2026 年 5 月 28 日　全 5 頁

量子コンピューターは暗号資産の前提を壊すのか？

デジタルソリューション研究開発部 シニアセキュリティ・スペシャリスト　　山崎 禎章

1. はじめに

ビットコインやイーサリアムなどの暗号資産は、分散型台帳技術によって支えられていると説明されることが多い。しかし、その安全性は分散型台帳に記録される取引が正当なものであると検証できることによって成立している。

具体的には、取引の正当性は「電子署名」によって確立されている。これは公開鍵暗号方式に基づいており、秘密鍵で署名された取引データを、ネットワークの参加者が秘密鍵に対応する公開鍵で検証する。この検証により、取引データの作成者が秘密鍵を保有していることを証明できる。この仕組みは、「公開鍵から秘密鍵を現実的に導出することは不可能である」という前提の上に成り立っている。

この前提に影響を及ぼしうる技術として、量子コンピューターの進展が注目されている。本稿では、電子署名と量子コンピューターの関係に注目し、暗号資産が直面しうるリスクと今後の課題を整理する。

2. 本稿で取り上げる視点

量子コンピューターについて、「いつ実用化するのか」という問いがしばしば議論される。しかし現時点では、量子コンピューターがいつ実現するかについて、明確な時期を断定することは困難である。

量子コンピューターが「いつ実現するか」も重要であるが、「実現した場合にどのような影響が生じるか」という点も重要である。

本稿では特に、暗号資産の基盤となる電子署名に焦点を当て、以下の観点について整理する。

- 量子コンピューター出現による電子署名への影響
- 暗号資産に対する攻撃パターン
- 対応策としての耐量子計算機暗号（PQC）とその課題

3. 量子コンピューター出現による電子署名への影響

現在広く利用されている公開鍵暗号は計算量的安全性に基づいているが、この安全性は量子コンピューターの出現によって揺らぐ可能性がある。

具体的には、量子コンピューターで使用できる Shor のアルゴリズムと呼ばれる量子アルゴリズムにより、RSA 暗号や楕円曲線暗号といった公開鍵暗号の基盤となる数学的問題が効率的に解けることが知られている。公開鍵暗号に基づく電子署名についても同様に影響を受けることとなる。

そのため、電子署名の正当性が脅かされることで、送金の正当性が保証されなくなり、資金が乗っ取られてしまうなどのリスクにつながる可能性がある。

量子コンピューターは現実的な脅威として意識され始めている。Google の量子コンピューターの研究部門である Google Quantum AI は 2026 年 3 月 30 日、「Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations」という論文を公開し、ビットコインやイーサリアムで広く使われる暗号（楕円曲線暗号：secp256k1）が、従来考えられていたよりも少ない計算資源の量子コンピューターで解読される可能性があることを示唆した。

具体的には、特定の条件下において 50 万未満の物理量子ビットで、超伝導方式の量子コンピューター上における数分規模の実行が理論上可能であることが示されている。これは、従来の研究から 20 分の 1 程度となる試算であり、将来的な解読の可能性を十分示唆するものである。

ただし、これらの試算は量子誤り訂正を含む理想的な条件を前提としたものであり、実際の量子コンピューターの実現時期や到達可能性については依然として不確実性がある点には注意が必要である。

4. 暗号資産に対して想定される攻撃パターン

量子コンピューターの影響として、主に二つの攻撃パターンが考えられる。

① on-spend attack

取引をネットワークに送信してから台帳に記録されるまでの短時間を狙う攻撃である。取引をネットワークに送信すると公開鍵が露出する。露出した公開鍵から量子コンピューターを用いて秘密鍵を導出し、正規の取引よりも先に不正送金を成立させることで送金を乗っ取る。

論文によれば、この処理には約 18〜23 分、事前計算を活用すれば約 9〜12 分まで短縮可能とされている。ビットコインの平均ブロック生成時間は約 10 分であるため、攻撃が可能となる。

② at-rest attack

以前から公開鍵が露出している資産、特に長期間動いていない休眠資産を標的とする攻撃である。時間制約が緩いため、量子コンピューターが実用化された場合には現

実的な脅威となりうる。公開鍵が露出したままの休眠資産は推定で 230 万 BTC 存在する可能性があると指摘されている。これは、ビットコイン価格を仮に 1BTC＝1,000 万円と置いた場合、23 兆円に相当する。

