success and the price of Safecoins would rise. In April 2014 Maidsafe sold all of the available Safecoins for about six million dollars in just five hours.[24] There are several other companies for decentralized apps who work on similar solutions, for instance to rent out unused computational power.

Smart Property

Another very interesting aspect of Bitcoin is its programmability. You can include a limited amount of code into a Bitcoin transaction. This may contain conditions on when to execute a certain action, for instance only

after a specific payment has been received. By using this feature the ignition of a leased car could be blocked if the leasing rate has not been paid. One can also imagine vending machines that pay for their fresh supply from a given budget once they are empty. A popular umbrella term for this is *Smart Property*. The vision of an Internet of Things where objects of utility are connected and can communicate and trade with each other could become reality through Blockchain technology.

Decentralizing Everything

The *Ethereum* project goes beyond that. It is supposed to be a modular system which lets you build all kinds of services like voting, decentralized exchanges, crowdfunding and much more. Like Bitcoin it is built on the peer-to-peer principle and uses its own currency called *Ether*. It offers more possibilities than Bitcoin to define so-called *Smart Contracts*. These are contracts built out of software code containing contractual clauses. They will be executed automatically, so that most legal disputes can be avoided. For instance, meeting certain pre-defined benchmarks may lead to an automated payment without the need for a dunning program.

The term *Smart Contract* was coined by Nick Szabo, who also invented Bitcoin's predecessor *Bit Gold* (and who is believed by many to be the man behind Satoshi

Nakamoto). Whereas the programmability of smart contracts in the Bitcoin protocol is rather limited, Ethereum has its own programming language offering many more possibilities. Miners of the Ethereum network can execute its software code, enabling a decentralized Internet free of servers that works entirely as a peer-to-peer network. This grand vision has inspired many investors: during a crowd sale of about 60 million Ethers in July 2014, Ethereum cashed in 30.051 Bitcoins to fund its development, at the time worth about 14 million US dollars.[25] Big companies like IBM and Samsung have already announced partnerships with Ethereum to commercially exploit its technology once it is ready.[26]

Everything That Can Be Decentralized Will Be Decentralized

Blockchain technology has become one of the most popular buzzwords in the venture capital world. A lot of money has been invested in startups that work on services and applications using the Blockchain principle for all aspects of life. Some use the existing Bitcoin Blockchain and add extra layers to it. Others build their own Blockchain and mining network. Some even create private Blockchains that may be accessed and maintained only by authorized users. As it is always the case with waves of innovation, only a small percentage of these startups will succeed and survive. But one thing

is clear: this is a revolution. Blockchain technology lets people realize ideas that have been considered unrealizable before.

All these projects rely upon the insight that centralized solutions are prone to errors and manipulation. Decentralized solutions are by far superior. Errors will happen, too, but they do not jeopardize the whole system. This is something that was well understood by the old Austrians. Ludwig von Mises and Friedrich August von Hayek had no idea about peer-to-peer networks or decentralized applications, but they brilliantly analyzed why a centrally planned economy has to fail and why it is inferior to the dynamics of a free market. A market is a highly decentralized phenomenon, in which the individual decisions of millions of people lead to much better results than those of a central planning authority. The "decentralization of everything" as the Blockchain pioneers have it in mind, can be considered a coherent advancement of Austrian thinking.

INTERVIEW

SUSANNE TARKOWSKI TEMPELHOF

Rio de Janeiro

What fascinates you about Bitcoin?

When I learned about it, I was mostly fascinated by the fact that it was borderless, international, beyond the control of national governments.

Over time, as I learned more about Bitcoin and its underlying technology – the Blockchain – I realized perhaps 75% of the services the government provides could be replaced by that technology, which is nothing short of amazing.

How did you get involved with Bitcoin?

