# 10信任的要素：释放创造力

**Elements of Trust: Unleashing Creativity**

Blockchain Meetup; Berlin, Germany; March 2016

Video Link: <https://www.youtube.com/watch?v=uLpSM3HWU6U>

Today, I’m going to talk about the chemistry of money, specifically the chemistry of bitcoin. This is one of the aspects of bitcoin that makes it so exciting and so interesting. It’s one that most of us don’t even notice until we study bitcoin for a year or two. Bitcoin is a bit like an onion. You have to unwrap it. As you unwrap it, you find one more layer. I started five years ago. I am still unwrapping. I am finding more and more things that surprise me every day about bitcoin.

今天，我将要讨论货币的化学，特别是比特币的化学。

这是比特币让人如此兴奋和感兴趣的一个方面。

这是一个我们大多数人甚至没有注意到，直到我们研究了比特币一两年。

比特币有点儿像洋葱，你必须打开它。当你打开它时，你会发现另一层。

我五年前开始的。我还在打开它。对于比特币，我每天都会发现越来越多的让我惊讶的东西。

## 10.1发送者、接收者和账户的幻觉

**The Illusion of Senders, Receivers, and Accounts**

When I first encountered bitcoin, I was surprised to see that it looked like a relatively familiar banking system. I visited well-known bitcoin sites, like blockchain.info, and I could see transactions. I clicked on the transactions and I could see a sender, receiver, and account. I thought, This is pretty familiar. Banking. Great. Then, I decided to look at the source code and see how it worked.

当我第一次遇到比特币时，我惊讶地发现，它看起来像是一个比较熟悉的银行业务系统。

我参观了著名的比特币网站，例如blockchain.info，我可以看到交易。

我点击了交易，可以看到发送者、接收者和账户。我想，这很熟悉。银行业务。很好。

然后，我决定看一下源代码，看看它是如何工作的。

As a computer scientist, I figured I’d read the source code, and I’d try to understand how the system does these things. But when I searched the source code for sender, receiver or account, I didn’t find anything. Because none of those things actually exist in bitcoin. That really surprised me because when I looked at the source code, none of the things that I expected to find there were actually there. You’d expect that a banking system, as it appeared to be, had been designed to do certain things in a very specific way. Bitcoin isn’t like that. It’s not like that at all.

作为一名计算机科学家，我估摸我已经读了源代码，我试着去理解系统是如何做这些事情的。

但当我在源代码中搜索发送者、接收者或帐户时，我什么也没找到。

因为比特币中没有这些东西。这真的让我吃惊，因为当我看源代码时，没找到一样我期望的东西。

你期望的是一个银行业务系统，就像它看起来的那样，被设计为以非常特别的方式来做某些事情。

比特币不是这样，它根本不是那样的。

How many of you have looked into the source code or understand the technical underpinnings? A few people in this room. When you dig through the code, you find there is no balance, no sender, but there is UTXO unspent transaction outputs and there are inputs. But those inputs don’t really correspond to senders. And a transaction has outputs, which don’t really correspond to receivers. Suddenly, you realize what you’re looking at is almost this quantum or atomic nature of bitcoin.

你们中有多少人看了源代码，或了解了这个技术基础？这个房间里有几个人。

当你深入代码时，你发现没有余额，没有发送者，但是有UTXO（未花费交易输出），还有输入。

但这些输入并不真正对应发送者。一个交易有输出，它也并不真正对应接收者。

突然，你意识到，你看到的几乎是比特币的量子或原子性质。

## 10.2比特币的原子结构

**Bitcoin’s Atomic Structure**

In chemistry, we have elements like copper, iron, and helium. Chemistry gives you this enormous complexity of things that you can combine to make interesting things. Like people. And toasters. But when you dig into the chemistry, you realize copper isn’t a thing. Copper is a pattern of protons, neutrons, and electrons. There is no copper. One proton is the same as another proton; it can just as happily be part of helium or copper, it doesn’t care. There is nothing about that specific proton that makes it part of copper.

