# 8比特币设计原理

**Bitcoin Design Principles**

This talk was delivered in June 2015, at the Harvard Innovation Lab in Boston, Massachusetts, as part of an IDEO Lab design workshop. During this 2 day workshop, students competed to create prototype applications based on bitcoin and blockchains.

本次演讲于2015年6月在马萨诸塞州波士顿的哈佛创新实验室进行，是IDEO实验室设计研讨会的一部分。在为期两天的研讨会期间，学生们竞相创建基于比特币和区块链的原型应用程序。

Video Link: <https://www.youtube.com/watch?v=Ur037LYsb8M>

Good morning, everyone. Wow, what a difficult task you have. At a very basic level, you have to try to understand what is bitcoin. I can answer that question in four words. Bitcoin is digital money. But that doesn’t really capture it. It’s more like the internet of money. But really it’s a consensus decentralized network based on blockchain technology and a proof-of-work algorithm that allows a digital token to act as a reward system for a gametheoretical competition between decentralized miners who validate—and "Oh my…,” it immediately goes off the cliff.

早上好。 哇，你有一项艰巨的任务。

在最基本的层面上，你必须尝试理解什么是比特币。

我可以用四个词回答这个问题：Bitcoin is digital money（比特币是数字货币）。

但这并没有真正理解它。它更像是货币互联网。但实际上它是一个共识去中心化网络，基于区块链技术和工作量证明算法，这允许一个数字token作为游戏理论竞赛的一个奖励系统，在款共之间进行竞赛，他们验证……，“哦，我...”，它马上就要从悬崖上掉下来了。

Even after a couple of years of exploring "What is bitcoin?" you’ll find you’re still learning, you’re still trying to understand what it is. Part of the reason for that is because bitcoin is a really new technology, it’s a really disruptive technology, but it also is an abstraction on a technology that is really old. That technology is money. Money is a tool, it’s a technology. It actually shares commonalities with linguistic structures, because we use it almost like a language to communicate value among ourselves in a society.

即使经过几年的探索，“比特币是什么？”你会发现你还在学习，你仍在努力理解它是什么。

部分原因是，比特币是一种真正的新技术，它是一种真正颠覆性的技术，但它也是对一种古老技术的一个抽象。那个技术就是货币。货币是一种工具，是一种技术。它实际上与语言结构有共性，因为我们几乎把它当作一种语言，来社会中我们用它交流价值。

## 8.1货币的历史

**History of Money**

Who wants to tell me here how old money is? Audience member: “5,000?" Okay, that’s a good guess. A bit older. Try again. The problem with trying to understand the history of money is that money is older than history. We can go and look at the writing about money. Money is older than writing. That may confuse you a bit. You’re like, "Money’s older than writing? That can’t be.” In fact, if you look at the first forms of writing that we can find, they are spreadsheets. They are accounting ledgers. The first thing scratched onto tablets created with twigs and things like that are accounting ledgers. They represent how many amphorae of oil were given to the pharaoh. If you go even further back, we find ancient forms of money among the ruins of ancient civilizations: beads, feathers, shells, giant stones. Money has taken many forms, but it exists and has existed almost as long as language. This is a truly ancient technology. So, it’s not 5,000 years. It’s probably close to 500,000 years old.

谁想告诉我货币的历史有多长？观众：“5000年？”

好的，猜的很好。但还要长。再试一次。

试图了解货币历史的问题是货币比历史更古老。我们可以去看看关于货币的书写。货币比书写更古老。

这可能会让你有点儿困惑：“货币比书写更古老？不可能。”

事实上，如果你看看我们能找到的第一种书写形式，它们是表格,它们是记账的账目。

用树枝和诸如此类的东西刮到平板上所做的第一件事就是记账。它们代表给了法老多少个油罐。

如果你再往前走，我们会发现古代文明遗迹中的古代钱币：珠子、羽毛、贝壳、巨石。

货币有多种形式，但它几乎和语言的历史一样长。这是一项真正古老的技术。

所以，它不是5千年，可能接近50万。

### 8.1.1灵长类和货币

**Primates and Money**

In fact, we see money emerge within other species. Highly intelligent species like primates, certain types of birds like crows, even marine mammals likedolphins have forms of tokens that they use to express value to each other. Or they can very quickly learn the mechanics of money. You can teach primates that if you turn in this pebble, you get a banana. And then watch, within a very short period of time, how that not only becomes a part of the primate culture but gets passed down to the next generation, and they start inventing

economic activities. Not nice economic activities. They invent strong-armed robbery: beat up the other monkey and take its pebbles, so you can get bananas. They invent sexual favors for pebbles, so you can get bananas. They invent some of the earliest economic activities.

事实上，我们看到了货币出现在其它物种中。

高智能物种（例如灵长类），某些鸟类（例如乌鸦），甚至海洋哺乳动物（例如海豚），都有某些形式的token，用来向对方表达价值。

或者它们可以很快学会货币的机制。你可以教灵长类动物，如果你把这块鹅卵石弄进去，你会得到一根香蕉。然后观察，在很短的时间内，这不仅成为灵长类文化的一部分，而是传到了下一代，他们开始发明经济活动。不好的经济活动。他们发明了强有力的暴力抢劫：殴打其它猴子，拿走它的鹅卵石，这样它就可以得到香蕉。他们发明了换取鹅卵石的性行为，所以它可以得到香蕉。他们发明了一些最早的经济活动。

Money is ancient, it’s an absolutely ancient technology, and none of us really understands it. If you want a demonstration of that fact, sit down and have a conversation with a four-year-old and try to explain money. You’ll find out very quickly that the four-year-old has very good questions that you can’t answer. You can watch parents go through this, it’s hilarious:

货币是古老的，它是一种绝对古老的技术，没有人真正理解它。

如果你想演示一下这个事实，坐下来和一个四岁的孩子聊天，试着解释一下钱。

你很快就会发现这个四岁孩子有很好的问题你无法回答。

你可以看到父母经历了这一切，这真是太有趣了。

"Mommy, where does money come from?" "The banks make it." "How do they make it?" "Well, they print it." "Why can’t we have more, then." "Go clean your room."

“妈妈，钱从哪里来的？”

“银行是这样做的。”

“他们是怎么做的？”

“嗯，他们把钱打印出来。”

“那为什么我们不能有更多钱？”

“去整理你的房间。”

You’re about four questions from “Go clean your room” in a money conversation because adults don’t really understand money. Even though it is a cultural artifact that has existed in our species for hundreds of thousands of years, we don’t understand how it works.

在一次有关钱的对话中，你有四个问题，“去整理你的房间”，因为成年人并不真正理解钱。

尽管它是一种文化制品，在我们的物种中已经存在了几十万年，但我们还是不明白它是如何运作的。

## 8.2货币的特点

**Characteristics of Money**

We’ve gone through several technological iterations of money. We started with very basic forms of money. These basic forms had certain unique characteristics that made them good as money. What makes good money? Something that is rare. Shells, feathers. You can use shells as money, unless you live on a beach; if you live on a beach, you can’t use shells as money. You can transport the value easily. So, it has to be portable. With few exceptions, most forms of money are highly portable. If the amount of money you need to go to buy a cow is heavier than the cow, that’s not very good money. Which is why we don’t often see, for example, gold being used for large transactions. It’s too heavy. Other characteristics of money . . . It has to be difficult to forge; it has to be difficult to create more of it. You should be able to detect at a glance or relatively easily that it is real. It should be fungible. If I’m using shells, then this shell or that shell are both the same money. If I give you a dollar, it doesn’t matter which dollar I gave you; it’s fungible. Every dollar can substitute for every other dollar.

我们经历了几次货币的技术迭代。我们从非常基本的货币形式开始。

这些基本形式具有某些独特的特征，使它们成为货币。

什么是好的货币？

* 罕见：罕见的东西，贝壳、羽毛。你可以用贝壳作为钱，除非你生活在海滩；如果你生活在海滩，你就不能用贝壳当钱。
* 便携：你可以很容易地传递价值。所以，它必须便于携带。除了少数例外，多数形式的货币都是高度便携的。如果你买奶牛所需的钱比牛还重，那不是很好的钱。这就是为什么我们不经常看到黄金用于大型交易。它太重了。
* 防伪：它很难伪造，必须很难创造更多。
* 易于识别：你应该能够一目了然或相对容易地发现它是真的。
* 可替换：它应该是可替换的。如果我使用贝壳，那么这个贝壳或那个贝壳都是同样的钱。如果我给你一美元，我给你的那个一美元都没有关系，它是可以替换的。每个一美元都可以替代其它一美元。

"Money itself is an abstraction. If it’s not an abstraction, then it’s not money—it’s barter."

