# 3隐私、身份、监视和货币

**Privacy, Identity, Surveillance and Money**

Barcelona Bitcoin Meetup at FabLab; Barcelona, Spain; March 2016

Video Link: <https://www.youtube.com/watch?v=Vcvl5piGlYg>

Today, I’m going to talk about the concepts of neutrality, decentralization, privacy, and what makes bitcoin so special. You’ve heard me talk a lot about bitcoin. When I use the word bitcoin, I am not talking about the currency. I am talking about a broader concept: the concept of completely decentralized, network-based, flat networks for providing trusted applications. If you happen to have a completely decentralized flat network that could provide trusted applications, the most logical first application is currency. But currency is just the first app.

今天，我将讨论中立、去中心化、隐私的概念，以及什么使得比特币如此特殊。

你听我说过很多关于比特币的事。当我使用“比特币”这个词时，我并不是在谈论货币。

我说的是一个更广泛的概念：完全去中心化的、基于网络的、平面的网络，它提供可信的应用。

如果恰好有一个完全去中心化的平面网络，它可以提供可信的应用，最合理的第一个应用是货币。

但货币只是第一个应用。

## 3.1银行：解放者到限制者

**Banking: Liberator to Limiter**

We are restructuring society by rebuilding institutions. Traditionally, our institutions have been hierarchical in design. This was an invention of industrialization, an 18th-century concept to allow people to organize and communicate at a larger scale. It was very effective at breaking the monopolies of kings and feudal systems. It has now run its course.

我们通过重建机构来重建社会。

传统上，我们的机构在层级设计。这是工业化的一个发明，18世纪的概念，允许人们更大规模地组织和交流。它在打破国王和封建制度的垄断方面非常有效。它现在已经走到了尽头。

Sometimes people ask me what my political positions are, and it’s very difficult to explain, but one word captures it, I think: I am a disruptarian. What that means is that every 30 or 40 years at least, things that have settled need to be disrupted. Because as they settle, power accumulates, they become centralized, and with centralized power, corruption happens. This isn’t a new concept. My ancestors—I come from Greece—figured out that corruption happens in systems of power, and absolute power produces absolute corruption. There is no more absolute power than the power over money.

有时人们问我：你的政治立场是什么？

这很难解释，但有一个词抓住了要点，我想：我是一个颠覆分子。

意思是，至少每30年或40年，已经解决的问题需要被颠覆。

因为随着他们解决了问题，权力开始积累，他们变得集权，有了集中权力，腐败就会发生。

这不是一个新概念。我的祖先（我来自希腊）知道腐败发生在权力体系中，绝对权力产生绝对腐败。

没有比对金钱的权力更强大的绝对力量。

"Every 30 or 40 years at least, things that have settled need to be disrupted. Because as they settle, power accumulates, they become centralized, and with centralized power, corruption happens. There is no more absolute power than the power over money."

“至少每30年或40年，已经解决的问题需要被颠覆。因为随着他们解决了问题，权力开始积累，他们变得集权，有了集中权力，腐败就会发生。这不是一个新概念。我的祖先（我来自希腊）知道腐败发生在权力体系中，绝对权力产生绝对腐败。没有比对金钱的权力更强大的绝对力量。”

We live in a world where banking was once a great liberator. It was an invention that moved finance from the realm of kings to the realm of everyday people. That system liberated billions of people. And then it got concentrated, it acquired power, and the power led to corruption. What we’re left with today is not a liberating system, and it’s time to disrupt it. Bitcoin is one of the things that will greatly disrupt centralization of power. Why is that?

在我们生活的世界里，银行曾经是一个伟大的解放者。

这项发明将金融从“国王的王国”转到“凡人的王国”。

这个系统解放了数十亿人。然后它变得集中，它获得了权力，权力导致了腐败。

今天留下的不是一个解放系统，而是时候颠覆它了。

比特币是极大颠覆中央集权的事物之一。为什么是它？

## 3.2设计的负面结果，不是故意的

**Negative Outcomes by Design, Not Intent**

One of the things that interests me as a computer scientist working in distributed systems is the architecture of systems. Architecture is a great topic for this city. The architecture of systems is what ultimately produces the outcomes.

作为一个研究分布式系统中的计算机科学家，我感兴趣的一件事是系统的架构。

建筑风格是这座城市的一个重要话题。系统的架构决定了最终会产生什么结果。

I’ve worked with a lot of bankers. They’re nice people. They try to feed their family, pay their mortgage, keep a steady job. Among them, there are a few sociopaths who inevitably rise to the highest positions of power because sociopathy is an advantage in hierarchical systems. But most of the problems with traditional concentration of power in money has nothing to do with the people being evil. It has to do with the fact that these institutions — through their shape, through their architecture — produce outcomes that are not good. They produce outcomes that are not egalitarian. They produce outcomes that are restrictive. They start to express nativism, nationalism, tribalism, class structure, and all of these things make the world a smaller place.