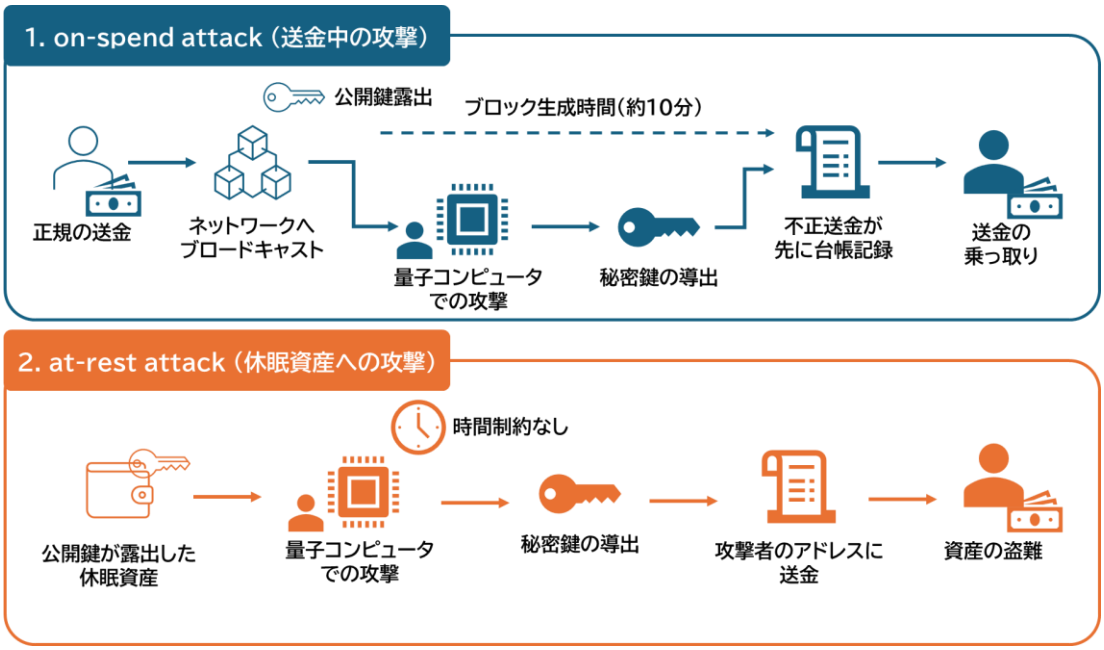

図 1 量子コンピューターの二つの攻撃パターン（大和総研作成）

5. 対応策として考えられる耐量子計算機暗号（PQC）とその課題

これらの脅威への対処としては、量子コンピューターによる攻撃にも耐えることを目指した暗号方式である耐量子計算機暗号（Post-Quantum Cryptography、以下 PQC）への移行が考えられている。

ただし、PQC 移行は過去のブロックチェーン記録を作り直すことではない。これから使う署名方式や鍵管理を、量子コンピューターでも破られにくい方式へ切り替えることが中心となる。

したがって、耐量子計算機暗号が導入されても、以前から公開鍵が露出している資産については、既に公開された鍵の情報自体が変わるわけではないため、そのリスクが自動的に消えるわけではない。こうした資産は、新しい量子耐性アドレスへ移し替える必要がある。

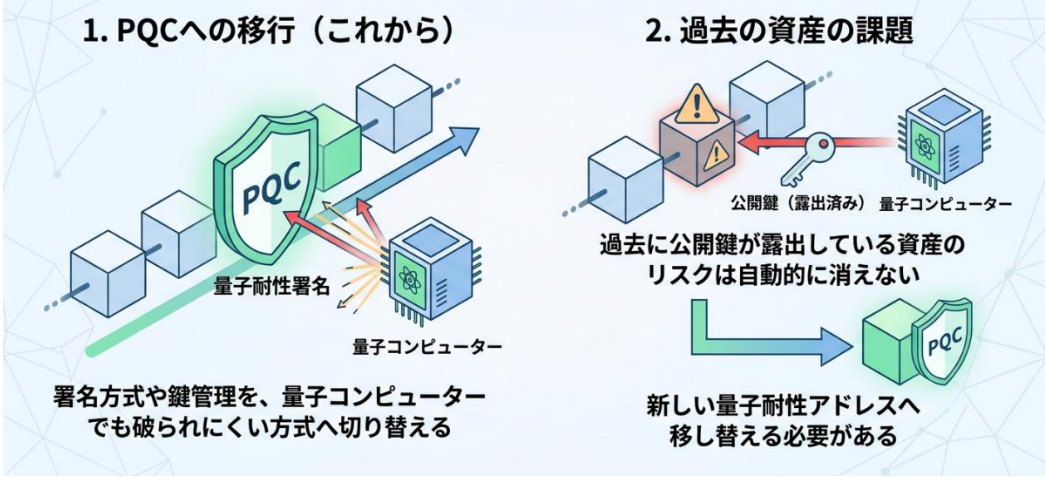

図 2 PQC 移行の課題(過去の資産)
（大和総研により Gemini 3.1 Flash Image を使用して作成）

加えて、PQC への移行には性能と分散性の面で課題もある。ブロックチェーンでは、取引を台帳に記録させる前にネットワーク全体へブロードキャストする必要があり、現行でも一定の通信負荷がかかる。

