

PKTネットワーク

ケイレブ・ジェームズ・デリーズル (cjd@cjdns.fr), ジェームズ・バーガー (jesse@radicalstudios.com)

2021年2月1日

バージョン1.0

<https://pkt.cash>

概要

インターネットは、20世紀に発明された中でも最も影響力のある物の1つである。しかし、世界の多くの地域において、インターネットは、独裁的な機関によってアクセスが制限され、世論に影響を与え、自由を制限する形で制御されている。このホワイトペーパーでは、インフラストラクチャの運用をインターネットサービス提供から切り離すためのフレームワークを実現するための、新たなネットワークモデルを提案する。このモデルは、自律システムとピアリング関係の実証済みの概念を土台とし、グローバルメッシュネットワーク上の仮想ドメインに移動し、ネットワーク資金を調達するために、帯域幅のハード・ブルーフ・オブ・ワークに基づくPKTブロックチェーンを導入する。次に、インターネットサービスプロバイダー (ISP) がインフラストラクチャオペレーターからリソースを借り上げる分散型帯域幅市場を導入することにより、両ドメインでの競争が促進されるシステムとなっている。

1. 導入

インターネットは基本的に、共有される物理的インフラストラクチャ上で帯域幅をリースする多数の独立した組織で構成される。このような組織は、自発的な関連付けを通じ、ネットワークにおける任意の2人のユーザー間での生の非独断的なデータ転送を促進する[1]。このシステムは、特に競争が激しく、ポイント・ツー・ポイントの帯域幅が広く利用できるインターネットコアで非常に効果的であることが証明されているが、世界中の多くの地域で、インターネットアクセスは、依然としてインフラストラクチャを所有および運用する機関によって制御されているのである。この独占的状況を緩和するために、多くの国や地域でローカルループ・アンバンドリングの方針が定められ、独占通信会社がラストマイルインフラストラクチャへのアクセスを競合他社と共有することが求められている[2, 3]。とはいえ、ローカルループ・アンバンドリングの方針はサービスの質を向上させる一方、インフラストラクチャへの投資を鈍化させ、アクセスを制限していると批判されているのも事実である[4]。

インターネットアクセスの独占により一般ユーザーがアクセスできる情報が制限されるとき、間違いなく、市民の自由が侵食されていると言えるだろう[5]。さらなる問題点としては、社会自体を包み込むまでに広がる可能性のある、明確に定義されない「敵」に対するフルスペクトラムドミナンスを求める大量監視の効果が挙げられる[6, 7]。国有化されたインターネットが、政局が安定する限り高品質で低コストのサービスを提供できる可能性は否定できないが、言論や報道の自由に対する権力の集中化を生み出し、政治的混乱の際は壊滅的な悪影響を及ぼす可能性が予想される。

ここで求められるのは、一般ユーザーがインフラストラクチャプロバイダーとサービスプロバイダーの両方になるための障壁を下げるシステムである[8,9]。つまり、最小限の技術的知識でインターネットアクセスを提供するよう市民にインセンティブを与える新しいネットワークモデルだ。これにより、インターネットインフラストラクチャを集合的に分散化、帯域幅あたりのコストを削減し、世界中の農村部と都市部のインターネット接続のあり方を改善するよう、人々の行動を促すことができるだろう。

1.1. ホワイトペーパーの構成

当ホワイトペーパーのセクション2ではPKTネットワークアーキテクチャを、セクション3-5ではcjdnsおよびルートサーバーとフリーティアの統合について説明する。次に、PKTブロックチェーン設計の概要、新しいインターネットインフラストラクチャの展開を促進する新しい帯域幅のハード・プルーフ・オブ・ワークについて（セクション6）想定されるルーティングデバイスハードウェア（セクション7）と分散型帯域幅市場（セクション8）の高レベルの技術的説明を行う。最後に、分散型帯域幅市場と参入を促進するテクノロジーについて（セクション9）結論で締めくくる。