“货币本身是一种抽象。如果它不是一种抽象的话，那么它就不是钱，那是易货。”

These are the technologies, and gradually over time we’ve created abstractions. Money itself is an abstraction. If it’s not an abstraction, then it’s not money—it’s barter. If I give you bananas for your goat, that’s not money. Bananas are not money because you eat them. You don’t use them to do further exchanges. Therefore, that’s barter. You’re exchanging one commodity for another. If it’s abstract—if it doesn’t have any practical use in itself—then as an abstraction of money it represents something else, some shared value.

这些是技术，随着时间的推移，我们已经创建了很多抽象。

货币本身是一种抽象。如果它不是一种抽象的话，那么它就不是钱，那是易货。

如果我拿香蕉跟你换山羊，那不是钱。香蕉不是钱，因为你吃了它们。你不用香蕉做进一步的交换。

因此，这是易货贸易。你在用一种商品换另一种商品。

如果它是抽象的，如果它本身没有任何实际用途，那么作为一种抽象的货币，它代表了其它东西，一些共同的价值。

Which leads to the one inescapable conclusion about money: Money is a shared cultural hallucination. It’s a shared delusion. We walk around and associate with other people on the basis of germ-ridden pieces of cotton printed with green ink. If you were to observe that as an alien anthropologist that landed on Earth, you’d think it was very very weird. That just by exchanging these pieces of cotton, you could create social relationships, transactions, and trade— you could feed yourself, shelter yourself, etc., etc. It doesn’t make much sense but it’s based on a shared hallucination. It’s based on the assumption that if you give me a dollar today, someone else will accept that dollar in exchange for something of value tomorrow. If I still believe that is the case, then it has value. Value comes from the assumption that I can use it again.

这导致了关于货币的一个不可避免的结论：货币是一种共同的文化幻觉。它是一种共同的妄想。

我们四处走动，并以绿色墨水印刷的沾满细菌的棉花为基础与其他人交往。

如果你从一个外星人的角度观察，你会认为这非常非常奇怪。只需通过交换这些棉花，你就可以建立社交关系、交易和贸易，你就可以给自己吃的东西、给自己住的地方，等等。

它没有多大意义，但它是基于一种共同的幻觉。

它是基于这样的假设：如果你今天给我一美元，我明天就可以拿这一美元跟其他人交换其它东西。如果我仍然相信这种情况，那么它就有价值。价值来自于这个假设：我可以再次使用它。

### 8.2.1只是货币的另一种抽象

**Just Another Abstraction of Money**

Bitcoin is just the latest iteration of abstraction. We’ve done abstraction before but every time we do abstraction of money, society freaks out because this new thing can’t possibly be real money. Go back and look at what happened with the introduction of coins stamped onto nonprecious metal, and then eventually paper notes. When paper notes were first circulated, no one believed that they had value. The shared hallucination had not taken hold yet. It was very difficult to persuade people to exchange real gold coins or silver coins for pieces of paper that said that they had gold in a vault. Then, take it a step further, and disappear the gold from the vault and say, "Turns out, it’s just the paper."

比特币只是最新迭代的抽象。

我们以前做过抽象，但是每次我们做货币抽象时，社会都会害怕，因为这个新事物不可能是真正的钱。

回头看看，当出现非贵金属货币时发生了什么，当出现纸币时发生了什么。当纸币初次流通时，没有人相信它有价值。共同的幻觉尚未形成。很难说服人们把金币或银币换成纸片，上面写着他们把金子放在金库里。然后，再往前走一步，把金库从金库里消失了，说：“它只是纸而已。”

You ask people about bitcoin, and one of the first things I hear from most people is that it’s not real money because it’s not backed by gold like the US dollar—which I find astonishing. The dollar hasn’t been backed by gold since 1936. Yet, most people think that somewhere in the vault, possibly at Fort Knox or some other movie location, there are bars of gold that correspond ingot to ingot to the pieces of paper that you have in your pocket. They don’t. There’s no such thing. Why is bitcoin money? Because other people think it’s money. You can write a dozen Ph.D. dissertations explaining exactly why bitcoin is not money . . . and I have lived on it for two years. Therefore, it doesn’t matter what your dissertation says. To me, it is money, because I have lived on it for two years. So have thousands of other people. Therefore, to me, it is very much real money.

你问人们关于比特币的事情，我从大多数人那里听到的第一件事是，它不是真正的货币，因为它不像美元那样由黄金支持，我觉得这很让人惊人。

自1936以来，美元已经不再由黄金支持。然而，大多数人认为，在某个地方，有一些金条，它们对应着你口袋里的纸片。他们没有。没有这样的事。

比特币为什么是货币？因为其他人认为这是货币。

你可以写十几篇博士学位论文，来解释为什么比特币不是货币 … 我已经靠它生活了两年。因此，你的论文说什么并不重要。对我来说，它是货币，因为我已经靠它生活了两年。还有成千上万的其他人。因此，对我来说，这就是货币。

## 8.3比特币和设计

**Bitcoin and Design**

You’ve been tasked with creating designs and concepts around the oldest technology in the world that very few people really understand. Its latest, most abstract expression, that is brand new, is completely disjointed from previous expressions of money and is extremely complex as a technology. That is a really difficult task. When faced with that task, your go-to technique is the use of metaphor. Design metaphors are extremely powerful tools. They allow us to create expectations. Metaphors are tools by which we create expectations. When you have a desktop computer and it has a desktop, you assume that something will happen when you drag something across the desktop. Because you’ve actually used a real desk, that assumption will inform your expectations. You expect it to behave like the object that it’s pretending to be. That’s a design metaphor. Design metaphors are extremely powerful, but they’re also extremely dangerous when misapplied.

你的任务是围绕世界上最古老的技术创建设计和概念，很少有人真正理解这些技术。

它的最新、最抽象的表达，是全新的，与以前的货币表达完全脱节，作为一种极其复杂的技术。

这是一项非常艰巨的任务。当面对这项任务时，你的首选技巧是使用比喻。

设计比喻是非常强大的工具。 它们使我们能够创造期望。比喻是我们创造期望的工具。

当你有一个台式电脑并且它有一个桌面时，你可以假设，当你在桌面上拖动某些内容时会发生某些事情。

因为你用过办公桌，所以这个假设会告知你的期望。你希望它的行为就像它假装的东西一样。

这是一个设计比喻。设计比喻非常强大，但是当误用时也很危险。

"Design metaphors are extremely powerful, but they’re also extremely dangerous when misapplied. In bitcoin, every single term and design metaphor is wrong and broken."

设计比喻非常强大，但是当误用时也很危险。

在比特币中，每个术语和设计比喻都是错误的和被打破的。

### 8.3.1大写钱包，不是小写钱包

**Wallets aren’t wallets**

In bitcoin, every single term and design metaphor is wrong and broken. Let’s go through the list. You’ve probably struggled with this as you’ve engaged with this technology of bitcoin and looked at all of the terminology. First of all, a “wallet.” What is a wallet? A wallet is something that stores money. Not in bitcoin it isn’t. The money isn’t in the wallet; the money is on the network. The wallet contains keys. So, it’s not a wallet; it’s a keychain. How can you tell it’s not a wallet? Can you copy a wallet? No. But you can copy a key. A keychain is a far better metaphor. If I have a keychain—imagine a big ring of keys like a janitor or a custodian—I have a bunch of keys, and I can go into a shop and have all of those keys duplicated and create a second keychain. Both of those keychains will work interchangeably in all of the locks that the original keychain worked. That’s how a keychain works. If you understand what a keychain does, then you will understand how a bitcoin wallet works. You can copy it, you can make copies of the keys. If you give someone a copy of the key, they can open the door. They don’t need your permission anymore to open the door.

在比特币中，每个术语和设计比喻都是错误的和被打破的。

让我们看看这个清单。在你从事比特币这种技术和看这些术语时，以及与之进行了斗争。

第1，一个“钱包（wallet）”。

钱包是什么？钱包是储钱的东西。但在比特币中，它不是，钱不再钱包中，钱在网络上。钱包里有钥匙。所以，它不是钱包，而是钥匙链。你怎么能说它不是钱包？你能复制一个钱包吗？不能。

但是，你可以复制一个钥匙钥。钥匙链是一个更好的比喻。

如果我有一个钥匙链，我有一把钥匙，我可以到一家商店，复制所有这些钥匙，创建了第二个钥匙链。

这两个钥匙链都能用。钥匙链就是这样用的。

如果你理解钥匙链做了什么，那么你就会理解比特币钱包是如何工作的。

你可以复制它，你可以复制钥匙。如果你给某人一个钥匙副本，他们就可以打开这扇门。他们不需要你的许可就可以打开门了。

So, a “wallet” is not a wallet; it’s a keychain. That’s a terrible metaphor. You have expectations of what a wallet will do. It will contain things. These contents will be discrete and enumerated. None of that exists in bitcoin.

