**4.量子区块链**

**Quantum-Fintech——冯艺涵**

# **一、背景：**

区块链是随着数字加密货币而逐渐兴起的一种全新的去中心化基础架构。以区块链为底层技术的应用范畴早已超越数字加密货币，延伸到了金融、经济、科技和政治等各个领域。与此同时，具有重大科学意义和战略价值的量子科技正在迅速发展，在即将到来的量子时代，区块链将面临量子科技带来的前所未有的机遇和挑战。主要体现为：一是强大的量子计算对区块链密码体系造成极大威胁，二是在区块链中应用量子科技能有效提高系统的安全性。

“区块链+量子计算”的交叉融合研究具有重大的现实意义，量子区块链必将成为未来高新技术产业的研究热点。

# 二、机遇：

## 1、量子通信

### a.技术背景：

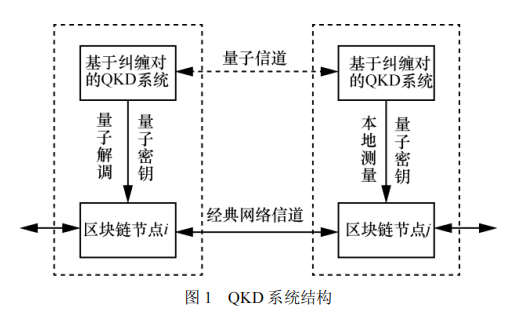
当前的量子通信技术主要分为量子密钥分发(quantum key distribution, QKD) 和量子隐形传态(quantum teleportation, QT) 两类。QKD 确保发送的信息只有使用量子密钥解密之后才能阅读信息，QT 保证了密钥共享与信息传输的安全性，且能防窃听，为区块链可信环境的进一步构建提供了一种可行的思路。

量子纠缠是量子力学中一个经典的现象，它指的是量子粒子之间相互作用后，各个粒子的特性不再是独立的，而是具有相互参照的整体性质。因此，2 个处于纠缠态的量子不管分开多远，在不存在任何信息交互的情况下，通过测量其中一个粒子的状态就可以知道另一个粒子在同一时刻的状态。量子通信是利用量子纠缠效应进行信息传递的一种新型通信方式，它主要涉及量子密码通信、量子远程传态和量子密集编码等，近年来逐渐从理论走向实验以及实用化发展。

量子通信过程中如果出现任何攻击拦截行为，都会导致信息传递载体——量子态发生变化，通信双方能轻易发现攻击行为，从而终止通信。这样一来，任何攻击方式都无法得到量子态上所传递的原有信息，信息泄露等问题不会发生。“一次一密”(one-time pad, OTP)加密技术已被证明能够保障通信过程中信息的绝对安全。

### ****b.量子通信在区块链中的应用：****

针对区块链面临的加密方式安全性问题，QKD和 QT 是可以应用在区块链中的重要技术。考虑到量子通信技术的特点，利用 QKD 进行信息加密/解密的密钥分发，利用 QT 进行对称密钥的共享，即使攻击者拥有量子计算机，也无法破解或者窃听通信双方的密钥和内容，其QKD系统结构如下图所示：



以密码学的经典例子进行说明：在传统的区块链中，当 Alice 需要在区块链网络中向 Bob 发送数据时，Alice 通过非对称加密对信息进行加密，使用了自己的私钥和 Bob 的公钥，Bob 利用 Alice 的公钥和自己的私钥进行解密，从而获取了 Alice 发送过来的数据。这是典型的非对称加密方式，能在传统网络环境下保证通信的安全，然而其加密原理可以被量子计算攻破，这也是其缺陷所在。然而，在基于量子通信的区块链中，当 Alice 需要在区块链网络中向 Bob 发送数据时，Alice 随机选择纠缠量子对，在量子信道中发送随机选择的纠缠量子对代号给 Bob，然后利用量子解调形成对称加密密钥，并在经典信道中发布已加密的密文。与此同时，Bob在本地观测与 Alice 对应的纠缠量子态，利用量子解调生成对应的对称加密密钥，并对 Alice 发起的数据分组进行解密从而获取数据。值得注意的是，即使攻击者在经典信道中窃听且得到了已加密的密文，他仍然无法获取与密文对应的对称密钥，原因主要有 2 个：一是攻击者无法得知纠缠量子对的量子态，从而无法获得密钥；二是攻击者在量子信道中窃听，会引起量子态的改变，被窃听的量子偏振态对应的将是无意义的信息，同时也会被发送双方察觉。这一原理已经被众多科学家所验证，因此，基于量子通信的区块链可以克服传统区块链的缺陷，以应对量子霸权带来的巨大威胁。

## 2、量子拜占庭共识算法

量子通信技术结合量子计算可以无条件安全分发秘密数字列表，实现可检测的拜占庭共识协议；

详见本人对应的文章。

## 3、量子数字签名

量子数字签名的应用主要分为密钥分发阶段和签名验证阶段。各节点间密钥分发阶段的安全性由量子密钥传输保障，签名验证阶段需要结合量子特性和具体协议完成设计；

详见本人对应的文章。

## 4、量子随机数

量子不可测量原理能够实现具有不可预测性、不可重复性和无偏性等特征的无条件安全的量子随机数；

详见本人对应的文章。

## 5、量子区块链

目前已有不少学者尝试探索研究独立完整的量子区块链系统，但均有较大的局限性；

## 6、量子货币

### a.发展背景：

20 世纪 60 年代末，哥伦比亚大学的年轻学者 Wiesner首先想到把量子力学特性应用到防伪和版权保护需求中，首先提出了量子货币的概念，但其成果直到 1983 年才得到认可和发表，如今这篇论文也被视为量子密码学的起源。