2. PKTネットワークアーキテクチャ

PKTネットワークは、誰もがISPになれる状態を促進し、世界中のインターネットアクセス分散化を推し進めるよう設計されている。ISPの技術的側面を仮想化するために、インフラストラクチャオペレーターの場合固有の役割を分散させながら、エッジポイントとクラウドISPの概念を導入し、エッジポイントは、個人、企業、またはコミュニティグループによって一般に公開された状態で運営され、PKTネットワークへのアクセスを提供するデバイスとして機能する。クラウドISPは、従来のISPとVPNプロバイダーを混合した、所謂ハイブリッド型であり、エッジポイントの帯域幅リースを集約および仲介し、顧客にインターネットサービスを提供する上での管理を担う。PKTネットワークのクラウドISPシステムは、仮想ルーターリースと帯域幅リースの2種類の仮想資産を中心に設計されており、仮想ルーターリースは、一定期間、ルーティングデバイス内のリソースに対する一時的な権利を意味する。帯域幅リースは、2つの物理的ルーティングデバイス間のリンクを介した一定期間の最小帯域幅を保証し、従来のTCP / IPおよびボーダーゲートウェイプロトコル（BGP）ネットワークングモデル[1]と同様に、PKTネットワークはクラウドISP間のプロバイダー、顧客、ピア関係を促進する。このような関係は、1) パケットの優先度、2) カスタマービットの2つの主要コンポーネントを介して実現する。

2.1. パケット優先度

従来のネットワークでは、通常プロバイダーは、顧客が送信できる帯域幅の量を制御するために、低速のネットワークリンクを提供することでネットワークの輻輳を緩和している。ただし、利用可能なネットワークリソースが十分に活用されないことが問題点として挙げられているのが実情だろう。PKTネットワークでは、ネットワーク容量がアイドル状態のときにパケット送信を拒否しないように、パケットの優先度は、利用可能なインフラストラクチャを介したデータ送信を最大化するように設計されている。

パケットの優先順位付けにおいては、パケットヘッダーの優先フィールドとmax-priority-bandwidthと呼ばれる設定可能な要素を使用する。max-priority-bandwidthを構成できるCloud ISPは、毎秒帯域幅リースを通過できる最大量のpriority-bandwidth（優先度の単位にキロバイトを掛けたもの）を設定できる。設定された制限よりも多くの優先帯域幅が帯域幅リースを通過する場合、ルーティングデバイスはトラフィックの優先度を動的に引き下げ始め、トラフィックを不必要に排除することなくクラウドISPネットワークを保護することが可能になる。パケットの優先度は、リンクが過負荷になった場合にクラウドISPが切り落とすパケットを選択する際に参照される。

構成可能なmax-priority-bandwidthは、事実上、特定のネットワーク内の帯域幅の共有である。Cloud ISPのネットワークが過負荷になり、各顧客のmax-priority-bandwidthが同等になると、渡されたパケットシェアも同時に同等となる。ただし、1人の顧客が他の顧客の最大優先帯域幅の1/10しか持たない場合、1/10のトラフィックしか通過できない。優先度が乗法的に削減されるため、各顧客のトラフィックの相対的な優先度は、あるクラウドISPから別のクラウドISPに渡される際にも保持される。

2.2. 顧客ビット

PKTネットワークでは、TCP / IPネットワークオペレーターがトラフィック交換方法を改善するピアリング機能を提供する。従来であれば、2つのネットワーク事業者がピアリング契約を締結する場合、顧客のトラフィックを直接交換することに同意するが、他のトラフィックが相互に伝送されることはない。このタイプのピアリング契約はお互いにとり有益であるため、通常、いかなるタイプの金銭的和解も介在しない[1]。ただし、一方の当事者が他方の当事者の顧客ではない宛先にトラフィックを送信する場合、ルーターはそのトラフィックをアップストリームプロバイダーに転送する。このタイプのトラフィックをピアユーザーに送信すると、有料接続が使用され、結果的に盗むことになるのだ。TCP / IPインターネットのネットワーク事業者には、これを完全に防止するテクノロジーがないため、ピアリングにおける軽率な行動をケースバイケースで処理する必要がある。PKTネットワークでは、1) clear-customer-bitと2) deprioritize-non-customerの2つの構成可能要素とともに、パケットヘッダーに1ビットの「customer」フィールドを含めることでこの機能を改善する。