During my years as a government contractor I ran into a guy working for DARPA on the Afghan/Pakistan border, and he immediately struck me as someone super smart and fun, someone who was up to speed on all the most radically disruptive stuff going on. He was

a burner, living in California, experimenting with bio-hacking and all sorts of things. On one of his trips to DC where I was based out of at the time, in 2012, he showed me a Bitcoin – a physical one in gold – and explained what it was. I was totally mind blown and fell instantly in love with the concept.

What really struck me was that all these years I had thought somehow that changing the system from the inside was the most realistic option, although I had slowly starting to realize it wasn't really at all. And then insert Bitcoin: a brand new currency, created from nothing, set to outcompete fiat. Built without government permission, intervention, lobbying etc. That was one of the reasons I left my work with the government – I suddenly realized doing stuff outside of the system was not only doable – but also more efficient to achieve real change.

Just create something better, and outcompete the old outdated paradigm through making it irrelevant!

What are your Bitcoin-related activities now?

I'm the founder and CEO of Bitnation, the world's first fully virtual nation. We provide all the services traditional governments provide, but in a non-geographically contingent way, meaning that it doesn't matter where you're born or what passport you hold, you have the

right to enjoy the best services on the market. It's also voluntary, meaning it's not imposed through any nation state or transnational organization, and anyone can fork the code and create their own competing alternative.

We use the Blockchain technology – a decentralized distributed public ledger and database – to expedience most of the services governments provides, everything from record keeping, timestamping, dispute resolution, insurance, ID and reputation systems, and more.

I do it, because I want a world where people are free to choose whichever government they want, regardless where they live. I want to live in a world with thousands or millions of governments that competes for its citizen through providing better services, not through enforcing violence within arbitrary borders.

What are the most important use cases of Bitcoin as money and payment system?

In frontier and emerging markets, amongst the billions of unbanked people.

What has to happen for Bitcoin to gain mainstream adoption?

Adaption in the frontier and emerging markets.

Where do you see the biggest obstacles for that? How can they be overcome?

I don't think the obstacles are very big at all, it's just a question of communication and engagement with those audiences. It's already happening all around the world, particularly in remittance heavy markets.

What else can be done with Blockchain technology? Which useful applications can you imagine?

While there are obviously a multitude of financial application being built on the Blockchain which will no doubt revolutionize the financial industry, I'm more interested in the governance related applications, such as ID/reputation systems, dispute resolution, marriage, land titles, family contracts of all sorts, etc – frontier applications with Bitnation is working on.

The basic functions of those applications are different combinations of smart contracts, tokenization and time stamping.

How will Bitcoin and Blockchain technology change the way we live? What are the implications for society?

It will make nation state governments irrelevant.

How do you imagine the world after Bitcoin and Blockchain technology have gained mainstream adoption?

I imagine a much freer and wealthier world, based on voluntary agreements and a reputation economy, as opposed to the use of force imposed through arbitrary borders. I imagine a global world of free movement, where nation states will gradually fade away over the next 50–100 years, and gets replaced by a combination of city states and communes on a local level, and organizations like Bitnation on a global level. As we say at Bitnation: *'Blockchains, Not Borders.'*

8. Agora 2.0

Towards A Free Society

The Austrian School has proven that state interventions into the economy have harmful long-term effects leading to an impoverishment of society. As Hayek pointed out in his book *The Road to Serfdom*, state interventions tend to gain their own, uncontrollable momentum. The undesired side effects of a first intervention inevitably lead to a second, ostensibly better one. Naturally, this 'better' solution generates even more undesired side effects, and the chain of state intervention adds another link. This vicious circle will inevitably lead to a

totalitarian dictatorship if it is not consciously broken. Every centralized institution suffers from the basic problem of a "pretense of knowledge," as Hayek calls it. It is virtually impossible for a centralized organization to dispose of all information necessary to serve the needs and desires of millions of people. A much more powerful alternative that leads to more wealth and welfare than a centralized system is a spontaneous order such as a market which co-emerges from the many voluntary decisions of independent individuals.