在化学中，我们有铜、铁、氦等元素。化学给了你这些复杂的东西，你可以把它们组合在一起，制造有趣的东西。例如人、烤面包机。

但是当你深入研究化学时，你会发现铜不是一个东西。铜是质子、中子和电子的一种模式。没有铜。

一个质子和另一个质子一样，它也可以是氦或铜的一部分，它并不关心。

没有什么特殊的质子使它成为铜的一部分。

Chemistry is one layer, but underneath that is atomic physics. That layer is very simple. It has a handful of elements. This handful of just a few elements makes up all of the chemistry we know, 100+ elements in nature that all have unique and different properties, that are completely different. Some of them are liquid, some of them are metals, some of them are gases. They behave differently. Some are acidic, some are not. But none of that is their basic makeup. These are just patterns.

化学是一层，但在下面是原子物理。那层很简单。它有一些元素。

这些元素构成了我们所知道的所有化学，自然界中有100多种元素，它们都有独特的性质，它们都是完全不同的。有些是液体，有些是金属，有些是气体。它们的行为不同。有些是酸性，有些不是酸性。但这些都不是它们的基本组成部分。这些只是模式。

Bitcoin has this fundamental atomic structure, this elemental structure. The elements of bitcoin are the components of transactions and the elements of the scripting language. Those elements have nothing to do with traditional banking. There are no accounts and balances and senders and receivers. Instead, bitcoin’s elements are looking for fundamental mathematical properties and cryptographic properties — such as whether a hash is equal to another hash, whether an elliptic curve signature matches another elliptic curve signature, manipulation of numbers, etc., etc. What you see on the surface — the transactions — are just constructs. They’re a specific way of mashing up the elements that creates something that kind of looks like a bank. Which is great because if you’re new to bitcoin and someone tells you, "Well, there is an account, a sender, and a receiver,” you think, Okay, I understand this.

比特币有这个基本的原子结构，这个基本结构。

比特币的元素是：交易的组件、脚本语言的元素。

这些元素与传统银行业务没有关系。没有账户、余额、发送人、接收人。

相反，比特币的元素在寻找基本的数学特性和加密特性，例如：一个哈希是否等于另一个哈希，一个椭圆曲线签名是否与另一个椭圆曲线签名匹配、数字的操作，等等。

你在表面（交易）上看到的知识构件。它们是一种特殊的方法，把这些元素混在一起，创造了与银行看起来类似的东西。

这非常棒，因为如果你是比特币新手，有人告诉你：“嗯，有一个账户，一个发送者，一个接收者，”

你想，OK，我明白了。

Then you learn that you have a wallet, but your wallet doesn’t have coins, it has keys, and those keys could be copied, and now you’re thinking, You’re losing me. This doesn’t quite match my experience. Things get complicated because bitcoin isn’t what you think it is. It’s a platform. It’s not a payment network. It’s not a currency. It’s not a banking system. It’s a platform that guarantees certain trust functions. If you happen to have a platform that guarantees certain trust functions, one very useful application for that is to build a currency and a payment network, but you can build more things.

然后你听说你有一个钱包，但是钱包里没有钱，它有钥匙，钥匙可以被复制的，现在你在想，byebye了。

这与你的经验不太相符。事情变复杂了，因为比特币不是你想象的那样。

它是一个平台，不是一个支付网络。它不是一种货币。它不是一个银行业务系统。

它是一个保证某些信任功能的平台。如果恰好有一个保证某些信任功能的平台，那么，一个非常有用的应用就是建立一个货币和一个支付网络，但你可以建造更多的东西。

### 10.2.1乐高的积木

**Building Blocks of Lego**

When I was a child, my favorite toy was Lego. The reason my favorite toy was Lego was not because of what was on the box. Because I did not build what was on the box. If the box had a red firetruck, I would build a dragon, or a hippopotamus-giraffe, something that didn’t exist or some strange idea that I had. That’s what I liked about it. I could take these basic building blocks, and I could build whatever I wanted.

当我还是个孩子的时候，我最喜欢的玩具是乐高。

不是因为盒子上有什么东西。因为我没有建造盒子上的东西。

如果盒子有一个红色的鳄鱼，我会建造龙、河马-长颈鹿，一种不存在的东西，或者我的奇怪想法。

这就是我喜欢它的原因。我可以用这些积木，建造任何我想要的东西。

From an abstract perspective, Lego is messy. And the thing I built didn’t quite look like a firetruck or a spaceship. If someone had given me a toy that was a firetruck, like a plastic-injected, smooth-edged, completed red firetruck, it would be the perfect firetruck. But it could only ever be a firetruck, and 20 minutes after I start playing with it, I am bored. Because my smooth, rounded firetruck that is only a firetruck, is a perfect firetruck. But it could never be a hippopotamus-giraffe or a tomato or a spaceship. But Lego allows more.

