加密货币玩法这个概念很早就在学术界发生了，但很多人对它的想法却不太了解。

”加密货币”是一种使用密码学原理来确保交易安全及控制交易单位创造的交易媒介，是一种数字货币(或称虚拟货币)的形式。

1：如今，加密货币已经发展到一种不同的应用场景，例如，利用区块链技术的去中心化特性来对资产进行确认、追踪及所有权转移等。但这个理念却是完全颠覆了大多数”加密货币”的想法，因为传统的金融世界早已崩溃，而加密货币之所以如此重要的一个原因就是为了对抗货币滥发的现象，为了应对金融危机，经济遭受了严重的破坏。

2：”加密货币”是一种由密码学原理确保的电子现金系统，具有强大的抗审查性，且被”匿名”(non-custodialize)，安全性较高，其唯一的产生方式是使用加密算法，加密的结果则是加密的结果将具有较强的隐私性，并且能够追踪特定地址的所有交易行为。更高效的加密货币交易还可用于提高匿名性，因为加密货币的交易需要经过交易各方，如交易者或其他成员的同意才能确认，交易各方能够追踪货币的来源，并追溯资金来源的来源。

1：Monero，Zcash，Dash的匿名币各有优缺点，但基本思路就是用匿名交易来混淆币的发送者和接收者。从不同角度看，隐私币使用的匿名技术有如下几个要点:隐私技术可以被用于让用户隐藏交易的去向，匿名交易的发送者以及交易金额等信息。

2：通过匿名交易，用户只需要持有相关代币的私钥，即可对交易的接收者和使用者进行地址的关联。交易信息和交易记录都是对用户公开的，只有发送者和接收者是匿名的。

3：私人交易也是为了保护用户隐私。私人交易是指使用数字货币进行的非法交易。

4：一般来说，从私人交易的角度看，比特币通过广播、验证区块的合法性来保障交易的安全，而Zcash则通过混合区块链和链下交易来保护交易的隐私。关于门罗币，您能告诉我们一些关于门罗币的知识吗?门罗币使用环形签名来进行交易，而Zcash使用了经典的加密算法。

5：Zcash 使用的环形签名算法(RingCT)是一种零知识证明协议，可以将交易从一方发送到另一方。交易仅包含一个交易有效，而不包含一个已验证交易(RingCT)。