我曾和很多银行家一起工作过。他们是好人。他们努力养家糊口、支付抵押贷款、保持稳定的工作。

其中，其中，有一些反社会人士不可避免地上升到最高权力位置，因为社会病在层级系统中是一个优势。

但是，对货币的传统权力集中的大多数问题与人们的邪恶无关。

它与这个事实有关，这些机构（通过它们的形状，通过它们的架构）产生了不好输出。

他们产生的结果不是平等的。他们产生的结果是限制性的。

他们开始表达本土主义、民族主义、部落主义、阶级结构，所有这些都使世界变成了一个更小的地方。

## 3.3通信在扩展，而银行业务在下滑

**Communications Expanding While Access to Banking Is Declining**

In fact, over the last 15 years, we’ve seen the internet become an enormous power for the decentralization of communications. It has been a very liberating force. But if you look at economic inclusion and how banking works, we haven’t expanded opportunity. We haven’t expanded access. In fact, we’re now regressing. Economic inclusion is decreasing.

事实上，在过去的15年中，我们已经看到，互联网成为去中性化通信的巨大力量。

它是一支非常自由的力量。但如果你看看经济包容性和银行业如何运作，我们就没有扩大的机会。

我们还没有扩大的访问权限。事实上，我们现在正在倒退。经济包容性正在下降。

The reason it’s decreasing is because these isolated structures of finance, their very architecture, raise walls: national borders, class structures, and differences in how your money and your commerce are treated. We live in a world that is increasingly global and interconnected. There is even an emergent global culture through the internet. And yet our financial systems are parochial, insular, and they’re separated.

下降的原因是，这些孤立的金融结构（它们的架构）筑起了围墙：国界、阶级结构，以及你的钱和你的贸易如何被处理的差异。

我们生活的世界日益全球化和相互联系。通过互联网，甚至有一个新兴的全球文化。

然而，我们的金融体系是狭隘的、孤立的，它们是分离的。

"We live in a world that is increasingly global and interconnected, and yet our financial systems are parochial, insular, and separated."

我们生活的世界日益全球化和相互联系。然而，我们的金融体系是狭隘的、孤立的，它们是分离的。

If you look at it from a network perspective, there are systems of money for transmitting small amounts and systems of money for transmitting large amounts. Systems of money for consumer payments, systems of money for business-to-business payments. All of these are separated geographically based on borders, legal jurisdictions, nation-states. What the structure produces is separation. It means that, as people, we are less and less free to transact with the rest of the world. Geopolitics is affecting finance in a serious way because the combination of state and money produces toxic results.

如果你从网络的角度来看它，有些货币系统用于传输少量货币，有些货币系统用于传输大量货币。

有用于消费支付的货币系统，有用于商业支付的货币系统。

所有这些货币系统都是分开的，基于地理边界、法律管辖区、民族国家。

这个结构产生的是分离。这意味着，作为人民，我们越来越少自由地与世界其他国家进行交易。

地缘政治正在严重影响金融，因为国家和货币的结合产生了有害的结果。

And we’re about to disrupt all that.

我们要颠覆这一切。

## 3.4新的架构，新的通路

**New Architecture, New Access**

What bitcoin’s architecture gives us is a new way of organizing the world, exactly the same way that the internet flattened access to communication and made every system that connects to it an equal peer. If I have an IP address, my packets are treated no differently than the packets of anybody else on the network. For the most part, that gives voice to everyone. It gives everyone the power of the printing press on a global scale. Bitcoin will do the same by giving everyone the power of banking on a global scale.

比特币架构给我们的是一种新的组织世界的方式，它与互联网扁平化的通信方式完全一致，使每个系统都能与一个平等的peer连接。

如果我有一个IP地址，我的数据包与网络上任何其他人的数据包没有任何区别。

在很大程度上，这让每个人都能发声。它给了每个人在全球范围内的印刷出版的力量。

比特币也做同样的事情，它给每个人在全球范围内的银行力量。

*"What bitcoin’s architecture gives us is a new way of organizing the world, exactly the same way that the internet flattened access to communication and made every system that connects to it an equal peer."*

Think of it like desktop banking. In the way desktop printing, desktop publishing and websites changed communications, desktop banking — individually controlled banking with all of the power of the largest bank in the world — will create disruption.