The Libertarian View of the State

Libertarian political philosophy, which is deeply connected to the Austrian School of Economics, has a critical eye turned towards the state. As Ludwig von Mises famously opined:

"The state is an apparatus of force and coercion. The essence of the state's activity is to use force or threaten to use it in order to make people behave in a different way than they would behave voluntarily."[27]

Libertarian-minded people fascinated by Bitcoin and the Blockchain see these technologies as a chance to build a better and freer society based on voluntary action rather than on force and coercion. They view the

state in its current form as obsolete, arguing that it can be replaced by new methods of societal organization.

From Tribes to States

The nation-state we know today is a relatively young phenomenon. For the better part of human history, humans lived together in small groups, like tribes or clans. In these small groups members were all familiar with one another, making it relatively easy to solve problems and come to a consensus. This was no longer possible after the introduction of agriculture, when people started to live in bigger cities. Centralized structures of command and control were established, with a king-figure and a small nobility caste at the top. This seemed to be the only way to organize a society of a certain size.

But even the big empires we remember from our history classes were relatively loose, decentralized formations if we compare them to the states of today. Kings, emperors and pharaohs demanded tributes and soldiers from local rulers, but they had little impact on people's daily lives. The Industrial Revolution brought a dramatic increase in the level of government centralization. People were seen as small cogs in the giant machine of the state. This culminated in the totalitarian dictatorships of the 20th century that controlled each aspect of a citizen's life.

The modern welfare state appears less aggressive than these regimes, but while claiming to create "social justice" it also invades people's lives and creates dependency. In reality, the so-called social state makes people more anti-social. The natural solidarity that we have deteriorates when the state takes over. If you're already forced to pay high taxes to a government that claims to be responsible for the "common good," why provide for your neighbors? Unfortunately, the state is as incapable in running schools, hospitals and social security systems as it is in producing cars, cell phones or computers. The insights of the Austrian School about the shortcomings of a centralized bureaucracy are equally true for education, health and social security. Leaving these important areas to the state is not a good idea.

A Trend Towards Decentralization

While past advancements like the agricultural and the Industrial Revolution made society more centralized and hierarchical, new technologies like the Internet and the Blockchain have caused an opposing trend towards decentralization.

The Internet has decentralized communication. The days are over when one was dependent on a few sources of easily censorable information. We now have access to millions of information sources from all around the

world. At hardly any cost we can communicate directly with friends living anywhere on the planet. Every blogger or editor of a video podcast has the potential to reach a massive audience, all without the need for a government license or significant investment capital. The power of states and big media corporations has withered, while the power of the individual has increased.

Bitcoin and Blockchain technology are supercharging this trend. By using a digital payment system like Bitcoin, everyone can take part in the global economy without the need for a bank account or credit card. This opens up opportunities for people in developing countries, who can now offer their skills to the world. All they need to receive payments is Internet access, usually on a cheap smartphone.

Direct economic relations between people are now possible. Before, high fees for international transactions kept this from being a viable solution. Banks and credit card companies are no longer needed as gatekeepers, and the state no longer has power to control transactions or freeze accounts. This became obvious when the US government forced Visa, Mastercard and PayPal to freeze all accounts associated with Wikileaks. Julian Assange's popular whistleblower website subsequently started using Bitcoin in June 2011, bringing untold amounts of attention to the new digital currency.

Decentralized apps based on Blockchain technology give even more power to the individual and put the very existence of central institutions like the state into question. When you do not need government services to issue a passport, to register real estate or to resolve a legal dispute, what is the state good for at all?

Police and Jurisdiction

One of the few areas in which also die-hard libertarians consider coercion necessary is the fight against crime. Libertarians would only consider a deed a crime if there were a real victim. Laws against the "dispraise of state symbols" or the "disturbance of public order" are therefore not justified, as they do not protect the life, liberty or property of individual human beings. Laws which dictate what people may eat, drink or smoke are equally invalid according to the libertarian view, as everyone is responsible for his or her own body.

