NKN：スケーラブルな自己進化・自己インセンティブ型分散ネットワーク

NKN ラボ

www.nkn.org

(2018 年 3 月 13 日バージョン：1.0)

NKN（New Kind of Network）は、スケーラビリティ、自己進化性、自己インセンティブを特徴とする新世代のブロックチェーンネットワークインフラストラクチャです。NKN は、ダイナミズムと効率の両面からセル・オートマトン（セル・オートマトン）のメソドロジー[1、2]を導入して、ネットワークの分散化と自己進化に取り組みます。NKN は、ネットワークコネクティビティとデータ送信容量を、斬新で有用なプルーフ・オブ・ワーク（PoW）によってトークン化します。NKN は、ビットコイン[3]とイーサリアム[4]が計算能力を分散するのと同様に、また IPFS [5]と Filecoin [6]がストレージを分散するのと同様に、ネットワークリソースの分散化に重点を置いています。これらはともに、次世代のブロックチェーンシステムのための、インターネットインフラストラクチャの３つの柱を形成します。NKN は最終的にネットワークの、分散、効率、均質さ、堅牢さ、安全さをさらに高め、健康で安全でオープンなインターネットを実現します。

Contents

1. 課題

インターネットは元のビジョンと精神を失いつつあります。例えば、すでにネットワーク中立性は失われています[7]。スペクトルと帯域幅は効率的に利用されません。情報は断片化され、検閲されています。プライバシー保護は限定的です。

これらの問題は、ネットワークが改革を必要としていることを示しています。既存のソリューションは、次の理由により次世代のブロックチェーンシステムには適していません。

- 効率を向上させるための集中化されたアプローチを活用している。
- ネットワークのスケーラビリティを犠牲にしてコンセンサスをスピードアップしている。
- ノードの参加率を制限する、または「安全性」を高めるために、承認を要求する。
- 数学や技術によって解決すべき問題を、純粋に金銭的な動機や、信頼できる第三者を使って解決している。

1.1. P2P ネットワークの限界

ピアツーピア (P2P) ネットワークは現在、いくつかの大きな課題に直面しています。しかし、これはNKN にとってのチャンスでもあります。

最初の静的ネットワークトポロジは、不具合や悪意のある攻撃に対して脆弱です。第二に、ネットワーク接続およびデータ送信のための経済的な自己重視スキームは存在しません。最後に、ネットワークスケーラビリティは、制御性を高めるために大きく犠牲にされています。これらはすべて図 1 に示すようにNKN によって解決されるべきものです。

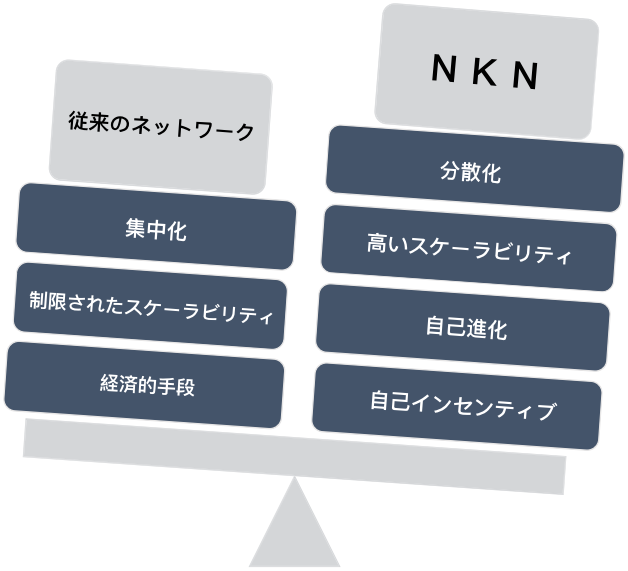

図 1. 既存のソリューションと NKN の機能比較

1.2. リソースの活用

信頼性が高く、安全で多様なインターネットは誰にとっても不可欠です。しかし、グローバルなコネクティビティと、情報伝達を提供する場合、現在のネットワークには大きな非効率性が存在します。ネットワークにパッチを当てるだけでなく、ネットワークを根本的に再構築する時が来ました。完全に分散された匿名のピアツーピアシステムは、産業と社会の効率性、持続可能性と安全性の向上という点で大きな可能性を秘めています。

1.3. ネット中立性＆フラグメンテーション

連邦通信委員会 (FCC) が 2017 年末までにネットの中立性に関するルールを削除する措置を承認しました。それ以降、市場を独占する巨大電気通信業者への依存から脱却し、分散型の安いローカルインターネットインフラストラクチャを構築する必要性はますます高まっています。無制限のプライベートインターネットアクセス環境は、無限の攻撃と閉塞の流れの中で持続不可能になっており、選択的かつ偏りのある情報伝播につながります。

適切なインセンティブ付与スキームがなければ、一定で安全な情報伝播チャネルを維持することはほと

んど不可能です。

さらに、様々な理由から、インターネットはより断片化しています。これは分離を悪化させるだけでなく、科学技術、経済の革新に悪影響を及ぼします。

2. ビジョン

NKN はネットワーク技術とビジネス全体に革命を起こそうとしています。NKN は、1 兆ドルの通信サービス事業で、中央集権的な存在がない、Uber または Airbnb になることを望んでいます。NKN はビットを解放し、理想的なインターネットを構築したいと考えています。

2.1. NKN の目的

NKN は以下の目標を設定します：

- どのノードも、この完全にオープンなネットワークに任意の場所から接続できます
- ネットワーク共有を促進する
- ネットワーク層の革新によるネットの中立性の確保
- 常にネットワークを開いてスケーラブルに保つ
- 効率的でダイナミックなルーティングを実行する
- ネットワーク接続とデータ転送資産をトークン化し、参加ノードにインセンティブを与える
- 次世代のブロックチェーンネットワークの設計と構築

2.2. 第三の柱：ネットワーキング

ビットコイン[3]とイーサリアム[4]のブロック化された計算能力と IPFS[5]と Filecoin[6]のブロックチェーン化されたストレージの後、NKN はインターネットインフラストラクチャの 3 番目の、おそらく最後のインターネットインフラストラクチャをブロックチェーン化することによって、ネットワーク層の革新によってブロックチェーンのエコシステムに革命を起こします。NKN に基づく次世代のブロックチェーンは、より強力なコネクティビティと送信能力を持つ新しい種類の分散アプリケーション（DApp）をサポートできます。NKN のビジョンは、分散型ネットワーク層に革命をもたらすだけでなく、次世代ブロックチェーンのコア技術を開発することです。

図 2. ブロック化されたインターネットインフラストラクチャの第 3 の柱としての NKN

2.3. 基本コンポーネント

NKN は、図 3 に示すように、既存のソリューションとは異なるいくつかの革新的な基本コンポーネントをベースにしています。

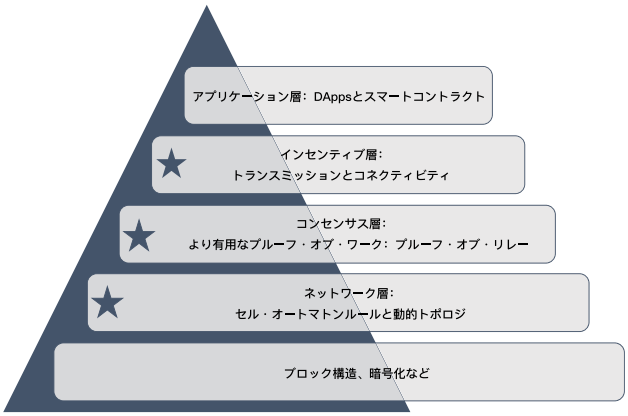

図 3.　NKN の基本コンポーネント

1. **コンピューティングインフラストラクチャの残りのコア構築ブロックをブロック化する：** NKN は、分散型データ伝送ネットワーク（DDTN）方式の概念を導入し、真に分散したブ