把它想象成桌面银行业务。

在桌面印刷的方式中，桌面出版和网站改变了通信；

桌面银行将创造颠覆，个人控制的银行，拥有世界上最大银行的全部权力。

Imagine a world where every person has the ability not only to execute transactions but also to create complex financial systems and instruments without asking for anyone’s permission. Simply by connecting to the network, anyone can start a new application. Centralized systems can’t do that.

想象一个世界，每个人不仅能执行交易，而且能创造复杂的金融系统和工具，而不需要任何人的许可。

只要连接到网络，任何人都可以启动一个新的应用。集中式系统不能做到这一点。

In a centralized system, the further out you are, the less control you have. The closer you get to the system, and the farther you move up the hierarchy, the more controlled, the more limited the access is. But not with bitcoin. With systems like bitcoin, every node on the network has equal access to all of the financial services. In a centralized system, if you want to build a new application, you must first ask permission. And then permission is only granted if that application can apply to a very large population and be profitable.

在一个集中的系统中，你离得越远，你的控制就越少。

你越接近系统，你就越往上爬，层次越高，访问越受限。

当比特币不是这样。对于比特币这样的系统，网络上的每个节点都可以平等地访问所有的金融服务。

在集中式系统中，如果要构建一个新的应用，你必须先请求许可。

然后，如果这个应用适用于很多人，并且是有利可图的，那么得到批准。

On the internet or on bitcoin, all that is needed to start an application is two nodes, two people, two systems. They can start communicating, construct their own protocols, their own systems, and that application with only two people using it is just as valid as every other application on the network.

在互联网或比特币上，启动一个应用只需要两个节点、两个人、两个系统。

他们可以开始通信，构建自己的协议，他们自己的系统，只有两个人使用的应用，与网络上的其它所有应用一样有效。

## 3.5网络中立与非歧视

**Net Neutrality and Non-Discrimination**

When you look at the internet, the fundamental misunderstanding is that people think that the power of the internet comes from the ability to transmit information fast. But the real power of the internet comes from net neutrality. Net neutrality is the concept that the internet does not discriminate based on source, destination or content.

当你看互联网时，最基本的误解是人们认为互联网的力量来自于快速传递信息的能力。

但互联网真正的力量来自于网络中立。

网络中立是指：互联网不基于来源、目的或内容进行区分。

"Bitcoin is the first financial network that exhibits neutrality."

“比特币是第一个展现中立的金融网络。”

Bitcoin is the first financial network that exhibits neutrality. In a bitcoin transaction, the network doesn’t care about the source, the destination, the amount or what type of financial application it’s supporting. The only relevant question is, did you pay a sufficient fee to use the network resources? And if you did, your application is valuable.

比特币是第一个展现中立的金融网络。

在比特币交易中，网络不关心它支持的金融应用的源、目的、数量或类型。

唯一相关的问题是，你是否支付了足够的交易费来使用网络资源？

如果你这么做，你的应用就是有价值的。

### 3.5.1比特币中没有垃圾交易

**There Are No Spam Transactions in Bitcoin**

We have an interesting conversation happening in bitcoin right now. Perhaps some of you have heard the term “spam transactions.” What is a spam transaction? What does it mean for a transaction to be “spam”? I think that term is meaningless because to decide which transactions are spam and which are not, you’re making a top-down judgment. You’re imposing, in the architecture, the choices of which applications are legitimate. Then the question is legitimate to whom? The end user? There is no such thing as a spam transaction simply because if a transaction carries enough fee, that means that the sender of that transaction felt it was valuable enough to transmit—and therefore, it is a legitimate transaction. This replaces the concepts of control and content by making decisions about what is good, what is bad, what is legitimate, what is illegitimate, what is a valuable application, what is not a valuable application, with a simple market mechanism. If you paid essentially a tiny fee for your transaction, then because of the democratization of finance, your transaction is valuable and is not spam.

我们现在聊比特币的一个有趣话题。

也许你们中的一些人听说过“垃圾交易”这个词，什么是垃圾交易？什么样的交易是“垃圾”？

我认为这个术语是没有意义的，因为要决定哪些交易是垃圾，哪些不是邮件，你就做出了自上而下的判断。

你在这个架构中强加了哪些应用是合法的选择。

那么这个问题是对谁来说是合法的？最终用户？

没有垃圾交易这回事，因为一个交易有足够的交易费，就意味着交易的发送者认为有发送它的价值，因此，它是一个合法的交易。

这就取代了控制和内容的概念，通过简单的市场机制来决定：什么是好的、什么是坏的、什么是合法的、什么是非法的、什么是有价值的应用、什么是无价值的应用。

如果你为你的交易支付了一些交易费，那么因为金融的民主化，你的交易是有价值的，而不是垃圾交易。

## 3.6网络中心货币

**Network-Centric Money**

Starting in the 1970s, we have seen the world begin to adopt digital currencies. When people call bitcoin a “digital currency,” they’re missing the point. The euro is a digital currency, the US dollar is a digital currency. Less than 8 percent of these currencies exist in physical form; the rest is bits on ledgers. But the fundamental difference is that these ledgers are controlled by centralized organizations, whereas in bitcoin, they’re not. Bitcoin has a decentralized network, an open network.

