QDay: 世界初の量子耐性 EVM 互換レイヤー2

アーベル
2025 年 1 月
バージョン 1.0

概要: QDay は、イーサリアム仮想マシン (EVM) との互換性を維持しながら、量子耐性アルゴリズムを使用してブロックチェーンのセキュリティを強化するように設計された、世界初の量子耐性、EVM 互換のレイヤー 2 ネットワークです。

QDay はブロックチェーン技術の画期的な進歩であり、量子耐性と EVM 互換を備えた初のレイヤー 2 ソリューションを提供します。革新的な 2 段階実装戦略により、QDay は既存のブロックチェーン インフラストラクチャの実用的な利点を維持しながら、量子コンピューティングの脅威という重大な課題に対処します。

QDay は、包括的なエコシステム アプローチを採用し、コア DeFi アプリケーションとクロスチェーン ブリッジを統合して、ブロックチェーン環境に完全な耐量子ソリューションを提供します。プラットフォームのトークンノミクスは、広範なネットワーク参加を促進しながら長期的な持続可能性を保証します。

QDay の 2024 年から 2026 年までのロードマップは、プラットフォームの革新的な技術的特徴を統合し、QDay を量子耐性ブロックチェーン技術の先駆者として位置付け、完全な実装への明確な道筋を示しています。

1. はじめに

ブロックチェーン技術のダイナミックな領域では、セキュリティ、スケーラビリティ、相互運用性の向上を継続的に追求することが最も重要です。量子コンピューティングの台頭は、現在のブロックチェーン インフラストラクチャの暗号基盤に実存的な脅威をもたらします。この差し迫った量子革命に対応して、当社は、先駆的な量子耐性アーベル ブロックチェーン (レイヤー 1) 上に構築された、この種では世界初のポスト量子 EVM 互換レイヤー 2 ネットワークである QDay を誇りを持って発表します。QDay は、ブロックチェーンを量子脅威から保護しながら、そのパフォーマンスと機能を向上させるという当社の取り組みの証です。

1.1. レイヤー2 と量子耐性基盤の相乗効果

QDay は単なる拡張機能ではありません。世界初の量子耐性ブロックチェーン プラットフォームである Abelian Blockchain の共生的な強化です。Abelian ですでに運用されている量子耐性アルゴリズムを活用することで、QDay はセキュリティ対策を前例のないレベルに強化します。レイヤー 2 ソリューションとして、QDay は Abelian Blockchain 上で動作し、トランザクション処理を合理化し、コストを削減し、確認時間を短縮します。レイヤー 1 の量子耐性特性をすべて継承しています。

1.2. POS-over-POW モデルによるイノベーション

QDay は、新境地を切り開き、アーベルブロックチェーンのプルーフオブワーク (POW) システムにプルーフオブステーク (POS) モデルを実装することで、革新的なコンセンサスメカニズム戦略を導入します。この斬新な POS と POW の関係は業界初であり、POW の堅牢なセキュリティと分散化、POS のエネルギー効率とスケーラビリティという両方のシステムの利点を組み合わせたものです。この戦略的な融合により、QDay は量子耐性だけでなく、環境的に持続可能で、将来の成長に向けて準備が整っていることが保証されます。

1.3. QDay の量子耐性 EVM 互換レイヤー 2: コアの利点

量子耐性セキュリティ: アーベルブロックチェーンの量子耐性アルゴリズムを基盤とする QDay は、セキュリティの追加レイヤーを導入し、ユーザー資産とデータの整合性と安全性を維持しながら、量子脅威からネットワークを保護します。

- 拡張性の向上: QDay のレイヤー 2 ソリューションは、Abelian の堅牢な基盤を活用してトランザクション スループットを大幅に向上させ、開始時に 1,000 TPS を達成することを目指しています。これにより、ブロックチェーン アプリケーションの増え続ける需要に対応できるスケーラブルなネットワークが確保されます。
- コスト効率の高いトランザクション: トランザクションをオフチェーンで処理し、POS コンセンサス メカニズムを利用することで、QDay はトランザクション手数料を大幅に削減し、さまざまなアプリケーションやユーザーがブロックチェーン テクノロジーをより利用しやすく、手頃な価格で利用できるようにします。

- 高速化されたトランザクション確認: QDay のネットワークは速度を重視して設計されており、ほぼ瞬時にトランザクションを完了します。これは、迅速で信頼性の高いトランザクション処理に依存するアプリケーションにとって非常に重要です。
- 開発者の遊び場: EVM 互換性を中核に据えることで、開発者は好みの Ethereum ベースの開発ツールと言語を使用して QDay に簡単に移行でき、イノベーションを促進し、開発プロセスを合理化できます。
- 相互運用性を優先: QDay は、他のブロックチェーン ネットワークとのシームレスな相互作用を保証し、クロスチェーン トランザクションを促進し、よりまとまりのある多用途のブロックチェーン エコシステムに貢献するように細心の注意を払って作成されています。

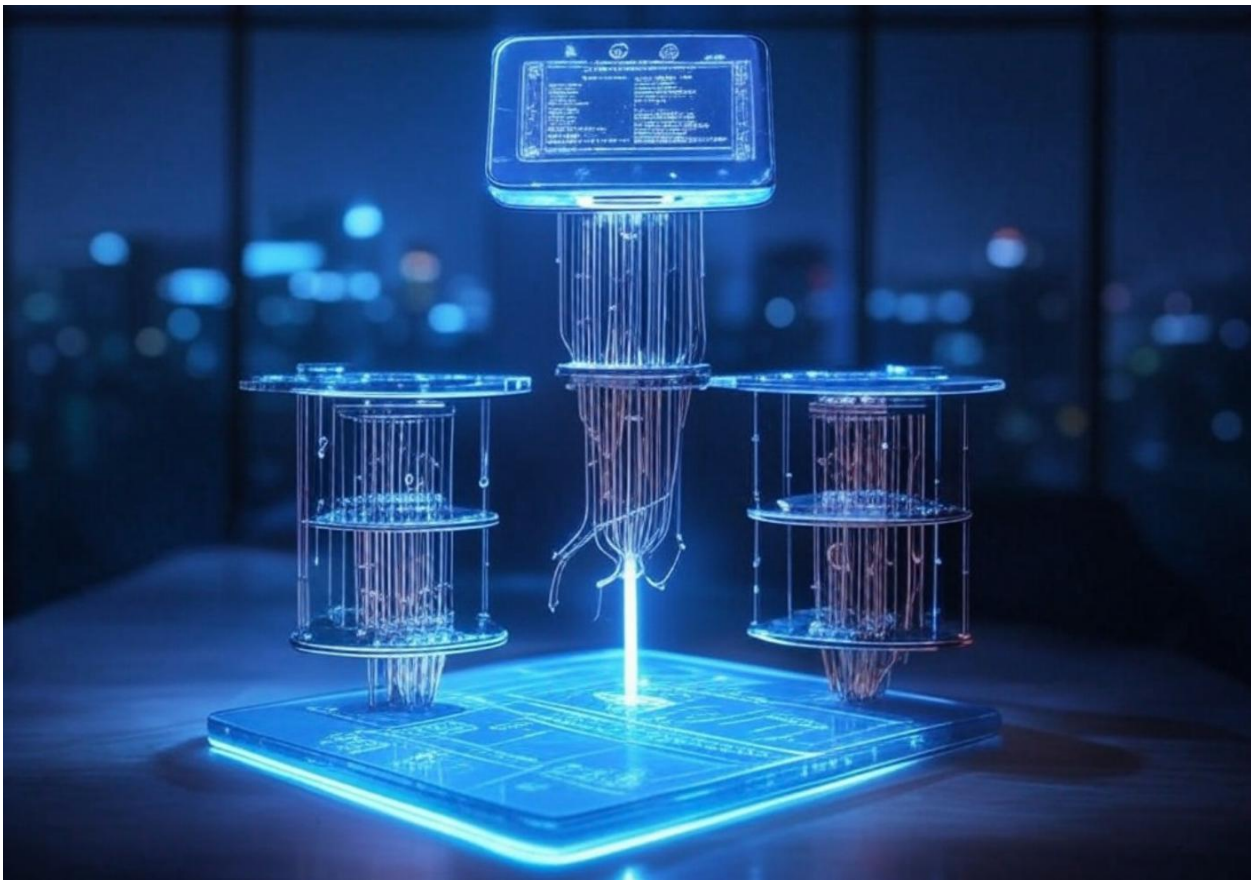
1.4. 今後の展望**:** 量子耐性ブロックチェーンの未来を切り拓く

QDay における量子耐性セキュリティの開発は、主に 2 つのフェーズで実施されます。

- フェーズ 1: EVM 互換性を備えた L1 支援の耐量子ロールアップ - このフェーズでは、QDay は ZK ロールアップをアーベル ブロックチェーンに統合して耐量子台帳を実装し、アカウント モデルとスマート コントラクト機能の採用により EVM 互換性を維持します。これにより、イーサリアム開発者はスムーズに移行でき、既存のイーサリアム ツールと言語を使用できるようになります。このような L1 支援の耐量子ロールアップにより、QDay はトランザクションの順序、金額、状態構造などの台帳データの変更を狙った量子攻撃に耐性を持つようになります。さらに、攻撃が検出されると、QDay はロールアップの実行を一時的に停止して量子耐性を持たせることで資金の損失を防ぐことができます。つまり、ロールアップが停止すると、攻撃者はロールアップ オペレーターによって生成された耐量子署名を偽造できないため、先に進めなくなります。
- フェーズ 2: L2 ネイティブの耐量子アカウントとスマート コントラクト - このフェーズでは、QDay は既存のアカウントに新しい安全なキーを追加し、これらのキーを必要とする操作を有効にすることで、耐量子アカウントを導入します。これを可能にするために、QDay の EVM はポスト量子暗号キーとアルゴリズムを

サポートするように更新されます。QDay は、従来型と耐量子型の 2 種類のスマート コントラクトもサポートします。EVM スマート コントラクトですでに動作しているウォレットは、従来のコントラクトを引き続き使用できますが、耐量子コントラクトは QDay の高度なセキュリティ機能をサポートするウォレットでのみ動作します。

