2008年10月31日，一个自称是中本聪的人在一个密码学讨论组上发布了白皮书，阐述了他的电子货币新想法，——个比特币问世了。。这个密码学讨论组见证了大量的创新提议，包括大卫乔姆&#039；s数字现金。但当人们看到比特币这个全新的概念时，依然是眼前一亮。

作为这个密码学讨论组的操作者，PerryMetzger见证了比特币从概念到现实的过程。梅茨格是一位经验丰富的计算机安全专家，精通密码学和其他相关领域。他说早在中本聪发布比特币白皮书之前，这个讨论组就经常讨论数字货币、隐私技术、密码学和系统安全等话题。也许正是理解了这个群体对数字货币的狂热，中本聪选择在这里发表作品。。谁是中本聪？当我第一次看到比特币白皮书时，梅茨格并没有&#039；我不认为它会取得巨大成功，甚至认为这个机制存在漏洞。事实上，这个通过密码学把世界各地的人聚集在一起的讨论组是被审查的。。梅茨格表示，他不得不审查帖子的内容，因为他担心成员情绪过于激动，进行了一些极端的讨论。当时有很多关于比特币的讨论，有很多重复。梅茨格一度阻止相关讨论继续进行。。那么既然见证了比特币的诞生，梅茨格有没有可能知道这个神秘人物的真实身份呢？梅茨格说，当时这个讨论组的大多数人都是匿名的，因为隐私技术也是他们关注的焦点。。他怀疑中本聪在这里使用了许多不同的绰号。至于中本聪是谁，他说，只要ta愿意，ta自然会用私钥证明自己的身份(比特币诞生初期，中本聪挖出了100万个比特币)。此外，他认为只要一项创新就足以改变世界，那么它的创造者的身份并不重要，除非他们之间有某种不可分割的利益关系。02PoW&#039在密码学家眼中，数字货币并不是一个全新的概念。Chaum&#039的Digicash甚至被马克吐温银行使用。。那么比特币为什么能吸引他们的注意力呢？在梅茨格&#039；在美国看来，比特币的成功在于其去中心化的本质。帮助比特币实现这一特性的是PoW机制。很多数字货币概念缺乏，一直在寻找这样的机制。。梅茨格说，比特币的账本就是拜占庭共识。PoW是实现去中心化的天才设计，通过去中心化的拜占庭共识帮助陌生人进行可信的交流。当时人们认为这是一个近乎完美的方案。。03比特币的三大问题虽然有近乎完美的解决方案，但梅茨格认为比特币仍然存在缺陷。首先，比特币的交易费用太高，无法用于支付。梅茨格说，维护PoW机制需要大量的

电力成本。这种设计可以使网络更加安全，可以抵御攻击。但比特币的交易确认时间较长，手续费相对于传统金融机构仍然较高，不适合支付。此外，梅茨格认为，权力在一定程度上确保了分权和安全。，但是成本太高。相比之下，PoS在扩展性上会表现得更好，如果使用得当，还可以创建一个分布式、去中心化的网络。其次，比特币缺乏匿名性。比特币账本是一个完全开放的网络，交易可以自由查询。。但是，在某些情况下，如一些企业的商业交易，如果需要匿名，就比较困难。梅茨格认为，这也是比特币需要解决的问题。最后，比特币缺乏治理机制。他认为加密货币社区存在一些差异。但是技术问题应该用治理机制来解决，而不是一味的吵架。去中心化的理想比特币诞生至今已有10年，从最初无人问津的时候收获了大量热情的支持者。尤其是在一些经济动荡的地区，比如委内瑞拉。比特币已经成为人们生存的工具，成为人们获取食物和其他必需品的唯一途径。梅茨格承认，比特币确实是一个非常实用的工具，但对于大多数人来说，比特币仍然不是生活中不可替代的一部分。仍然没有智能手机普及。或许在未来，比特币会成为真正的全球货币，或许会出现更好的加密货币。30年后我们还会记得比特币吗？梅茨格说它&#039；现在谈论它还为时过早。但至少我们知道比特币是一种创新技术。梅茨格认为自己懂得很多，但比特币的出现教会了他更多。他不&#039；我不想预测这项技术最终会是什么，因为在他看来，最重要的不是技术，而是人们追求去中心化货币的理想。