Avoiding crimes like murder, robbery or theft is obviously not possible without using force. A potential murderer won't be stopped by an empathic talk. Although the state does not have the best track record in stopping crime, many libertarians still consider jurisdiction and law enforcement to be a domain of the state.

Radical thinkers like Murray N. Rothbard have developed alternative models showing how even these state functions could be handled by private agencies competing against one another. Citizens would commission companies to provide security and solve legal disputes. Rothbard claims that an apparatus of police and jurisdiction that is funded by taxes has no real incentive for reducing crime, as it justifies their very existence. Private security companies would be paid for successfully avoiding crimes. The lower the crime rate, the higher their profit. So there would be a competition for the best methods to reduce crime, rather than a race for higher budgets funded by taxes.

Flaws of the State

There are lots of rather academic discussions among libertarians about whether the state should be abolished and replaced by private law and competition, or whether it should be limited to core areas and controlled by a system of checks and balances. In any case, we are far away from a free society that works with a limited or nonexistent state. In many countries the state still dominates a huge part of the economy. In my home country of Germany, about 70% of an average worker's income goes through direct and indirect taxes and compulsory social security contributions to the government apparatus.[28]

Ludwig Erhard, the architect of the German "Economic Miracle" of the 1950s and 60s, warned in vain against the cancer-like growth of the welfare state:

"People always have to pay dear for so-called 'welfare,' as no state can give more to its citizens than what he has taken away from them beforehand – and you have to deduct the costs of a welfare bureaucracy that inevitably degenerates into an end in itself."[29]

Our current system has an essential problem. If someone has the privilege to spend other people's taxes, he will naturally not act as responsibly as he would with his own money. This inevitably leads to waste, mismanagement and growing debts, as you can see in nearly all state-driven matters. Funding activities by coerced taxes has proven to be malfunctioning.

Even more harmful is the government's monopoly on money. Very few people are aware of the damage done on society by subtle inflation and the Cantillon effect, which benefits the ones close to the source of money at the expense of everyone else.

End the Money Monopoly!

A first and crucial step on the way to a free society is the reform of the monetary system. The government's

monopoly on money and all "legal tender" laws have to be abolished. State currencies such as dollar, euro or yuan may continue to exist, but there needs to be a fair competition for all currencies. Bitcoin and other decentralized currencies must have the same chances as money issued by the state or by private companies.

As in every fair competition, the best products will win. It is likely that people will continue to use the money they know by habit for a while. But in the long run, the inferiority of state-issued, unbacked money compared to currencies backed by gold or based on Blockchain technology will become so obvious that it will lose its importance.

Competition of Currencies

The competition for the best currency has already started. Besides Bitcoin, there are a few hundred digital coins that work by similar principles. Bitcoin has a huge and growing lead over competitors such as Litecoin, Peercoin or Dash because of its early start and network effects that benefit the leader of the pack. But there is no guarantee that this will stay like that forever. Maybe another digital currency will prove itself so superior to Bitcoin that it will outperform Satoshi's creation. Maybe a gold-backed currency or one that is backed by the shares of a company will win. The great thing about a

competition that is fair and not distorted by state-granted privileges for some players: the best one will win. Or, the best *ones*, as there may as well be several winners. Maybe some currencies will be used mostly for day-to-day payments, others for savings, others for international transactions. Bitcoin has opened the competition, and we should be grateful for Satoshi Nakamoto for making this possible. His invention made many people investigate and question the fiat money system and search for better alternatives.

Free market money

The Virtues of Voluntariness

If the state loses its monopoly on the money supply, it can no longer fund its activities by printing money and piling up debts. Using force to collect taxes will also be

less and less effective as the citizens' incomes are no longer traceable thanks to encryption technologies. The old method of extorting money by force from people without letting them decide how to spend it becomes obsolete. Voluntary payments will replace coerced taxes. Many activities that were organized by the state so far can be taken over by private enterprises, either profit-oriented or not-for-profit ones.