ロックチェーンを使用して、大規模な独立したリレーノードを使用してネットワーク上の冗長データの問題を解決し、ネットワーク接続性とデータ伝送能力を提供します。

2. **セル・オートマトンによる DDTN**：NKN は、セル・オートマトンを使用してネットワーク層を再構築するという新たな発想を導入します。セル・オートマトンの本質的な特徴、例えば分散、ピア等価性、並行性は、真に分散したブロックチェーンネットワークの構築を可能にします。

3. **セル・オートマトンによるコンセンサス**：NKN は、信頼できるサードパーティのない分散システムに不可欠な、セル・オートマトンをベースにした大規模分散システムで、フォールト・トレラント性の高い状態で、効率的にコンセンサスを達成します。

4. **プルーフ・オブ・リレイ（PoR）、プルーフ・オブ・ワーク（PoW）の進化形**：NKN は、参加者がコネクティビティと帯域幅を共有して報酬を獲得し、ネットワークコネクティビティとデータ送信容量を増強し、ネットワークのブロックチェーン化に貢献できるようにするメカニズムである、プルーフ・オブ・リレイ（PoR：プルーフ・オブ・リレイ（PoR））を提案しています。PoR は、より有用なプルーフ・オブ・ワーク（PoW）です。

5. **ネットワーク接続とデータ送信機能のトークン化**：NKN は、参加者がトークンと引き換えに接続と帯域幅を共有するように促すことによって、ネットワーク接続とデータ送信機能をトークン化します。このような共有メカニズムにより、アイドル状態のネットワークリソースをより有効に活用できます。NKN は、ネットワークリソースの利用率とデータ転送効率を向上させます。詳細は、経済モデルに関する論文を参照してください[8]。

6. **迅速で簡単な DApp 開発のためのネットワークツールキット**：DApp 開発者は、NKN をで、真に分散アプリケーションを迅速かつ容易に構築するための新しいネットワークツールキットを利用できます。DApp の開発者は、創造性、イノベーション、ユーザーインターフェイス・ユーザーエクスペリエンス、ビジネスロジックに専念できます。このネットワークツールキットは、アイデンティティ、機械学習、支払い、ストレージなどを扱う他のブロックチェーンプロジェクトによる他のツールキットを補完します。

NKN は、セル・オートマトンの手法を利用して完全な分散化を実現します。すべてのノードは同等であり、真にピアツーピアであり、それぞれがデータの送信、受信、および中継が可能です。セル・オートマトンにより、基盤となる物理的および論理的インフラストラクチャに依存しない、ダイナミックでスケーラブルなグローバルネットワークのオーバーレイトポロジを生成する、シンプルなローカルルールを持てます。シンプルさとルールのローカリティは、モノのインターネット（IoT）、スマートフォン、ルータまで、あらゆるタイプのネットワークデバイスでコスト効率の良い実装を可能にします。セル・オートマトン対応ルーティングは、そのシンプルさにもかかわらず、非常にランダムで予測できないため、優れたセキュリティとプライバシーを提供します。

NKN ノードは、コネクティビティとデータ転送のためのリソースを提供し、報酬を得て、ネットワーク容量を最大限に活用するために最適化された完全競争市場のマーケットプレイスをもたらします。既存のネットワークについては、NKN が、参加ノードの未使用帯域幅を共有することにより、コネクティビティおよびデータ送信容量の利用を増加します。

より多くの新しいノードが報酬を得るためにノードに参加し、そのため、迅速に NKN ネットワークのブートストラップと拡張が進みます。既存のノードには、データ送信容量をアップグレードし、増加するインセンティブがあります。上記のすべてにより、ネッ

トワークが全体的なネットワーク容量をさらに向上するだけでなく、ネットワークの経路選択に自由度があるため、ダイナミックトポロジが改善されます。

さらに、NKN は、新しく、より有用なプルーフ・オブ・ワーク（PoW）を提案します。NKN は、従来のハッシュ演算タイプのプルーフ・オブ・ワーク（PoW）とは異なり、長時間のオンライン、ピア接続の拡大、高速かつ低いレイテンシリレーの提供など、多くの有用な活動に基づいた、プルーフ・オブ・リレイ（PoR）を導入しています。そのために、コンセンサスアルゴリズムすらも、効率的かつ公平性を向上させるために、一から設計した一方で、ローカルな知識をグーロバルに収束させました。さらに、NKN は、ユーザーによるネットワーク共有とネットワーク所有を促進します。NKN の経済モデルとガバナンスモデルは、これを設計と実装に反映します。これらの技術と経済モデルの革新はお互いを補完し、ともに NKN ネットワークの力を増幅します。

2.4. 迅速かつ頑強な DApp 開発のためのネットワークツールキット

DApp の開発者は NKN を使用して、真に分散アプリケーションを迅速かつ無駄なく構築するための、新しいネットワーキングツールキットを手に入れました。DApp の開発者は、アイデアやイノベーション、UI（ユーザーインターフェイス）/、UX（ユーザーエクスペリエンス）、およびエンドユーザーに製品を成功させるビジネスロジックに全面的に注力することができます。もはや野生のジャングルのようなブロックチェーン、暗号、コンセンサスのメカニズム、アイデンティティとセキュリティについて、コードを書くために調べ回る必要はありません。

たとえば、SaaS（Software as a Service）サービスを中心とする伝統的なアプリケーション開発では、クラウドコンピューティングプラットフォーム上でアプリケーションをホストし、クラウドストレージにデータを格納し、テキストメッセージ、電話通話および支払いに Web サービスを使用できます。分散型ブロックチェーンの世界では、コンピューティング用のイーサリアム [4] / NEO [9]、ストレージ用 IPFS [5]、ネットワーク用 NKN を使用して、新しい種類の Facebook を構築が考えられています。この新しいパラダイムの美しさは、ユーザーが自分の ID とデータを個人的に所有し、システム全体で消費者とプロバイダの両方になるということです。さらに、各レイヤーには、ネットワーク効果を最大化し、コミュニティ全体をブートストラップするための自己インセンティブメカニズムが組み込まれています。NKN は 3 つの基本要素の 1 つとなり、この分散型パラダイムにおいて重要な役割を果たします。

3. 技術基盤

このホワイトペーパーでは、インスピレーションとして新しい種類の科学（A New Kind of Science：NKS）[2]の選択要素を取り上げます。NKN は、セル・オートマトンに基づくマイクロルールを利用してネットワークトポロジを定義し、自己進化行動を達成し、既存のブロックチェーンネットワーク層とは根本的に異なるセル・オートマトン主導のコンセンサスを探索します。