1970年代开始，我们已经看到，世界开始采用数字货币。

当人们称比特币为“数字货币”时，他们忽略了要点。

欧元是一种数字货币，美元是一种数字货币。

这些货币只有不到8%是以实物形式存在，其余都在账本上。

但根本区别在于，这些账本是由中央组织控制，而比特币不是这样。

比特币有一个去中性化的网络，一个开放的网络。

"Bitcoin isn’t a digital currency. It’s a cryptocurrency. It’s a network-centric money."

“比特币不是一种数字货币，这是一种加密货币，这是一个以网络为中心的货币。”

Bitcoin isn’t a digital currency. It’s a cryptocurrency. It’s a network-centric money. I really like the idea of a network-centric money. A network that allows you to replace trust in institutions, trust in hierarchies, with trust on the network. The network acting as a massively diffuse arbiter of truth, resolving any disagreements about transactions and security in a way where no one has control.

比特币不是一种数字货币。这是一种加密货币。这是一个以网络为中心的货币。

我非常喜欢这个想法：以网络为中心的货币。

这个网络允许你用“对网络的信任”替代“对机构的信任”和“对等级的信任”。

网络作为一个真理的广泛扩散仲裁者，它以任何人无法控制的方式解决交易分歧和安全。

## 3.7对所有金融交易的极权主义控制的梦想

**Dreaming of Totalitarian Control over All Financial Transactions**

Starting in the 1970s, our currencies began to be digital, but this is not the same “digital” as bitcoin. This started a dream for governments, the dream of being able one day to control every financial transaction of every human being on the planet in a way that everything was visible to the power structures. Where privacy dies. Where the ability to make a transaction immediately puts you under the lens of systems that surveil you. We have been creating a system of global financial surveillance. A system of totalitarian financial surveillance throughout the world.

从1970年代开始，我们的货币开始数字化，但这与比特币的“数字化”不同。

这为政府开创了一个梦想，梦想有一天能够控制地球上每个人的每笔金融交易，权力结构能够看到所有事情。

在这里，隐私不存在了。在那里，交易的能力立即使你处于监视你的系统的镜头之下。

我们一直在建立一个全球金融监管体系。全世界的一个极权金融监管系统。

"This started a dream for governments, the dream of being able one day to control every financial transaction of every human being on the planet in a way that everything was visible to the power structures. Where privacy dies."

“这为政府开创了一个梦想，梦想有一天能够控制地球上每个人的每笔金融交易，权力结构能够看到所有事情。在这里，隐私不存在了。”

That system, which requires identification and credit checking and limited access, is responsible for the fact that economic inclusion is regressing. It is responsible for the fact that 2 1/2 billion people have absolutely no access to banking. That’s just the heads of household, not counting their families. That’s not counting people who have limited access to banking in a single currency within a single border. If you count all of them, it’s billions upon billions.

这个系统要求身份和信用检查和限制访问，它要为经济包容性的下降负责。

它要为这个事实负责：25亿人绝对没有机会进入银行业。这只是户主，还没算他们的家庭。

也没计算在一个边界内的一种货币的银行业有受限访问的人们。如果全都算上，有数十亿。

### 3.7.1金融交易的审查制度

**Censorship of Financial Transactions**

As a member of the privileged elite of the developed world, I have the ability to open a brokerage account in 24 hours, electronically. And within 24 hours, I can be trading in yen on the Tokyo stock market. I can be sending and receiving money anywhere in the world without really any limits. All I have to do is sacrifice my privacy and my freedom.

作为发达国家的特权精英的成员，我有能力以电子方式在24小时内开立一个经纪人账户。

在24小时内，我可以在东京股票市场上交易日元。

我可以发送和接收世界上任何地方的钱，没有任何限制。

我所要做的就是牺牲我的隐私和自由。

Because while I can do all of those things and they’re very powerful, there are some things I can’t do. I am not talking about buying drugs. That’s not really that interesting. What I am talking about are simple things?—?for example, donating to an activist organization like WikiLeaks. A few years ago, WikiLeaks was completely cut off from the world’s financial system simply with extrajudicial pressure applied on the few major payment providers: Visa, MasterCard, the banking transfer system, PayPal, etc. Without any legal process, without any conviction, and perhaps, in my opinion, without absolutely any crime other than revealing the truth of crime, WikiLeaks was cut off from the world’s financial system. This is now happening not just to activist organizations; it’s happening to entire countries.