所以，这个“钱包”不是钱包，而是钥匙链。这是一个非常好的比喻。

你对钱包会做什么有了期望。

它将会包含一些东西。这些内容是离散和列举的。这些东西都不存在于比特币中。

### 8.3.2比特币中没有硬币

**No Coins in Bitcoin**

Let’s get down to basics: “Bit - coin.” Coin. What a terrible word. What a terrible brand. Coin. Take the most abstract form of money we have ever created, that is based on a completely decentralized network that has no coins, and then name it “bitcoin.” Just to confuse everyone. A coin, which is two generations of technology back and a far less abstract, much more tangible, physical representation of money. You took the most abstract representation of money and named it after the most tangible representation of money. Only an engineer could come up with that brand.

让我们来谈谈基础：“Bit-coin”硬币。多么好的一个词。多么好的一个品牌。

硬币。采用了我们创造过的最抽象的货币形式，它基于一个完全中心化的网络，这里没有硬币，然后将其命名为“比特币”。

只是让每个人都感到困惑。一枚硬币，它是两代以前的技术，远不那么抽象，更有形，货币的物理表示。你采用了最抽象的货币表示，然后用最有形的货币表示来命名它。只有工程师才能想出这个品牌。

Here’s a little secret: There are no coins in bitcoin. When miners mine, they don’t create coins; they create ledger entries. Those ledger entries do not enumerate coins. They have outputs—transaction outputs—which are chunks of value that are infinitely divisible and recombinable. Coins don’t do that. You can’t track a coin in bitcoin because there are no coins.

这里有一个小秘密：比特币中没有硬币。

当矿工挖矿时，他们不会制造硬币，他们创建的是账目。

这些账目没有列举硬币。它们有输出（交易务输出），这些输出是价值块，可以无限分割，可以重新组合。 硬币不是这样。你不能在比特币中跟踪一个硬币，因为没有硬币。

So, you’ve got a “wallet” that doesn’t contain “coins”—because the coins are actually on the network and they’re not coins, they’re outputs—and what you’re really holding is a keychain. Transactions are not from a sender to a recipient. Addresses don’t have balance in bitcoin. There’s no such thing as a balance of an address. An address controls outputs, and if you trawl through the blockchain and add up all of the outputs, you can figure out some notional balance. Whether that’s actually spendable or not, how much it is, is actually quite difficult to determine. There is no “balance.” You have no “account” in bitcoin.

所以，你有一个不包含“硬币”的“钱包”，因为硬币实际上是在网络上，而且它们也不是硬币，它们是输出，而你真正持有的是钥匙链。交易不是从发送人到接收人。在比特币中，地址没有余额。没有一个地址的余额这样的东西。地址控制输出，如果你浏览区块链，并将所有输出相加，你可以得到一些名义余额。

实际上是否可以花费，是多少，实际上很难确定。没有“余额”。比特币中没有“账户”。

All of the terms are broken. The problem is, from a design perspective, instead of the metaphor informing our expectations, it is misinforming our expectations. It is creating the grounds for massive misunderstanding, because we think it’s going to do something in a certain way, and it ends up doing something completely different, something unexpected. Kind of like the Windows desktop. I don’t know if you’ve ever compared a Mac and a Windows desktop. To me Windows desktops have no consistency. The metaphor is completely broken. You expect it to do one thing, it does something completely different and confuses. The essence of good design is picking the metaphor that informs expectations.

所有术语都被打破了。从设计的角度来看，问题不是隐喻告知了我们的期望，而是它误导了我们的期望。

它创造了大量的误解，因为我们认为它会以某种方式做某事，但最终做出了完全不同的事情，这是意想不到的事情。

有点像Windows桌面。我不知道你是否比较过Mac和Windows桌面。

对我来说，Windows桌面没有一致性。这个比喻完全被打破了。

你希望它做一件事，它做了一些完全不同的事情，并且让人困惑。

良好设计的本质是选择能够告知期望的比喻。

### 8.3.3比喻设计

**Skeuomorphic Design**

Here’s the next big problem with metaphors and design. There’s a certain concept called skeuomorphic design. The word skeuomorphic means “a shadow of its former self.” It’s form as a shadow. What it means is when you create elements in design that give you references or hints of some previous form. For example, a classic example, in the first iteration of iPads, the iOS software had a lot of skeuomorphic design. If you opened your contact database, it was bound in leather. That leather had stitching. That stitching didn’t do anything. It was just a design element which had no functional purpose, whose intent was to put you into a familiar set of mind so that you could understand the metaphor. When you’re playing a card game on your computer and it has fake felt under the cards, that’s because it’s trying to draw out the metaphor of a casino by introducing this design element. Skeuomorphic design is extremely powerful. It’s also extremely dangerous. If you don’t use it correctly, again, it creates different expectations as to what is going to happen next.

下面是比喻和设计的下一个大问题。

有一个被称为“比喻设计”的概念。“比喻”一词的意思是“它从前的影子”，它是影子。

它的意思是，当你在设计中创建元素时，它给你一些以前形式的参考或提示。

例如，一个经典的例子，在iPad的第一次迭代中，iOS软件有很多的比喻设计。

如果你打开联系人数据库，它是用皮革装订的。那皮革已经缝好了。这个缝合不做任何事情。它只是一个没有功能目的的设计元素，它的目的是把你置于一个熟悉的环境中，这样，你就可以理解这个比喻。

当你在电脑上玩纸牌游戏时，纸牌下面有假的毛毡，这是因为它试图通过这个设计元素来比喻赌场。

比喻设计是非常强大的，也是非常危险的。如果你没有正确使用它，它会对下一步会发生什么产生不同的期望。

In bitcoin, we have a lot of skeuomorphic design. My favorite and most hated form of skeuomorphic design is the picture you will see in every single article written about bitcoin: a pile of gold coins with a letter B on them, usually the Casascius coin designed by Mike Caldwell, but possibly some other rendering of that. Taking the worst design metaphor of bitcoin, the word “coin,” and then instantiating it in a beautiful rendering that makes it even more physical looking, in a skeuomorphic design that completely misleads everyone. People are actually going out on eBay and they’re buying what they think is “bitcoin.” They’re buying gold-plated, physical coins that have nothing to do with the blockchain but have the letter B stamped on them. "Look, I’ve joined the revolution of digital money" they say, but these tangible replicas rarely have any value in bitcoin. This is the result. Then, people write articles, and they look at the picture and they think, "So that’s what a bitcoin looks like." That’s not what a bitcoin looks like, because if you remember, I may have mentioned, there are no coins. This is the danger.

在比特币中，我们有很多的比喻设计。

我最喜欢和最讨厌的比喻设计是，你在每篇关于比特币的文章中看到的图片：一摞有字母B的金币，通常是由Mike Caldwell设计的卡萨诸斯硬币，但可能还有其它的渲染。

去了比特币的最坏的设计比喻“coin”这个词，然后在做了漂亮的渲染，使它更具物理外观，这个比喻设计完全误导每个人。人们真的到eBya上去购买他们认为是“比特币”的东西，他们买的是镀金的实物硬币，它们与比特币毫无关系，却把字母B印在上面。他们说：“看，我加入了数字货币革命。”但这些有形复制品在比特币中没有任何价值。这就是结果。然后，人们写文章，他们看着这个图片，想：“这就是比特币的样子。”这不是比特币的样子，因为我说过，没有硬币。这就是危险。

## 8.4创新的设计

**Designing for Innovation**

It’s a really difficult task to design good metaphors for bitcoin because there is no parallel. We have never done this before. We fall into these traps of trying to extrapolate from our previous experience, and fall short. Disruptive technologies do this. In an incremental technology, if you take what you currently understand and then just use a milligram of vision and extend it just a tiny bit, you understand the new technology because it really is just a slight extension of the past. Bitcoin is a radical break from the past, so understanding the way traditional money works doesn’t help you understand bitcoin. If anything, it hinders your understanding of bitcoin. The people who understand bitcoin the least are monetary economists. They cannot wrap their heads around it. They will write long theses on how bitcoin is not money, despite the fact that I’ve been living on it for years.