複雑なシステムを研究するための強力なツールとして、セル・オートマトンは、シンプルおよびコンプレックス、マイクロおよびマクロ、ローカルおよびグローバル、有限および無限、離散および連続などの哲学的カテゴリに密接に関連しています。

3.1. セル・オートマトン

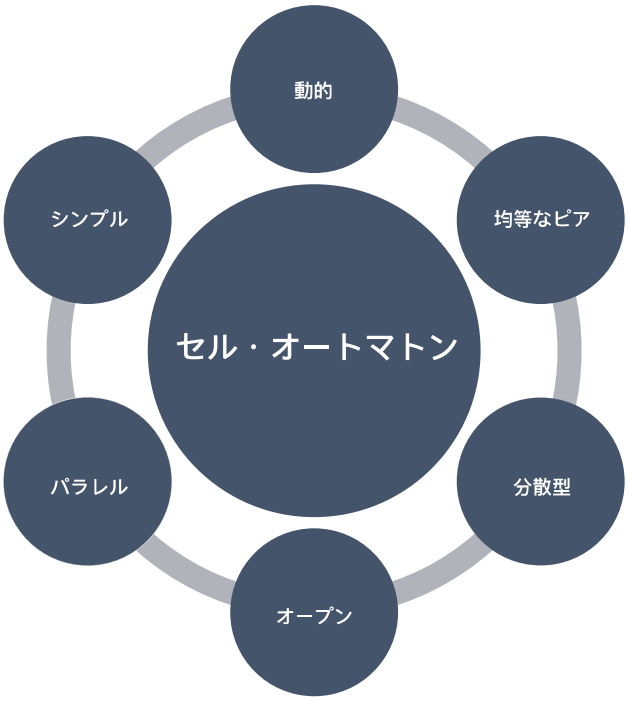

図 4. セル・オートマトンの特性。

セル・オートマトン（セル・オートマトン）は、ノードの集合を持つ状態機械であり、それぞれが隣接ノードにのみ依存するローカルルールに従って状態を変更します。各ノードは、数個の隣接ノードしか有していません。ローカルのインタラクションを伝播することで、結果的にローカルな状態がセル・オートマトンの世界的な行動に影響を与えます。ネットワークの望ましい開放性は、すべてのノードが同一であり、完全に分散型の P2P（ピアツーピア）ネットワークを形成するセル・オートマトンの同質性によって決定されます。NKN ネットワーク内の各ノードは、その現在の状態ならびに隣接ノードの状態に基づいて常に更新されます。各ノードの近隣ノードも動的に変化し、ネットワークトポロジがその基盤となるインフラストラクチャとプロトコルを変更することなく動的にします。

NKN は、セル・オートマトンを利用して効率的な分散型ダイナミックトポロジを実現し、情報とデータを集中的な接続なしで効率的かつ動的に送信できるようにします。

3.2. 数式としてのルール

NKN の次世代ネットワークに不可欠なルールであり、ネットワークトポロジーに重要な影響を及ぼします。[2, 10-13]。

ローカルルールを適切に選択すると、安定性とカオスの境界上に複雑であるが自己組織化された行動を持つセル・オートマトンに至ります。ルールは、セル・オートマトンとオートマトンネットワークをプログラミングするための式であるため必須です。セルオートマトンの静的特性は、有限数のノードが規則的なネットワークで相互作用するように定義された離散的な動的システムです。

$$CA=(S, N, K, f) \quad (1)$$

S はノードの状態を表し、各ノードはローカル状態を有します。すべてのノードの状態がグローバル状態を決定します。N はネットワーク内のノード数を示します。K は近隣セットを示し、すなわち、どの隣接ノードがローカル状態遷移において考慮されるかを示します。f は状態遷移関数であり、システムのグローバルな進化に劇的な影響を与えます。

セル・オートマトンの動的特性を図 5 に示します。動的な進化は初期状態から始まります。ノードは、現在の状態と近隣ノードの状態に基づいて状態を変更します。グローバル状態は、すべてのノードのローカル状態によって完全に決定され、それに応じて進化します。

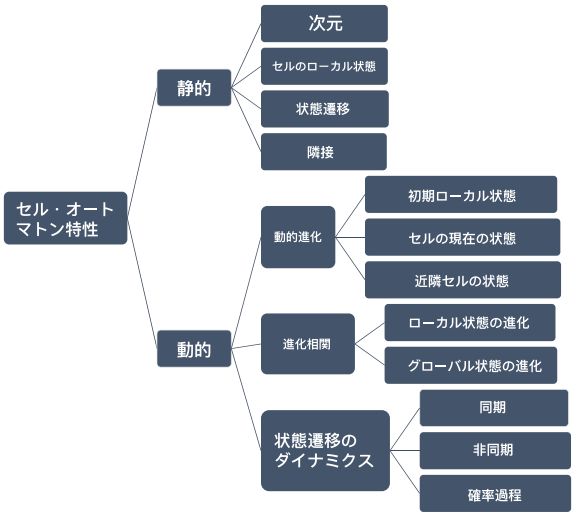

図 5. セル・オートマトンの特性。

NKN チームは、静的で完全に接続されたトポロジを利用する現在のアプローチよりも、セル・オートマトンベースまたはセル・オートマトンドリブンのシステムがより自然で有機的であると考えています。

このようなシンプルな構造の複雑なシステムは、自然なシステムに近く、自己進化を可能にします。

4 新しい種類のネットワーク

NKN は、真の分散化とネイティブトークンによる、インセンティブメカニズムを使用し、インターネットに革命をもたらすことを目指した、セル・オートマトン理論に裏打ちされたブロックチェーンテクノロジをベースとする、次世代のピアツーピアネットワークインフラストラクチャです。

4.1. 次世代分散ネットワーク

ブロックチェーンの現在のリーダーであるビットコインとイーサリアムは、プルーフ・オブ・ワーク (PoW) を通じて計算能力をトークン化します。一方、IPFS [5]、Filecoin [6]、Sia [14]および Storj [15]は、ストレージをトークン化します。しかし、ネットワーク接続とデータ転送のためのリソースをブロックするシステムはほとんどありません。これは、インターネットの 3 番目の不可欠な要素です。NKN は、有用な PoW としてネットワークコネクティビティおよびデータ転送のためのリソースをトークン化するように設計されています。

NKN は、ネットワーク内のすべてのノードを等化することによって、ブロックチェーンの「効率」問題を解決します。各ノードは、セル・オートマトンのルールに従い、ローカル規則に基づいて状態を更新します。セル・オートマトンは、1940 年代、Von Neumann によって提案され、離散時間、空間、相互作用によって特徴づけられる数理モデルの一種です[16,17]。特定の規則に従ってローカルに進化し、複雑なシステムの進化をエミュレートする個別のシステムです。

セル・オートマトンは、分散化、同等性、並行性の特徴を持っています。NKN は初めて、ネットワーク層全体が恩恵を受けることができるように、セル・オートマトンをブロックチェーンのネットワーク層の基本要素として提案しました。

セル・オートマトンの式を更新することは、ローカルルールと呼ばれ、セル・オートマトンの安定性とカオスの間の移行を制御する重要な要素であることがわかりました[2]。NKN の不可欠な部分である、これらのルールはネットワークトポロジに影響を与える主な要因の 1 つです。