clear-customer-bit構成可能セットを使用した帯域幅リースの着信トラフィックではすべて、顧客ビットがクリアされる。この仕様は、問題の帯域幅リースがネットワークをピアまたはプロバイダーに接続することを示すためのものである。構成可能なdeprioritize-non-customerは、帯域幅リースの発信トラフィックに影響を与えるため、顧客ビットが設定されていない場合、パケットの優先度は指定された値以下に低下する。同じクラウドISPによって制御される2つの仮想ルーター間の帯域幅リースには、これらの構成可能なもののいずれも設定されない。

3. CJDNS

PKTネットワークのアーキテクチャを理解するには、まずcjdnsと呼ばれるオープンソースネットワークテクノロジーを理解しておく必要がある。

Cjdnsは、簡単に構成できる分散型メッシュネットワークを作成できるオープンソースのメッシュルーティングプロトコルであるが、敵対する参加者に直面した場合でも、それに対処できるだけの堅牢なセキュリティプロパティを備えている。Cjdnsでは、常時オンのエンド・ツー・エンド暗号化と生成されたIPv6アドレスの指定が定められている。各IPv6アドレスは事実上キーフィンガープリントであるため、すべてのcjdnsトラフィックは、PKIまたは他の同様の中央機関を必要とせずに暗号化および認証可能となる。IPv6アドレスはfc00::/8の一意のローカルアドレススペース[10]にあり、アドレス衝突のリスクを無視できるほど大規模なものである。

Cjdnsは、コンパクトソースルーティングと呼ばれるテクノロジーを導入し、宛先のIPアドレスを含む全データパケットの代わりに、到達するためのルートが用意されている。加えてIPアドレスとほぼ同等のサイズでこのルートのコンパクトな形態が使用される。「どこに行きたいか」を「どのように行きたいか」に置き換えることで、cjdnsは、データが必要な場所に到達するための方法を最適化している。Cjdnsは2011年から開発が続けられており、Hyperboriaネットワークで稼働している[11]。

4. ルートサーバー

ルーターの効率的な仮想化をサポートするために、ルーティングプロセスの意思決定は、各エンドユーザーのクラウドISPに属するルートサーバーによって調整される。ルートサーバーは、**cjdns**コンパクトソースルーティングを使用して、PKTネットワークを介して事前に計算されたパスを提供する。パケット転送の決定は**cjdns**にて事前に決定されているため、ルーティングデバイスは実行のために状態を維持する必要はない。クライアントデバイスがPKTネットワークを介してパスを学習するために、DNSルックアップと同様にソースルートの解決策が照会され、これがルートサーバーに対して実行される。

PKTネットワークモデルでは、ネットワーク内のすべてのデバイスが何らかのルートサーバーとやりとりを行う。ルートサーバーはソフトウェアとして実装されているため、ルートを解決するための新規テクノロジーを時間の経過とともに改善できる仕様である。デバイスに既知のルートサーバーがない場合は、DHCPを使用してDNSサーバーを検索するのと同様に、デバイスは最も近いネイバーに照会を行う。ネットワーク内デバイスは、必要に応じてルートクエリを実行するだけでなく、直接接続されているすべてのデバイスID（キーフィンガープリント）、リンク品質、帯域幅リソース関連情報を含む、定期的な署名付きのタイムスタンプを伴うメッセージも送信する。このようなメッセージは署名済みであるため、メッセージの1つを所有するルートサーバーは、すぐに検証可能となる。**cjdns**コンパクトソースルーティングとルートサーバーの組み合わせにより、クラウドISPはソフトウェア定義ネットワーク（SDN）を使用できるようになり、ネットワークを制御するための優れた柔軟性を確保できるのだ。クラウドISPは、仮想プライベートネットワーク（VPN）サービスプロバイダーから進化を遂げ、ローカルエッジポイントを介してインターネットアクセスの提供を開始できるようになることが期待されている。