Only those tasks that are probably better executed by the state will remain in its domain, but they need to be funded by voluntary donations. One could imagine an individual Bitcoin address for every task. By sending money to a specific address, citizens will decide which tasks are the most important ones for them. By using multiple signatures and smart contracts, they will remain in control of their funds. Their money will only be paid out if well-defined criteria are fulfilled.

People are interested in things like museums, public libraries and public transport, so they will continue to exist in a system that is based on voluntary payments. The difference is, that people can decide by themselves on what to spend their money rather than delegate the decisions to bureaucrats and politicians. Civil associations, foundations and cooperative societies will take over most of the activities that are handled by government agencies today. Instead of voting for politicians every four years, we will use Blockchain technology to come

to a consensus about critical questions, even with people we have never met. These decisions will not resemble today's referendums, as only those who actively support a project may take part in a decision, either by financial contributions or by voluntary work. A "dictatorship of the majority" which forces a minority to pay for the others is no longer possible.

The democracy of the future will be much closer to the Greek original. It is no coincidence that the Greek word *Agora* describes not only the central square in a city which was used for elections and referendums, but also means *market*. Thanks to Blockchain technology, human cooperation will again be based on individual decisions and self-responsibility, as you can observe them on a truly free market.

It's the Technology, Stupid!

Is this vision of a free society realizable? It is up to us. For the first time in history, technologies like cryptography and the Blockchain make it possible. Big leaps in civilization were usually triggered by new technologies – be it the wheel, the printing press, the steam engine or the computer. Most people were not even aware of the giant disruption they were experiencing, as new inventions usually take quite a while to come into popular use. After having reached a tipping point, it is hard to

remember how the world could have ever worked without them. This will be similar in the case of decentralized money. We are still in its very early stage, in which most Bitcoin users are idealists who dream of a better world without banks and governments. But most people do not think like that. They do not care for cryptography, the monetary system or an economic school from ancient Austria. But they would use a new technology if it saves them time and money.

As we have seen, Blockchain technology has the potential to provide this. Many services that required significant time and effort in the old world become faster, cheaper and more secure if realized with Blockchain technology, be it worldwide payments, smart contracts, the transfer of assets and many other things.

Now it is up to entrepreneurs to create useful and user-friendly products and to market them efficiently. In most cases, one would not even know that they are based on Bitcoin and Blockchain technology. People would not use them because they want to change the world, but because they serve their daily needs in a more economic way. So if you really want to do something for a free society, you do not have to found a "Bitcoin Party" or start a University for Austrian Economics. The best way to make the world a better place is to create Blockchain based products that wow people and are really useful for them.

The Honeybadger of Money

At the moment it is not easy to be a Bitcoin or Blockchain startup. You have to cope with all kinds of regulatory issues, pay expensive lawyers and spend a lot of time talking to clueless regulators. In some countries it is nearly impossible to get a bank account if you do any kind of Bitcoin business. Some governments have banned Bitcoins, but most of them try to apply rules to it that were made for the old financial system. This doesn't make much sense, as the old rules were only necessary because you had to entrust third parties like banks or credit card companies. But Bitcoin works without trust in third parties. The software protocol itself already contains the regulation. Additional regulation would only stifle innovation and scare away companies into other jurisdictions.

A good example of the damage that can be done by regulation is the *Red Flag Act* of 1865, which regulated locomotives and automobiles in Britain. It determined a maximum speed of four miles per hour and a minimal staff of three people to steer any car: a driver, a mechanic and a third guy who would walk in front of the vehicle with a red flag to warn other road users. Only when this absurd rule was repealed in 1896 could a car industry develop in Britain. In unregulated Germany, many car companies were already flourishing. The British car industry could never catch up with this lead.

Today, most of the originally British car brands and factories belong to German companies.

The way Bitcoin is handled today reminds of the attitude many people had towards the Internet in the early 90s, when it was first gaining popularity. If you had anything to do with it, people would sneer at you like you were some weird computer nerd. Big companies like AOL or Deutsche Telekom had their own online services. They did not consider the Internet to be a serious competitor, but a strange playground for geeks.