NKN は、分散データ送信ネットワーク（DDTN）という概念を導入しました。DDTN は、複数の独立した自己組織化リレーノードを組み合わせて、クライアントにコネクティビティとデータ送信能力を提供します。

この調整は分散化されており、関係者の信頼を必要としません。NKN の安全な動作は、各ノードによって実行される操作を調整し、検証するコンセンサスメカニズムによって実現されます。DDTN は分散アプリケーション（DApp）のために、さまざまな戦略を提供します。

集中型ネットワーク接続およびデータ送信とは対照的に、DDTN 内のノード間には、データ送信容量を向上させるために使用できる複数の効率的なパスが

存在します。ネイティブトークンは、ネットワークリソースの共有を奨励し、最終的に無駄な接続と帯域幅を最小限に抑えることができます。この特性を「自己インセンティブ」と呼びます。

4.2. 有用なプルーフ・オブ・ワーク（PoW）

先駆的な仮想通貨として、ビットコイン[3]は、マイニングというプロセスを生み出しました。複雑なハッシュ課題を解決にたいして、マイナーに取引を検証するようインセンティブを与える、プルーフ・オブ・ワーク（PoW）メカニズムです。ビットコインマイニングの欠点は、効率的なマイニングには特殊で高価なハードウェアが必要であり、大量の電力を消費することです。Digiconomist によると、ビットコインの電力消費量は、2018 年 2 月中旬に 50TWh/年にもおよび、さらに依然として増加しています。イーサリアムでも 14TWh/年に近くなります。これらの 2 つの仮想通貨によって消費された電気は、多くの国の電力使用量を上回っています。

消費リソースの低い、プルーフ・オブ・ワーク（PoW）の代替手段には大きな潜在的な需要があります。NKN は、より分散化され、動的に進化し、自己組織化し、自己進化するネットワークインフラストラクチャを提供し、全く新しいコンセンサスメカニズムを設計することによって、現在の PoW の代替を提案しています。この新しい PoW はリソースを無駄にしません。ブロックチェーンレベルでのピアツーピア共有メカニズムです。参加者は、消費するよりも多くのネットワークリソースを提供して報酬を受け取ります。NKN は、ネットワークのコネクティビティとデータ送信容量を保証するために、プルーフ・オブ・リレイ（PoR）メカニズムを使用します。

4.3. ネットワークトポロジとルーティング

ネットワーク上のセル・オートマトン（CAoN）は、非幾何学的な隣接接続を有するネットワークをモデル化できるセル・オートマトン [10,11,18]の自然な拡張です。

ローカルルールに基づいてトポロジが進化しているネットワークをモデリングする場合はとくに強力です。ダイナミックトポロジを持つ分散型ブロックチェーンシステムを構築することが目標であるため、CAoN はシステムの自然なモデルといえます。

当社は、N 個のノードを有する動的 P2P ネットワークを検討しています。

時間 t におけるネットワーク接続は、時間とともに進化する $N\times N$ 隣接行列 $A(t)$によって記述できます。

ノード間の接続は、各タイムステップで追加、削除、または変更できます。A のダイナミクスがマルコフ式である場合、更新プロセスは

$$A(t+1) = f[A(t)]; \quad (2)$$

と書くことができます。ここで、fはネットワークトポロジーの更新ルールです。更新規則をローカルに保つために、fは、各ノードの隣接ノードの情報のみが、その接続を更新するときに使用すために、選択されるべきです。上記の更新規則にはノードの状態が含まれていないため、トポロジの進化はどのノードの状態にも依存しません。

より一般的なマルコフ的更新規則は、ネットワークのトポロジーとノードの状態の両方を考慮します。

$$\begin{aligned} A(t+1) &= f[A(t); S(t)] \\ S(t+1) &= g[A(t+1); S(t)] \end{aligned} \quad (3)$$

は、時刻 t におけるネットワーク内のすべてのノードの状態を表すベクトルであり、f は更新トポロジー g は状態更新ルールです。

同様に、fおよび g は、更新の際、現在の近傍情報のみが使用されるように選択されるべきです。状態は履歴情報が含むことができます。ノードがローカルに格納するすべてのブロックが、ブロックチェーンシステムの状態の例です。グローバル状態 S とグローバルコネクティビティ A を正式に使用してシステムを記述しますが、各ノード i はローカル状態 Si と

近傍 $\{j|A_{ij} \neq 0\}$ のみ知るだけで十分です。ブロックが生成されているブロックチェーンシステムのCAoN を考えてみましょう。ノードはブロックを受信するたびにその状態を更新し、そのブロックをデジタル署名付きの近傍ノードに送信します。近傍は、ブロックを受信したかどうか、ブロックが有効であるか、または状態の他のブロックと競合しているかなど、状態に応じてメッセージを転送するかどうかを決定し、物理レイヤまたは基礎となるプロトコルを変更することなく、トポロジに効率的に影響を与えます。

ネットワークをモデル化する方法を示す例として、任意の値の近傍を許可する一般的なネットワーク・オートマトンがあります。説明のために簡略すると、最小限のアプローチを採用し、小さな一連のマイクロルールからブロックチェーン拡張とデータリレーをエミュレートします。最初 (時間ゼロで) ネットワークは、図 6 に示すように、8 つのノードを有する 3D 立方体構造であり、各々は 3 つの近隣を有します。

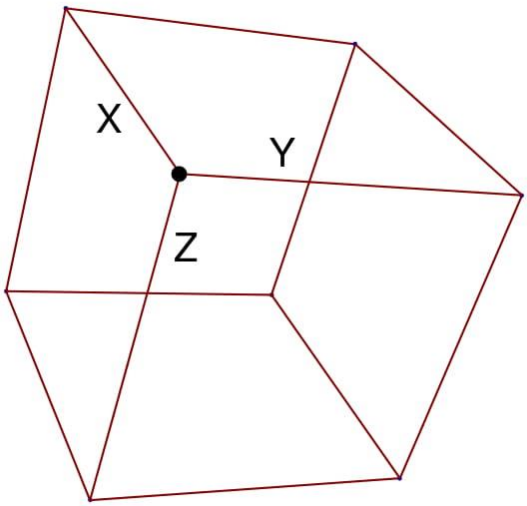

図 6. 初期状態で 3 次元空間に 3 次ネットワークを形成する 8 ノードのネットワーク・オートマトンの例。

図 6 の単純なネットワークから始めて、さまざまな更新規則に従ってノードを追加することによってシステムが拡張されます。図 7 に示すように、異なるルールを使用すると、結果として得られるトポロジが大きく異なる可能性があります。

NKN は、微視的なルールを持つ同様のネットワークモデルを使用し、ネットワークの進化とブロックチェーン機能を橋渡しします。シンプルなローカルルールは、複製を簡単にし、システムの実装を単純化と加速を実現します。