2 つの耐量子メカニズムは独立して機能しますが、相互に補完し合います。1 つ目は量子攻撃から台帳データを守り、2 つ目は個々のアカウントを保護します。これらを組み合わせることで、QDay に強力で包括的なセキュリティが提供されます。たとえば、攻撃者が秘密鍵を盗んだ場合でも (コンピューターのハッキングなどにより)、ロールアップを停止し、影響を受けるアカウントを凍結してからロールアップを再開することで、資金を保護できます。これらのアクションはロールアップ オペレーターのコンセンサスに基づいており、プロセスが分散化され、量子脅威に対して安全であることが保証されます。



2. 技術概要

2.1. アーベル量子暗号（レイヤー1）

Abelian は、QDay 実装の基盤となるフェーズ 0 として機能します。長年にわたる成功した運用実績により、QDay の強力で強固な基盤が確立されます。

Abelian ブロックチェーンは、量子コンピューターの出現に対するシステムのセキュリティを確保するために、量子耐性キーとアルゴリズムを採用しています。Learning With Errors (LWE) や Ring-LWE などの格子ベースの量子耐性仮定を利用することで、Abelian は量子攻撃に対する強力な保護を保証します。これらのアルゴリズムはブロックチェーンの堅牢な基盤を提供し、将来の量子コンピューティングの進歩に直面しても、トランザクションとユーザー データが安全に保たれることを保証します。

- セキュリティ: 格子ベースの暗号化は、従来の攻撃と量子攻撃の両方に抵抗することで、セキュリティを強化します。これにより、アーベル ブロックチェーンは将来の量子脅威に対して耐性を維持し、ユーザー データとトランザクションの整合性と機密性を保護します。
- 効率: これらのアルゴリズムはパフォーマンスが最適化されており、安全で効率的なトランザクション処理を可能にします。Abelian は、格子ベースの暗号化技術を活用して、速度やセキュリティを損なうことなく、ネットワークが大量のトランザクションを処理できるようにします。
- スケーラビリティ: ラティスベースの技術のスケーラビリティにより、セキュリティと効率性を維持しながらネットワークを拡張できます。これにより、Abelian は拡大するユーザー ベースをサポートし、より広範な採用と使用を促進します。
- 将来性: Abelian は、継続的な研究開発を通じて、耐量子技術の進歩に取り組んでいます。ネットワークは、セキュリティとパフォーマンスを強化するために暗号化アルゴリズムを定期的に更新し、耐量子ブロックチェーンのイノベーションにおけるリーダーシップを維持します。

2.2. QDay-アーベルロールアップにおける量子耐性暗号（レイヤー2からレイヤー1）

これは QDay 実装のフェーズ *1* です。

革新的な POS-over-POW コンセンサス統合

POS-over-POW は、Proof of Stake (POS) と Proof of Work (POW) の両方の長所を組み合わせて、より安全で効率的なブロックチェーン ネットワークを作成する革新的なコンセンサス メカニズムです。このハイブリッド アプローチは、POW の確立されたセキュリティを活用しながら、POS のエネルギー効率とスケーラビリティを導入します。

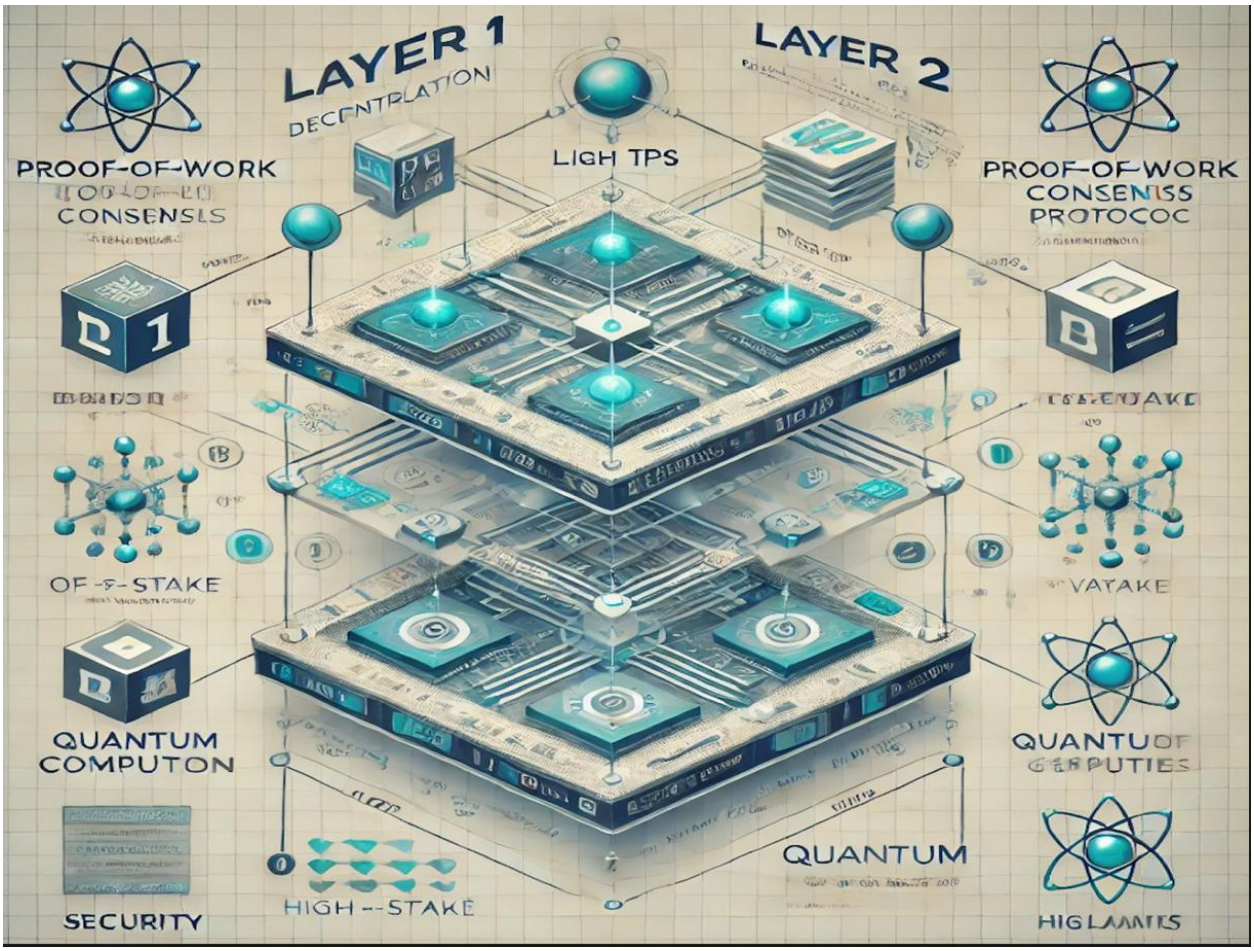
POS-over-POW システムでは、基盤となるブロックチェーンは、堅牢性とセキュリティで知られる POW コンセンサス メカニズムに基づいて動作します。POW では、マイナーが複雑な数学パズルを解くために競い合い、トランザクションを検証してネットワークを保護します。このプロセスは計算集約的でエネルギーを大量に消費しますが、ネットワークを侵害するために必要な膨大な計算能力により、高いレベルのセキュリティが実現されます。

POW 基盤の上に POS レイヤーが実装されています。POS では、保有および担保として賭けているコインの数に基づいて、新しいブロックを作成し、トランザクションを検証するバリデーターが選択されます。このプロセスは、複雑なパズルを解く必要がなくなり、バリデーターの誠実な行動を促す経済的インセンティブに依存するため、POW よりもはるかにエネルギー消費が少なくなります。

POS-over-POW コンセンサス メカニズムは、純粋な POS-over-POS システムに比べていくつかの利点があります。

1. 強化されたセキュリティ:
    - POW Foundation: 計算上の困難さによって強力なセキュリティを提供し、攻撃にコストと困難さをもたらします。
    - 相乗的なセキュリティ: POS と POS の長所を組み合わせて、ネットワーク全体のセキュリティを強化します。
2. エネルギー効率:
    - エネルギー消費の削減: POS レイヤーは、POW のみを使用する場合と比較して、エネルギー消費を大幅に削減します。
    - 最適化されたリソース使用: セキュリティには POW を活用し、検証には POS を活用することで、セキュリティとエネルギー効率のバランスをとります。
3. スケーラビリティ:
    - スループットの向上: POS レイヤーはトランザクションをより効率的に処理し、スケーラビリティを向上させます。
    - 階層化アーキテクチャ: モジュール式のアップグレードが可能になり、継続的なスケーラビリティの向上が実現します。
4. 経済的インセンティブ:
    - バランスのとれたインセンティブ構造: マイナーとバリデーターの両方に報酬を与え、POS インセンティブを通じて積極的な参加を促進します。
    - ステークホルダーの関与: 幅広い参加者を巻き込み、分散化と回復力を強化します。
5. 中央集権化への抵抗:
    - 分散セキュリティ: POW レイヤーは、広範なマイナー ネットワーク全体にセキュリティを分散することで分散化を保証します。
    - 集中化リスクの軽減: 計算要件とステークされたコインを組み合わせることで、純粋な POS システムに見られる集中化のリスクを軽減します。

QDay の POS-over-POW 実装は、Abelian ブロックチェーンの POW 基盤の堅牢なセキュリティを活用しながら、POS レイヤーを統合してスケーラビリティと効率性を向上させます。



量子耐性ロールアップ

耐量子ロールアップの目的は、量子コンピューターを使用する攻撃者であっても、QDay の台帳データを変更または偽造できないようにすることです。攻撃が検出されると、QDay はロールアップの実行を安全に停止し、ロールアップ オペレーターによって生成された耐量子署名を偽造できないため、攻撃者の続行を阻止できます。この停止中、影響を受けるアカウントは凍結され、当局に通知され、是正措置が講じられ次第、ロールアップの実行が再開されます。QDay とは異なり、既存のレイヤー 2 ソリューションにはこの機能がありません。量子攻撃者がロールアップ オペレーターの秘密鍵を解読するのを阻止できないためです。