It was a long way from the early days of the Internet in the late 60s and early 70s, when it was only known to a handful of academics, to the World Wide Web of today with its billions of users. It took the Internet more than 30 years to reach mass adaptation. Fortunately its development was not stifled by regulation. Even totalitarian regimes do not succeed in completely blocking the net. They likely regret that the Internet was not forbidden in the early days, as it is now impossible to roll it back. Some publishing houses and record companies who went out of business may have the same regrets. But I assume that most people are happy about the Internet and could not imagine a world without it.

Similarly, some banks and government may hope that decentralized money disappears again, but the odds are low. Bitcoin has been declared "dead" numerous times:

the website *www.bitcoinobituaries.com* counts 72 death notices as of September 2015. But Bitcoin has always come back. Backlashes like hacked exchanges or drastic price drops have not killed Bitcoin, quite the contrary, they have made it even more persistent. Some call it the "honey badger of money," as the honey badger (*mellivora capensis*) has an extremely thick skin that even bears snake bites. It is such a fearless fighter that it takes on lions and hyenas. Bitcoin users like this attitude and wear t-shirts and buttons sporting the "badass" animal.

The honeybadger – the bitcoin-mascot

Even if Bitcoin itself fails for whatever reason – the genie is out of the bottle. Many potential successors like Litecoin, Peercoin or Dash stand in line to take over. Blockchain technology has proven to be robust and reliable. Even big players of the financial industry start using it. And as we have seen, it can be utilized for many other things than payments.

We should get ready for a world without a state monopoly on money, maybe a world without monopolies and states at all. Let's make the best of it!

INTERVIEW

SATOSHI NAKAMOTO

When did you start to work on Bitcoin?

I've started the work about two years before I released the white paper. I actually did this kind of backwards. I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper.

Why did you invent it?

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

So it's all about not having to trust anybody?

(Nods his head) A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

Why did you choose a peer-to-peer solution?

Governments are good at cutting off the heads of a centrally controlled network like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.

Why did you chose a fixed total amount rather than a money supply that grows with the economy? Is it because of decentralization?

Indeed, there is nobody to act as central bank or Federal Reserve to adjust the money supply as the population of users grows. That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that. In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is determined and the value changes. As the number of users grows, the value per coins increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value.

Can you elaborate on Bitcoin's similarity to gold?

As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: it is boring grey in color, not a good conductor of electricity, not particularly strong, but not ductile or easily malleable either and not useful for any practical or ornamental purpose.

But it has one special, magical property: it can be transported over a communications channel.

You mean, the qualities that make up gold's so-called "intrinsic value" are not that important?

I think the traditional qualifications for money were written with the assumption that there are so many competing objects in the world that are scarce, an object with the automatic bootstrap of intrinsic value will surely win out over those without intrinsic value. But if there was nothing in the world with intrinsic value that could be used as money, I think people would still take up something.

It seems that it is possible to spend to Bitcoin address that are invalid, making the coins lost forever. Wouldn't that mean the effective number of coins go down – as a sort of "natural deflation"?

"Natural deflation"… I like that name for it. Yes, there will be natural deflation due to payment mistakes and lost data. Coin creation will eventually get slow enough that it is exceeded by natural deflation and we'll have net deflation. Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone.

Isn't Bitcoin mining a waste of resource?

It's the same situation as gold and gold mining. The marginal cost of gold mining tends to stay near the price of gold. Gold mining is a waste, but that waste is far less than the utility of having gold available as a medium of exchange. I think the case will be the same for Bitcoin. The utility of the exchanges made possible by Bitcoin will far exceed the cost of electricity used. Therefore, not having Bitcoin would be the net waste.