为比特币设计一个好的比喻真的是一项困难的任务，因为没有类似的东西。

我们以前从来没有这样做过。我们陷入了这些陷阱，试图从我们以前的经验中推断出来，结果却落空了。

颠覆性技术做到了这一点。在一个增量技术中，如果你采用你现有的理解，然后只使用一点儿想象，对它做一点儿扩展，你就能理解这个新技术，因为它只是对过去的一个微小的延伸。

比特币是对过去的一个彻底的颠覆，所以，理解传统货币的运作方式并不能帮助你理解比特币。

如果有的话，它会阻碍你对比特币的理解。理解比特币最少的人是货币经济学家。他们理解不了它。他们会写很长的论文来论述为什么比特币不是货币，尽管事实上，我已经靠它生活了好几年。

Understanding disruptive technologies is even harder than understanding incremental technologies because the most interesting things they do have no previous parallel. Think about it this way . . . Look back at Star Trek in the 1970s. What did they get right? They got tricorders. They got portable communicators. They got video telephony. They got all that was predictable with the technology of the 1970s. They couldn’t possibly get the internet. They couldn’t possibly understand the idea of networked information stores. They had fantastical computers that could talk to you, but they didn’t have access to any data. They couldn’t possibly predict things like social media. Most importantly, if you pay attention, you will notice something very strange. Star Trek doesn’t have any money at all. There is no money anywhere in the Star Trek universe. Why is that? Because their furthest vision of the possibility of society is a society without money, a society without a language for transmitting value, which is probably the most radical departure from reality.

理解颠覆性技术比理解增量技术更难，因为他们所做的最有趣的事情都没有先例。

这样想一想 …… 回顾1970年代的《星际迷航》，他们做对了什么？他们有手持科学分析仪。他们有便携式通讯设备。他们有视频电话。他们有1970年代的技术所能预见的所有东西。

他们不可能有互联网。他们不可能理解网络信息存储的概念。他们有可以与你交谈的神奇电脑，但他们没有访问任何数据。他们不可能预测像社交媒体之类的事情。

最重要的是，你会注意到一些非常奇怪的东西。《星际迷航》根本没有任何货币。在星际迷航宇宙中，任何地方都没有货币。为什么会这样？因为他们对社会的可能性的最远愿景是一个没有货币的社会，一个没有用于传递价值的语言的社会，这可能是最彻底地脱离现实。

### 8.4.1. 预言未来

**Predicting the Future**

When we try to predict the future, there are certain areas that are completely dark to us. These are the areas that have never been seen before. These are the applications that we cannot imagine because, in order for them to come into being, many things have to fall into place. For the web to happen, you needed a common standardized transmission protocol. For the web to give birth to social media, you needed massive penetration of basic email and TCP/IP connections. You needed penetration of those connections on an always-on state. You needed to have mobile devices with high-density computing in the palm of your hand that were internet connected. All of those things had to come to fruition before social media was even possible.

当我们试图预测未来时，某些领域对我们来说是完全黑暗的。

这些是我们从未见过的地方，是我们无法想象的应用，因为，为了让它们出现，许多事情必须要到位。

要使Web出现，需要一个通用的标准传输协议。

为了让Web产生社交媒体，你需要大规模渗透基本电子邮件和TCP/IP连接。

你需要在持续的状态下渗透这些连接。

你需要有互联网连接的高性能计算的移动设备。

所有这些都必须在社交媒体成为可能之前实现。

If you look at the internet in 1992, you think that it will replace the phone. That’s the only experience that you have. The internet is a fancy phone. Perhaps it’s a fancy phone/fax, perhaps a multifunctional printer/fax/phone. It’s very fancy. So, the phone companies look at this and say, "Oh, it’s a fancy phone. We can do this." They were wrong, fortunately. Otherwise, every time I went on a Skype call, there would be a little slot on the side of my computer, and I would have to deposit quarters every three seconds to make a Skype call. Fortunately, the phone companies didn’t get to write the rules. They couldn’t possibly predict the outcomes we saw on the internet, because most of the interesting things were not incremental improvements or extensions of the things before. They were radical departures from the past, because they created the conditions for things that were not possible before.

如果你看看1992年的互联网，你认为它会取代电话。这是你唯一有的经验。

互联网是一个花哨的电话。也许是一个花哨的电话和传真，也许是多功能打印机、传真、电话。很花哨。

所以，电话公司会看着这个说：“哦，这是个花哨的电话。我们能做到这一点。”幸运的是，他们错了。

否则，每次我拨打Skype电话时，我的电脑旁边都会有一个小插槽，而且我必须每三秒钟存一个季度的钱才能拨打Skype电话。幸运的是，电话公司没有写出规则。他们不可能预测到我们在互联网上看到的结果，因为大多数有趣的事情不是之前的增量改进或扩展。它们从根本上偏离了过去，因为他们为以前不可能的事情创造了条件。

Let’s go back to bitcoin and think about this for a second. Consider what we’ve been talking about: financial transactions, banking, payments. “It’s a fancy credit card.” “It’s Paypal, basically. It’s a global Paypal." But it’s not. It’s something completely, radically different, but we can’t see where that’s going to go. The applications that are going to happen on bitcoin, the really interesting applications, are those that can only happen when you have sufficient adoption and penetration of this technology—the ability to do cross-border transactions on a level that has never been done in the history of humanity before.

我们回到比特币，考虑一下这个。

考虑我们一直在谈论的内容：金融交易、银行业务、支付。

“这是一张花哨的信用卡。”“这就是Paypal，这是一个全球性的Paypal。”

但事实并非如此，完全不同，但是我们无法看清它要去哪里。

比特币上将要发生的应用，真正有趣的应用，只有在这项技术得到充分采用和渗透时，才会出现。能够在在人类历史上从未做过的水平上进行跨境交易。

Today, there are 3 billion people with no banking facilities whatsoever. Three billion more people—“underbanked,” as we call them—without any access to international credit or finance. You or I can go to a brokerage website right now and within 24 hours have a US-dollar-denominated account that can trade on the Tokyo stock exchange. That is privilege. That is a facility afforded to less than a billion people in the world. One out of seven. The other 6 billion? They barely have basic checking, if that. A lot of them live in cash- or barter-based societies. So, the question you then have to ask is what happens when a farmer in Kenya who has a Nokia 1000 text-messaging phone, and suddenly that phone is a Bloomberg terminal, a loan-origination terminal, a Western Union remittance-termination terminal, a stock market, is a bank—not a terminal to a bank, but a bank, on the phone? And what happens when that is afforded to the other 6 billion all over the world.

今天，有30亿人没有任何银行业务工具。

这30亿人我们称之为“无银行账户”，他们无法获得国际信贷或金融。

你或我现在可以去经纪网站，并在24小时内有一个美元计价的账户，可以在东京证券交易所交易。

这是特权。这是一个为全世界不到10亿人提供的设施。只有七分之一，另外60亿人呢？

如果是这样，他们几乎没有基本的活期存款。他们中的很多人生活在以现金或易货交易为基础的社会中。

那么，你要问的问题是，肯尼亚的一位农民，拥有诺基亚1000短信手机，突然该手机是彭博终端、贷款发起终端、西联汇款终端、股票市场、一个银行（不是银行终端，而是银行），会发生什么呢？

当全世界其他60亿人获得这种情况时，会发生什么。

Part of the reason bitcoin is unstoppable is because there is this great need for this technology. Banks in the developing world cannot extend services to these populations. Recently, I was talking to a banker who told me, “Half our population is 100 miles from the nearest branch, upstream, on a canoe. We can’t serve them.” But even the remotest village in the Amazonian basin has a cell phone tower, and someone in that village has a solar panel and a Nokia 1000 text phone. There are more Nokia feature phones in the world than any other kind of electronic device. It is the most massively produced device humanity has ever produced. Almost 5 billion people have access to cell phones. Almost 3 billion people have access to cell phones and do not have access to safe drinking water. Think about that. Cell phones are more widespread than water on our planet. What happens when each and every one of those is a banker. For me, the vision of bitcoin is not to bank the other 6 billion; it’s to unbank all of us. We can do it. Banking is an app.