QDay の量子耐性ロールアップの実装は、シンプルさを重視して設計されています。各ロールアップ オペレーターは、アベル ブロックチェーン上のアカウントを使用し、ロールアップ データは、レイヤー 1 固有の量子耐性キーとアルゴリズムによって保護されます。この量子耐性基盤を活用する以外に、ロールアップ実装の残りの部分は、他のレイヤー 2 ソリューションと同様に機能します。具体的には、QDay は、アベル ブロックチェーンの独自の機能と統合するために、Polygon の ZK ロールアップを採用しています。技術的な詳細については、次のセクションで説明します。

2.3. QDay における耐量子アカウントとスマートコントラクト（レイヤー2）

これは QDay 実装のフェーズ *2* です。

QDay は、EVM 互換性、高いトランザクション速度、低レイテンシを維持しながら、レイヤー 1 基盤と同等以上の耐量子セキュリティを提供することを目指しています。これを実現するために、QDay はレイヤー 1 およびロールアップとは別に、独自の耐量子アカウントとスマート コントラクトを実装します。このアプローチにより、QDay は耐量子ロールアップのセキュリティ強化のメリットを享受しながら、完全な耐量子セキュリティを実現できます。

フェーズ 2 の実装は複雑です。既存のキーやスマート コントラクトとの互換性を保ちながら、量子耐性キーとアルゴリズムをサポートするために QDay の EVM を再設計す

る必要があるためです。これを管理するために、QDay はレガシー トランザクションと量子耐性トランザクションという 2 つのトランザクション モードを導入します。

レガシートランザクション

レガシー トランザクションとは、QDay バリデータ ノードの現在の EVM 実装でサポートされている既存のトランザクション形式を指し、量子耐性トランザクションとは区別されます。レガシー トランザクションは、次の 2 つの場合にサポートされます。

- レガシー キーを使用してレガシー スマート コントラクトと対話するアカウント。
- レガシー キーをサポートするフォールバック メカニズムを含む、耐量子スマート コントラクトと対話するためにレガシー キーを使用するアカウント。

2 番目のケースでは、アカウントはスマート コントラクトが量子耐性キーとアルゴリズムをサポートしているかどうかを知る必要がありません。フォールバック メカニズムはシームレスでユーザーにとって透過的であるため、量子耐性キーをサポートしていないサードパーティのウォレットでも、これらの量子耐性スマート コントラクトとやり取りできます。

ただし、量子耐性のあるキーが従来の（量子耐性のない）スマート コントラクトとやり取りできるようにすることはあまり意味がありません。このいわゆる下位互換性は、セキュリティ上の懸念から推奨されません。

量子耐性トランザクション

量子耐性トランザクションは、量子耐性キーとアルゴリズムをサポートする QDay バリデータ ノードのアップグレードされた EVM 実装によって処理されます。これらのトランザクションは、次のシナリオでのみサポートされます。

- 耐量子キーを使用して耐量子スマート コントラクトと対話するアカウント。

言い換えれば、量子耐性トランザクションは従来のキーから完全に独立しています。量子耐性キーとアルゴリズムのサポートを備えたウォレットのみがこれらのトランザクションを開始できます。フェーズ 2 を正常に完了するために、QDay はコア コンポーネントとして量子耐性ウォレットのリファレンス実装を提供します。これらのウォレットの設計と実装の詳細は、別のホワイト ペーパーで公開されます。

3. トークンノミクス

QDAY の総供給量は 225,179,981 で、ABEL の総供給量と一致しています。QDAY の配布は、ネットワーク セキュリティを確保し、参加を奨励し、コミュニティの成長を促進するように設計されています。QDay DAO (分散型自律組織) は、TGE (トークン生成イベント) 後の QDAY の割り当てを担当します。

3.1 トークンの配布

カテゴリ	%	数（百万）	ロックアップ	権利確定

バリデーター	50%	112.59		
コミュニティの成長	4.5%	10.13		
初期流動性	0.5%	1.13		
投資家	10%	22.52	24 ヶ月	12 か月
ABEL ステーキングエアドロップ	10%	22.52	48 ヶ月	
チーム	15%	33.78	48 ヶ月	24 ヶ月
保険基金	10%	22.52	DAO が決定するまで	
合計	100%	225.18		

すべての QDAY トークンは TGE で生成され、上記の表に概説されている割り当てに従って配布されます。ロックアップおよび権利確定ルールは、QDay に展開されたスマート コントラクトを通じて、または DAO の監督下で適用されます。

バリデーター - QDAY の大部分 (50%) はバリデーターに割り当てられます。バリデータは、QDay バリデーター ノードの実行とネットワークのセキュリティ保護を担当します。報酬は、その期間中のバリデーターのオンライン時間に基づいて毎日計算され、4 週間ごとに分配されます。バリデーターとして活動するには、次の要件を満たす必要があります。

- 当事者は法人または 20 歳以上の個人である必要があります。
- 当事者は、（1）バリデータノードを安全かつ確実に運用するか、（2）バリデータ運用を有能な第三者に委任する必要があります。
- 当事者は、QDay DAO によって確立されたガバナンスおよびコンセンサス ルールを遵守することに同意する必要があります。
- 当事者は、バリデータノードに最低 100,000 QDAY をステークする必要があります。最初の QDAY は、エアドロップを取得するために ABEL をステークするか、市場から購入することで取得できます。

コミュニティの成長 - QDAY の 4.5% は、コミュニティの取り組み、マーケティング、助成金、パートナーシップ、および関連活動を奨励するために割り当てられます。配布は、QDay エコシステムへの貢献に基づいて、QDay DAO によって管理されます。長期的なコミュニティ インセンティブを確保するため、QDAY のこの部分は 12 ～ 48 か月かけて徐々に配布されます。

初期流動性 - QDAY の 0.5% は、分散型取引所 (DEX) の QDAY 取引ペアの初期流動性プールを確立するために割り当てられます。これにより、TGE 直後に市場価格が生成され、すべての QDAY 関連 DeFi dApp が適切に機能するために必要不可欠となります。

投資家 - QDAY の 10% は、長期的に QDay をサポートすることを約束する戦略的投資家に割り当てられます。これらのトークンは投資後 24 か月間ロックされ、その後 12 か月間にわたって徐々に配布されます。

ABEL ステーキング エアドロップ - QDAY の 10% が ABEL ステーカーにエアドロップとして割り当てられ、特に Abelian の長期支持者に報います。QDay で ABEL ステーキングに参加することで、ステーカーは QDAY の一部を報酬として受け取ります。エアドロップはステーキング直後に行われ、受け取った QDAY はステーカーが選択したバリデータ ノードに自動的にステーキングされます。エアドロップされた QDAY の 48 か月のロックアップ期間中、ステーカーはバリデータ操作から QDAY 報酬を獲得し続けます。

チーム - QDAY の 15% がチーム メンバーに割り当てられます。トークンは 48 か月間ロックされ、24 か月間にわたって徐々に配布されます。QDAY のこの部分のロックアップ期間が最も長いのは、チーム メンバーが QDay の長期的な成功にコミットできるようにするためです。

保険基金 - QDAY の 10% は、ハッキングやバリデーターの不正行為など、公式に認められたケースで発生する可能性のある資金損失をカバーするために確保されます。QDay の堅牢なセキュリティを考えると、このようなインシデントが発生する可能性は極めて低いです。そのため、保険基金は使用されることは想定されておらず、損失が発生しない場合は永久にロックされたままになります。

4. フェーズ 1: EVM 互換性を備えた L1 支援の量子耐性ロールアップ

フェーズ 1 では、QDay は、Ethereum Virtual Machine (EVM) との互換性を維持しながら、ZK Rollups を Abelian Blockchain に統合することで、量子耐性のある台帳を導入します。これにより、Ethereum 開発者はシームレスな移行が可能になり、既存のツール、言語、EVM の使い慣れたアカウントとスマート コントラクト モデルを使用できるようになります。L1 支援の量子耐性ロールアップは、トランザクションの順序、金額、状態構造などの台帳データの変更を目的とする量子攻撃から QDay を保護します。さらに、攻撃が検出された場合、QDay はロールアップの実行を量子耐性のある方法で一時的に停止することで、資金の損失を防ぐことができます。停止すると、攻撃者はロールアップ オペレーターによって生成された量子耐性のある署名を偽造することができないため、先に進むことができません。このセクションでは、QDay の量子耐性ロールアップの技術的な詳細に焦点を当てます。

4.1. ZK ロールアップの紹介

ZK ロールアップ (ゼロ知識ロールアップ) は、特にスケーラビリティとトランザクション スループットにおけるブロックチェーンの制限を克服するために設計された高度な

レイヤー 2 スケーリング ソリューションです。複数のトランザクションを 1 つのバッチに集約し、レイヤー 1 ブロックチェーンに送信することで機能します。このアプローチにより、メイン チェーンの計算負荷とストレージ要件が大幅に軽減され、より高速で効率的な処理が可能になります。

ZK ロールアップの核となるイノベーションは、ゼロ知識証明の使用にあります。ゼロ知識証明とは、ステートメント自体の詳細を明かすことなく、一方の当事者がステートメントの有効性を証明できる暗号化技術です。ZK ロールアップのコンテキストでは、これにより、基礎となるトランザクション データを公開することなく、トランザクションの正確性を検証できます。このアプローチは、プライバシーを強化するだけでなく、安全で効率的な検証プロセスを保証します。

ZK ロールアップは、分散化、セキュリティ、スケーラビリティを同時に実現することは本質的に難しいというスケーラビリティの三難問に対する効果的なソリューションも提供します。レイヤー 1 の堅牢なセキュリティ保証を維持しながらトランザクション処理をレイヤー 2 に移行することで、ZK ロールアップは分散化やセキュリティを犠牲にすることなくネットワーク パフォーマンスを向上させるバランスの取れたアプローチを実現します。

4.2. QDay による Polygon ZK Rollups テクノロジーの採用

QDay が Polygon ZK Rollups テクノロジーを採用したのは、現在入手可能な最も先進的で信頼性の高いレイヤー 2 ソリューションの 1 つを活用するための戦略的なステップです。強力な暗号化基盤の上に構築された Polygon ZK Rollups は、大量のトランザク

