(H) Aidos Kuneen White Paper

日本語訳

※この版は、概要、第１章、第２章を翻訳したものです。

本書は公式のWhite Paperではありません。

運営の許可を得てslackの有志チームが、その一部を翻訳したものになります。

正式なホワイトペーパー全文は、公式発表をお待ちください。

v.1.2

Agenda (目次)

Abstract (概要)

本書は、仮想通貨「Aidos Kuneen（ADK）」について説明するものです。Aidos Kuneenは、量子コンピュータ時代にふさわしく、ブロックレスで匿名性に優れており、分散処理とスケーラビリティを一切の手数料なしに実現した仮想通貨です。

このコインでは、トランザクションが互いに参照しあい、DAG（Directed Acyclic Graph）構造を形成する「iMesh」を採用しています。悪意のある二重支払いを防ぐためにDAG構造を調べ、どの取引が高い確率で正規のものであるかを「SPECTRE」に基づき判断します。署名には、数ある耐量子コンピュータのアルゴリズムのなかで最も実用的で、署名サイズと公開鍵サイズが比較的小さいハッシュベースの署名「XMSS」を採用しています。耐量子コンピュータのためのゼロ知識証明「ZKBoo（ZKB ++）」も備え、AKShuffleと呼ばれる匿名転送にも利用されます。IoT機器への対応については、coPoW(cooperative Proof of work)を導入。コインの送信者は、共同でPoWを実行することができます。最後に、あるトランザクションをDAG上で確定させるために必要な、最小の参照トランザクション数を求めるために、iMeshにおける葉ノード数ごとにおきうる状況のシミュレーションを行いました。これは、トランザクションサイズにできるだけ影響を与えない形で、より短い承認時間になるシステムを目指すために行われました。

1章 Introduction (序論)

2008年にSatoshi Nakamoto [1] により発明されたビットコインは現在、世界中で広く使われています。ビットコインは10分に一度、Proof of Work(PoW)により周期的にブロックチェーンにトランザクションが保存されており、トランザクション利用者が手数料をマイナーに支払います。トランザクションは入出力により構成されており、前のトランザクションをElliptic Curve Digital Signature Algorithm (ECDSA:楕円曲線電子署名アルゴリズム)を使い署名する

事でオーナーが正規であるかを確認しています。然しながら近年ビットコインは以下の様な問題を抱えている事が明らかになっています。

・スケーラビリティが低い

ビットコインはブロックサイズに限りがあり、上限を超えたトランザクションの保存ができません。その為、多くのトランザクションが送信された場合に現行ブロックにトランザクションの保存がされなくなってしまうスケーラビリティ問題が生じてしまいます。その上でビットコインの取引が増え、更に多くのブロックが10分で生成されてしまうと、より多くのトランザクションの確定に10分以上待たなくてはならなくなってしまいます。

・高い手数料

トランザクションの利用者はインセンティブとしてブロックのマイナーに手数料を払わなければなりません。ビットコインの取引が増えビットコインの価格が上昇すると、ビットコインの手数料も相対的に高くなります。手数料より少額の決済を行う場合は、少額決済の為の複雑なスキームが必要となってしまいます。(例：マイクロペイメントチャンネル)

・量子コンピューターに対する脆弱性

2017年時点で量子コンピューターの開発は未だ初期段階ですが、量子演算の実験は着々と進められています。Googleは量子演算技術の商用実用化を5年以内に実現するとレポートしています。[11]
その一方でShor'sアルゴリズム[10]によると、ビットコイン等に使われているECDSAを含む楕円曲線離散対数署名は量子コンピューターの圧倒的な演算力により容易に突破されてしまいます。

・脆弱な匿名性

ビットコインを利用する為には、過去に利用されたトランザクション情報は全て公開されています。故に、誰でもアドレス間のビットコインの移動を見ることができるのです。

私たちはこれらの問題を解決する新しい暗号通貨"Aidos Kuneen"を紹介します。Aidos KuneenはiMeshと呼ばれるDAG(Directed Acyclic Graph:有向非巡回グラフ)技術を採用しています。これはブロックやブロックチェーンが存在せず、トランザクションが直接別のトランザクションを参照する技術です。トランザクションの確定はDAG構造に基づく別トランザクションの投票(vote)により決定されます。iMeshにより、スケーラビリティと手数料なしの恩恵を受けることができるのです。