因为虽然我能做所有这些事情，并且他们非常强大，但有些事情我做不到。

我不是在说买毒品。那不是很有趣。

我所说的是简单的事情，例如，给像维基解密这样的维权组织捐赠。

几年前，只是对少数主要支付提供商施加了法庭之外的压力（Visa、万事达卡、银行转账系统、PayPal、等），维基解密完全被排除在世界金融体系之外。

没有任何法律程序，没有任何定罪，也许在我看来，没有任何绝对的犯罪，除了揭露犯罪真相，维基解密被排除在世界金融体系之外。

现在，这不仅仅发生在激进组织身上，也发生在整个国家。

The dream of nation-states, to create a totalitarian financial system, died on January 3rd, 2009, with the invention of bitcoin and the mining of the genesis block.

随着比特币的诞生和创世区块的挖掘，民族国家的梦想（建立一个极权金融体系）破灭于2009年1月3日。

### 3.7.2以网络为中心的货币抵制审查

**Network-Centric Money Is Censorship Resistant**

Bitcoin is censorship-resistant. You may have heard this term. You cannot control where money is transmitted in bitcoin. It’s not attached to identities or geography. In bitcoin, surveillance of everyone is not possible. In bitcoin, censorship resistance is an artifact that is created by neutrality, the architecture of a flat network without borders. The architecture of neutrality that doesn’t ascribe any meaning to source, destination or value, is what creates censorship resistance.

比特币是抵制审查的。你可能听过这个词。

你没法控制比特币中的钱传到哪里。它不与身份或地理联系在一起。

在比特币中，监视每个人是不可能的。

在比特币中，审查阻力是这个创造的人为产物：中立性、没有边界的扁平网络架构。

中立的架构并不把任何意义归于源、目的或价值，它造成了抵制审查。

## 3.8 Sousveillance（反向监控）,不是Surveillance（监控）

**Sousveillance, Not Surveillance**

Privacy is very important but it’s a term that often has very deep political meaning. I like to juxtapose it to another term, secrecy. What is the difference between privacy and secrecy? Ultimately, and practically in today’s vocabulary, privacy is the right of billions of individuals to not be surveilled. Secrecy is the power of the very few to escape accountability, to have no transparency.

隐私是非常重要的，但这是一个经常具有很深政治意义的术语。

我喜欢把它并入另一个术语，保密。隐私和保密有什么区别？

最终，实际上，在今天的词汇表中，隐私权是数十亿人不被监视的权利。

秘密是极少数人逃避问责，没有透明度的力量。

We live in a world where every individual transaction you do through the financial system is cataloged, analyzed, and transmitted to intelligence services all around the world that collaborate, and yet we have no idea what our governments do with money. The financial systems of the powerful are completely opaque. Our transactions are completely visible through this system of surveillance. This world is upside down. Bitcoin rights it.

我们生活在这样一个世界里，你做的每笔交易都要通过金融系统，被编目、分析和传送到世界各地的合作的情报机构，但我们不知道我们的政府对货币做了什么。

强大的金融体系完全是不透明的。通过这种监管系统，我们的交易是完全可见的。

这个世界颠倒了。比特币对它进行纠正。

Privacy is a human right and secrecy is a privilege of power, and we need to be in a world where we have complete, ultimate, strong privacy for the billions of people. Because that is a human right, because that is a cornerstone of the freedoms of expression, association, political speech, and all of the other freedoms that are very much attached to privacy. We need to live in a world where secrecy is fickle and easily pierced, where power has to face accountability because they are under the spotlight of transparency. We need to flip the system upside down.

隐私是一项人权，保密是一项特权，我们需要一个这样的世界，数十亿人有完整、终极、强有力的隐私。

因为这是一项人权，因为这是表达自由、结社自由、政治言论自由，以及与隐私息息相关的所有其他自由的基石。

我们需要生活在一个秘密很薄、容易被刺穿的世界里，在这个世界里，权力必须面对问责，因为他们处于透明的聚光灯之下。我们需要把这个系统颠倒过来。

*"Privacy is a human right. Secrecy is a privilege of power. We need to live in a world where secrecy is fickle and easily pierced, where power has to face accountability because they are under the spotlight of transparency."*

One of my favorite words is a French word: sousveillance. It is the opposite of surveillance. Surveillance means to look from above; sousveillance means to look from below. In their dream of nation-states controlling all of our financial futures, they made one major miscalculation. It’s a hell of a lot harder for a few hundred thousand people to watch 7 1/2 billion. But what do you think happens when 7 1/2 billion of us stare back? When the panopticon turns around. When our financial systems, our communication systems, are private, and secrecy is an illusion that can’t be sustained. When crimes committed in the names of states and powerful corporations are vulnerable to hackers and whistleblowers and leakers. When everything eventually comes out. We have a great advantage because the natural balance of the system is one in which individuals can have privacy but the powerful cannot have secrecy anymore. Bitcoin is one of the first steps in that.