ションを効率的に処理するように設計されています。これは、スケーラビリティの向上とプライバシーの強化を実現するという QDay の目標と完全に一致しています。

Polygon の ZK Rollups は、ゼロ知識証明の非常に効率的な形式である zk-SNARK (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) を活用しています。これらの証明はコンパクトで、証明者と検証者の間で複数のやり取りを必要とせずに迅速に検証できます。この効率性により、zk-SNARK は、速度とスケーラビリティが最も重要となるブロックチェーン アプリケーションに特に適しています。

実際には、QDay は Polygon ZK Rollups を活用してオフチェーンでトランザクションを処理し、Abelian メインチェーンの負荷を大幅に軽減します。複数のトランザクションが 1 つの証明に集約され、Abelian チェーンに送信されて確定されます。この方法により、トランザクションのスループットが向上し、ガス料金が下がり、ユーザーにとってネットワークのコスト効率が向上します。

さらに、Polygon の ZK Rollups は高い相互運用性を実現するように構築されており、多様なブロックチェーン エコシステムとのスムーズな統合を可能にします。この適応性は、ブロックチェーン業界の変化する需要に合わせて進化できる、スケーラブルで柔軟なレイヤー 2 ソリューションの提供を目指す QDay にとって不可欠です。

Polygon の ZK Rollups は高い相互運用性を実現するように構築されており、多様なブロックチェーン エコシステムとのスムーズな統合を可能にします。この適応性は、ブロックチェーン業界の変化する需要に合わせて進化できる、スケーラブルで柔軟なレイヤー 2 ソリューションの提供を目指す QDay にとって不可欠です。

QDay の実装の特徴は、ZK Rollups のレイヤー 1 基盤として、ビットコインに似たブロックチェーンである Abelian を使用していることです。このアプローチは、レイヤー 1 ベースとして EVM 互換チェーンを使用する従来の方法とは異なります。その結果、Abelian のアーキテクチャとの互換性を確保するには、標準の Polygon ZK Rollups フレームワークに大幅な変更を加える必要があります。

Abelian は、Bitcoin と同様に、EVM 互換チェーンとは異なるコンセンサス メカニズムとトランザクション モデルを採用しています。EVM 互換チェーンはアカウント ベースのモデルに依存していますが、Abelian は UTXO (未使用トランザクション出力) モデルで動作します。この基本的な違いにより、ZK Rollups のデータ構造と証明生成メカニズムを UTXO モデルに合わせて再設計する必要があります。

さらに、Abelian の量子耐性コンセンサス アルゴリズムをロールアップの検証プロセスに組み込む必要があります。そのためには、Abelian のコンセンサス ルールに合わせて、証明の提出と検証のプロトコルを変更する必要があります。これらの変更の詳細は複雑ですが、主な目的は、ロールアップと Abelian メイン チェーンのシームレスな統合を実現し、両方のレイヤーのセキュリティと効率の利点を維持することです。

4.3. 量子耐性ロールアップの利点

量子耐性ロールアップには重要な利点があります。ロールアップがアベルブロックチェーンによって確認されると、台帳データが量子耐性を持つことが保証されます。このセキュリティは、確認済みデータと保留中のデータ（QDay に送信されたがアベルによってまだ確定されていないトランザクション）の両方に適用され、量子コンピューターにアクセスした場合でも 51% 攻撃から保護します。

QDay の画期的な機能は、ロールアップの実行を量子耐性のある方法で停止できることです。ロールアップが停止すると、攻撃者はロールアップ オペレーターによって生成された量子耐性のある署名を偽造することができないため、攻撃を続行できません。重要なのは、この停止メカニズムはロールアップ レイヤーでのみ動作し、QDay ブロックチェーン自体の機能には干渉しないということです。

この機能は既存のレイヤー 2 ソリューションではサポートされていないため、具体的な例を使用してその機能を説明します。

タイムラインでは以下のイベントが発生する予定です:

1. 量子コンピュータにアクセスできる攻撃者が QDay に DeFi dApp の脆弱性を悪用し、ラグプルでプールからすべての資金を流出させました。
2. 盗まれた資金は、攻撃者が管理する QDay アカウントに送金されます。
3. ユーザーはラグプルに気づき、そのインシデントを dApp プロバイダーに報告します。
4. dApp プロバイダーは攻撃者のアカウントを凍結し、インシデントを QDay DAO にエスカレートします。
5. QDay DAO は、ロールアップの実行を 12 時間停止する投票提案を開始します。
6. すべての DAO メンバーは、30 分以内に提案に投票するよう求められます。
7. 投票が通過すると、ロールアップの実行は直ちに停止されます。この時点から、QDay Bridge はロールアップによって確認されたトランザクションのみを処理するため、攻撃者は QDay から資金を移動できなくなります。
8. dApp プロバイダーには、ユーザーの資金を保護するために必要な措置を講じるのに約 12 時間の猶予があることが通知されます。さらに時間が必要な場合は、QDay DAO に停止期間の延長をリクエストできます。
9. dApp プロバイダーはトークン発行者に連絡して、攻撃者が管理するすべてのアドレスを凍結します。注目すべきは、この凍結操作は QDay のスマート コントラクト呼び出しとして実行され、ロールアップ停止の影響を受けないことです。
10. トークン発行者は、dApp プロバイダーにラグプルの確固たる証拠を要求します。この例では、dApp プロバイダーが必要な証拠を提出し、トークン発行者のレビューに合格します。

11. トークン発行者は攻撃者のアドレスを凍結します。
12. ロールアップの実行は、(1) 12 時間後、または (2) dApp プロバイダーが QDay DAO に、必要なアクションがすべて実行され、ロールアップの実行を再開できることを通知した時点で再開されます。後者の場合、QDay DAO はロールアップの実行を再開する提案にも投票します。
13. QDay ブロックチェーンは通常の運用に戻ります。dApp プロバイダーは、警察またはその他の関係当局にこの攻撃を報告し、攻撃者に対するさらなる法的措置を開始します。
14. 追加の措置が必要な場合、QDay DAO は関連する提案に投票します。通常、このような措置は警察やその他の関連当局からの勧告に基づいて開始されます。

上記の例では、攻撃者が量子コンピュータにアクセスできることを前提としていることに留意してください。それにもかかわらず、ロールアップ プロセスはロールアップ オペレーターによって生成された量子耐性署名に依存しているため、攻撃者は QDay ブリッジを介して QDay から資金を転送することはできません。この例は、量子耐性停止メカニズムによって QDay に展開された dApp のセキュリティが大幅に強化されることを示しています。

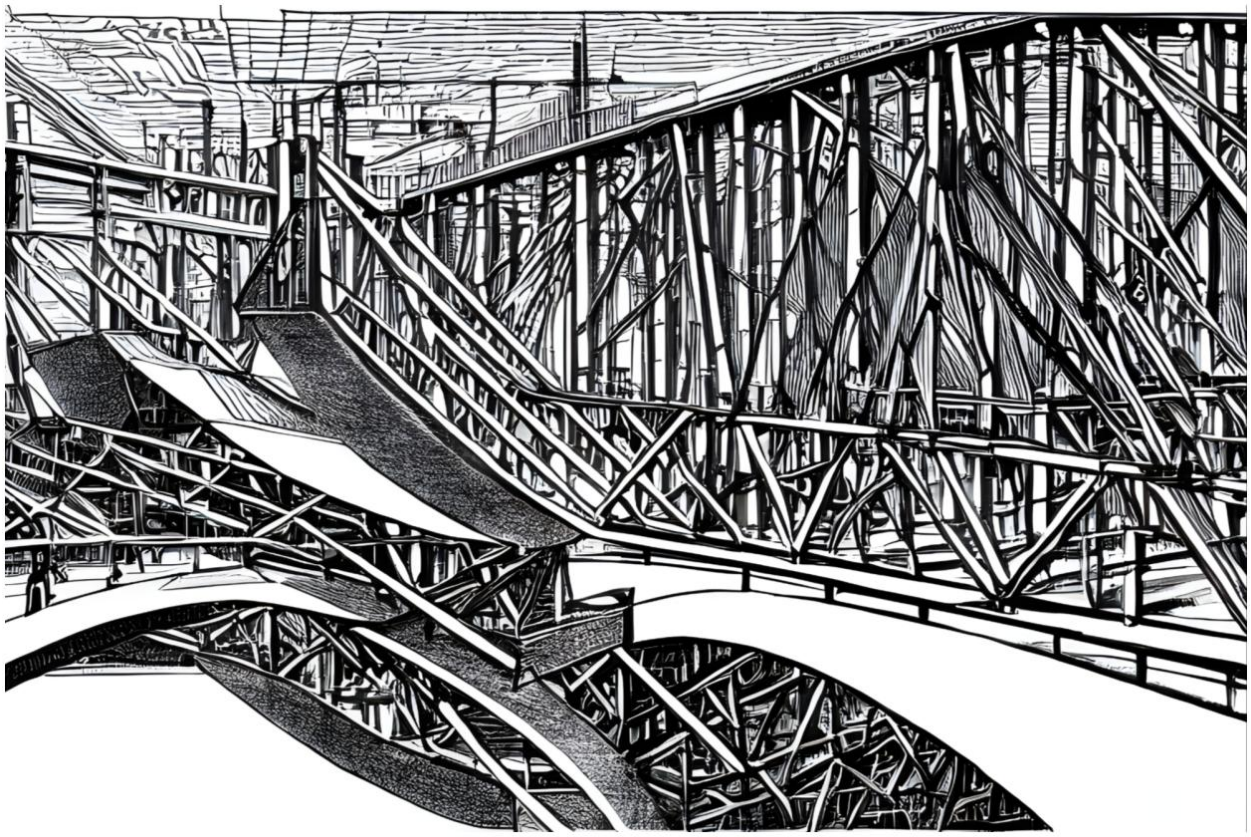
4.4. 今後の課題: PQZK ブリッジ

PQZK ブリッジとは何ですか?