比特币是不可阻挡的，部分原因是因为，对这项技术有着巨大的需求。

发展中国家的银行无法向这些人口提供服务。

最近，我和一位银行家交谈，他告诉我，“我们有一半的人口距离最近的分支银行有100英里，在上游，在独木舟上。我们无法为他们服务。”

但即使是亚马孙盆地最偏远的村庄也有一个手机基站，村里有人用太阳能电池板和诺基亚1000功能手机。

诺基亚功能手机比世界上其它类型的电子设备都多。它是人类生产的最多的设备。将近50亿人有手机。近30亿人有手机，但无法获得安全饮用水。

想想看。在地球上，手机比水更普遍。当每个人都是银行家时会发生什么。

对我来说，比特币的愿景不是为了把另外60亿人纳入银行，而是让我们所有人都不要银行。我们可以做到。银行业务是一个应用程序。

## 8.5间隙创新

**Interstitial Innovation**

That’s just the beginning. The really interesting things in bitcoin happen in what I call “interstitial innovation”—the innovation and the gaps, the places where today’s systems cannot go. Technologies have an interesting effect where they suddenly change basic assumptions. Some of the most powerful things that happen on the internet happen not just because of connectivity, but because of the marginal cost of transmitting information over distance. Before the internet, moving information from point A to point B cost a lot of money. The internet drove that cost almost to zero. The result was that millions of applications that could not happen on the previous cost basis, even if we could imagine them, suddenly became possible. Why on earth would you stream music instead of buy it and store it locally? Because it costs nothing. Once it costs nothing and you can stream music, then you suddenly realize that ownership is kind of overrated. If an entire generation realizes that, then intellectual property is kind of overrated. Bye-bye, recording industry. These effects happen because the technology changes the fundamental costs of doing things.

这只是开始。比特币真正有趣的事情发生在我所说的“间隙创新”——创新和间隙，就是今天的系统不能到达的地方。

技术有一个有趣的效应，它们会突然改变基本的假设。

互联网上发生的一些最有影响力的事情不仅是因为连接性，还因为远距离传输信息的边际成本。

在互联网之前，把信息从A点移到B点要花很多钱。互联网将成本几乎降到了零。结果是数百万的应用程序突然可行了，即使我们之前能想象到它们，但因为成本原因无法实现。

为什么你会在网上听音乐，而不是购买它，把它存储在本地？因为它基本上不花钱。一旦不花钱，你可以通过网络听音乐，然后你突然意识到所有权有点儿被高估了。

如果一代人都意识到这一点，那么知识产权就有点儿被高估了。

再见，唱片业。这些影响的发生，是因为技术改变了做事情的主要成本。

Let’s think about what happens when bitcoin changes the fundamental cost of transacting—transacting across distance, transmitting value, recording information, and recording information in an immutable way. What happens when, for the first time ever, there is a system that can evaluate rules without human intervention and be trusted without having to put trust in any single human? In bitcoin, we call this the removal of counterparty risk. If I create a transaction and I sign it, everyone on the bitcoin network can validate that transaction independently. They don’t have to ask anyone. They can go through the blockchain on their own machine, which they know is correct and true because they have been tracking it and building it based on proof of work. They can check that transaction, 350 bytes, and they can validate that transaction without asking anybody else. A self-verifying system, a system of rules that exists independent of human actors, that exists based on this network topology.

让我们来思考一下，当比特币改变交易的主要成本时，会发生什么，比如远距离交易、传递价值、记录信息、并以不可修改的方式记录信息。

这时会发生什么：当有史以来第一次，有一个系统可以在没有人为干预的情况下计算规则，并且可以得到信任，而不需要信任任何某个人。

在比特币中，我们称之为消除对手风险。如果我创建一个交易，我签署它，比特币网络上的每个人都可以独立地验证这个交易。他们不必问任何人。他们可以在自己的机器上浏览这个区块链，他们知道它是正确的和真实的，因为他们一直在跟踪它，并根据工作量证明在建造它。他们可以检查那个交易，350字节，并且可以在不询问其他人的情况下验证那个交易。

一个自验证系统，一个独立于人类角色的规则系统，它基于这个网络拓扑存在。

What does that mean? What does it do to commerce, to transactions? We can understand what it does to banking. We can understand that Western Union is going down hard this decade. You charge 30 percent on the poorest people in the world, you deserve to go down by disruptive technology. Last year, the CEO of Western Union said, “In the medium term, we are not worried about bitcoin." I want that framed on my wall. It’s one of those phrases, like the boss of Kodak saying things like that when Nokia took away their lunch. Kodak was the largest camera company in the world until a company that wasn’t in the camera business shipped a billion cameras in one year and destroyed their industry. They never saw it coming. Nokia, by the way, is the world’s largest manufacturer of cameras, by far. That’s going to happen to Western Union.

这意味着什么？它对商业、交易有什么影响？

我们可以理解它对银行业的影响。我们可以理解，西部联盟在这十年里正在艰难地走下去。

你在世界上最贫穷的人身上收取30%的费用，你应该被颠覆性的技术打败。

去年，西部联盟的CEO说：“从中期来看，我们并不担心比特币。”

我想把这句话挂到我的墙上。这句话就像柯达老板在诺基亚拿走他们午餐时说的那样。

柯达是世界上最大的照相机公司，但一家不在照相机行业的公司在一年内卖出十亿台照相机，摧毁了他们的产业。他们从来没有看到它的到来。

顺便说一下，诺基亚是迄今为止世界上最大的照相机制造商。这种事将发生在西部联盟。

That’s the easy stuff. What happens when you are able to do this validation of rules without a third party? It changes several fundamental societal institutions that we have today. It changes what’s called the Coase coefficient, which is the overhead created by organization. If we want to do something as a team, two people can do more than what one person can do. Three people can achieve even more. But there’s a limit to that. Once you get too big, the communication overhead between participants in the group is greater than the marginal increase in efficiency. So, adding more people makes it worse, because the group is getting bigger too fast. Bitcoin changes that, because it now reduces the coefficient of organizing on a transactional, on a commercial, on an independent-validation basis, on an extremely large scale. We can now get about a million people, about 5,000 machines, to agree on the state of a ledger every ten minutes at extremely low cost. That has never happened before. It opens the door for things that we can’t even imagine. Bitcoin is radically discontinuous from the past.

这是简单的东西。当你能够在没有第三方的情况下进行规则验证时，会发生什么？

它改变了我们今天的几个基本社会机构。它改变了科斯系数，它是组织创造的开销。

如果我们想作为一个团队做一些事情，两个人能比一个人做的多。三个人可以做到更多。但这是有限度的。一旦你变得太大，组织中的参与者之间的沟通开销大于效率的边际增加。

因此，增加更多的人会使情况变得更糟，因为这个组织变大地太快。

比特币改变了这一点，因为它在一个交易的、在一个商业的、在一个独立验证的基础上，在一个非常大的规模上，降低了组织的系数。

我们现在可能有大约一百万人，大约5000台机器，每十分钟以一个极低的成本来对一个账目的状态达成一致。这以前从未发生过。它为我们无法想象的事情打开了大门。比特币从根本上与过去是不连续的。

Let’s take one simple example: personhood. Personhood is required for financial ownership. In order to own money, in order to control funds, in order to have a bank account, to receive a bill, to pay someone, you must be a person. Everywhere in the world in every payment and financial network that exists, people own money. They may own it in the form of corporations, but that’s just people grouping together. They may use proxies, agents, things like that, but that’s just people working together. Bitcoin does not require personhood. A software agent can own money. A piece of software can be autonomously controlling money without any human intervention. This is completely unheard of in the history of man. We have never seen what happens next.

我们举个简单的例子：人格化。

金融所有权需要人格化。为了有钱，为了控制资金，为了有一个银行账户，来接受一个账单，来付钱给别人，你必须是一个人。

在世界各地的每个支付和金融网络中，人拥有金钱。他们可能以公司的形式拥有它，但那只是人们组织在一起。他们可以使用代理（proxy、agent），诸如此类的东西，但那只是人们一起工作。

比特币不需要人格化。一个软件代理可以有钱。一个软件可以自动控制钱，而不需要任何人干预。

这在人类历史上是前所未闻的。我们从未见过接下来会发生什么。

Here’s a little thought experiment. Let’s take three radically disruptive technologies and mash them together. Bitcoin. Uber. Self-driving cars. What happens when you mash the three together? The self-owning car. A car that pays for its Toyota lease, its insurance, and its gas, by giving people rides. A car that is not owned by a corporation. A car that is a corporation. A car that is a shareholder and owner of its own corporation. A car that exists as an autonomous financial entity with no human ownership. This has never happened before, and that’s just the beginning. Audience member gasps: "Oh shit!"

