量子コンピューターが仮想通貨に与える影響

原文:
https://www.btcc.com/ja-JP/academy/research-analysis/quantum-computer

「量子コンピューターが仮想通貨に与える影響は何ですか？」という疑問を持っている方は多くいるかと思います。そこで本記事では、量子コンピューターがビットコインに与える影響をわかりやすく説明します。

目次

1. 量子コンピューターとは？

量子コンピューターとはその名の通り、量子力学の原理により並列性を実現するコンピューターです。従来のコンピューターは、0と1の2つの状態で情報を表現します。電圧のオン・オフで、0か1のいずれかの状態に1ビットは定まります。これの膨大な繰り返しで、Youtubeで動画が観られたり美しい写真を保存できたりするのです。

このビットに代わり、量子ビットで情報を処理するのが量子コンピューターです。従来のビットと異なり、この量子ビットは0と1が同時に成立している状態(重ね合わせの原理)も考えることができます。0の状態と1の状態が決定的ではなく、確率的に決まっているということです。

この原理の画期的な応用により、1度で扱える情報量が増えます。コンピューターで取り扱う量子ビットの数がn個のとき、1度で処理できる情報量が2のn乗となります。2量子ビットなら4つのデータが取り扱えるということです。

量子コンピューターの台頭で、現在一般的に使われているRSA暗号や楕円曲線暗号などの現代暗号理論が安全ではなくなる(危殆化していく)ことが問題視されています。

2. 量子コンピューターが与えるビットコインへの影響

従来のコンピューターとはそもそもの構造が大きく異なる量子コンピューターですが、仮想通貨の脅威になることが予想されます。**ショアのアルゴリズムとグローバーのアルゴリズムによってビットコイン**

の安全性が脅かされている状況です。

ビットコインを保有している方ならばご自身の秘密鍵をお持ちでしょう。誰にも公開してはいけない、自分だけが知っているべきランダムな数字とアルファベットの羅列です。公開鍵は名前の通り公開して良い鍵です。なぜなら、現在ではその公開鍵からいくら頑張っても秘密鍵を知るすべがないからです。公開鍵はこの秘密鍵から生成されるので、ビットコイン取引の安全性は公開鍵から秘密鍵を割り出されないことを根拠としています。

ビットコインプロトコルで秘密鍵から公開鍵を生成する暗号技術が、上記で触れた楕円曲線暗号です。画像にもあるように、秘密鍵から公開鍵を生成できても、公開鍵から秘密鍵を割り出すことはできないようになっています。しかしこれは従来のコンピューターでの話であり、**量子コンピューターと量子アルゴリズムを使えば解けてしまう時代がいずれ来ることが理論上わかっています**。

理論上、ショアのアルゴリズムによって、離散対数問題と素因数分解が高速で解けるようになります。現在最も普及しているRSA暗号と楕円曲線暗号は、それぞれ素因数分解と離散対数問題の計算困難性に支えらています。実際、現在使われている2048ビットの大きさの数を素因数分解するには、スーパーコンピューターで30年ほどかかると言われています。**これほど強固な暗号理論を量子コンピューターは破る可能性があるのです。**

また、扱うデータ量が増えてもさほど計算量が変わらないところもショアのアルゴリズムが突出している点です。ですから、扱うデータ量を増やすという対処法が通用しません。これによりRSA暗号と楕円曲線暗号が危殆化を迎え、耐量子計算暗号へと移行しなければいけなくなります。これは、ビットコインを保有する上でも重大な事実となります。楕円曲線暗号が破られるということは、公開鍵から秘密鍵が割り出されてしまうことを意味するからです。**本来なら公開できるはずの公開鍵から誰にも教えてはならない秘密鍵がバレてしまい、保有するビットコインがウォレットから盗まれるなどの被害も考えられます。**

3．今後の予想・展望

ブロックチェーンのシステム上、ビットコインのプロトコルや規格に対して変更を加えることは難しいです。その場合、楕円曲線暗号ではなく(格子暗号や多変数多項式暗号などの)耐量子計算機暗号をプロトコルとして備え、かつSHA-384と今よりも桁数が長いハッシュ関数を採用しているシステムがビットコインからハードフォークするか、全く新しいコインが作られるかの2通りが考えられます。

既存のコインの中には、Cardano、IOTA、NEOなど耐量子性を持ったものが存在します。ただし、これからより一層量子コンピューターの理論・実証双方からの研究が盛んに行われることも予想されます。

これからの研究により、新たに効率的なアルゴリズムが開発されたり、量子コンピューターでしかなせない計算手法が編み出されたりすれば、今存在する耐量子仮想通貨の安全性が脅かされる可能性も十分にあるでしょう。