PQZK ブリッジ (ポスト量子ゼロ知識ブリッジ) は、ブロックチェーン システムをポスト量子セキュリティ標準に安全かつ効率的に移行するために設計された暗号化プロトコルです。ゼロ知識証明とポスト量子暗号化アルゴリズムを統合することで、量子コンピューターの高度な機能に耐えられる、回復力のあるフレームワークを確立します。

ゼロ知識証明 (ZKP) を使用すると、一方の当事者が、ステートメント自体の詳細を開示することなく、もう一方の当事者に対してステートメントの真実性を証明することができます。ブロックチェーンでは、ZKP により、プライバシーを保護しながらトランザクションの正確性を検証できます。一方、耐量子暗号 (PQC) は、量子コンピューターからの攻撃に耐えるように設計された暗号化アルゴリズムに重点を置いています。

PQZK ブリッジは、ポスト量子暗号プリミティブを使用してゼロ知識証明を構築することで、これら 2 つのテクノロジーを統合します。これにより、量子攻撃者が存在する場合でも証明が安全に保たれます。PQZK ブリッジは、既存のブロックチェーン プラットフォームへの PQZK ロールアップの展開を容易にするミドルウェア レイヤーとして機能し、量子セキュリティへのシームレスなアップグレード パスを提供します。



PQZK ブリッジを使用した QDay の PQZK ロールアップの実装

PQZK ロールアップを実装するために、QDay は PQZK ブリッジを活用して、従来の ZK ロールアップから完全に量子耐性のあるソリューションに移行します。このプロセスは次のように実現されます。

- ポスト量子暗号プリミティブの統合: 最初のステップは、ロールアップ フレームワークにポスト量子暗号プリミティブを統合することです。格子ベースの暗号化やハッシュベースの署名などのこれらのプリミティブは、ゼロ知識証明で使用される従来の暗号化アルゴリズムに代わるものです。
- PQZK 証明の構築: これらのポスト量子プリミティブを使用して、QDay は PQZK 証明を構築します。これらの証明はゼロ知識プロパティを保持し、機密情報を公開せずにトランザクション検証を可能にすると同時に、量子攻撃に対する耐性も提供します。

- ロールアップ プロトコルの変更: ロールアップ プロトコルは PQZK 証明を統合するように更新され、新しいポスト量子暗号構造に対応するために証明の生成、送信、検証のプロセスを変更する必要があります。
- Abelian レイヤー 1 への展開: PQZK 証明を組み込んだ更新されたロールアップ プロトコルは、Abelian レイヤー 1 ブロックチェーンに展開されます。Abelian の量子耐性特性は PQZK ロールアップを補完し、量子攻撃に耐性のある堅牢なエンドツーエンドのソリューションを提供します。
- テストと最適化: PQZK ロールアップの機能と効率性を検証するために、広範囲にわたるテストが行われます。最適化の取り組みでは、ポスト量子暗号操作に関連する計算オーバーヘッドを最小限に抑えることに重点を置き、ロールアップ ソリューションがスケーラブルで高性能であることを保証します。

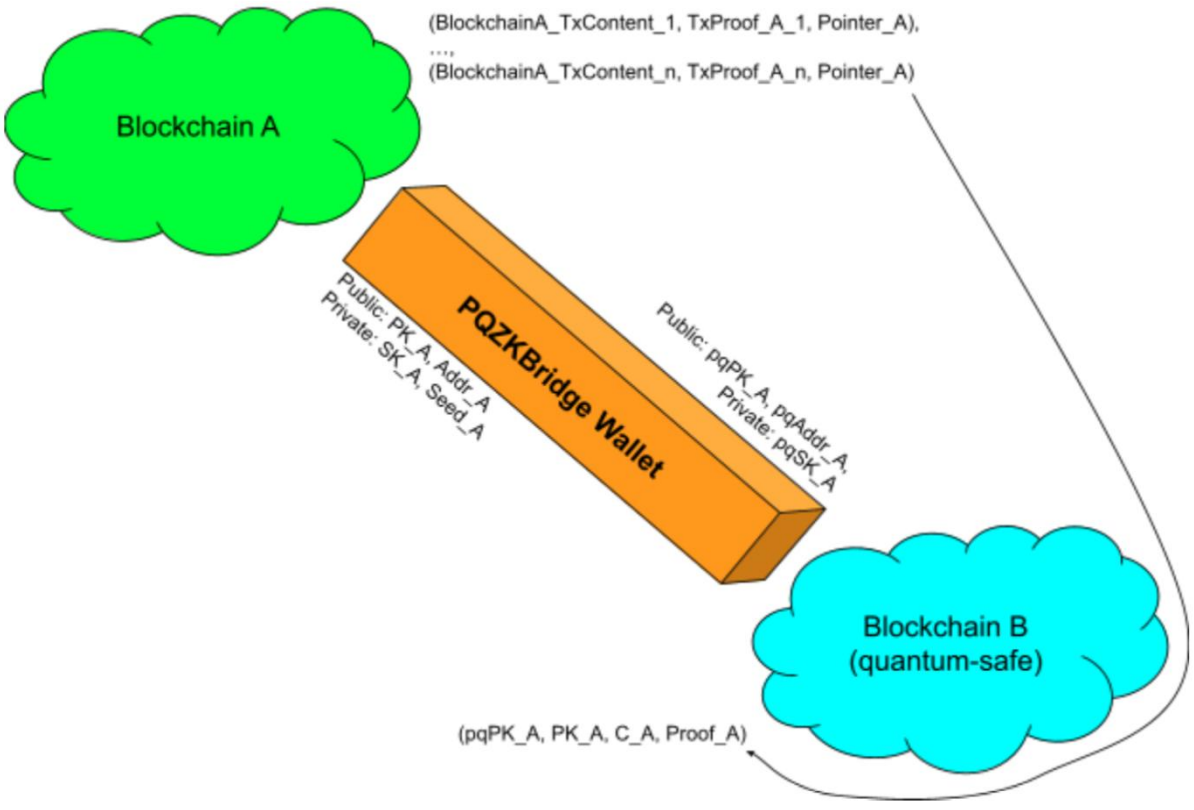
PQZK ロールアップを他の EVM 互換チェーンに拡張する

PQZK ロールアップの利点は、QDay と Abelian だけにとどまりません。PQZK ブリッジ テクノロジーは、他の EVM 互換チェーンにも適用でき、量子セキュリティを実現できます。その実現方法は次のとおりです。

- EVM 互換チェーンへの PQZK ブリッジの適応: PQZK ブリッジは、EVM 互換チェーンの独自のアーキテクチャおよびコンセンサス メカニズムと統合するようにカスタマイズできます。これには、ブリッジ プロトコルを変更して、Ethereum 仮想マシン (EVM) およびその他の関連テクノロジとの互換性を確保することが含まれます。
- EVM 互換チェーンへの PQZK ロールアップの展開: 適応後、PQZK ブリッジはさまざまな EVM 互換チェーンへの PQZK ロールアップの展開を容易にすることができます。これにより、これらのチェーンは量子耐性のある方法でオフチェーンでトランザクションを処理できるようになり、スケーラビリティとセキュリティが向上します。
- 相互運用性とエコシステム統合: PQZK ブリッジの相互運用性機能により、さまざまなブロックチェーン エコシステム間で PQZK ロールアップをシームレスに統合できます。これにより、より安全で相互接続されたブロックチェーン環境が促進され、複数のチェーンが量子耐性トランザクション処理のメリットを享受できるようになります。

- コミュニティと開発者のサポート: PQZK ロールアップの採用をサポートするために、包括的なドキュメント、開発者ツール、コミュニティ リソースが提供されます。これらのリソースにより、ブロックチェーン開発者はプラットフォームに PQZ K ロールアップを効率的に実装および展開できるようになり、量子セキュア ブロックチェーン テクノロジーへの移行が加速されます。

QDay は、PQZK ブリッジを通じて PQZK ロールアップを採用することで、量子脅威に対するより広範なブロックチェーン エコシステムの耐性を高めながら、自社のセキュリティを強化します。この先進的なアプローチにより、量子コンピューティング技術が進歩し続けても、ブロックチェーン システムの安全性、拡張性、効率性が維持されます。



5. フェーズ 2: EVM 互換性を備えた量子耐性アカウント

フェーズ 2 では、QDay は、量子耐性アカウントとレガシー アカウントに加えて、次の関連概念を導入します。

- 量子耐性ウォレットとレガシーウォレット。
- 量子耐性コントラクトとレガシーコントラクト;
- 量子耐性のある *dApp* とレガシー *dApp* 。

レガシー アカウントの各ニーモニック フレーズは、対応する耐量子アカウントをシームレスに導出できるため、ユーザーは簡単に移行できます。この設計により、ユーザーは同じニーモニック フレーズを使用して両方のアカウント タイプにアクセスできます。EVM 対応ウォレットは、変更なしでレガシー アカウントで引き続き機能し、耐量子アカウントを認識しません。対照的に、耐量子ウォレットは、同じニーモニック フレーズでレガシー アカウントと耐量子アカウントの両方をサポートします。採用を促進するために、QDay は耐量子ウォレットのオープンソース リファレンス実装を提供し、透明性と統合の容易さを促進します。

同じニーモニックフレーズを共有すること以外、耐量子アカウントはレガシーアカウントから完全に独立しています。これは、新しいアカウントのポスト量子セキュリティを確保するために意図的に設計されています。具体的には、フェーズ 2 では次の目的が達成されます。

- レガシー アカウントは、レガシー ウォレットとレガシー スマート コントラクトによって完全にサポートされ、これまでどおり機能し続けます。
- 耐量子アカウントは耐量子ウォレットと互換性がありますが、従来のウォレットは耐量子アカウントをサポートしない予定です。