5. フリーティア

PKTネットワークを使用する場合、クラウドISPは、帯域幅リソースと仮想ルーターリソースを使用してネットワークを構築できる。これにより、物理的リンクが飽和状態にならない限り、パケットが放棄されることはない。加えて、すべての物理的リンクに利用可能なフリーリソースを用意することが推奨される。これはつまり、帯域幅がゼロであることが保証された、ハードワイヤードの誰にも所有されていない帯域幅リソースである。すべてのルーティングデバイスには、すべての物理的リンクのフリーリソースに常に相互接続されている、かつ非所有の仮想ルーターが必要となる。これにより、インフラストラクチャがアイドル状態になった場合でも帯域幅を無料で使用できるフリーティアを確保できる。

私たちは、ユーザーによる支払い不能のためにアクセスを拒否しながらリソースを浪費することは、非倫理的かつ非効率的であると考えている。フリーティアは、以下2つの主要なサービスをサポートする。1) クラウドISPが帯域幅リソースを購入する前に帯域幅、遅延、およびジッターのテストを実行2) 偶発的な設定ミスからの保護。ルーティングデバイスが正しく構成されておらず、リソース所有者がアクセスできなくなった場合には、フリーティアにアクセスして、該当デバイスのオンボードコンピューターにアクセスできる仕様となっている。フリーティアの存在は、本質的に幅広いタイプの障害をフェールクローズからフェールオープンに変えることになる。

6. PKTブロックチェーン

PKTネットワークはブロックチェーン[12]を利用することで、ノードがエッジポイントおよびクラウドISPになるように経済的インセンティブを与える。PKTは、ビットコインのコードベースを基本とし、ビットコインのSHA-256ハッシュアルゴリズムを、世界初の帯域幅ハード・プルーフ・オブ・ワークである

PacketCryptに置き換える。加えて、インターネットインフラストラクチャやネットワークテクノロジーなど、開発資金調達のためのネットワークスチュワードという新しいメカニズムを導入している。

6.1. PKTキャッシュ

ノードは、帯域幅とCPU時間を消費、暗号化を実行し、PKTキャッシュと呼ばれる新しいPKTコインを流通させることでネットワークをサポートする。PKTキャッシュは、マイナーがエッジでネットワークスループットを向上させるインセンティブを提供する。ビットコインよりも10倍高速であり、コインあたり10億原子単位をわずかに超える1分あたりのブロック時間でマイクロトランザクションのスケラビリティを拡張するように設計されている。63年という期間で、全く中央発行機関が存在しない状態で合計60億のコインが発行される。ブロック報酬は繰り返し間引きされ、100日ごとに分配が10%減少し、スムーズな発行の減衰を保証できる仕組みである。