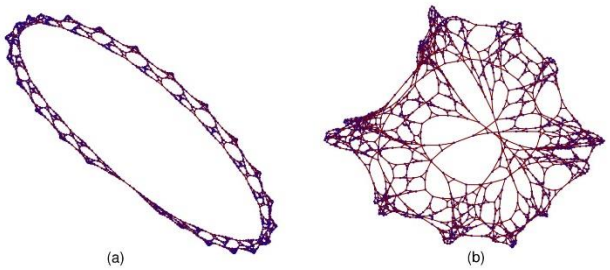

図 7. 種々の単純なルールを有する、複雑なブロックチェーンネットワークトポロジの例：(a) リングトポロジ、ルール 1655146、時間ステップ 1573、(b) 擬似ランダムトポロジ、ルール 1655185、時間ステップ 1573。

4.3.1. ダイナミクス

CAoN のダイナミクスは純粋にローカル的なものであり、各ノードは他のノードとは独立に状態遷移を評価し、それに応じて状態を変化します[19]。ノード状態は、図 8 に示すように、ノード間の相互作用、または外部情報のいずれかによって駆動します。

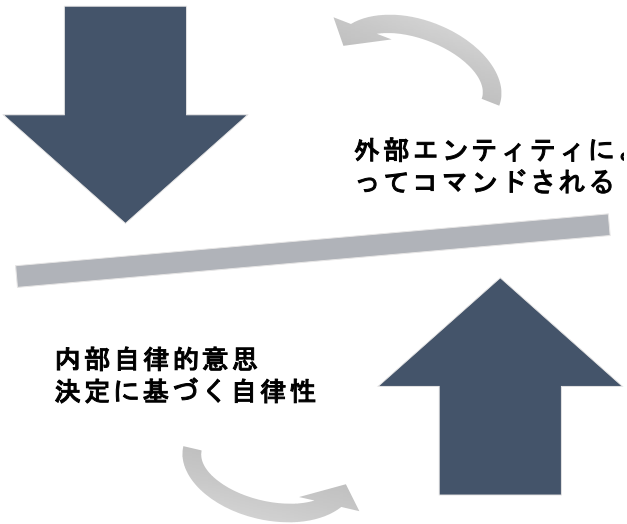

図 8. ノードが CAoN で状態を変更する可能性のある条件。

CAoN のトポロジには、ルールが不可欠です。

ネットワークトポロジは、図 9 に示すように、更新規則の小さな変更が与えられた場合には非常に異なるでしょう。

数学的記述では、離散時間ステップを便宜上使用しましたが、CAoN はノードにグローバル時間または離散時間を必要としません。代わりに、各ノードは非同期的に更新を実行します[19]。これは実際のブロックチェーンネットワークのものより一般的で現実的な記述です。

4.3.2. 自己組織化

セル・オートマトンのグローバルダイナミクスは、定常、周期、カオス、複合の 4 種類に分類することができます。

私たちの焦点は複雑なタイプ（クラス 4）であり、すべての初期パターンが複雑なやり方で相互作用する構造に発展し、長期間生き残ることができるローカル構造が形成される、カオスの縁として知られています。ウルフラムは、クラス 4 セル・オートマトンのすべてが普遍的な計算が可能ではないが、その多くはチューリング完全であると推測しています。

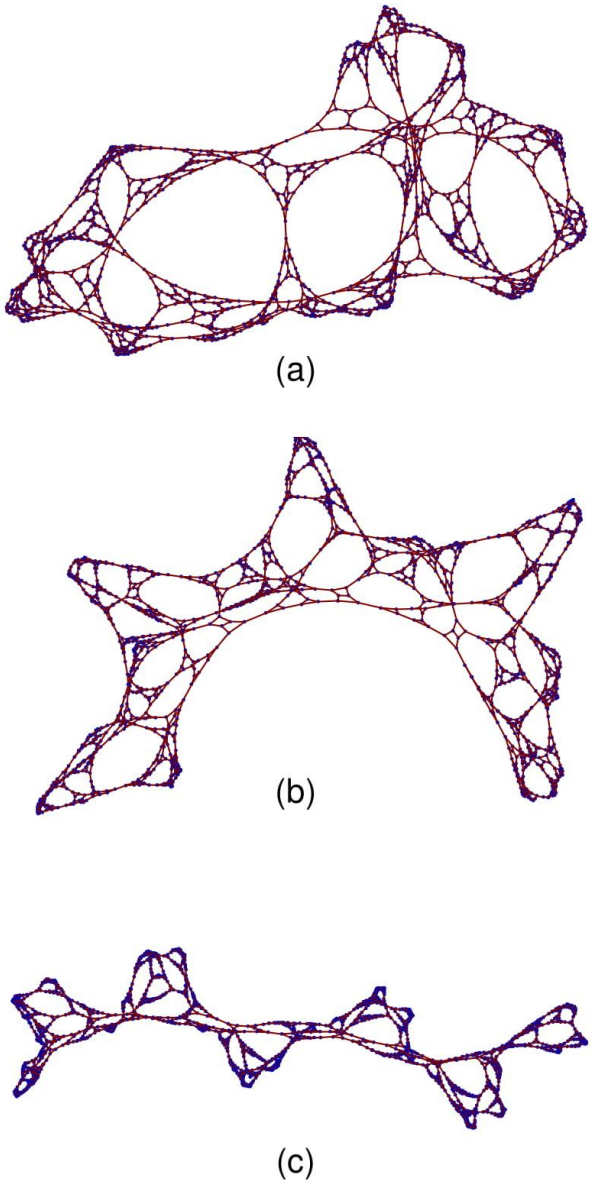

図 9. セルラーオートマトンのルールを同じタイムステップインデックスで書き換えることによるネットワークトポロジーのダイナミクス。(a) rule 1655163, time step 1573; (b) rule 1655175, time step 1573; (c) rule 1655176, time step 1573.

この見解は、ルール 110 [2、20]とコンウェイの『ライフゲーム』 [21]によって証明されています。複雑な自己組織化と動的構造は、クラス 4 セル・オートマトンで自発的に出現し、分散システムの基盤として理想的な候補になります。

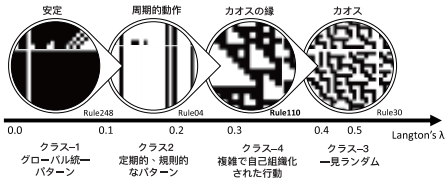

図 10. ウルフラムは、1D セル・オートマトンのラングトンのλパラメータに対して、4 つの動作クラスを使用しています。セル・オートマトンの動作タイプを説明および予測できるルールの定量的尺度は、アクティブ状態になるルールテーブルエントリの割合によって定義されるラングトンのλパラメータです。λが８０から増加するにつれて、システムは、図 10 に示すように、定常状態から周期状態に、次に複素状態に、そして最後にカオス状態に遷移します。最近接の相互作用を伴う古典的な 1D セル・オートマトンでは、クラス 4 の挙動は、λが約 0.3 であるときに現れます。ラングトンのλパラメータは、高次元システムに不可欠な、望ましい更新規則を見つける方法に関する理論的なガイドを提供します。

4.3.3. 自己進化

CAoN は、シンプルで強力なローカルダイナミクスであるため、自己進化をします。更新規則は、本質的に進化の方向を設定し、システムは初期状態またはノードがネットワークにどのように追加されるかにかかわらず、その方向に向かって連続的に進化します。図 11 は、CAoN における自己進化の例。

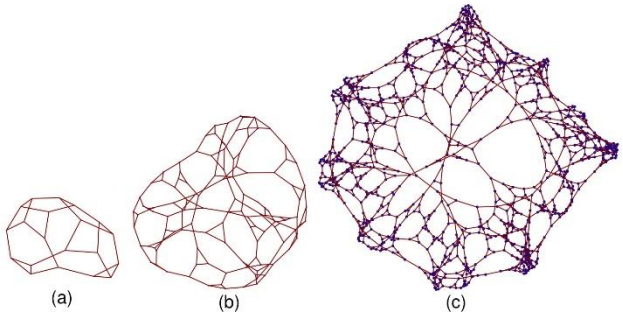

図 11. 様々なタイムステップインデックスにおけるルール 1655185 の 3D CAoN モデルの自己進化

(a) 100; (b) 1000; (c) 10000.