- QDay チームの耐量子ウォレットのリファレンス実装は、レガシー アカウントをサポートします。サードパーティによって実装された耐量子ウォレットの場合、レガシー アカウントのサポートはオプションになります。
- 量子耐性コントラクトは、従来のアカウントをサポートしません。これは、量子耐性のない暗号化プリミティブの使用によってポスト量子セキュリティが侵害されないようにするための鍵です。
- 量子耐性コントラクトは、次の 2 つの方法で従来のコントラクトとの互換性を維持します。1) 量子耐性のない従来の関数を含めることができます。2) 量子耐性関数には、外部の量子耐性署名ジェネレーターを介して従来のウォレットからアクセスできます。
- 一部の耐量子 dApp は、耐量子プロトコルとレガシープロトコルの両方を実装することで、レガシー アカウントをサポートする場合があります。
- 耐量子アカウントは、耐量子ウォレットを使用して、耐量子スマート コントラクトおよび dApp と対話できます。耐量子ウォレットにこれらのシナリオに対するフォールバック メカニズムが含まれている場合は、従来のスマート コントラクトおよび dApp と対話することもできます。
- 以下の表は、量子耐性オブジェクトがレガシー オブジェクトと対話したりサポートしたりできるかどうかを示しています。レガシー オブジェクトは量子耐性オブジェクトと対話できないため、対応する逆表は含まれていません。

物体	レガシーアカウント	レガシーウォレット	レガシーコントラクト	レガシー**dApp**
量子耐性アカウント	フォールバックする可能性がある	使用できません	相互作用する可能性がある	相互作用する可能性がある
量子耐性ウォレット	サポートするかもしれない	同じ記憶法	サポートするかもしれない	サポートするかもしれない

量子耐性コントラクト	互換性がない	互換性がない	互換性がない	互換性がない
量子耐性 dApp	サポートするかもしれない	使用される可能性がある	サポートするかもしれない	サポートするかもしれない

-

要約すると、フェーズ 2 の目的は、従来のオブジェクトとの下位互換性を最大限に維持しながら、ポスト量子セキュリティ機能を損なうことなく、量子耐性オブジェクトのサポートを追加することです。このセクションの残りの部分では、QDay フェーズ 2 のコア コンポーネントの全体的な設計の概要を説明し、その後、設計の原則とトレードオフについて詳しく説明します。

5.1. 量子耐性アカウント

QDay の耐量子アカウントは、アーベルブロックチェーンと同じ耐量子暗号プリミティブを使用します。従来のアカウントと同じニーモニックフレーズを共有していますが、その時点から機能と構造は完全に異なります。

BIP-39 ニーモニックフレーズから量子耐性アカウントを導出するプロセスは、AIP-11 (Abelian Improvement Proposal 11) で定義されています。読者の便宜のために、ここでそのプロセスについて簡単に説明します。

ステップ 1: ニーモニックからエントロピー シードへ: AIP-11 は、BIP-39 と同じエントロピー シード導出プロセスを使用します。ただし、AIP-11 では、エントロピー シードの長さが 256 ビットである必要があります。これは、24 個のニーモニック ワードに相当します。これに対処するために、24 個未満のニーモニック フレーズの場合は、24 個になるまで「abandon」(BIP-39 ワードリストの最初のワード) という単語でニーモニック フレーズを埋め込みます。一方、24 個を超えるニーモニック フレーズの場合は、24 個にニーモニック フレーズを切り捨てます。

ステップ 2: エントロピー シードからマスター シードへ: 次に、エントロピー シードを使用して、決定論的なキー導出関数を使用して 512 ビットのマスター シードを導出します。キー導出関数は次のように定義されます。

マスターシード=PRF(エントロピーシード、'アカウントマスターシード')マスターシード=PRF(エントロピーシード、'アカウントマスターシード')

ここで、PRFPRF は、KMAC256 を基礎ハッシュ関数として使用する耐量子鍵導出関数であり、次のように定義されます。

PRF(0,1):=KMAC256(0,1,512,'ABELIANPRF')。

ステップ 3: マスター シードからアカウント ルート シードへ: Abelian では、各アカウントはルート シードのセット *(CoinSpKeyRootSeed* 、 *CoinSnKeyRootSeed* 、 *CoinDetectorRootKey* 、 *CoinVKRootSeed)* で構成され、総称してアカウント ルート シードと呼ばれます。すべてのルート シードは 512 ビットの長さで、次のキー導出関数を使用してマスター シードから導出されます。

CoinSpKeyRootSeed=PRF(MasterSeed,'CoinSpendKeyRootSeed'),
CoinSnKeyRootSeed=PRF(MasterSeed,'CoinSerialNumberKeyRootSeed'),

コイン検出器ルートキー=PRF(マスターシード、'コイン検出器ルートキー')、CoinVKRootSeed=PRF(Master-Seed、'CoinValueKeyRootSeed')。

PRF 関数は前の手順で使用した関数と同じであることに注意してください。

ステップ 4: マスター シードからパブリック ランドへ: AIP-11 では、ルート シードの各セットを使用して、パブリック ランドの異なる値に対応する複数のアドレスを導出できます。QDay では、既存の階層的決定論的ウォレット (HDW) の規則に準拠するために、AIP-11 で定義された次の決定論的関数を使用して、マスター シードとシーケンス番号からパブリック ランドを導出します。具体的には、パブリック ランドは次のように導出されます。

PublicRand($seqNo$)=PRF(PublicRandRootSeed,$seqNo$),

where

PublicRandRootSeed = PRF(MasterSeed、'PublicRandRootSeed')。

ステップ 5: アカウント ルート シードと公開乱数からアドレスと秘密鍵へ: アカウント ルート シードと公開乱数の両方が導出されると、対応するアドレスと秘密鍵を決定論的に導出できます。このプロセスは AIP-11 の範囲外であるため、L1 チェーンのエコシステムとの一貫性を高めるために、Abelian SDK v2 に実装されている同じプロセスを使用します。

5.2. QDay ノードのアップグレード

耐量子アカウントの機能を有効にするには、まずブロックチェーンが、従来のアカウントと耐量子アカウント間のネイティブ トークン QDAY の転送をサポートする必要があります。そのためには、QDay ノードをアップグレードして、1) 耐量子アカウントで使用される新しいアドレス形式を認識し、2) 耐量子アカウントによって生成された署名を検証し、3) 従来のアカウントと耐量子アカウント間の QDAY の転送を容易にする必要があります。ただし、3 番目の要件を満たすのは簡単ではありません。これは、下位互換性を維持し、耐量子アカウントで使用される新しいアドレス形式を意識せずに従来のウォレットが転送を実行できるようにするためです。

課題: 従来のウォレットを変更せずに、従来のアカウントと量子耐性アカウント間でネイティブ トークン QDAY の転送をサポートすることは可能ですか?

この課題を克服するために、私たちは QDay ブロックチェーン上で、従来のアカウントと量子耐性アカウントの橋渡しとなるスマート コントラクトを開発します。このスマート コントラクトは従来のコントラクトとなり、従来のウォレットとの互換性が確保されます。一般的なプロセスは次のとおりです。

1. レガシー アカウントはスマートの送信関数を呼び出し、量子耐性アカウントを受信者として指定し、転送する QDAY の量を入力として指定します。
2. スマート コントラクトは、レガシー アカウントの署名を検証し、受信者のアドレスを検証します。
3. スマート コントラクトは、レガシー アカウントから QDAY を受け取り、それを量子耐性アカウントに転送します。

最後のステップでは、スマート コントラクトは QDAY を自身のレガシー アドレスから受信者の量子耐性アドレスに転送します。これは、QDay ノードによって実装された新しいプリミティブ関数 legacy_to_quantum_resistant_transfer を呼び出すことによって実行されます。QDay ノードの EVM 実装は、このプリミティブ関数と、逆のプロセス

を処理する別のプリミティブ関数 quantum_resistant_to_legacy_transfer をサポートするようにアップグレードされます。

上記の 2 つの基本関数のインターフェースはシンプルに見えますが、実装は簡単ではありません。従来のアルゴリズムと量子耐性アルゴリズムの両方を含む包括的な暗号化操作が必要です。技術的な詳細はこのホワイトペーパーの範囲を超えており、QDay ノードの実装をオープンソース化するときに詳しく説明します。

5.3. 量子耐性ウォレット

既存の EVM ベースのウォレットはすべて、ポスト量子セキュリティ機能をサポートするように設計されていないため、QDay が定義する量子耐性アカウントをサポートしないことは明らかです。したがって、QDay の量子耐性アカウントをサポートするには、新しいタイプのウォレットが必要です。QDay はフェーズ 2 でこのウォレットのリファレンス実装を提供し、ソース コードはオープンソース化され、コミュニティや他の関係者が互換性のある量子耐性ウォレットを構築できるようになります。

耐量子アカウントを作成またはインポートするには、ユーザーはレガシー アカウントと同じニーモニック フレーズを使用します。ウォレットはニーモニック フレーズから耐量子アカウントを派生し、ネイティブ トークン QDAY を転送し、耐量子スマート コントラクトおよび dApp と対話できるようにします。

QDAY を耐量子アカウントからレガシー アカウントに転送するには、耐量子ウォレットがトランザクションをブロックチェーン ノードに直接送信します。これは、前のセ

クションで説明したように、レガシー ウォレットを使用して QDAY をレガシー アカウントから耐量子アカウントに転送することとは異なります。フェーズ 2 のアップグレード後、QDay ノードはこのようなトランザクションを直接処理できるようになり、この場合、スマート コントラクト ブリッジは不要になります。

耐量子ウォレットの主な目的は、耐量子スマート コントラクトおよび dApp とやり取りすることです。耐量子ウォレットがこれらのスマート コントラクトとどのようにやり取りするかを理解するには、まず耐量子スマート コントラクト自体の設計と実装を調べることが不可欠です。そのため、次のセクションでは、耐量子スマート コントラクトについて詳しく説明します。

リファレンス実装では、これらのシナリオをサポートするためのフォールバック メカニズムを提供します。具体的には、レガシー スマート コントラクトとやり取りする場合、ウォレットは対応するレガシー アドレスを使用してスマート コントラクトを呼び出します。ウォレットは資産の移行を自動的に処理します。たとえば、QDAY を PQUSD にスワップするスマート コントラクトとやり取りする場合、ウォレットはまず QDAY をレガシー アドレスに転送し、スマート コントラクトの呼び出しを実行し、トランザクションが完了すると PQUSD を量子耐性アドレスに転送します。

5.4. 量子耐性のあるコントラクト

QDay フェーズ 2 では、量子耐性コントラクトは、ポスト量子署名検証の追加レイヤーを備えたレガシー コントラクトと見なすことができます。呼び出し元の観点からは、