6.2. PacketCrypt

PacketCryptのプルーフ・オブ・ワークにより、プロセッサに代わりにマイナー間の通信を代用できるため、最適なマイニング戦略は帯域幅を大量に消費できる[13]。マイニングは、アナウンスマイニングとブロックマイニングの2つの段階に分けられ、アナウンスマイニングでは、CPU作業が消費され、効率的に圧縮できない構造を持つ1KBのアナウンスが多数作成される。ブロックマイニングにおいては、マイナーは収集したアナウンスのマークルツリールートに事前にコミットしてから、収集したアナウンスに対してメモリハードマイニングアルゴリズムを実行する。ハッシュサイクルごとに4つのランダムなアナウンスにアクセスし、ブロックのマイニングが成功した場合、アクセスしたアナウンスと、プレコミットメントにリンクするマークルブランチを提供する。したがって、マイナーが所有を主張するアナウンス数が実際に存在したことを統計的に証明することになる。これにより、ブロックマイナーがアナウンス所有を偽ることが不可能になる。アナウンスは使用できなくなるまで価値が低下するため、ブロックマイナーは、アナウンスマイナーに新しいアナウンスの安定した供給に対して支払うように奨励され、アナウンスマイニングアルゴリズムは、ランダムプログラムを使用して、GPUまたはASICマイニングよりもCPUを優先することにより、集中型のファームリングではなく、アイドル状態のリソースでのマイニングが促進される。ブロックマイニングアルゴリズムはメモリのハードのみに依存しているため、GPUハードウェアはブロックマイニングの優れたターゲットになる。どちらのアルゴリズムも暗号化技術を利用しているため、高性能のマイニングデバイスはVPNパケットの暗号化にも貢献できる。

プルーフ・オブ・ワークによって発行される仮想通貨は、関連する作業に対する本質的かつ人工的な市場の需要を生み出す。静的経済分析では、プルーフ・オブ・ワークはリソースを浪費するが、実体経済では、需要が供給を後押しし、最終的にはコストの低下へとつながる。PacketCryptは、帯域幅に対するバックグラウンド需要を生み出すように設計されており、ネットワークインフラストラクチャへの投資が増加し、将来的に帯域幅のコスト削減が期待される。

帯域幅のハードマイニングとマイナーコラボレーションは結果的に、分散型の低遅延ネットワーク接続と暗号化スケリングを含むネットワーク効果を促進し、このネットワーク効果は、分散型帯域幅市場を含む商品市場をサポートするだけでなく、cjdnsにも貢献する（セクション8）。

6.3. ネットワークスチュワード

PKTは、ネットワークスチュワードをブロックチェーンデザインに実装し、新しい各ブロックからPKTキャッシュの20%を受け取るアドレスとなる。PKTエコシステムの開発に資金を供する目的として存在し、プルーフ・オブ・ステーク・ベースの投票によって変更可能である。投票は、トランザクション出力に追加

のメタデータを「マーク」することで実行される。アクティブな投票とは、そのようなメタデータを含む未使用のトランザクションを指し、トランザクション出力を使用すると投票が取り消される。各投票のメタデータには、賛成票と反対票の2つのPKTアドレスを付加することができる。現状のネットワークスチュワードに対する投票の合計が、これまでに作成されたすべてのPKTの50%を超えたとき、コンセンサスルールにより、投票数が最も多いPKTアドレスが特定され、そのアドレスが新しいネットワークスチュワードとなる仕組みである。

ネットワークスチュワードは、プロジェクトの提案が1人の参加者（申請者を含む）にとって不当に有益であってはならず、これがPKTエコシステム開発に資金を供することになる。この競争力のあるリサーチモデルは、プロジェクトに対する予算の呼び出しを随時生成し、ネットワークスチュワードの基準をベースにプロジェクトの提案を相互に評価する。ネットワークスチュワードポリシーでは、受け入れられたすべてのプロジェクトがオープンソースソフトウェア、公開ドキュメントの作成を中心に構成され、PKTネットワークのインフラストラクチャの成長を促進することが奨励される。進行中の資金提供を受けたプロジェクト、完了した提案、拒否された提案はすべて、ネットワークスチュワードのgitリポジトリに公開される[12]。ネットワークスチュワードがPKTキャッシュ作成日から90日以内にウォレットアドレスに保持されている資金を展開しない場合、コインは焼却され、各プロジェクトの提案では、それがもたらす価値が、焼却されるコインよりもPKTネットワークに大きな利益をもたらすように評価される必要がある。