・スケーラビリティの向上

iMeshではトランザクションのPoWが相対的に容易に行え、即時にiMeshに保存されます。故に、iMeshにトランザクションが保存されるのを待つ必要はありません。iMeshの利用が増え、より多くのトランザクションが行われると、トランザクション確定はより早く強固になっていきます。

・手数料なし

マイナーが存在しないので、手数料を払う必要がありません。つまり、極少量の通貨を特別な技術なく送金する事が可能です。

加えて、Aidos KuneenはECDSAに代わり強力な量子コンピューターセキュリティを持つハッシュ構造ベース署名を採用しています。量子コンピューター時代には、Ring-LWEを含む多くの格子構造ベースやハッシュ構造ベースの署名があります。しかし、その多くは暗号鍵や署名のサイズから実用的とは言えません。Ring-LWEや格子構造ベースの署名の暗号鍵のサイズは数キロバイトになります。それはつまり、アドレスが非常に長い文構造となり、それをウェブサイト上にコピー＆ペーストしなければならなくなります。これは、暗号通貨の一般的な使い方としては実用的ではありません。SPHINCSの様なハッシュ構造ベースの署名では、暗号鍵のサイズは僅か1 KByteに収まります。ハッシュ構造ベースの暗号鍵サイズは確かに相対的に小さいけど、現実で使うにはまだ足りません。その為、私たちはeXtended Merkle Signature Scheme(XMSS)を利用することにしました。

これにより1000回以上の公開鍵に利用が可能となり、公開鍵と署名鍵のサイズが3KByteになりました。加えて、XMSSは128bitsの量子コンピューターセキュリティにも対応しているので、長期に渡って量子コンピューターシステムでの利用に耐えられます。[12]
耐量子コンピューターの匿名性ではゼロ知識証明(ZKBoo)[7]を採用しています。コインをハッシュに送る際にはインプットしか分かりません。そして、コインはそのインプットが明かされる事なく利用されることで匿名性を保ちます。

このホワイトペーパー上では複雑な方程式を極力除き、厳密な理論ではなく直観的な理解の為の説明を行っております。これは、より多くの人々にAidos Kuneenの全体像を理解して貰いたいからです。また、複雑な公式により暗号通貨の僅かな部分だけを説明したホワイトペーパーで誤解を生じさせたり悩ませたりすることを私たちは望んでおりません。より詳細な理論やセキュリティレベルの証明に関しては、参考文献をご参照頂ければと思います。

2章 Related Works (関連研究)

匿名性のために、Monero[1]やByteCoin[2]はCryptoNote[13]で言及されているリング署名を利用しています。しかし、残念なことに、リング署名は、ハッシュベースの署名を持たない落とし戸関数（公開鍵の暗号化に使う）を持つ署名に頼っています。Zcoin[3]はzksnarksと呼ばれるゼロ知識非対話証明(zero-knowledge non-interactive proof)を使用していますが、zksnaksは、量子コンピュータ時代に安全とは言えません。なぜなら、Zcoinの開発者が議論しているように[4]ペアリングベースの暗号を用いているためです。ここの議論において言及されているように、量子コンピュータ時代に安全なペアリングベースの暗号を私たちは見つけることができませんでした。その代わりに、Aidos KuneenではZK-Booと呼ぶハッシュ関数と暗号関数(AES等)のみを用いて、量子コンピュータに対しても安全な署名を使用します。

手数料の掛からないDAGベースの暗号通貨として、IOTA[5]について記載してお

かねばなりません。しかし、IOTAの開発者とユーザはIOTAを批判することを誰にも許さず、また私たちはいつでもどこでも、彼らの言葉に攻撃されて辟易としています。したがって、私たちが真似出来ないIOTAの特徴を挙げることにします。

1つ目は、Curlと呼ばれる独自のハッシュ関数です。彼らはIOTAのプログラムコードが安易に流用されないように、意図的にデータ異常を起こすハッシュ関数を開発しました。これは誰もが自由にソースコードを使えるオープンソースの暗号通貨界隈では画期的な発明でした。残念なことに私たちには、故意に衝突が起きるようなハッシュ関数を開発する余裕がないため、既に存在するハッシュ関数であるSHA256を利用することにします。