量子耐性コントラクトはレガシー コントラクトと同じように機能します。唯一の違いは、量子耐性を意図したコントラクト メソッドを呼び出すたびに、呼び出し元が追加の量子耐性署名を提供する必要があることです。この署名は、コントラクト メソッドの標準パラメーターとして渡され、コントラクト自体によって検証されます。

量子耐性のある ERC20 契約における転送方法を考えてみましょう。従来の ERC20 メソッドの署名は次のとおりです。

関数 transfer(address to, uint256 value) external は (bool) を返します。

この方法の量子耐性バージョンは次のとおりです。

関数 pq_transfer(bytes pq_sig_data、address to、uint256 value) 外部は (bool) を返します。

ここで、pq_sig_data は量子耐性署名です。

QDay で定義された規則として、関数名の前には必ず pq_ を付け、署名は必ず最初のパラメータにする必要があります。この規則により、量子耐性メソッドを従来のメソッドと簡単に区別できます。さらに重要なのは、この規則により、QDay ノードはコントラクトに追加のコードを追加することなく、量子耐性署名を自動的に検証できることです。具体的には、署名データが QDay で定義された標準的な方法で生成され、名前の前に [pq_]{.underline} が付けられた関数の最初のパラメータとして渡される限り、QDay ノードは組み込みの量子耐性署名検証メカニズムを使用して署名を検証します。

理論的には、次の問題に対処すれば、EVM 互換チェーン上のレガシー コントラクトに同じメカニズムを実装できます。

1. 量子耐性署名は、量子耐性ウォレットまたは QDay によって定義された標準に準拠した外部ツールによって生成できます。
2. 量子耐性署名は、通常の EVM 命令を使用してコントラクト関数内で検証できます。

最初の問題は比較的簡単に解決できますが、従来のウォレットを外部ツールと併用すると、ユーザー エクスペリエンスが理想的とは言えない可能性があります。2 番目の問題は、通常の EVM 命令を使用して契約機能内に耐量子暗号操作を実装するのが複雑なため、より困難です。また、これらの操作はリソースを大量に消費するため、ユーザーにとって法外なガス料金につながる可能性があります。

2 番目の問題は QDay には存在しないことに注意することが重要です。これは、量子耐性のある署名検証が組み込み機能として実装されているためです。計算は QDay ノードのオペレーティング システムでネイティブに処理されます (EVM 経由ではなく)。つまり、計算コストがガス料金の形でユーザーに転嫁されることはありません。

5.5. 量子耐性 dApp

上で見たように、スマート コントラクトは量子耐性署名をサポートするためにアップグレードする必要があります。スムーズな移行を確実にするために、フェーズ 1 で展開された dApp は、次のアプローチを採用して、量子耐性署名に段階的にアップグレードできます。

1. dApp のユーザー インターフェースは変更しません。従来のウォレットは、これまでどおり dApp と対話できます。

2. 既存のレガシーメソッドはすべて変更せずに維持しながら、dApp で使用されるスマートコントラクトに新しい量子耐性メソッドを追加します。
3. dApp のユーザー インターフェイスをアップグレードして、量子耐性ウォレットのサポートを追加します。

ただし、場合によっては、従来のウォレットと互換性のない、量子耐性のある別の dApp のバージョンを実装して、量子耐性のある契約が従来の契約の影響を受けないようにする必要があります。QDay では、dApp が量子耐性のあるバージョンにアップグレードされる時期、方法、またはアップグレードされるかどうかについて制限を設けていないことに注意してください。この決定は、dApp 開発者に完全に委ねられています。

5.6. 設計原則

QDay フェーズ 2 の設計は、次の基本原則に従います。

1. 下位互換性
- 従来のアカウントとウォレットは変更されることなく引き続き機能します。
- 従来のスマート コントラクトは引き続き完全に動作します。
- 既存の dApp は、徐々に量子耐性バージョンに移行できます。
2. セキュリティ分離
- 量子耐性アカウントは、従来のアカウントから完全に独立しています (ニーモニックフレーズのみを共有します)。
- 量子耐性のあるスマート コントラクトは、従来の暗号化プリミティブによって侵害されることはありません。
- 量子耐性トランザクション タイプと従来のトランザクション タイプを明確に分離します。
3. シームレスなユーザーエクスペリエンス

- 同じニーモニックフレーズで、従来のアカウントと量子耐性アカウントの両方を導出できます。
- 量子耐性ウォレットは、オプションで従来の操作をサポートできます。
- 必要に応じて、従来のアカウントと量子耐性アカウント間で資産を自動的に移行します。

4. 効率的な実装
- 量子耐性署名検証は QDay ノードに統合されています。
- 量子耐性操作のための追加ガスコスト。
- 量子耐性のある契約方法の標準化されたプレフィックス (pq_)。

5. 柔軟な導入
- dApp の開発者は独自のアップグレード タイムラインを選択できます。
- 複数の実装アプローチが利用可能です (段階的なアップグレードまたは完全な置き換え)。
- 従来の互換性のためのオプションのフォールバック メカニズム。

6. 明確な基準
- 量子耐性メソッドの一貫した命名規則。
- 標準化された署名データ形式。
- レガシーコンポーネントと量子耐性コンポーネント間の明確に定義されたインターフェース。

これらの原則により、QDay は使いやすさを維持し、有機的なエコシステムの成長をサポートしながら、量子耐性セキュリティにスムーズに移行できるようになります。

6. アプリケーションエコシステム

前のセクションで説明した機能に応じて、QDay アプリケーション エコシステムは次のカテゴリで構成されます。

カテゴリー1: アーベル関連のアプリケーション

Abelian は QDay のセキュリティの中核となる基盤であり、特にフェーズ 1 では L2 チェーンのポスト量子機能が L1 チェーンへのロールアップから完全に派生するため、QDay では Abelian に関連するアプリケーションが最初にリリースされます。L1 チェーンと L2 チェーンの両方を管理するのは複雑なため、QDay の Abelian に関連する初期段階のアプリケーションはすべて、QDay チームまたは Abelian チームのいずれかによって開発される予定です。現在、このカテゴリに分類される主なアプリケーションは、Wrapped ABEL (wABEL) と Abelian Staking です。

- ラップされた ABEL (wABEL) - wABEL は QDay の QRC20 トークンで、Abelian の ABEL コインに 1:1 で固定されています。QDay ブロックチェーンと Abelian ブロックチェーンの間で ABEL トークンをブリッジするために使用されます。wABEL をミントするには、ユーザーは Abelian で ABEL コインをロックし、QDay で対応する量の wABEL を受け取る必要があります。wABEL をバーンするには、ユーザーは QDay で wABEL をバーンし、Abelian で対応する量の ABEL コインを受け取る必要があります。このような操作をサポートするために、QDay チームは wABEL のミントおよびバーン用のオンライン サービスを実装します。このサービスは、Trust Service Provider (TSP) 認定を受けた機関の連合によって運営されます。
- Abelian Staking - Abelian Staking は、ユーザーが QDay で ABEL をステークしてエアドロップとステーキング報酬を獲得できるようにする dApp です。エアドロップとステーキング報酬の具体的な詳細は、QDay メインネットの立ち上げ時に発表されます。

カテゴリー2: レガシーEVM 互換アプリケーション

最初のカテゴリを除き、フェーズ 1 で展開されるすべての dApp は、既存の EVM 互換チェーン上の dApp と同様に機能します。これらは、レガシー アカウントおよびレガシー ウォレットと互換性があります。コミュニティで開発された dApp をより適切に

サポートするために、QDay チームは一連の基本的な DeFi dApp を実装し、テストネットとメインネットの両方の起動時にコミュニティに提供します。

- QDay Bridge - QDay Bridge は、クロスチェーン資産転送機能を提供する dApp です。wABEL とは異なり、QDay Bridge は、QDay と他の EVM 互換チェーン間の ERC20、TRC20、QRC20 トークンのブリッジに重点を置いています。
- QDay Swap - QDay Swap は、トークン交換機能を提供する分散型取引所 (DEX) dApp です。QDay がコールド スタート期間をできるだけスムーズに乗り越えられるように、QDAY、wABEL、および対応するステーブル コインの初期流動性は、QDay と Abelian の資金から提供されます。
- QDay ステーキング - QDay ステーキングは、QDAY のステーキング機能を提供する dApp です。Lido と同様に、ステーキングされた QDAY はバリデーターのコンセンサス メカニズムに使用され、報酬はバリデーター報酬から得られます (詳細については、トークノミクスを参照してください)。
- QDay Lending - QDay Lending は、QRC20 トークンの貸出および借入機能を提供する dApp です。これは、Aave や Compound などの既存の EVM 互換チェーンの貸出プロトコルに似ています。
- QDay Finance - QDay Finance は、QDay Bridge、QDay Swap、QDay Staking、QDay Lending などのすべての金融サービスを統合する統合 dApp です。QDay Finance の助けを借りて、ユーザーは簡単に DeFi 資産を管理し、統一されたインターフェースでさまざまな DeFi dApp に参加できます。

カテゴリー3: 量子耐性アプリケーション

QDay フェーズ 2 では、既存の dApp の耐量子バージョンを提供することに重点を置きます。これらの dApp は、コミュニティ向けの耐量子コントラクトおよび dApp のリファレンス実装として機能します。さらに、従来のウォレットが耐量子コントラクトおよび dApp とやり取りできるように、外部の耐量子署名ジェネレーターも提供します。フェーズ 2 はまだ計画の初期段階にあるため、耐量子アプリケーションに関する詳細は今後共有される予定です。

7. ロードマップ

QDay の主なマイルストーンは以下の通りです。

日付	マイルストーン
2024 年第 2 四半期	フェーズ 1 開発の開始
2024 年第 3 四半期	QDay テストネットの立ち上げ
2025 年第 1 四半期	QDay メインネットと ABEL ステーキングの開始
2025 年第 2 四半期	QDay Finance dApps のリリース
2025 年第 3 四半期	フェーズ 2 開発の開始

2026 年第 2 四半期	QDay テストネットのフェーズ 2 アップグレードのメジャー アップグレード
2026 年第 4 四半期	QDay メインネットのフェーズ 2 アップグレードのメジャー アップグレード