7. ルーティングデバイス

PKTネットワークのスケラビリティには、高性能の細分化可能なルーティングデバイスの開発が必須である。このハードウェアの革新は、PKTネットワークのスケラビリティを促進し、支える。PKTネットワークハードウェア実装最適化の基本要件を決定するには、このようなデバイスをシリコンに実装することの複雑さを理解し、デバイスを通るデータパケットの流れを調査する必要がある。

パケットは物理的ネットワークリンクの1つを介してルーティングデバイスに流入し、着信パケットにはタグが付けられ、属する帯域幅リースとパケットの優先度が表示される。パケットが経由する最初の処理は、max-priority-bandwidthに従った再優先順位付けであり、これには、IIRフィルターなどの帯域幅や優先度の指標が必要になる。

デバイスは、コンパクトな送信元ルートラベルを解析して、パケットの送信先となる帯域幅リースを決定する。次にデバイスはコンパクトソースルートラベルを更新してcjdnsスイッチアルゴリズムを使用することでパケットの発信元を表示する[11]。Cjdnsでは、物理的インターフェース番号を計算し、送信に使用する帯域幅リースタグを決定するために、小さなインデックステーブルにアクセスする必要がある。

ルーティングパスが解決されると、パケットはスイッチ回線へと移行する。クロスバーやCLOSなどの設計はすでに商用可能なレベルとなっている[14、15、16]。パケットがデバイスを離れる前に、パケットを放棄する必要があるかどうかは決定される。このプロセスはプライマリレベルが発信帯域幅リースの保証された帯域幅をベースにしており、セカンダリレベルが宣言されたパケット優先度に基づく二層のトークンパケット設計を使用して実現する必要がある。ちなみにこれは、シンプルなイーサネットスイッチで使用される一般的なテクノロジーである。

8. 分散化帯域幅市場

ルーティングデバイスがPKTネットワークに接続されると、即座に1) 各ネットワーク接続で利用可能な帯域幅とその他の指標測定、アナウンスを開始2) 各ネットワーク接続と仮想ルーターの帯域幅を表すトーク

ンを作成3) 分散型帯域幅市場での販売用にトークン提供が始まる。このトークンは、あらゆる参加者が売買できるようになり、トークン所有者は誰でも、署名済みの構成要求をルーティングデバイスに送信することで、基盤となる帯域幅と仮想ルーターを使用できる。これを可能にするには、ほぼ費用ゼロのトークン発行とほとんど摩擦のない取引機能を備えた分散型帯域幅市場を構築する必要がある。ほとんど摩擦のない資産取引技術は、HTLCアトミックスワップ[17]を使用してすでに実装可能な状態であり、現在OpenDEXプロジェクト[18]によって活用されている。現状、私たちはほぼ費用ゼロのトークン発行を可能にするために、複数種類の選択肢を検討している。

8.1. TokenStrike

トークン化された帯域幅とルーターリソースには、「発行者と同等に有益」という興味深い特性がある。というのも、最悪の場合、発行者はルーティングデバイスをオフにすることができるからである。このプロパティは、発行者が秘密裏にプロトコルに違反できない限り、トークントランザクションのグローバル検証は発行者による検証よりも安全ではないことを意味する。ここでTokenStrike [19]と呼ばれる新しいトークン標準を提案したい。この標準においては、発行者によるほとんどすべての不正アクティビティが検出され、発生したことが証明されるように、発行者によって署名されたプライベートブロックチェーンを使用して各トークンが描写される。TokenStrikeはHTLCと互換性のある設計であり、TokenStrikeベースのトークンをTokenStrikeトークンまたはその他のライトニングネットワークアセットと交換できる。

8.2. オープントランザクション

スケーラブルなトークントランザクションには、さらに有望な技術が存在する。公証サーバーのプールを使用してコインまたはトークントランザクションを検証し、マルチシグネチャを使用してそれに署名するオープンランザクションである[20]。オープンランザクションとTokenStrikeプロジェクトは、分散型帯域幅市場に並列するかたちでトークン発行ソリューションを提供することが期待される。