4.4. 効率的な分散化

NKN のダイナミックな性質を持つため、ノード間のネットワークトポロジは常に更新されます。適切な更新メカニズムは、結果として生じるトポロジの分散を達成するために重要です。例えば、新しく結合されたノードがより多くの隣接ノードを有するノードをその隣接ノードとして選択する機会がより高く、ノードを選択する確率がそのノードの次数に比例するように更新メカニズムが選択された場合、スケールフリーとなります[22]。次数分布はべき乗則の形式に従いますこのようなネットワークは、巨大なノードによって定義された集中ハブを有します。ハブは効率を高める可能性がありますが、ハブの障害が他のノードの障害よりもはるかに大きな影響を及ぼすため、ネットワークの堅牢性は低下します。

NKN の目標の 1 つは、情報の送信において効率的でありながら分散化されたネットワークを設計し、構築することです。これは、アルゴリズムとインセンティブの両方を考慮した適切なトポロジ更新メカニズムを使用する必要があります。アルゴリズムについて、近傍をサンプリングしてランダムに選択する必要があります。インセンティブ側では、ハブを使用しないように、データ送信の報酬は線形関数よりも線形関数（線形関数よりも遅くなります）にする必要があります。スパースランダムネットワークは、そのようなメカニズムから生成される可能性のあるトポロジの 1 つです。

分散化されているため、ノードの障害に対して堅牢でありながら、ネットワークの直径が小さいためにルーティングが効率的です[12]。

5. セル・オートマトンによるコンセンサス

ブロックチェーン内のノードは、分散したブロックチェーンの性質のためにピアにより成り立ちます。ブロックチェーンシステムに対する信頼の欠如は、いずれのノードもブロックチェーン内の任意のノードに情報を送信できるため、特に注目に値する。ピアは情報を評価し、ブロックチェーンが正しく機能するための行動を合意する必要があります[23]。

NKN は、低レイテンシ、高帯域幅、非常に高いスケーラビリティ、および合意に達するための低いコストを必要とする、未来的なブロックチェーンインフラストラクチャとして設計されています。

これらのプロパティは、将来の DApp にとって重要です。したがって、NKN は、そのような高い要求を満たすことができる新しいコンセンサスアルゴリズムを必要とします。

5.1. 主流のコンセンサス

現在、ブロックチェーンにおけるコンセンサスに達するためのアプローチがいくつか存在します：ビザンチン・フォールトトレラント（BFT）性アルゴリズム[24]、実用的ビザンチン・フォールトトレラント（PBFT）性アルゴリズム[25]、プルーフ・オブ・ワーク（PoW）アルゴリズム [3] プルーフ・オブ・ステーク（DPoS）アルゴリズム[26,27]、委任型プルーフ・オブ・ステーク（DPoS）アルゴリズム（DPoS）[28]です。

1. 実用的ビザンチン・フォールトトレラント（PBFT）性アルゴリズム

ビザンチン・フォールトトレラント性は、1982 年に Leslie Lamport が合意の問題を説明するために提案したモデルです。いくつかのノードが不正（偽造メッセージなど）なシナリオの下でコンセンサスを議論し、最悪の場合の保証を提供するものです[24]。ビザンチン・フォールトトレラント性では、ノードの総数を N、不正ノードの数を F とすると、N≥3F +1 ならば、問題はビザンチン・フォールトトレラント性（BFT）アルゴリズムで解決できます。

Lamport は、不正ノードの割合が 3 分の 1 を超えない場合、不正ノードが送信するメッセージが何であっても健全なノードが常にコンセンサスに達する、有効なアルゴリズムがあることを証明しました。

1999 年に Castro と Liskov によって最初に提案された実用的ビザンチン・フォールトトレラント（PBFT）性アルゴリズムは、実際に広く使用された最初の BFT アルゴリズムでした[25]。PBFT は、はるかに効率的で非同期的に動作しますが、BFT と同じ数の障害ノードにも耐えられるので、実際のシステムで使用するのにより現実的です。

2. プルーフ・オブ・ワーク（PoW）：ビットコインブロックチェーンネットワークは革新的なプルーフ・オブ・ワーク（PoW）アルゴリズムを導入しました[3]。このアルゴリズムは、コストを増やすことによって提案数を制限し、全員が最も長く知られているチェーンの承認に同意することで、一致の最終確認の必要性を緩和します。そのため、破壊行為を試みる人は、大きな経済的費用を支払うことになります。つまり、システムの計算能力の半分以上を支払うことです。後に、スポイラーを制限するために経済的なペナルティを使用し、この考えに沿って、様々な「PoX」シリーズアルゴリズムが提案されています。PoW はビットコインで使用されているコンセンサスであり、ブロックチェーンシステムで最も初期に使用されています。手短に言えば、PoW とは、マイナーがどれだけの仕事をしたか、どれだけの利益を得るかを意味します。

マイナーは、計算能力と時間提供することで、ブロックチェーンシステムに貢献します。これは「マイニング」と呼ばれている PoW の報酬を割り当てる仕組みでは、マイニング報酬が計算力に比例します。より強力なマイニング用のコンピュータを使用するほど、マイナーの報酬は増えます。

3. **プルーフ・オブ・ステーク (PoS)**：最初に、プルーフ・オブ・ステーク（PoS）は、保持されたトークンの量に応じてハッシュを計算する難しさを軽減します。PoS は、一定期間に利害関係者が保有する資産の金額に比例した、金銭的収益を分配する銀行の金融資産に類似しています。同様に、PoS では、ブロックチェーンシステムは、利害関係者のトークン量と保留時間に応じて「利子」を割り当てます[26,27]。委任型プルーフ・オブ・ステーク（DPoS）では、一部のステークホルダーのみがブロックを作成できます。代わりに、ノードは議会に入り、ブロックを作成するために自分を代表する受託者に投票します。受託者になりたいユーザーは、コミュニティの信頼を得るために、コミュニティの調査を行う必要があります[28]。

5.2. セル・オートマトンによるコンセンサス

5.2.1. BFT と PBFT のスケーラビリティに関する問題

BFT と PBFT アルゴリズムでは、大規模な分散システムでコンセンサスを得ることが困難です。BFT アルゴリズムでは、システム内で送信されるメッセージの総数は *O(N!)* [24]であり、実用的ではありません。PBFT アルゴリズムは、総メッセージ数を$O(N^2)$に減らしました。これは、扱いやすいけれど、N が大きいときはスケーラブルではありません。さらに、BFT と PBFT の両方とも、すべてのノードにネットワーク内の他のすべてのノードのリストを持たせる必要があります。これは、動的ネットワークでは困難です。