这里有一个小小的思考实验。我们采用三种彻底颠覆性的技术，把它们混在一起。

比特币、Uber、自动驾驶汽车。当你把这三个东西混在一起时，会发生什么？

自拥有备汽车。一辆汽车通过让人们乘坐，支付它的租金、保险、汽油。

一辆不属于公司的汽车。一辆汽车就是一个公司。一辆汽车就是它自己公司的一个股东和所有者。

一个作为一种无人所有的自治金融实体而存在的汽车。

这以前从未发生过，这只是个开始。

观众们很惊讶：“哦，胡扯！”

I can guarantee you that one of the first distributed autonomous corporations is going to be a fully autonomous, artificial-intelligence-based ransomware virus that will go out and rob people online of their bitcoin, and use that money to evolve itself to pay for better programming, to buy hosting, and to spread. That’s one vision of the future. Another vision of the future is a digital autonomous charity. Imagine a system that takes donations from people, and using those donations it monitors social media like Twitter and Facebook. When a certain threshold is reached and it sees 100,000 people talking about a natural disaster, like a typhoon in the Philippines, it can marshal the donations and automatically fund aid in that area, without a board of directors, without shareholders. One hundred percent of donations goes directly to charitable causes. Anyone can see the rules by which that autonomous altruistic charity works. We are beginning to approach things we have never seen before. This is not just a currency.

我可以向你保证，第一个分布式自治公司将是一个完全自治的、基于人工智能的勒索病毒，它会出来抢夺在线人的比特币，并使用这些钱来发展自己：付钱给更好的编程、购买托管、传播。

这是未来的一个愿景。未来的另一个愿景是数字自主慈善组织。

想象一个从人们那里得到捐赠的系统，使用这些捐款，它监视社交媒体，例如Twitter和Facebook。当达到一定的阈值时，它看到10万人在谈论自然灾害，如菲律宾的台风，它可以召集捐款，并自动资助那个地区，没有董事会，没有股东。捐款全部直接用于慈善事业。任何人都可以看到这个独立自主慈善事业的运行规则。我们开始接近以前从未见过的东西。这不仅仅是一种货币。

Now, let’s look at how the bitcoin community is addressing this incredible potential with their design choices and metaphors. Oh boy, it’s a mess.

现在，让我们看看，比特币社区如何用他们的设计选择和比喻来解决这个难以置信的潜力。

哦，孩子，真是一团糟。

## 8.6 ATM体验

**ATM Experience**

Let’s take a simple example. How many of you had an experience with a bitcoin ATM—or BTM, as it’s known? How was that experience? Who enjoyed it? Nobody, that’s about right. What is an ATM? ATMs have been around for 25 years now. What purpose does an ATM serve? What is its goal? Audience member: “It’s a cash dispensary.” Okay. When you interact as a person with an ATM: you have a pre-existing relationship with the bank or financial institution, you have a pre-existing balance, your primary objective is to get in, get cash, get out. Twenty seconds is too long. Three clicks is too long. The most incredible innovation in ATMs in the last 25 years has been Fast Cash. That’s it. They haven’t really changed much. You press a button. Now, I can get cash in one click. Wow—15 seconds, in and out. Why is this important? Because one of the primary uses of ATMs is that at 1:00 in the afternoon, 100 people line up in front of four or five ATMs in the center of town and all try to take out 20 dollars to buy lunch. You see this all around the world.

我们举个简单的例子。有多少人用过比特币ATM（BTM）？感觉怎么样？谁喜欢它？

没人，这就对了。什么是ATM？ATM已经存在25年了。

ATM服务的目的是什么？它的目标是什么？观众：“它是一个现金药房。”

当你与ATM互动时：你与银行或金融机构有一个预先存在的关系，你有一个预先存在的余额，你的主要目标是进入、获得现金、离开。二十秒太长了。三次点击太长了。

在过去25年中，ATM最不可思议的创新是Fast Cash。就是这样。他们没有太大的变化。

你按下一个按钮。现在，我可以一次点击就能获得现金。哇，15秒，进出。

为什么这很重要？因为ATM的一个主要使用时间是下午1点，在市中心，四五个ATM前面排了100多人，所有人都要取出20美元来买午餐。你在全世界都能看到了这个场景。

What is the purpose of an ATM? For a bank, the purpose of an ATM is reducing the overhead of having a human, and reducing the interaction to the shortest possible time for someone who has a pre-existing relationship with that bank. What does that have in common with the bitcoin ATM? Absolutely nothing.

ATM的目的是什么？对于一家银行来说，ATM的目的是减少有人的开销，对于与银行有预先存在关系的人，把交互减少到最短可能时间。

这与比特币ATM有什么共同点？绝对没有。

## 8.7比特币ATM体验

**Bitcoin ATM Experience**

Now let’s look at the experience of a bitcoin ATM. The average user of a bitcoin ATM is someone who has never seen bitcoin before. It is a person who doesn’t understand what bitcoin is, and the ATM is their first introduction to this currency. It’s a person who does not have a pre-existing relationship with anyone in the bitcoin space. It is a person who does not currently have a wallet, because they didn’t know they needed one. They don’t know what a wallet is, they certainly don’t know it’s actually a keychain. They walk up to this machine, and this machine has been designed by engineers to simulate the experience of an ATM, even though the experience shares absolutely nothing with the use case we’re putting it to.

现在我们来看看比特币ATM的体验。

比特币ATM的普通用户是以前从未见过比特币的人。

他不理解比特币是什么，ATM是向他们第一次介绍这种货币。

这个人与比特币空间的任何人都没有预先存在的关系。

这个人现在没有一个钱包，因为他不知道他需要一个钱包。他们不知道钱包是什么，他们当然不知道它实际上是一个钥匙链。

他们走到这台机器上，这台机器是由工程师设计的，模拟一台ATM的体验，即使这种体验与我们要用的方式之间绝对没有任何相同的地方。

So, you walk up and the ATM tries to give you bitcoin in as few clicks as possible with a minimum amount of interaction. Is that a way to build brand loyalty? Is that a way to build user experience? Is that a way to introduce new users? I mean, it just throws it at you. You’re not ready for that. Please open your phone and display your QR code. You’re like, “What? What’s a QR code? . . . Hang on, let me go to Google Play and search for ‘QR code.’ There’s an app that scans them, . . . maybe I should use that one. Shouldn’t use that one. Maybe I should use a bitcoin wallet. Oh, there are 26 of them. Which one’s the best? I don’t know. I’ll use Circle. . . . Oh, that requires a pre-existing relationship, whoops. I’ll use Coinbase. . . . Oh, that requires a pre-existing relationship, oops. . . .”

所以，你走过去，ATM试图给你比特币，尽可能少点击，尽可能少的互动。

这是建立品牌忠诚度的一种方式吗？这是一种建立用户体验的方法吗？这是一种引入新用户的方式吗？

我的意思是，它只是把它扔给你。你还没有准备好。

请打开你的手机，显示你的二维码。

你会说：“什么？什么是二维码？…等等，我到Google Play上搜索二维码，有一个app扫描它们 … 也许我应该用那个。不应该用那个吗？也许我应该用一个比特币钱包。哦，有26个钱包。哪个是最好的？我不知道。我用Circle … 哦，这需要一个预先存在的关系，哎呀。我用Coinbase … 哦，这需要一个预先存在的关系，哎呀 …”

Finally, I’ve got my wallet and I display the QR code, put some money in, and I’ve got the bitcoin. What am I going to do with it? I have all these questions. Who takes bitcoin? Where can I spend this? How do I send it? How do I secure it? Will it get lost if I lose my phone? I have no clue. Why? Because this bloody infernal machine didn’t tell me anything. It just threw the bitcoin at me, and in 15 seconds it’s off to the next customer.

最后，我有了我的钱包，我展示了二维码，投入了一些钱，我得到了比特币。

我用它做什么呢？我有很多问题。

谁要比特币？我可以在哪花呢？我怎么发送它呢？如何保证它的安全？如果我丢了手机，钱会丢吗？

我没有头绪。为什么？因为这该死的机器没有告诉我任何事情。

它只是把比特币扔给了我，15秒钟后，它就转到下一个客户那里去了。

If I was designing a bitcoin ATM, first of all, I’d put it in bodegas. Secondly, it wouldn’t have a lick of English on it; it would be all Spanish because I’m going to really push the remittance model. Thirdly, the first function on the ATM would be Send Money to Mexico City. That’s it. Because I want people to use the bitcoin for something. Fourth, I’d have a big button on the front that says Talk to a Human. I’ve got an internet-connected device with a forward-facing camera and a tablet screen, and I’m not using it to do video customer service, are you kidding me? Boom: Skype. A person. “What the hell is bitcoin? Where do I spend it?” "Oh, sir, I see that you’re in the bodega on 25th Avenue. There are three stores that take bitcoin in your area. Let me show you a brief introductory video. Gather all the children in the store and we can all dance to a little bitcoin song. Let’s watch another video.” I don’t want to interact for 15 seconds. I want to interact for two hours and get all of my friends to sit in front of the machine and watch the little bitcoin videos and learn about bitcoin. It’s got pretty colors, and it tells me where I can spend it. It gives me suggestions on wallets. It can send them directly to my phone. It’s building loyalty, brand, and experience. That’s not a 15-second interaction. This is the first experience that many people will have with bitcoin. You have the opportunity to make this a deep, meaningful, educational experience. But you don’t.