8.3. RGB - カラーコイン

最後に、帯域幅とルーターリソースを表すためにカラーコインを活用できると考えている。カラーコインとは、トークン発行者が申告[21]によって特別な意味付けができる、微量の仮想通貨を表す。カラーコインでは、プライバシーのないブロックチェーンにおいて、コインをある当事者から次の当事者まで追跡できるという事実依存しているが、イーサリアムベースのトークン同様、取引するにはグローバルな検証が必要となる。現在、RGBプロジェクト[22]は、ライトニングネットワークを使用してカラーコイン取引を可能にする技術の研究を続けており、私たち自身ではRGBを使用する技術に取り組んではいないものの、3つ目の候補として注目している。

結論として、私たちはほぼ費用ゼロのトークン発行という問題は解決可能であり、PKTネットワークは分散型帯域幅市場にこのようなテクノロジーを応用できると確信している。HTLCで行われた作業をベースにし、選択された技術がどの技術であれ、トークン化された帯域幅とルーターリソースを、ビットコイン、ライトコイン、イーサリアムなどの他のHTLCサポートブロックチェーン上のアセットとすばやくアトミックスワップできると考えている。最終的に参加者がトークン化された帯域幅、VPN、ルーターリソースを取引するために、集中管理組織や取引所を必要とせず、完全に分散化されたマーケットプレイスが出現することを目指している。

9. 結論

インターネットがコアデータセンターを超えてさらに拡張するためのスケーリングソリューションとして、PKTネットワークとPKTブロックチェーンを導入した。PKTネットワークは、インターネットルーティング

とパケット送信効率を向上させるエンド・ツー・エンドの暗号化技術の進歩によって生まれたcjdnsを利用した分散型ネットワークである。PKTネットワークアーキテクチャは、エッジポイントとクラウドISPがエッジでインフラストラクチャを運用することを奨励するものであり、PKTネットワークのフリーティアにより、リソースが使用されていない場合でもインターネットアクセスが常に利用可能になる。このホワイトペーパーでは、帯域幅の人工的需要を生み出すPacketCryptプロトコルと、ユーザーがエッジでインターネットインフラストラクチャを運用するための経済的インセンティブを提供するPKTCashについて、そして決済、帯域幅リースの提供、および市場の伝播にブロックチェーンテクノロジーを活用する分散型帯域幅市場について説明した。高速データ伝送、暗号化、VPNなどの日常における使用に関する技術的進歩をさらに最適化するためのルーティングデバイスは、PKTネットワークの関連性を強化し、インターネットアクセス、ネットワーキング、およびデータ通信の低価格化、容易なアクセス、分散化を保証する。

将来のインターネットインフラストラクチャは、多くの小規模事業者に所有および運営され、個人が最大グループを構成し、零細企業が**2番目に大きなグループ**を構成することが予想される。衛星ベースのインターネットアクセス分野におけるイノベーションは、世界中のインターネットの可用性に大きな影響を与えるはずである。しかし、隣人の家からのWi-Fi接続など、短距離通信リンクは、衛星通信よりも常に効率的である事は間違いない。大陸間通信の場合、インフラストラクチャのコスト削減に基づいて衛星が最も効率的なソリューションになると考えられるが、技術が進化するにつれて、地上シールドケーブルが自由空間通信よりもはるかに高い処理能力に達する可能性を排除することはできない。現時点で断言できるのは、インターネットの進化には分散型帯域幅市場の存在が不可欠であり、PKTネットワークのオープンプロトコルと相互運用性に対するニーズが高まっているという事実である。