5.2.2. イジングモデルで記述されたセルオートマトンのコンセンサス

セル・オートマトンは、ローカル接続のみを持つ大規模な分散システムです。システムの漸近的挙動は、その更新規則によって制御されます。一組の更新規則に対してスパースローカル近傍のみに基づく、メッセージパッシングアルゴリズムを使用して、セル・オートマトンにおいて保証されたグローバルコンセンサスを達成できます。

物理学のイジングモデル[29]のために最初に開発された数学的フレームワークを使用することで、CA からゼロ温度イジングモデルまでの正確なマップによってスパース近傍状態のみを使用する、CA 規則のクラスが最大でも O (N) 回のイテレーションでコンセンサスに達することを保証することを発見し、証明したました。

いくつかの研究では、セル・オートマトンのフォールト・トレラント性と、セル・オートマトンベースのシステムの堅牢性を向上させる方法を検討しました[30-32]。さらに、結果がランダムおよび悪意のある障害ノードに対して堅牢であることを示し、必要な合意ができない場合にはしきい値を計算しました。

5.2.3. イジングモデル

イジングモデルは外部磁場の下でペアワイズ相互作用を持つスピン系のモデルです[29]。外部磁場のない系のハミルトニアン（エネルギー）は

$$H(S) = -\sum_{i,j} \quad J_{ij}S_iS_J \quad (4)$$

と書くことができます。ここで、$S_i = \pm 1$はノード i のスピン、J_{ij}はノード i とノード j の相互作用です。J_{ij}は 1（強磁性相互作用）または 0（相互作用なし）のみである場合を考えます。平衡状態でシステムが状態になる確率は、ボルツマン分布

$$P(S) = \frac{1}{Z} e^{-\beta H(s)} = \frac{1}{Z} e^{\beta \sum_{ij} J_{ij} s_i s_j}) \quad (5)$$

に従います。ここで

$$\mathrm{Z} = \sum_S e^{-\beta H(s)}$$

は区画関数であり、K_Bがボルツマン定数の場合、

$$\beta = \frac{1}{K_B T}$$

となり、T はシステムのノイズレベルを表す温度です。K_B = 1 のユニットはシンプルにするために使用されます。

格子状のイジングモデルは広範に研究されています[29,33]。最も近い隣接相互作用を有する D 次元格子上のイジングモデルでは、臨界温度$T_c = 0$である D = 1 を除いて有限臨界温度T_cで相転移が起きます。T < T_cのとき、システムは、ノードが好ましいスピン（自発磁化）を有する 2 つの状態のうちの 1 つに崩壊するが、システムはT = T_cのときに好ましいスピンがありません。

例えば、最近隣の相互作用を有する 2 次元正方格子の場合、イジングモデルの正確な解を得ることができます。臨界温度は

$$T_c = \frac{2}{\ln(1+\sqrt{2})} \approx 2.27 \quad (6)$$

自発磁化は

$$\langle s \rangle = \pm[\ 〚 1 - (\sinh 2\beta)\{\hat{}(-4)\ ]^{\frac{1}{8}} \quad (7)$$

です。

T→0 のとき、すべてのスピンは同じ（1 または-1 のいずれか）になります。関心のある分散システムがイジングモデルによって数学的に記述できる場合、システムは、温度がゼロのときにコンセンサス（すべてのノードが同じ状態を有する）を保証します。有限温度は、状態遷移にランダム性を加えることによって故障の役割を果たし、有限臨界温度は、そのような故障に対する堅牢性をもたらします。

5.2.4. セル・オートマトンとイジングモデルの関連

セル・オートマトン（CA）は、イジングモデルと密接に関連しています。セル・オートマトンは、時刻 t においてシステム状態S^tを与えられた時間 $t+1$ において状態$S^t + 1$にシステムが移行する確率を表す更新規則

$$\mathrm{p}(s^{t+1}|s^t) = \prod_i p\,(s_i^{t+1}|s^t) \quad (8)$$

によって特徴付けられます。転送確率は、CA のすべてのノードが以前のシステム状態のみに依存して状態を更新するため、条件に依存しない。決定論的 CA の場合、伝達確率$\mathrm{p}(s_i^{t+1}|s^t)$はデルタ関数です。形式 $\mathrm{H(s)} = -\sum_{i,j} J_{ij} s_i s_j$のハミルトニアンが CA のために定義される場合、

$$p(s_i^{t+1}\big|s^t) \propto e^{-\beta H\left(s_i^{t+1}\middle|s^t\right)} = e^{\beta \sum_j j_{ij} s_i^{t+1} s_j^t} \quad (9)$$

は$H(s_i^{t+1}\big|s^t)$が与えられた状態$s_j = s_j^t, \forall j \neq i$かつ$s_i = s_i^{t+1}$のハミルトニアンであるとします。その転送確率は

$$p(s_i^{t+1}\big|s^t) \propto e^{\beta \sum_j j_{ij} s_i^{t+1} s_j^t} \quad (10)$$

となります。

ここで、関数$p(S^t) \equiv p(s^{t-1}, s^t)$のような関数$s^{t-1}$と関数$s^t$との結合状態である新しい状態関数$S^t$を定義する。

S^tの伝達確率は、今度は、S^t内およびS^{t-1}内の相互作用がゼロであるハミルトニアン$\mathrm{H}(S^t) \equiv -\sum_{t,j} J_{ij} s_i^{t+1} s_j^t$での、ボルツマン分布関数

$$\mathrm{p}(S^{t+1}|S^t) = \mathrm{p}(s^{t+1}|s^t) \propto e^{\beta \sum_{t,j} J_{ij} s_i^{t+1} s_j^t} \quad (11)$$

に比例します。

したがって、CA は状態 S のイジングモデルにマッピングされます。S の定常分布はボルツマン分布

$$p(S) = \frac{1}{Z} e^{-\beta H(S)} \quad (12)$$

に従いますが、s の定常分布は

$$p(s) = \frac{1}{Z} \sum_{s*} e^{\beta \sum_{l,j} J_{lj} s_l s_j^*} \quad (13)$$

で与えられます。

決定性のある CA は、ゼロ温度でイジングモデルにマッピングできます。ここで、$T \to 0, \beta \to \infty, p(S)$と$p(s)$は、エネルギーが最も低い状態(s)でのみゼロではありません。私たちが興味を持っている A$J_{ij} = 1$ or 0 の場合、ゼロ温度で２つの状態、($s_i = 1, \forall i$ または $s_i = -1, \forall i$)しか許されません。

5.2.5. 合意アルゴリズムとしての多数決セル・オートマトン

多数決セル・オートマトン（MV セル・オートマトン）は、多数決を更新規則として使用するセル・オートマトンです。それは、$J_{ij} = 1$で、ノード i と j が接続されている

$$S_i^{t+1} = sign\left(\sum_j J_{ij} S_j^t\right) \quad (14)$$

として形式化することができます。そうでない場合は、0 となります。x > 0 の場合、sign(x) = 1、または-1C または x < 0 の場合 sign(x) = -1 となります。sign(0) = 1 または -1 を等確率で接続します。