我最喜欢的一个词是法语单词：sousveillance。它是监管的反面。

监管意味着从上面看，sousveillance意思是从下面看。

在民族国家控制的金融未来的梦想中，他们犯了一个重大的错误估计。

几十万人监视75亿人是件困难的事。但是当75亿人反过来盯着看时，你认为会发生什么？

当全景旋转时。当我们的金融系统，我们的通信系统，都是隐私的，保密是一种无法维持的幻觉。

当国家和强大公司的名义犯下的罪行容易受到黑客、告密者和泄密者的攻击时。

当一切最终出现时。我们有一个很大的优势，因为这个系统的自然平衡是每个人都有隐私，但权力不能有秘密。比特币是其中的第一步。

*"We have a great advantage because the natural balance of the system is one in which individuals can have privacy but the powerful cannot have secrecy anymore. Bitcoin is one of the first steps in that."*

## 3.9每个人的银行

**Banks for Everyone**

The ability to transact across borders means that we will now be able to extend financial services to billions of people who have no access. Not through complicated technology necessarily. Sometimes I speak to various regional banks, the ones that are not afraid of bitcoin. They tell me things like 80 percent of our population is a hundred miles from the nearest bank branch and we can’t serve them. In one case, they said a hundred miles by canoe. I’ll let you guess which country that was. Yet, even in the remotest places on earth, now there is a cell-phone tower. Even in the poorest places on Earth, we often see a little solar panel on a little hut that feeds a Nokia 1000 phone, the most produced device in the history of manufacturing, billions of them have shipped. We can turn every one of those into, not a bank account, but a bank.

跨国界交易的能力意味着，我们现在能够将金融服务扩展到数十亿无法访问的人。

不必通过复杂的技术。有时我会对各种地区银行说，对那些不害怕比特币的银行说。

他们告诉我，我们80%的人口离最近的银行分支机构有一百英里，我们不能为他们服务。

在一个案例中，他们说一百英里要乘独木舟。你来猜猜是哪个国家。

然而，即使在地球上最偏远的地方，现在也有一个手机基站。

即使在地球最贫穷的地方，我们也经常在一个小棚屋里看到一个小的太阳能电池板，它为诺基亚1000手机供电，它是制造业史上生产最多的设备，出货量有数十亿。

我们可以把每个人变为一个银行，而不是银行帐户。

"I don’t have a Swiss bank account in my pocket. I have a Swiss bank."

“我口袋里没有瑞士银行账户。我有一家瑞士银行。”

Two weeks ago, President Obama at South by Southwest did a presentation and he talked about our privacy. He said, ”If we can’t unlock the phones, that means that everyone has a Swiss bank account in their pocket." That is not entirely accurate. I don’t have a Swiss bank account in my pocket. I have a Swiss bank, with the ability to generate 2 billion addresses off a single seed and use a different address for every transaction. That bank is completely encrypted, so even if you do unlock the phone, I still have access to my bank. That represents the cognitive dissonance between the powers of centralized secrecy and the power of privacy as a human right that we now have within our grasp. If you think this is going to be easy or that it’s going to be without struggle, you’re very mistaken.

两周前，奥巴马总统在西南部的South做了一次演讲，他谈到了我们的隐私问题。

他说：“如果我们不能解锁手机，那就意味着每个人口袋里都有一个瑞士银行账户。”

这并不完全准确。我口袋里没有瑞士银行账户，我有一家瑞士银行，能够用一个种子生成20亿个地址，每个交易使用不同的地址。

这家银行是完全加密的，所以即使你解锁了电话，我仍然可以进入我的银行。

这代表了集中保密权力与隐私权力之间的认知不一致，这是我们现在理解的人权。

如果你认为这将是容易的，或者不需要斗争，那你就错了。

## 3.10比特币，货币的僵尸

**Bitcoin, the Zombie of Currencies**

If you read anything about bitcoin, you’ll see the very same things that they said about the internet in the early '90s. It is a haven for pedophiles, terrorists, drug dealers, and criminals. How many of you in this room have bitcoin? How many of you in this room are terrorists, pedophiles, drug dealers or criminals?