如果我要设计一个比特币ATM。

第一，我会把它放在酒店。

第二，它不会有一点点英语，它将是西班牙语，因为我要真正推动汇款模式。

第三，ATM上的第一个功能是向墨西哥汇款。就是这样。因为我希望人们用比特币做某事。

第四，我前面有一个大按钮，跟人说话。我有一个带有前向摄像头和平板屏幕的互联网连接设备，我不是用它来做视频客户服务，你在开玩笑吧？Boom：Skype。一个人。

“比特币到底是什么？我在哪里花它呢？”

“哦，先生，我看到你在第二十五大街的酒店。在你的地区有三家商店使用比特币。我给你看一段简短的介绍视频。把商店里的所有的孩子聚在一起，我们都可以跳一首小比特币的歌。我们看另一个视频。”

“我不想互动15秒。我想互动两个小时，让我所有的朋友坐在机器前看小比特币视频，了解比特币。它有漂亮的颜色，它告诉我我可以在哪里花它。它给我一些关于钱包的建议。它可以把它们直接发送到我的手机。它建立忠诚、品牌和体验。这不是一个15秒的互动。这是许多人对比特币的第一次体验。你有机会使这成为一个深刻、有意义、教育的经历。但你没有这样做。

## 8.8孩子们使用比特币

**Kids Use Bitcoin**

Here’s another little clue, kids are using bitcoin. On average around the world, the earliest age at which you can open a bank account is 16 years old. By the time that 16-year-old goes to the bank, I want them to have at least six years of active bitcoin use in their experience. Because then, when they face their first banker, they’re going to be, "Three to five days?! Business days?! What the hell is a business day? What do you mean you close at 5:00? I barely get off of work at 5:00. What do you mean I have to pay for you to store my money. This is ridiculous. Have you people even heard of bitcoin?!”

这里是另一个小线索，孩子们在使用比特币。

在全世界，平均要16岁才能开银行帐户。16岁时去银行，我想他们有至少有六年比特币的使用经验。

因此，当他们面对第一个银行人员时，反应会是“三到五天吗？工作日？什么是工作日？你的意思是5点钟要关门？我在五点还没下班。我存钱，还要付钱给你，什么意思？这太搞笑了，你听说过比特币吗？”

"For many young people, bitcoin will be their first economic experience. By the time they get to a bank, they will be done with banking in advance."

对许多年轻人来说，比特币将是他们的第一次经济体验。

当他们到银行时，他们将提前完成银行业务。”

That’s the experience I want. Guess what? Ten-year-olds are opening bitcoin accounts. You know why? They can go download the app on the internet, and they can be in control of money for the first time. So, you need to have the birds-and-bees discussion, but you also need to have the private-keys discussion. This is a huge generational divide. For many young people, bitcoin will be their first economic experience. By the time they get to a bank, they will be done with banking in advance. That’s a huge advantage.

这就是我想要的经历。你猜怎么着？十岁的孩子开设比特币账户。你知道为什么吗？

他们可以在互联网上下载应用程序，他们可以在第一时间控制金钱。

所以，你需要有公开的讨论，但是你也需要有私钥的讨论。这是一个巨大的代际分歧。

对许多年轻人来说，比特币将是他们的第一次经济体验。当他们到银行时，他们将提前完成银行业务。

这是一个巨大的优势。

## 8.9全新的技术，相同的老术语

**Brand New Tech, Same Old Terms**

So, how do you appeal to a completely new demographic? Part of the trick is not trying to be a bank. Do not try to do anything related to traditional banking. All that does is pollute their mind. You want new users to have a brand new experience with bitcoin that is unlike any banking they will ever see. You don’t want it to look like a checking account. God forbid you use the word "checking.” Open any one of the exchanges right now—Circle, Coinbase. What is the name of your account on Coinbase? It is a checking account, and it has a balance, and it shows you a statement. Who did they hire for this design? What does the word “checking” mean? It means an account on which you can write checks. I know this is America and we’re 25 years behind on fintech. The rest of the world doesn’t do checks, I guarantee you. What is a check? A check is the device by which a grandma can make 20 people in line behind her in the supermarket simultaneously groan. I use it to pay my rent every month. I don’t know why. I can’t do it any other way. It’s insane that I’m signing a piece of paper and sending it through the postal system in 2015. So that my landlord can walk it through the bank and deposit it. So that it might clear three to five business days later, after they’ve charged him five dollars to own his own money.

那么，你如何吸引一个全新的人口呢？其中的一个诀窍是，不是试图成为一家银行。

不要试图做任何与传统银行相关的事情。所有这些都污染了他们的思想。

你希望新用户对比特币有一个全新的体验，这与他们讲过的任何银行都不同。

你不想让它看起来像支票账户。上帝禁止你使用“支票（checking）”这个词。

现在打开任何一个交易所，Circle、Coinbase。你在Coinbase上的帐户名称是什么？这是一个支票账户，它有一个余额，它给你显示一个声明。他们雇佣了谁来做这个设计？“支票”这个词是什么意思？这意味着你可以写支票的账户。我知道这是美国，我们落后于金融科技25年。我向你保证，世界其它地方不做支票。支票是什么？一张支票是一个装置，一位奶奶通过它可以让超市里在她后面排队的20个人同时叹气。我每个月都用它来付房租。我不知道为什么。我不能用别的方法去做。我签了一张纸，并在2015年通过邮政系统发送它，这简直狂了。这样，我的房东就可以通过银行存款。因此，在银行向他收取了三美元来让他拥有自己的钱之后，五个工作日后，账可能结清了。

We don’t really need a hard sell to make bitcoin win on the banks. All you need in order for bitcoin to win against banks is for a person to use bitcoin for a week, and then the bank will take care of the rest. They’ll freeze their account, they’ll tell them they’re closed, they’ll hold it for three to five business days. They just sold bitcoin. Banks will sell it for you every single time.

我们真的不需要硬销售，来让比特币胜过银行。

你需要做的是，让一个人使用比特币一个星期，然后银行将负责其余事情。

他们会冻结他的帐户，会告诉他账户被关闭，他还能用三到五个工作日。

他们刚刚卖掉比特币。银行会每隔一段时间卖给你。

### 8.9.1国际电汇的乐趣

**The Joys of International Wire Transfer**

I was invited to do a talk at the Bundesbank, the German Federal Bank. They were paying me for this speaking engagement, but they didn’t know how to do bitcoin, which is a real problem because I usually get paid in bitcoin. So, we agreed to do a wire transfer. It took 16 days. First, they asked for my account number. Then, the next day they said they needed the SWIFT number. By that time, my bank was closed, so I couldn’t get the SWIFT number. The next morning, I got the SWIFT number and I sent it to the Germans. By that time, their bank was closed. The next morning, they used the SWIFT number and discovered it was the wrong SWIFT number. It was the SWIFT number for US dollars, not for foreign currency. So, they sent me an email, but by that time my bank was closed. The next day, I got the other SWIFT number and I sent it to the Germans, but by that time their bank was closed. They sent me the wire. My bank took one look at this wire and said, "Bundesbank. Never heard of them. Sounds dodgy. Let’s freeze this for 14 days, just in case it bounces.” This is the third largest central bank in the world. This is the German Federal Bank. They do not bounce checks. 14 days later—and this is the great part—they said, "Money held. Money released." They released 80 dollars of the total amount, which was a four-figure amount. 80 dollars. Why 80? What the hell is that? What am I going to do with that? Just hold all of it. Are you teasing me? This makes no sense.