1982 年，美国物理学家 William Wootters 等人基于 Heisenberg“测不准原理”推论出量子不可克隆定理，为创造一种直接接受物理定律保护的防伪标识提供了方案。

2012年，Lutomirski等人利用扭结不变量的方法提出了一个真正意义上的量子货币公钥方案。

2015年，Subhayan等人提出量子支票协议，该协议中可信银行的任何一个合法客户端都持有一个“量子支票书”，可以发行支票，并与银行之间共享一个经典信道，由银行或它的分支机构完成货币验证。

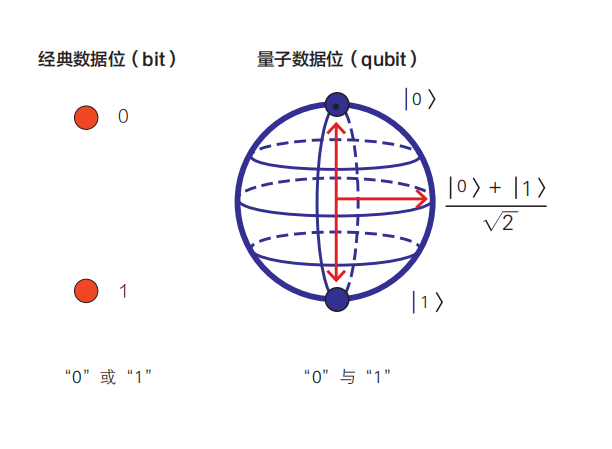
2016 年 4 月，瑞典林学平大学的 Jogenfors把量子力学基本原理与比特币设计思想结合提出了第一个去中心化的分布式量子货币系统——量子比特币方案。

### b.技术背景：

**量子比特：**

在经典计算机中，比特“0”和“1”都是用经典物理量编码表示的，例如可以用电压、磁场方向等，而经典物理量测量结果是唯一确定的，即一个经典比特不可能同时处于两个状态（比如同时处于“高电压”和“低电压”状态）。而量子比特是基于微观粒子的量子态存储的，其不同于经典物理状态的最重要的特点在于可以同时处于若干个微观量子态的叠加态。例如用|0>表示一个电子的基态或自旋向下，用|1>表示激发态或自旋向上，则一个微观量子态可以表示成| >=a|0>+b|0>，其中a，b都是复数，且它们的模长平方和为1。图1显示了经典数据位与量子数据位对比图，经典数据位的表示要么是0，要么是1，而量子数据位是│0>和│1>的叠加态，即可以是0也可以是1。

经典比特与量子比特的对比如下图：



**量子不可克隆定理：**

量子不可克隆定理最早是由 Wootters 和Zurek 于 1982 年提出的，它的内容是：一个未知量子态不能被完全克隆。该定理指出，任何物理手段都不可能精确地复制未知量子态，否则将会违背量子态叠加原理。它也可以看作是测不准原理的一个推论。

### c.量子货币优势：

**防伪造、防双花：**

货币发展史是防伪技术的发展史，也是生产者与伪造者不断斗争的历史。

传统货币伪造屡禁不止的一个根本原因是经典物理的易伪造特征。按照经典物理的基本原理，物理状态都可以被精确测量，只要能按照测量结果，以足够应对检验的精度重新组织物质，就可以达到伪造货币的目的。虽然说可以让伪造的成本足够高以至于伪造货币无利可图，从而避免伪造，但随着技术的不断发展以及高精尖技术向民用领域的广泛应用，伪造的技术门槛亦可能下降。若伪造者投入足够物力、财力和智力，任何传统货币防伪技术在理论上都有可能被破解。

对于电子货币和数字货币而言，其形式上就是一串二进制的信息，在计算机里更容易被复制。现在一般利用密码学技术来防止伪造。对于双花问题，解决的方案是采用一个账本的形式来记录已经发生的交易，以此避免同一笔数字货币被多次花费。这个账本既可以是像传统银行一样的中心化账本，也可以是像比特币一样的基于区块链技术的分布式账本。量子货币则采用不引入记账机制的第三种方案：通过量子不可克隆原理来解决货币的伪造和双花问题。

对于量子货币，人们希望用理论上无法复制未知量子态的特点彻底杜绝伪造量子货币的可能性。

进一步来说，由于量子货币通过叠加态的量子比特形式实现信息存储，其能够保存远比经典比特更丰富的信息，并且这些信息无法被精确测量。由于量子一旦被观测就会坍塌，而观测量子货币中的内容是复制量子货币的前提，因此从根本上杜绝了他人获取货币全部特征从而伪造货币。经过观测坍缩之后，量子货币便已销毁，无法继续使用。

**点对点支付：**

相对于传统货币，数字货币的最大优点就是在于传输方便，仅需要通过网络传输信息，而不需像传统货币那样传递实物。量子货币也一样，只需要传递量子态所包含的信息即可。传递的量子态信息既可以通过发送包含这些信息的粒子（比如光子）实现，也可以通过量子通信在经典信道实现——即通信双方事先分享一个纠缠的量子态，然后仅通过经典信道传输经典的二进制信息就可以实现传递复杂的量子态的任务。

因此，基于量子货币的交易可以在交易方之间直接进行（至多只需要一个可信的第三方事先分发纠缠的量子态），不需要通过第三方账本验证。

### d.量子货币缺陷：

**验钞困难**

### e.量子货币的具体应用：

#### (1)、量子钞票

#### (2)、量子硬币

#### (3)、量子支票

#### (4)、量子比特币

## 7、量子金融

为了更好地对金融市场进行模拟，近年来量子场论方法被逐步引入到金融研究之中。量子金融市场模型可对金融市场的传统理论模型进行有益改进。