QDay メインネットの TGE に続いてエコシステムの強固な基盤を確立するために、QDay チームはブロックチェーン技術だけでなく、重要なエコシステム サービスと dApp の開発にも注力します。以下では、四半期ごとに詳細な計画を概説します。

2024 年第 2 四半期

1. QDay ノードの開発 - すべてのタイプの QDay ノード (バリデーター、ロールアップ ノードなど) を実装します。
2. ZK ロールアップの開発 - QDay から Abelian までの ZK ロールアップを実装します。

2024 年第 3 四半期

1. QDay テストネット (v1) - QDay テストネットの最初のバージョンは、完全な EVM 互換性を備えたアベルへのロールアップの組み合わせの実現可能性を証明するための POC (概念実証) テストネットです。
2. QDay Faucet (テストネット) - QDay Faucet は、ユーザーや開発者を含むコミュニティにテストネット トークンを提供するサービスです。
3. QDay Explorer (テストネット) - QDay Explorer (テストネット) は、QDay テストネットのブロックチェーン データ クエリおよび視覚化機能を提供するサービスです。

2024 年第 4 四半期

1. QDay テストネット (v2) - QDay テストネットの 2 番目のバージョンには、QDay エコシステムに本格的なテスト環境を提供するための包括的な dApp とサービスのセットが付属します。
2. QDay テストネット (v2) のテストネット ステーブル コイン - ステーブル コインは QDay エコシステムに不可欠です。テストネット ステーブル コインには実際の価値はなく、テスト目的でのみ使用されます。
3. QDay ブリッジ (テストネット) - QDay ブリッジは、クロスチェーン資産転送機能を提供するサービスです。テストネットでは、QDay テストネットといくつかの選択されたパブリック チェーンのテストネット間のステーブル コインのブリッジのみをサポートします。
4. QDay Swap (テストネット) - QDay Swap (テストネット) は、QDay テストネットのトークン交換機能を提供する分散型取引所 (DEX) dApp です。
5. QDay ステーキング (テストネット) - QDay ステーキングは、QDay ネイティブ トークンのステーキング機能を提供するサービスです。テストネット ステーキングの主な目的は、QDAY のステーキング、ステーキング解除、報酬分配プロセスをテストすることです。

2025 年第 1 四半期

1. EVM 互換性 - QDay メインネットは完全に EVM と互換性があります。
2. 量子耐性ロールアップ - QDay メインネットは、Abelian メインネットへのロールアップを実行します。
3. QDAY トークン配布 - QDAY トークン配布は、セクション 3 に記載されているトークノミクスに従って行われます。
4. QDay Explorer - QDay Explorer は、QDay メインネットのブロックチェーン データ クエリおよび視覚化機能を提供するサービスです。
5. QDay ブリッジ - QDay ブリッジは、QDay メインネットのクロスチェーン資産転送機能を提供するサービスです。メインネットでは、QDay メインネットと Tron のメインネット間のステーブルコインのブリッジと、Ethereum、BSC、Polygon などの豊富な EVM 互換チェーンをサポートします。
6. QDay Swap - QDay Swap は、QDay メインネットにトークンスワップ機能を提供する分散型取引所 (DEX) dApp です。
7. QDay ステーキング - QDay ステーキングは、QDay ネイティブ トークンのステーキング機能を提供する dApp です。QDay メインネットでは、QDAY 報酬のほとんどが QDAY ステーカーとバリデーターに分配されます。

8. Abelian ステーキング - Abelian ステーキングは、Abelian ネイティブ トークンのステーキング機能を提供するサービスです。

2025 年第 2 四半期

1. QDay メインネット (フェーズ 1) - QDay メインネット (フェーズ 1) は、次の機能を備えて開始されます。
2. QDay Lending - QDay Lending は、QRC20 トークンの貸出および借入機能を提供する dApp です。
3. QDay Finance - QDay Finance は、QDay Bridge、QDay Swap、QDay Staking、Abelian Staking、QDay Lending などのすべての金融サービスを統合する統合 dApp です。

2025 年第 3 四半期

1. QDay NFT マーケットプレイス - QDay NFT マーケットプレイスは、QDay メインネットに NFT 取引機能を提供する dApp です。
2. QDay 予測市場 - QDay 予測市場は、QDay メインネットに予測市場機能を提供する dApp です。
3. EVM 互換の量子耐性アカウントの開発 - フェーズ 2 開発の最初のマイルストーンは、完全な EVM 互換性を備えた量子耐性アカウントを実装することです。

2025 年第 4 四半期

1. QDay ウォレットの開発 - QDay ウォレットは、完全な EVM 互換性を備えた量子耐性アカウントをサポートする新しいタイプのウォレットです。
2. 量子耐性 dApp の開発 - 量子耐性 dApp は、量子耐性アカウントのサポートにより、従来のものからアップグレードされます。

2026 年第 1 四半期

1. フェーズ 2 テクノロジの統合 - 量子耐性アカウントを従来のアカウントと統合し、統合テストを実施します。

2026 年第 2 四半期

1. QDay テストネット (フェーズ 2) - 量子耐性アカウントと QDay ウォレットを使用して QDay テストネット (フェーズ 2) を起動します。
2. QDay テストネット上の量子耐性 dApp (フェーズ 2) - QDay テストネット (フェーズ 2) 上の QDay ウォレットで使用できる量子耐性 dApp を起動します。

2026 年第 3 四半期

1. 量子耐性 QDay ブリッジ (テストネット) - QDay テストネット (フェーズ 2) で量子耐性 QDay ブリッジを起動します。

2026 年第 4 四半期

1. QDay メインネット (フェーズ 2) - 量子耐性アカウントと QDay ウォレットを備えた QDay メインネット (フェーズ 2) を起動します。
2. QDay メインネット上の量子耐性 dApp (フェーズ 2) - QDay メインネット上の QDay ウォレットで使用できる量子耐性 dApp を起動します (フェーズ 2)。
3. 量子耐性 QDay ブリッジ (メインネット) - QDay メインネット (フェーズ 2) で量子耐性 QDay ブリッジを起動します。

8. 結論

QDay は、ブロックチェーン技術の先駆的な進歩であり、信頼性と実績のあるアーベル ブロックチェーンの基盤の上に構築された、世界初の量子耐性、EVM 互換のレイヤー 2 ソリューションを提供します。QDay は、先見性のある 2 段階の実装戦略を通じて、既存のブロックチェーン インフラストラクチャの長所を維持しながら、量子コンピューティングがもたらす重大な課題に対処します。

フェーズ 1 では、L1 支援ロールアップを通じて量子耐性台帳セキュリティを確立し、Abelian の量子耐性特性を活用しながら、EVM の完全な互換性を維持します。POS-over-POW コンセンサス メカニズムは、Proof of Work のセキュリティ上の利点と Proof of Stake の効率性を組み合わせて、回復力のあるセキュリティ モデルを作成します。量子耐性ロールアップの統合により、追加の保護層が提供され、安全なトランザクション処理と、検出された脅威に応じて操作を停止する機能が可能になります。

フェーズ 2 では、アカウント レベルで量子セキュリティを強化し、従来のシステムとの下位互換性を維持しながら、量子耐性のあるアカウント、ウォレット、スマート コントラクトを導入します。イノベーションと互換性のこの思慮深いバランスにより、既存のユーザーと開発者にとってスムーズな移行が保証され、必要なユーザーには強化されたセキュリティ機能が提供されます。

主要な DeFi アプリケーションやクロスチェーン ブリッジを含む QDay の包括的なエコシステム アプローチにより、完全な量子耐性ブロックチェーン環境が確立されます。バランスの取れた配布戦略を特徴とするプラットフォームのトークンノミクス モデルは、ネットワーク全体で幅広い参加を促進しながら長期的な持続可能性を保証します。

将来を見据えて、QDay の 2024 年から 2026 年までのロードマップは、徹底したテスト、段階的な展開、エコシステムの開発を重視し、完全な実装に向けた明確な道筋を示しています。この系統的なアプローチとプラットフォームの革新的な技術的特徴を組み合わせることで、QDay は量子耐性ブロックチェーン技術の先駆者としての地位を確立し、進化するブロックチェーン環境における現在のニーズと将来の課題の両方に対応できるようになります。

量子耐性、スケーラビリティ、実用的な使いやすさを組み合わせた QDay は、単なる漸進的な改善ではなく、ブロックチェーン技術の変革的な飛躍を表しています。分散型アプリケーションとデジタル資産のより安全で持続可能な未来への道を開きます。

9. 参考文献

---

[1]アベルアン公式サイト https://www.pqabelian.xyz/

[2] アベルのドキュメント。https ://community.pqabelian.io/guide/get-started

[3] アベル財団 (2023 年 5 月)。ポスト量子ゼロ知識 *(PQZK)* ブリッジ。https ://download.pqabelian.io/release/docs/Abelian PQZK Bridge.pdf

[4] アベルホワイトペーパー。https ://community.pqabelian.io/guide/abel-whitepaper.html

[5] アベル財団 (2025 年 1 月)。アベル改善提案 *0011:* 決定論的アカウントを生成するための記憶コード。https ://github.com/pqabelian/aips/tree/master/aips

[6] ファビアン・フォーゲルシュテラー、ヴィタリック・ブテリン。（2015 年 11 月）。 *ERC-20:* トークン標準。 https://eips.ethereum.org/EIPS/eip-20

[7] ポリゴン zkRollup。https ://docs.polygon.technology/cdk/concepts/zk-vs-optimistic/?h =polygon+zk+rollups#zero-knowledge-rollups

[8] 中本 誠（2008）「ビットコイン：ピアツーピア電子キャッシュシステム」https://bitcoin.org/bitcoin.pdf

[9] Wood, G. (2014). *Ethereum:* 安全な分散型汎用トランザクション台帳。*Ethereum* イエローペーパー。https ://ethereum.github.io/yellowpaper/paper.pdf

[10] イーサリアム財団。ERC *-20* 標準。https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

[11] イーサリアム財団。分散型アプリケーション（*dApps*）。https://ethereum.org/en/dapps/