如果你阅读了有关比特币的任何内容，你会看到他们在90年代早期对互联网说过相同的话。

它是恋童癖者、恐怖分子、贩毒者和罪犯的避风港。

这个房间里有多少人有比特币？

这个房间里有多少人是恐怖分子、恋童癖者、毒贩或罪犯？

You see the thing about bitcoin is while they push this story, every now and then someone who has never heard of bitcoin notices two important things. One, it’s still not dead, which is always surprising because every two or three months there is an article that says it’s dead. That’s great marketing. Because every time someone hears it’s dead and three months later they hear it’s still not dead, they think, "Huh, this thing really tends to survive." I call bitcoin“the internet of money,” but perhaps we should call it “the zombie of currencies.” It is the currency that is the undead.

你看到有关比特币的事情是，虽然他们推动这个故事，但不时地，从未听说过比特币的每个人都会注意到两个重要的事情。

一，它还没有死掉，这总是令人惊讶，因为每两三个月就有一篇文章说它已经死了。这是伟大的营销。因为每当有人听到它死了，而三个月后他们听说它还没有死，他们会想，“嗯，这个东西真的活下来了。”

我把比特币称为“货币互联网”，但也许我们应该把它称为“货币的僵尸”，它是是不死的货币。

*"I call bitcoin “the internet of money,” but perhaps we should call it “the zombie of currencies.” It is the currency that is the undead."*

The issue here is that we’re now creating a system that is threatening the largest industry in the world, and that is finance. They are going to object. They are going to push back, and they’re going to use the most common and effective emotional tactic there is, which is fear. They will treat you in such a way as if you are idiots and try to persuade you that this is something to fear. When people hear that message, maybe the next day they come to one of these meetups and they meet a dentist who owns bitcoin, an architect who owns bitcoin, a taxi driver who uses bitcoin to send money back to their family—normal people who use bitcoin to give themselves financial power and financial freedom. Every time that message is broken by cognitive dissonance, bitcoin wins. All bitcoin really has to do is survive. So far, it’s doing pretty well.

这里的问题是，我们现在正在创建一个系统，它在威胁世界上最大的行业，那就是金融。

他们打算要反击。他们打算要压制，他们打算使用最常见和最有效的情感策略，就是恐惧。

他们会以这样的方式对待你，好像你是白痴一样，并试图说服你这是恐惧的事情。

当人们听到这个消息时，也许第二天他们来参加一次聚会时，他们遇到了一位拥有比特币的牙医，一位拥有比特币的建筑师，一名出租车司机使用比特币将钱汇回家人，这些普通人使用比特币获得了金融权力和金融自由。

每当这个信息被认知不一致打破时，比特币就会获胜。

比特币真正要做的就是生存。到目前为止，它做得很好。

## 3.11货币演变

**Currencies Evolve**

In the new network-centric world, currencies occupy evolutionary niches. They evolve, like species, based on the stimulus they have from their environment. Bitcoin is a dynamic system with software developers that can change it. The question is, in which direction will bitcoin evolve? Which environmental niche will it attempt to fit in? And how will that be affected by the actions of the powerful? If they attack bitcoin, it evolves to defend itself against predators, just like any species. If they attack bitcoin anonymity, it evolves to become more anonymous. If they attack its resilience, it evolves to become more decentralized. In the end, despite all of the messages of fear, bitcoin is the cuddly little bear of currencies and you do not want to kick it. Because, as in evolution, if you stomp on the little gecko, it will evolve until it’s a Komodo dragon and then you can’t stomp on it.

在新的网络中心世界中，货币占据了进化的利基。

（注：利基niche是指针对企业的优势细分出来的市场，这个市场不大，而且没有得到令人满意的服务。）

它们像物种一样，根据环境对它们的刺激而进化。

比特币是一个动态系统，软件开发人员可以对其进行更改。

问题是比特币向哪个方向发展？它会尝试适应哪种环境利基？这将如何受到权势者行动的影响？

如果他们攻击比特币，它就会像任何物种一样防御掠食者。

如果他们攻击比特币的匿名性，它就会变得更加匿名。

如果他们攻击它的弹性，它就会变得更加去中性化。

最后，尽管有各种恐惧信息，但比特币是可爱的小熊货币，你不想踢它。

因为，就像在进化中一样，如果你踩着小壁虎，它就会进化，直到它成为科莫多巨蜥，然后你就无法踩到它。

Sometimes people ask me, “Do you think governments will ban bitcoin? Do you think they will try to regulate it out of existence? Do you think they will attack it with denial-of-service attacks?" The answer is really simple because in network-centric systems—systems that are dynamic and adaptable, systems that exhibit antifragility — attacks cause the system to adapt and evolve and become resistant. Think about this for just a second.