Bibliography

Andreas Antonopoulos: *Mastering Bitcoin*, O'Reilly, Sebastopol 2014

Roland Baader: *Geldsozialismus*, Resch, Gräfelfing 2010

Roland Baader: *Geld, Gold und Gottspieler. Am Vorabend der nächsten Weltwirtschaftskrise*. Resch, Gräfelfing 2004

Philipp Bagus: *Warum andere auf Ihre Kosten immer reicher werden – und welche Rolle der Staat und unser Papiergeld dabei spielen*, FinanzBuchverlag, München 2014

Phil Champagne: *The Book of Satoshi – the Collected Writings of Bitcoin Creator Satoshi Nakamoto*, E53 Publishing 2014

Dominic Frisby: *Life After the State*, Unbound, London 2013

David Graeber: *Debt: The First 5,000 Years*. Melville House, New York 2011

Friedrich August von Hayek: *The Road to Serfdom*, Routledge Press, London 1944

Friedrich August von Hayek: *The Denationalisation of Money*, Institute of Economic Affairs, London 1976

Hans-Herrmann Hoppe: *Der Wettbewerb der Gauner: Über das Unwesen der Demokratie und den Ausweg in die Privatrechtsgesellschaft*, Hubert W. Holzinger, Berlin 2012

Hans-Herrmann Hoppe: *Demokratie: Der Gott, der keiner ist*, Waltrop, Leipzig 2003

Karen Ilse Horn: *Hayek für Jedermann*, FAZ-Buch, Frankfurt am Main 2013

Ludwig von Mises: *Theorie des Geldes und der Umlaufmittel*, Duncker & Humblot, Leipzig & München 1912

Ludwig von Mises: *Human Action*, Yale University Press, New Haven, 1949

Ludwig von Mises: *Socialism: An Economic and Sociological Analysis*. Yale University Press, New Haven 1951

Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

Thorsten Polleit (Hrsg.): *Ludwig von Mises – Leben und Werk für Einsteiger*, FinanzBuchverlag, München 2013

Thorsten Polleit/Michael v. Prollius: *Geldreform – vom schlechten Staatsgeld zum guten Marktgeld*, Lichtschlag Medien, Düsseldorf 2011

Murray N. Rothbard: *America's Great Depression*, Van Nostrand, Princeton 1963

Murray N. Rothbard: *Das Scheingeld-System*, Resch-Verlag, Gräfelfing 2005

Murray N. Rothbard: *For a New Liberty – the Libertarian Manifesto*, Mises Institute, Auburn 1973

Nick Szabo: *Shelling Out – the Origins of Money*, http://szabo.best.vwh.net/shell.html

Rahim Taghizadegan: *Wirtschaft wirklich verstehen*, FinanzBuchverlag, München 2011

Paul Vigna/Michael Casey: *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*, St. Martin's Press, New York 2015

Thank You!

Boris Adloff, Dante Castiglione, David Johnston, Diego Guitérrez Zaldivar, Eddy Travia, Elisabeth Becker, Franco Daniel Amati, Felix Weis, Frank Schäffler, Gavin Andresen, Janina Lowisz, Jörg v. Minckwitz, Julia Tourianski, Marcin Dzieniszewski, Marek Palatinus, Maria Jones, Moran Shaked, Phil Champagne, Rodolfo Andragnes, Roger Ver, Satoshi Nakamoto, Steffen Krug, Stephanie Murphy, Susanne Tarkowski Tempelhof.

About the Cover

The cover picture of the author was taken by Marcin Dzieniszewski from TinType Berlin (*www.tintypeberlin.com*), using a photographic technique from the 1850s. We assume that the founders of the Austrian School of Economics were photographed using the same technique.