PQC では、従来の暗号方式と比べて鍵や署名のサイズが大きくなることが知られている。論文によれば、Algorand というブロックチェーンでは、米国の NIST が選定した耐量子計算機暗号の一つである Falcon が既に利用されている。Falcon の署名サイズは、現在ビットコインで用いられている ECDSA と比較して約 20 倍に及ぶ。ブロックチェーンでは取引ごとに署名が付与されるため、署名サイズの増大は通信量や台帳サイズの大幅な増加に直結する。

通信量や台帳サイズの増加は、個人や有志によるフルノード運用の負担を高め、十分な資源を持つ一部のノードしか完全な台帳保持ができない要因になりうる。分散型を志向するブロックチェーンにとって、これは量子耐性とは別の、無視できない課題といえる。

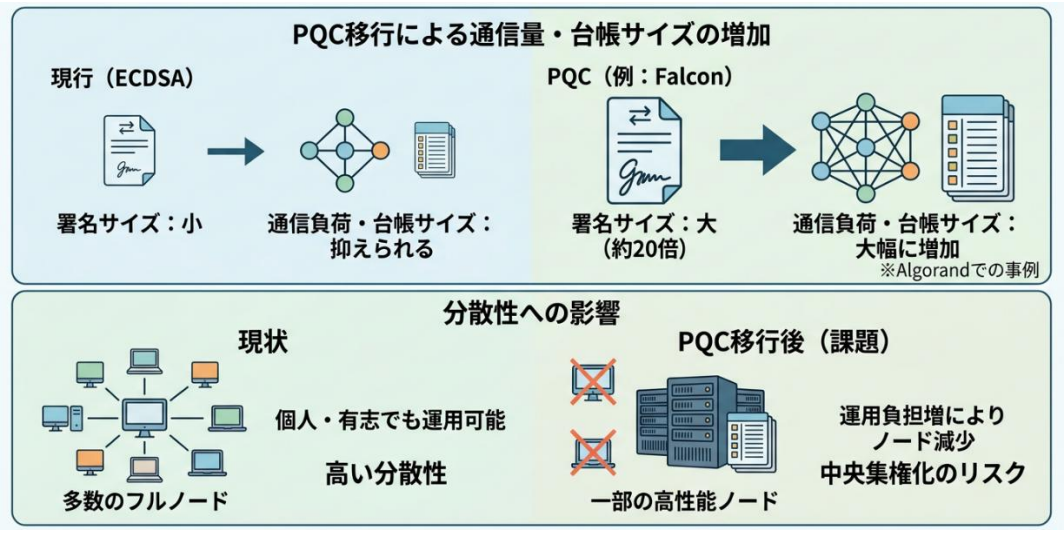

図 3 PQC 移行の課題(サイズの増加)
（大和総研により Gemini 3.1 Flash Image を使用して作成）

さらに、PQC 移行による通信量や台帳サイズの増加はそのブロックチェーンの設計自体にも影響を及ぼす可能性がある。ビットコインのようにブロックに収められるデータ量に制約がある仕組みでは、1件あたりの取引サイズが大きくなることで、同じブロックに収められる取引数が減少する。その結果、利用者が負担する手数料にも影響が及ぶ可能性がある。イーサリアムでも、署名検証やデータ保持にかかるコストは最終的にガス代（ブロックチェーン上で取引する際に発生するコスト）へ反映されうるため、同様の負担増が生じる可能性がある。

また、こうした変更はネットワーク参加者の利害にも影響を及ぼす可能性がある。ブロックチェーンではプロトコル変更に際してコミュニティ全体の合意が必要となるため、技術面だけでなく、合意形成の難しさも課題となりうる。

6. おわりに

量子コンピューターの実用化時期は依然として不確実である。しかし、量子コンピューターに関する研究は着実に前進しており、「まだ先の話」として扱うことは難しくなりつつある。一方で、PQC への移行には技術だけでなく、コミュニティの合意形成やシステム対応、ユーザー移行など、多くの時間と労力が必要となる。

量子コンピューターの進展は、暗号資産に対し「安全性」と「分散性」をどう両立するかという、ブロックチェーンの本質的な設計課題を改めて問い直しているともいえるのではないだろうか。