2つ目に、彼らはバイナリ(binary, 訳注:二進法)ベースの署名の代わりにトライナリ(trinary, 訳注:三進法)ベースの署名を使用しています。これは、理論的にはトライナリの方がバイナリよりも効率的であるためで、彼らは新しいトライナリベースのアナログ処理を行う回路を開発しはじめています。数十年前から、半導体は小さな電力とサイズでバイナリ計算が可能なCMOS(complementary MOS:相補型金属酸化膜半導体)がベースとなっています。半導体を設計するためのツールも、複雑なアルゴリズムを用いて完全にCMOS向けに最適化されています。
例えば、七十億(7×10^9)ものトランジスタが搭載されているIntelの(22-core Xeon Broadwell-E5)チップの面積はたった 680mm=2.6cm×2.6cm で、このチップは現実的なプロセスサイズ(14nm)で生産されており、御存知の通り大変速い計算能力をもっています。このチップのうち大した領域を使わずとも、伝統的なハッシュ関数の計算やそれを使ったPoWの演算ができることは、誰しも容易に想像がつくことでしょう。また、半導体業界の大量生産においては、チップを製造するために多額の初期投資が必要です。そのため、大量にチップを売るか、チップあたりの単価を驚異的な値段にするほかありません。これこそが、半導体業界でたくさんの合併・買収が起きてきた理由になります。さらに、IoT用途のチップのうち幾つかはSHA-2ベースのハッシュを生成する専用の回路を

既に持っています。このような状況にもかかわらず、IOTAの開発者は小型で省電力な性能の良い専用チップをアナログ回路ベースで作る方法を知っていて、それを小さいコストで大量に売る方法を知っていると主張しています。私たちにはそのような性能のチップを設計するノウハウが全くないためSIMD命令、専用SHA拡張などの既存のCPUの機能を最大限利用した、従来通りのバイナリベースの署名を使用します。更に、PoWをたくさんのIoT機器で協調して行う方法についても紹介します。(協調PoWは6章で言及します。)

3つ目に、「ネットワークの2/3が悪意のあるノードの場合のみ、ネットワークが破壊される」とIOTAの開発者は主張しています。しかし、参照トランザクション数を加算していくだけのIOTAの認証方式に従うと、DAG上に多量の葉ノードが存在する場合（それは普通に起きる状況ですが）、攻撃者は彼らの悪意のあるトランザクション群を容易に成長させることができる、ということに直感的に気がつくことになります。彼らは葉ノード数を最小にするため（つまりDAG上のトランザクションを確定させていく）ために、たった２つのトランザクションだけを参照すれば十分であることを知っている、と主張していますが、その理由はホワイトペーパーにおいてもトップシークレットということで明らかにされていません。(ホワイトペーパーでは「**L(t)** (葉ノード数の総和)は安定し続けることが期待できる」とだけ書かれています。)

私たちは文献 [9] で言及されている**SPECTRE**ベースの確認手順を紹介します。SPECTREではトランザクションの承認数は、参照トランザクション数だけでなく、そのトランザクションに投票した他のトランザクションの数も含みます。したがって、葉ノードの集合(訳補：ここは悪意のある葉ノードの集合という意味合いが重要だと考えます。)が、分岐していたとしても、攻撃者は悪意のあるトランザクションを成長させることはできません。しかし、私たちはより速い承認のため、より速いDAGの収束が必要となります。そのため、私たちはiMeshにおける葉ノードの振る舞いをシミュレーションして、DAGの収束がより早く行われることを確認しました。最後に、私たちはDAGベースの手数料なしの暗号通貨という革新を行ったIOTAに対して心から敬意を表します。

References(参考文献)

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' ,2008.

[2] Crypto Forum Research Group, draft-irtf-cfrg-xmss-hash-based-signatures-10 'XMSS:Extended Hash-Based Signatures',2017.

[3] Serguei Popov, 'The tangle' ,2017.

[4] Sheldon M. Ross, 'Introduction to Probability Models. 10th Edition' ,2012.

[5] Sergio Demian Lerner, 'DagCoin: a cryptocurrency without blocks' ,2015.

[6] Johannes Buchmann, Erik Dahmen, Andreas Hülsing, 'XMSS — A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions' , 2011.

[7] Irene Giacomelli, Jesper Madsen, Claudio Orland, 'ZKBoo: Faster Zero-Knowledge for Boolean Circuits' ,2016.

[8] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Greg Zaverucha, 'Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives' , 2017.

[9] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar, 'SPECTRE: Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections' ,2016.

[10] Peter W. Shor, 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer' ,1995.

[11] Masoud Mohseni, Peter Read, Hartmut Neven, 'Commercialize early quantum technologies' ,2017.

[12] PQCRYPTO, 'Post-Quantum Cryptography for Long-Term Security, Initial recommendations of long-term secure post-quantum systems' ,2015.

[13] Nicolas van Saberhagen, 'CryptoNote v 2.0' ,2013.