我被邀请去德意志联邦银行做一个演讲。他们付钱给我做这个演讲，但他们不知道怎么用比特币支付，这是个真正的问题，因为我通常用比特币支付。所以，我们同意做一个电汇。花了16天时间。

首先，他们要了我的账号。然后，第二天他们说需要SWIFT号码。那时，我的银行已经关门了，所以我没能拿到SWIFT号码。第二天早上，我得到了号码，把它发给德国人。到那时，他们的银行关门了。第二天早上，他们使用了SWIFT号码，发现这是一个错误的SWIFT号码。它是美元的SWIFT号码，不是外币的SWIFT号码。所以，他们给我发了一封电子邮件，但那时我的银行关门了。第二天，我拿到了另一个SWIFT号码，把它发给了德国人，但那时，他们的银行关门了。他们给我发了电报。我的银行看到了这个电报，说：“德国央行，从没听说过。听起来很狡猾。冻结14天，以防万一。”这是世界第三大央行。这是德国联邦银行。他们不会反弹支票。14天后，他们说：“Money held. Money released.”。他们释放了80美元的总金额，这是四位数的金额。80美元。为什么是80？那到底是什么？我该怎么办呢？就这些。你在取笑我吗？这没有道理。

## 8.10传统银行比喻的问题

**The Problem with Traditional Banking Metaphors**

This is what we’re addressing with bitcoin. If you are introducing a new product in this market and you are a designer, which parts of this design metaphor do you want to re-use in your product? According to the bitcoin marketplace, all of them, so that you can persuade people that this is just like your bank. It doesn’t have any of the good parts of a bank—like the ability to easily reverse transactions, to get a refund if you lose your private key. It doesn’t have any of those. It also doesn’t have any of the bad parts of banks, but we don’t pay attention to that. So, we’ve created expectations that are entirely misleading.

这就是我们用比特币解决的问题。

如果你在这个市场推出一个新产品，你是一位设计师，那么你想在产品中重用这个设计比喻的哪些部分？

按照比特币市场，所有这些，所以你可以说服人们，它就像你的银行。

它没有银行的任何好的部分，例如如果你丢了私钥，能够轻松地撤销交易，获得退款。

它没有任何这些。它也没有银行的任何坏的部分，但我们没有注意到这一点。

所以，我们创造了完全误导的期望。

"Bitcoin desperately needs design. It has been created by engineers and it is absolutely inscrutable."

“比特币迫切需要设计。工程师创造了他，它绝对是神秘莫测。”

## 8.11创新，设计和采用

**Innovation, Design, and Adoption**

Bitcoin desperately needs design. It has been created by engineers and it is absolutely inscrutable. But I have hope because we’ve done this before. I got on the internet in 1989, and at the time it was illegal to do commercial activities on the internet. It was owned by the National Science Foundation, and it was only for academics (or, let’s say, 15-year-olds who happen to find the password to an academic system). At the time, DNS was still in its infancy. Most systems didn’t really have DNS names assigned yet. It wasn’t very well structured. A lot of the most interesting things you could only find via IP address. I walked around with a list of IP addresses in my wallet, so I had access to these things. In order to use it, it required UNIX command-line skills.

比特币迫切需要设计。工程师创造了它，它绝对是神秘莫测。

但我有希望，因为我们以前做过这个。我在1989上了互联网，那时在互联网上做商业活动是违法的。

它由国家科学基金会所有，它只针对学术界（或是15岁的孩子，他碰巧找到了一个学术系统的密码）。

当时，DNS还处于起步阶段。大多数系统还没有真正指定DNS名称。结构不是很好。

你只能通过IP地址找到很多最有趣的事情。我带着一个IP地址列表到处游荡，所以我看到了这些东西。

为了使用它，需要UNIX命令行技能。

There was absolutely no way that was going to get used by my mom. My mom called me and told me her stereo was broken, and I tried to figure out why. She said, “It’s displaying an error message. It’s blinking at me ‘0:00.’” It took me a few minutes to figure out that she had pulled the plug and the clock had reset. So, the clock was waiting to be set again and was blinking “0:00.” That’s the person who I wanted to use the internet so we could talk, but that wasn’t going to happen. It took almost exactly 20 years from the day I sent my first email to the day my mom sent her first email. In order to do so, a lot of things had to happen. Most importantly, the iPad. She was able to do it with a swipe of a finger, and that was the only thing that made it possible.

绝对没有办法让我妈妈用。我妈妈打电话给我，告诉我她的音响坏了，我试着弄清楚原因。

她说：“它显示了一个错误信息。闪烁显示0:00。”

我花了几分钟才弄明白她拔了插头，时钟被复位了。所以，时钟在等待重新设置，闪烁着“0:00”。

我想让这样的人使用互联网，所以我们可以交谈，但那是不会发生的。

从我发第一封email给我妈妈，到她发第一封mail，我花了差不多20年的时间。

为了做到这一点，很多东西必须要出现。最重要的是iPad。她能用手指来操作，这是唯一能使它成为可能的东西。

There was no way that internet in 1989 could be used by the mainstream.

在1989年，互联网还没有办法让主流使用。

### 8.11.1用户体验和社会

**UX and Society**

There’s this fantastic outtake from a morning TV show in 1994 in which the journalists are in a huddle just before the show. They are discussing their upcoming internet story, and they’re trying to get their information right. One journalist is asking the other journalists, "So, wait, the internet is the thing with the ‘at’ sign?" "No, no, that’s email. The internet is the thing with the ‘www,’ with the dots and the slashes." "I thought that was the email.” "No, that’s the internet." "But isn’t that the web?" So there’s this circular discussion. A system designed by engineers. Inscrutable. Two things happened. One, we made the technology much easier to understand, much better, more polished. Another important thing happened: society moved. Today, the average person knows exactly the difference between an @ sign and a www, even though it’s a horrible design. Society learned the language of the internet because it was valuable enough to learn the language of the internet.

在1994年的一个早晨的电视节目秀中，有了一个神奇的超越，记者们就在节目上挤成一团。

他们在讨论他们即将到来的网络故事，他们正在努力得到正确的信息。

一位记者问其他记者：“那么，等等，互联网是有@标志的东西吗？”

“不是，那是电子邮件。互联网是有www的东西，有点和斜线。”

“我还以为那是电子邮件。”“不，那是互联网。”“但那不是web吗？”

所以，就有了一个循环讨论。一个由工程师设计的系统。难以理解。

发生了两个事情。首先，我们使这种技术更容易理解、更好、更优雅。第二：社会运动。

今天，普通人确切地知道@和WWW之间的区别，尽管它是一个极不友好的设计。

社会学会了互联网语言，因为学习互联网语言很有价值。

While we made the internet easier, society caught up and also understood the really inscrutable parts of the internet. The same thing is happening with bitcoin. I go to mainstream conferences where they have never heard of bitcoin before and I say, "Listen, don’t worry. Someone in your life can explain bitcoin to you. When they’re done cleaning their room, ask them to teach you bitcoin.” Their 10-year-old will understand it. I’ve met kids that use web-based interfaces to create altcoins of their own.

当我们使互联网更容易时，社会赶了上来，也理解了互联网的真正难以理解的部分。

比特币也在发生同样的事情。我去参加主流会议，他们之前从未听说过比特币，我说：“听着，别担心。在生活中会有人能向你解释比特币。当他们打扫房间时，让他们教你比特币。”

他们10岁的孩子会理解比特币。我见过这样的孩子，使用web接口创建他们自己的替代币。

One of the interesting questions I get often is "How many coins and currencies will there be?" The answer to that is exactly equivalent to "How many bloggers will there be on the internet?" All of us. All of them. Not hundreds of coins; thousands, tens of thousands of coins. When a 6-year-old can create a coin called Joeycoin to launch in his school as a popularity contest, the fact that that coin is also global, unforgeable, scalable, and can be used internationally doesn’t matter to Joey, as long as his five friends really like to use Joeycoin. Unfortunately, a competitor, Mariacoin, is launched on the scene, and an old-fashioned currency war starts. This is going to happen.

我经常被问的一个有趣的问题是：“会有多少种货币？”

这个答案完全等同于：“互联网上有多少博客？”我们所有人。

不是数以百计的货币，而是成千上万的货币。

一个6岁的孩子可以创建名为JoyBoin的货币，在学校里发起一个流行比赛，这个货币也是全球性的、不可伪造的、可伸缩的，并且可以在国际上使用，这对Joey来说并不重要，只要他的五个朋友真的喜欢使用JoeyCoin。

不幸的是，一位竞争者Mariacoin出现了，一场老式的货币战开始了。这是会发生的。

Part of the reason we know this is because children create currency. You leave children in a kindergarten by themselves, and they will invent currency —rubber bands, Pokémon cards, little cubes. They will start hoarding, trading, exchanging for favors, and then eventually getting into a fight over their imaginary currency that they just invented. This is a human experience.

我们之所以知道这一点，部分原因是因为孩子们创造了货币。

你让孩子上幼儿园，他们会发明货币：橡皮筋、扑克牌、小立方体。

他们会开始囤积、交易、交换，然后最终会为他们刚刚发明的假想货币打架。

这是人类的经历。

We just invented the world’s most awesome currency. Your job now is to create the right design metaphors to make it work for everybody else.

我们刚刚发明了世界上最棒的货币。

你现在的工作是创造合适的设计比喻，让它为其他人所用。

Thank you.