从抽象的角度来看，乐高是复杂的。我建造的东西看起来不像是一辆消防车或宇宙飞船。

如果有人给了我一个消防车玩具，塑料抛光，完成红色消防车。

这是一个完美的消防车，但它只能是一个消防车，20分钟后，我会感到无聊。

因为它只是一个消防车，是一个完美的消防车。它绝不可能是河马-长颈鹿、西红柿或太空船。

但乐高允许更多。

### 10.2.2烹饪的积木

**Building Blocks of Cooking**

As I grew older, I started getting into cooking as a hobby. What I loved about cooking is that it is the perfect combination of art and science. If you fundamentally understand how the ingredients work, how they behave, and how the chemistry changes when they’re combined or when you add a catalyst like salt or when you apply heat to them, then you can create. You can create almost anything. As long as you understand how the ingredients work, you can execute and deliver anything you want to create.

随着年龄的增长，我开始把烹饪作为一种业余爱好。

我喜欢烹饪是因为，它是艺术和科学的完美结合。

如果你从根本上了解这些成分是如何工作的，它们是如何表现的，当它们结合时，发生了什么化学变化，你几乎可以创造任何东西。只要你知道配料是如何工作的，你就可以执行和传递任何你想创造的东西。

### 10.2.3创造性的积木

**Building Blocks of Creativity**

Bitcoin encompasses that elemental nature. It doesn’t give you a final result. It gives you a set of ingredients and a recipe. It gives you a set of Lego blocks and a photo on the box that looks like a red firetruck. When we present that to the world, the financial companies look at that and say, “Well, your firetruck has sharp edges and it’s made of silly little blocks.” In bitcoin, we take the ingredients, we put them together and we’ve made a banking payment system. The banks look at it and it’s as if they’re saying to us, “Your burger is okay but at McDonald’s we can make it in 45 seconds and we can sell a billion of them. So, why do you need a chef, ingredients, a recipe, if you can just churn out a billion of them?" They’re missing the point.

比特币包含这种元素性质。它不会给你一个最终的结果。它给你一套配料和食谱。

它给你一套乐高块和一个盒子上的照片，看起来像一个红色萤火虫。

当我们向世界展示它时，金融公司看着这个说：“嗯，你的火鸡有锋利的边缘，它由愚蠢的小块组成的。”

在比特币中，我们把配料放在一起，我们造了一个银行支付系统。

银行看着它，就好像他们在对我们说：“你的汉堡还行，但是在麦当劳，我们可以在45秒内完成，我们可以卖十亿个。那么，如果你能生产出十亿个，为什么你需要一个厨师、配料、一个配方？”

他们没有抓住要点。

The point is not generating a billion copies of the same inferior product. The point is not getting the injection-molded plastic red truck that I am going to be bored of in 5 seconds. The point is unleashing my creativity by giving me the tools and the elements I need to build something unique.

要点不是生产十亿个相同的劣质产品。

要点不是得到我会在5秒钟内感到厌烦的注塑卡车。

要点是通过给我工具和元素来释放我的创造性，我用它们创造独特的东西。

I didn’t build a burger as fast or cheap as McDonald’s, and my little red firetruck isn’t as smooth as the molded copy. But I can make albondigas with red tomato sauce. I can also make a hippopotamus-giraffe. You can’t do that with a prefabricated toy. You can’t do that in your McDonald’s kitchen. I’ve unleashed my creativity.

我没有像麦当劳那样快速或便宜地制作汉堡，而我的小红色救火车也不像注塑玩具那样光滑。

但我可以用番茄酱制作墨西哥肉丸。我也可以做一只河马-长颈鹿。

你不能用预制玩具做到这一点。你不能在麦当劳的厨房里做到这一点。我释放了我的创造力。

### 10.2.4比特币的积木

**Building Blocks of Bitcoin**

We’re beginning to see people realize that bitcoin is a set of ingredients and you have one recipe, but you can make a different recipe. People are now trying to recombine these ingredients.