Endnotes

1 "Argentine Small Business Turning to Bitcoin," Financial Times, July 19, 2015.
2 http://www.marketwatch.com/story/argentina-suffers-beef-shortage-due-to-price-controls
3 Roland Baader: Geldsozialismus, Resch, Gräfelfing, 2010.
4 J.P. Morgan 1912 in a public hearing at the US Congress
5 http://www.libinst.ch/publikationen/LI-Paper-HuertadeSoto-Finanzkrisen.pdf
6 http://www.tradingeconomics.com/united-states/money-supply-m2
7 http://www.measuringworth.com/uscompare/relativevalue.php
8 http://www.usgovernmentdebt.us/debt_deficit_history
9 https://en.bitcoin.it/wiki/History
10 http://www.bitcoin-exchange-berlin.com/2013/12/wie-ensteht-der-wert-des-bitcoins.html
11 http://www.wired.com/2011/11/mf_bitcoin/
12 http://www.coindesk.com/bitcoin-petroleum-time/
13 http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/
14 http://p2pfoundation.net/Bitcoin
15 https://bitcoin.org/en/faq
16 http://cointelegraph.com/news/113440/forget-price-heres-how-bitcoin-really-performed-in-2014
17 http://bitcoinexaminer.org/bitcoin-developer-gavin-andresen-suspects-cloud-mining-operations-ponzi-schemes/
18 www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4
19 http://www.coindesk.com/missing-mt-gox-bitcoins-inside-job-japanese-police/
20 The Chinese government among others subsidizes the payment enabler Blockpay (verbal information from its founder Hitters Xu)
21 http://www.nydailynews.com/news/world/bitcoin-ceo-researched-suicide-life-coroner-article-1.1941010
22 http://www.coindesk.com/ceo-bitcoin-officially-bans-china/

23 http://panampost.com/belen-marty/2014/10/07/couple-make-history-with-worlds-first-bitcoin-wedding/
24 http://blog.maidsafe.net/2014/04/23/maidsafe-sells-6-million-of-bitcoin-2-0-software-in-five-hours-press-release/ http://www.forbes.com/sites/kashmirhill/2014/06/03/mastercoin-maidsafe-crowdsale/
25 http://bravenewcoin.com/news/ethereum-makes-contracts-easy/
26 http://www.handelszeitung.ch/invest/ibm-und-samsung-setzen-auf-bitcoin-technologie-725583
27 Ludwig von Mises: Im Namen des Staates oder die Gefahren des Kollektivismus. Verlag Bonn aktuell, München 1982
28 http://sachsen-anhalt.parteidervernunft.de/ihre-skandal-se-abgabenlast
29 Erhard: Die Zeit, 15.8.1958

List of Images

p. 21: Shutterstock
p. 22: Clément Magnin
p. 24: Clément Magnin
p. 25: Clément Magnin
p. 26: Clément Magnin
p. 27: Clément Magnin
p. 30: Shutterstock
p. 33: Clément Magnin
p. 41: Fotolia
p. 45: Shutterstock
p. 61: iStock
p. 64: Shutterstock
p. 68: Shutterstock
p. 73: Bitfilm Networks GmbH, from the movie »Das Scheingeldsystem«

p. 75: Bitfilm Networks GmbH, from the movie »Das Scheingeldsystem«
p. 83: Anastasya Stolyarov
p. 91: Bitfilm Networks GmbH, from the movie »Bitcoin Deutschland«
p. 95: Bitfilm Networks GmbH, from the movie »Bopshop«
p. 105: Fotolia
p. 107: Blockchain.info
p. 108: Bitfilm Networks GmbH, from the movie »Mycelium Entropy«
p. 110: Bitfilm Networks GmbH, from the movie »Bitcoin Deutschland«
p. 118: Bitfilm Networks GmbH, from the movie »Bopshop«
p. 129: Aaron Koenig using a Creative Commons licensed image by Arend Vermazeren and a Creative Commons licensed Bitcoin-logo
p. 147: Fotolia
p. 149: Bitnation
p. 150: Alakanani Motherpky Itireleng
p. 152: Bitnation
p. 154: Bitfilm Networks GmbH, from the movie »Colored Coins«
p. 165: Bitfilm Networks GmbH, from the movie »Das Scheingeldsystem«
p. 174: Collage Aaron Koenig, using a Creative Commons licensed image by Arend Vermazeren