出典

- [1] Woodcock, B. and Adhikari V. (2014). *Survey of characteristics of internet carrier interconnection agreements*. Packet Clearing House. <https://www.pch.net/resources/papers/peering-survey/PCH-Peering-Survey-2011.pdf>
- [2] de Bijl, P., & Peitz, M. (2005). Local loop unbundling in Europe: Experience, prospects and policy challenges. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.690582>
- [3] Ford, G. S., & Spiwak, L. J. (2013). Lessons learned from the U.S. unbundling experience. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2378925>
- [4] Nardotto, M. (2016). Local loop unbundling in the UK does not affect broadband penetration - but it does lead to better service. *DIW Economic Bulletin*, 6(28), 311-317.
- [5] Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? : Illusions of a borderless world*. Oxford University Press.
- [6] Munkholm, J. L. (2020). The pursuit of full spectrum dominance: The archives of the NSA. *Surveillance & Society*, 18(2), 244-256. <https://doi.org/10.24908/ss.v18i2.13266>
- [7] Shaw, I. G. R. (2016). *Predator empire: Drone warfare and full spectrum dominance*. University of Minnesota Press. <https://books.google.com/books?id=Gil0DwAAQBAJ>
- [8] Bourreau, M., & Doğan, P. (2004). Service-based vs. facility-based competition in local access networks. *Information Economics and Policy*, 16(2), 287-306. <https://doi.org/10.1016/j.infoecopol.2003.05.002>

- [9] Briglauer, W. (2014). The impact of regulation and competition on the adoption of fiber-based broadband services: Recent evidence from the European Union member states. *Journal of Regulatory Economics*, 46(1), 51–79.
- [10] Hinden, M. R., & Haberman B. (2005). Unique local IPv6 unicast addresses, RFC 4193, *RFC Editor*, <https://doi.org/10.17487/RFC4193>
- [11] *Cjdns project page*. <https://github.com/cjdelisle/cjdns>. 2020.
- [12] *Pktd project page*. <https://github.com/pkt-cash/pktd/>. 2020.
- [13] DeLisle, C. J., & Seesahai V. (2020, September 4). *PacketCrypt*. <https://pkt.cash/PacketCrypt-2020-09-04.pdf>
- [14] Ofori-Attah, E., & Agyeman, M. O. (2017, January 25). *A survey of low power NoC design techniques*. Proceedings of the 2nd International Workshop on Advanced Interconnect Solutions and Technologies for Emerging Computing Systems, Stockholm, Sweden. <https://doi.org/10.1145/3073763.3073767>
- [15] Sewell, K., Dreslinski, R. G., Manville, T., Satpathy, S., Pinckney, N., Blake, G., Cieslak, M., Das, R., Wenisch, T. F., Sylvester, D., Blaauw, D., & Mudge, T. (2012). Swizzle-switch networks for many-core systems. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2(2), 278-294. <https://doi.org/10.1109/jetcas.2012.2193936>
- [16] Xia, Y., Hamdi, M., & Chao, H. J. (2016). A practical large-capacity three-stage buffered clos-network switch architecture. *IEEE Transactions on Parallel and Distributed Systems*, 27(2), 317-328. <https://doi.org/10.1109/tpds.2015.2408614>
- [17] Herlihy, M. (2018, July 23-27). *Atomic cross-chain swaps*. Proceedings of the 2018 ACM symposium on Principles of distributed computing, United Kingdom. doi:10.1145/3212734.3212736
- [18] *OpenDEX project page*. <https://opendex.network/>. 2020.
- [19] *TokenStrike project page*. https://github.com/pkt-cash/ns-projects/blob/b0874ee/projects/2020_07_25_tokenstrike.md. 2020.
- [20] Odom, C. (2015). *Open-transactions: Secure contracts between untrusted parties*. <http://www.opentransactions.org/open-transactions.pdf>
- [21] Rosenfeld, M. (2012, December 4). *Overview of colored coins*. Bitcoil. <https://bitcoil.co.il/BitcoinX.pdf>
- [22] *RGB project page*. <https://rgb-org.github.io/>. 2020.