我们开始看到，人们意识到比特币是一套配料，你有一个配方，但你可以做出不同的配方。

人们现在正试图重新组合这些配料。

We’re building crowdfunding projects by combining atomic transactions and input-versus-output sums and digital signatures. By combining these ingredients, we can create a single transaction that can be funded by multiple people, but the transaction will only be valid if the threshold funding is met. Those are the same elements I use to make a payment of a dollar to you over bitcoin’s payment network, but you can recombine them differently and now you’ve got a crowdfunding platform.

我们可以构建众筹项目，方法是把原子交易、输入输出、数字签名结合在一起。

通过组合这些成分，我们可以创建一个交易，它由多人资助，但只有达到门槛资金时交易才有效。

这些与我通过比特币的支付网络向你支付一美元的元素相同，但你可以以不同的方式重新组合它们，现在你已经拥有了一个众筹平台。

We’re building payment channels by combining 2-of-2 signatures, multisignature, with transaction time locks. This allows us to charge for video-streaming by the second. That’s a whole new recipe.

我们可以构建支付通道，方法是把2-2签名、多签名和交易时间锁组合起来。

这允许我们按秒对视频流收费。这是一个全新的配方。

We’re building on top of payment channels. By taking them and adding a new ingredient, Hash Time Locked Contracts, we can connect multiple channels together. Then we’ve got Lightning Network, and that’s a new recipe that nobody has ever seen before.

我们可以在支付渠道之上构建。通过采用它们，增加新的成分，哈希时间锁合约，我们可以把多个通道连接在一起。然后我们得到了闪电网络，这是一个没有人见过的新配方。

The banks are saying, “Your truck has sharp corners and your burger is too expensive and took more than 45 seconds." What they’re really saying is, “Your transaction fees are too high and you’re too slow and you can’t possibly scale." They’re missing the point. The point is that we’re not trying to sell a billion burgers at 45 seconds each; we’re trying to unleash the creativity of an entire generation. We’re building a system, on top of which a thousand applications that require trust can be built.

银行说：“你的卡车拐角很锋利，你的汉堡太贵了，花了45多秒。”

他们真正说的是：“你的交易费太高了，你太慢了，你不可能扩展。”

他们没有抓住要点。要点是，我们不是试图每45秒钟的速度卖出十亿个汉堡；我们试图释放整整一代人的创造力。我们正在构建一个系统，在这个系统上，可以建立一千个需要信任的应用程序。

## 10.3焦点团体经济

**Focus-Group Economies**

When you have the ingredients, when you have these basic elements, what recipe you build is entirely up to you. Because when they build the little red firetruck, they create an entire factory that can only do little red firetrucks. I’m sure they’ll tell you, “Listen, our statistics say that 95 percent of children want a little red firetruck. We have tested this with focus groups and the marketing teams. We can produce them by the millions. They only cost 3 cents. They have a very small amount of lead paint and poisonous, toxic, carcinogenic hydrocarbons, not a problem. We can do that very cheaply and very profitably." And they can only build firetrucks.

当你有配料时，当你有这些基本元素时，你要做的配方完全由你决定。

因为当他们建造红色小消防车时，他们造了一个工厂，只做红色小消防车。

我相信他们会告诉你：“听着，我们的统计数据表明，95%的孩子想要一个红色小消防车。我们已经用焦点小组和营销团队测试了这一点。我们可以生产数以百万计的产品。它们的成本只有3美分。它们有非常少量的铅油漆和有毒、致癌的碳氢化合物，这不是问题。我们可以非常便宜和非常盈利的做到这一点。”然后，他们只能做消防车。

When you build a kitchen like McDonald’s, you can churn out burgers every 45 seconds, but you can’t make albondigas. You can’t make something else. You are streamlined to do one thing and one thing only, and as long as that serves your profit line, it’s okay. Because I am sure you focus-group tested it to make sure that is what everybody wanted.

当你建造一个像麦当劳一样的厨房时，你可以每45秒做出一个汉堡，但你不能做墨西哥肉丸。

你不能做别的东西。你只能流水线地做一件事，只要它服务于你的利润线，就行。因为我相信你的焦点小组测试过它，以确保这是每个人都想要的。

That is a terrible way to build an economy. That’s a terrible way to build a financial system. That’s a terrible way to build a payment network.