有时人们问我：“你认为政府会禁止比特币吗？你认为他们会试图把它排除在外吗？你认为他们会用Do攻击它吗？”

答案很简单，因为在网络中心系统中，系统是动态的和可适应的，它表现出的是抗脆弱性，攻击导致系统适应和进化，并变得有抵抗力。想一想。

*"In network-centric systems, attacks cause the system to adapt, evolve, and become more resistant."*

### 3.11.1攻击增进抗力

**Attacks Build Resistance**

I’ve been involved with the internet since 1989. I remember very clearly, in the early days when lots of articles were written about how the internet was not resilient, could not scale to do voice, was not secure. I remember times when denial-of-service attacks would take down Yahoo, AltaVista, and even Google for hours, sometimes days. What happened between then and now? How many times have you seen Google go down in the last five years? Have people stopped attacking Google? Quite the opposite. Google can now sustain gigabits of denial-of-service anywhere in the world and dynamically reroute. The same applies for all internet applications. The attacks didn’t stop. The system became immune because, like a human immune system, if you are exposed to a virus and it doesn’t kill you, you evolve resistance, and the next time you’re exposed to the virus, it does nothing to you.

自1989年以来，我一直参与互联网。

我记得非常清楚，在早期的时候，有很多关于互联网不具备弹性的文章，无法扩展到发声，也不安全。

我记得有时DoS攻击会使雅虎、AltaVista，甚至谷歌停顿数小时，有时几天。

从那时到现在发生了什么？ 你有多少次看到Google在过去五年中垮台了？人们攻击谷歌了吗？

恰恰相反。谷歌现在可以在世界任何地方维持千兆位的拒绝服务，并动态重新路由。

这同样适用于所有互联网应用。攻击没有停止。系统变得免疫，因为，就像人体免疫系统一样，如果你接触到病毒并且它不会杀死你，你会产生抵抗力，下次当你接触到病毒时，它对你没有任何作用。

Will governments try to ban bitcoin? Regulate bitcoin? Attack bitcoin? They already are. They have been, almost since the beginning, and bitcoin is still getting stronger. It’s a system that is under a constant denial-of-service attack, that is on the internet being attacked by hackers, by agents, by other systems, 24 hours a day.

政府会试图禁止比特币吗？监管比特币？攻击比特币？

他们已经在做了。几乎从一开始，它们就在做，但比特币仍然越来越强大。

这是一个持续收到DoS攻击的系统，它在互联网上被黑客、代理或其它系统一天24小时地攻击。

*"bitcoin is still getting stronger. It’s a system that is under a constant denial-ofservice attack, that is on the internet being attacked by hackers, by agents, by other systems, 24 hours a day."*

In security, we have a really funny term, which is a honeypot. A honeypot is a system that is designed to attract hackers. What bigger honeypot could you have than a financial network that has $6 billion on it? If you hack bitcoin, there is a $6 billion reward for you finding a way to hack it. No one has collected that reward yet, and it’s not because they haven’t been trying. They’ve been trying nonstop. But systems like bitcoin are resilient.

在安全方面，我们有一个非常有趣的术语，蜜罐。

蜜罐是一个旨在吸引黑客的系统。

你有什么比拥有60亿美元的金融网络更大的蜜罐？

如果你破解了比特币，那么你将获得60亿美元的奖励。

还没有人收到这个奖励，并不是因为他们没有尝试过。他们一直在不断尝试，但像比特币这样的系统具有弹性。

## 3.12欢迎来到货币的未来

**Welcome to the Future of Money**

Remember that what we’re doing here is not a currency. It is a reworking of the societal systems of organization that have failed us. The 18th-century systems of hierarchies that do not scale to a global, interconnected world are being replaced by network-centric, flat architectures—whether that’s the internet or any of the applications running of top of it or bitcoin itself. Currency is just the first app. When you have a network that can provide you with neutral trust, you can build myriads of applications on top, and you don’t have to ask for permission.

请记住，我们在这里所做的不是货币。

这是对我们社会组织系统的改造，这个系统使我们失望。

18世纪的层级结构体系无法扩展到全球互联的世界，正在被以网络为中心的、扁平架构所取代 —— 无论是互联网，还是运行在比特币之上的任何应用。

货币只是第一个应用。当你拥有了一个可以为你提供中立信任的网络时，你可以在上面构建无数的应用，而你无需获得许可。

Bitcoin is much more than currency. When I say that bitcoin is “the internet of money,” the emphasis is not on “money”; the emphasis is on internet. Welcome to the future of money.

比特币远远不只是货币。

当我说比特币是“货币互联网”时，强调的不是“货币”，而是互联网。

欢迎来到货币的未来。

Thank you.