这是建立一种经济的糟糕方式。

这是建立一种金融体系的糟糕方法。

这是建立一种支付网络的糟糕方式。

## 10.4银行特权与监管

**Banking Privilege and Surveillance**

Effectively, what the banks are saying to us is, "We focus tested this. What people want is the ability, instead of swiping their Visa card, to wave it over the reader, saving almost two seconds and reducing their effort by at least four calories. I mean, we could deal with the 4 billion people who have no access to banking or clean water. We could deal with the fact that our world is a fragmented mess, where the vast majority of humanity have no access to financial services. Or, we could reduce the shopper’s effort and make a swipe card into a float card.

实际上，银行对我们说的是：“我们集中测试了这一点。人们想要的不是刷卡，而是在读卡器上挥动一下，节省了近两秒钟，减少他们至少四卡路里的运动。”

我的意思是，我们可以处理40亿人，他们没有银行或干净的水。我们可以处理这样一个事实，我们的世界支离破碎、混乱不堪，大多数人无法获得金融服务。或者，我们可以减少购物者的努力，把刷卡变成浮卡。

We could face the fact that the reason more than 4 billion people are unbanked is because we require everyone to be identified on every side of every transaction, so that we can build a totalitarian surveillance system that the Stasi would be jealous of, to monitor every financial transaction from every corner of the planet. Because we have persuaded ourselves that our bourgeois sense of security will be protected, not by solving poverty, and not by reducing, perhaps, the bombing of other countries, but instead, by watching everyone all the time when they buy a burger—just in case.

我们可能面对这样一个事实，超过40亿人没有存款，是因为我们要求每个交易的人都能被识别出来，这样我们就可以建立一个极权的监管系统，来监控地球的每个角落的每一笔金融交易。

因为我们已经说服自己，我们的资产阶级的安全感将得到保护，不是通过解决贫困，不是减少对其它国家的轰炸，而是通过随时监视每个人，当他们买汉堡包时，以防万一。

We subject ourselves to this mechanism that has now streamlined itself, and like the factory that can only produce little red firetrucks, this is a system that can only deliver privileged financial services for a tiny elite sliver of the population worldwide, with totalitarian surveillance tied up in regulations of each country, with barriers on the borders not permitting international trade. A financial system where the government can apply pressure to stop you trading with WikiLeaks, because they don’t like them, but you can still send donations to the Ku Klux Klan—and that’s not a joke. That’s exactly what happened.

我们正致力于这一机制，现在这种机制已经流水作业了，就像工厂只能生产红色小消防车一样，这是一个系统，它只能为全世界人口中的一小部分精英提供特权的金融服务。

在各国的规章制度中，边界上的壁垒不允许国际贸易。一个政府可以施压的金融系统会阻止你与维基解密进行交易，因为他们不喜欢维基解密，但你仍然可以向Ku Klux Klan（三K 党，美国南部的白人秘密组织，利用暴力反对社会变革和黑人的平等权利）发送捐款，这可不是开玩笑。这就是事情的真相。

They have built a system that can only do one thing: enslave us. That can only do one thing: impoverish us. That system removes freedom in the most efficient possible way to deliver profits. That system is broken, and it doesn’t scale. But if that is what you’re trying to do, it’s the most efficient you’ve ever seen.

他们建立了一个只能做一件事的系统：奴役我们。

它只能做一件事：使我们贫穷。

该系统以最有效的方式来剥夺自由，以实现利润。

那个系统坏了，而且它不能扩展。

但如果这就是你想要做的，它是你所见过的最有效率的。

By comparison, the crazy little mishmash system that we’ve built with bitcoin, that’s wrong and it’s slow and it can’t scale. It’s inefficient and it’s not as serious and sophisticated as the international banking system. But it delivers freedom and it allows us to unleash creativity.

相比之下，我们用比特币建立的这个疯狂的小杂烩系统，它错误的，它很慢，而且不能扩展。

它效率不高，不像国际银行系统那样严肃和复杂。

但它提供了自由，允许我们释放创造力。

Thank you.