各ノードが奇数 (k) の接続を有する場合、sign (0) の定義は影響を及ぼしません。これは、最近接接続および自己接続を有する D 次元セルラーオートマトンに当てはまります。シンプルにするため、奇数 k のみが考慮されます。

ハミルトニアンは$H = -\sum_{i,j} J_{ij} 8_i 8_j$と定義することができます。多数決ルールがゼロ温度($\beta \to 0$) の $p(S_i^{t+1}|S^t) \propto e^{\beta \sum_j J_{ij} S_i^{t+1} S_j^t}$というマッピング条件を満たすことを確認することができます。前節では、MV セル・オートマトンが平衡に達すると、すべてのノードが初期状態に依存する同じ状態を持つことになります。

MVCA がその平衡に収束することを示すために、前項$p(S^{t*1}|S^t) \propto e^{-\beta H(S^{t+1})}$で導いた式を使用します。$\beta \to \infty$のため、$H(S^{t+1})$ が最小化されているときだけ$p(S^{t*1}|S^t)$がゼロに近くなります。$H(S)$の定義から、各ノードが奇数個のコネクションを持つ場合、すべてのノードが奇数の接続数を持つとき、s^{t+1}がs^tによって一意的に決定されるので、$s^{t+1} = s$が成り立つときのみ等価が可能な $-\sum_{i,j} J_{ij} S_i^{t+1} S_i^t \leq -\sum_{i,j} J_{ij} S_i S_j^t, \forall S_i$を得ます。具体的には、$s = s^{t-1}$については、$H(S^{t+1}) \leq H(S^t)$があり、等価は$S^{t+1} = S^{t-1}$、すなわち平衡状態のシステムまたは 2 つの状態振動の場合にのみ成立します。後者は、J が動的なときに避けることができるので、現在は無視しています。MVCA が平衡に達する前に$H(S^{t+1}) < H(S^t)$が成立します。一方、$H(S)$は 2 のステップで変化する整数のみであり、$-kN \leq H(S) \leq kN$とすることができ、ここで N はシステム内のノードの総数であり、k は各ノードには接続があります。したがって、MV セル・オートマトンは、いかなる初期状態においても kN 回のイテレーションでコンセンサス状態に収束することを保証します。同様に、初期状態が m 個の「間違った」値を有する場合、それらの「間違った」値を補正するために、最大で km がかかります。上記の派生ではモデルとしてセル・オートマトンを使用しましたが、ローカル接続は想定していませんでした。実際、この結果は対称性マトリックス J を持つネットワークトポロジーで有効です。

5.2.6. ランダム化された近傍

無作為化されたネイバーセル・オートマトンとイジングモデルは、相互作用強度が主にユークリッド距離に依存する格子ベースのシステムです。この種のモデルは数学的には解きやすく、分散システムでは 11 を実装するのは実用的ではありません。特に、ノードが動的で信頼性が低く、制御不能な場合は、これが顕著です。ここでは、ランダムネットワークは、動的ノードを持つ分散システムにおけるコンセンサスのための、より良いトポロジであるべきであることを提案します。私たちが提案したコンセンサスアルゴリズムは、すべてのノードが特定のコネクティビティを維持する必要がないように、無修正のランダムネットワークで動作します。ここで説明するランダムネットワークは、ノードが物理的にどのように

接続されているかにかかわらず、純粋にオーバレイネットワークであることに言及する必要があります。ノードが他のノードのリストを持たない分散システムでは、ピアサンプリングのようなアルゴリズムを使用してランダムなコネクティビティを実現することができます。

情報の伝搬速度を制御する重要なパラメータは、ネットワークの最も遠い 2 つのノード間の最短距離として定義されるネットワーク直径です。各ノードが k 個の近傍を持ち、k が O(logN)であるランダムなネットワークの場合、ネットワークの直径はせいぜい O(logN) [12]であり、格子ベースのシステムよりもはるかに小さくなります。これは、ランダムネットワークが長距離接続を有する可能性があり、これは格子システムでは不可能であるためです。結果として、ランダムなネットワークはコンセンサス状態にすばやく収束します。また、k が増加すると、より小さな直径が得られることも示されています[12]。ウルフラムのクラス 4 セル・オートマトンは、コンセンサスの優れたパフォーマンスを得るためにランダム化されたネットワークを構築するのに理想的です。クラス 4 セル・オートマトンでは、コネクティビティが効果的に予測できず、自己組織化され、自己進化しています。

5.2.7. セル・オートマトンコンセンサスアルゴリズムのシミュレーション

我々のコンセンサスアルゴリズムの性能を示すために、それを N = 1,000,000 ノードを有するシミュレートされたネットワークに適用します。各ノードは、ネットワークからランダムに選択された k 個の隣接ノードを有します。各イテレーションにおいて、その状態は、k 個の近傍の状態に加えて、上記で提案された MV セル・オートマトン規則を使用する自身の状態に基づいて更新されます。近傍は、J が対称であることが保証されないように一方向性になります。

最初（イテレーション 0）、各ノードの状態は、独立に、確率がある状態で、1 または-1 になるように選択されます。シミュレーションは、図 12 に示すように、異なる k を有するいくつかのイテレーションについて実行されます。理論上の上限 kN よりもはるかに速い k = 10 であっても、MV セル・オートマトンがわずかなステップでグローバルコンセンサス状態に収束することが分かります。初期状態に等しい数の 1 と-1 のノードが含まれていてもコンセンサスに達することに注意してください。k を大きくすると収束が早くなります。N が大きい場合、ランダムなネットワークのトポロジーは、N が増加するにつれて特定のコネクティビティを持つ確率が指数関数的に減少するため、典型的なケースに近いことに言及する必要があります。したがって、私たちのシミュレーションのように、N が大きいときに最悪の場合よりもむしろ平均収束時間を見なければなりません。

さらに、ノードの一部が悪意のあるシナリオをシミュレートします。この場合、正しいノードは初期状態 1 を有し、悪意のあるノードは初期状態-1 を有し、近隣ノードの状態に関係なく状態を更新しません。正しいノードの目標は、状態 1 でコンセンサスに達する一方、悪意のあるノードは状態-1 で合意に達することです。結果 (図 13) から、間違った状態 (-1) への崩壊と正しい状態 (1) の最も正しいノードの維持との間に遷移があることが分かります。N = 1,000,000、k = 10 の場合、悪意のあるノードの臨界率は約 30%であり、これは N のサイズを考慮すると有意である。臨界率は図 13 に示すように k にも依存する。k が大きくなると、悪意のあるノードの数が増え、悪意のあるノードの影響を受けるノードが少なくなるという 2 つの影響があります。

図 12 と図 13 の結果を合わせると、初期状態が不完全なネットワークダイナミクスの上限と下限が示されます。前者は、不正な初期状態のノードが悪意のあるものではない場合をシミュレートします。後者は、不正確な初期状態を持つノードはすべて悪意のあるものであり、ネットワークの残りの部分が誤った状態で一致することを望みます。ネットワークのダイ

ナミクスは、これらの 2 つの曲線の間にあり、どのような戦略の障害のあるノード（障害のある初期状態のもの）でも同じ初期状態です。

5.2.8. 非同期ネットワークと信頼性の低いネットワークへの拡張

システムを記述するためにイジングモデルを使用することの利点の 1 つは、ノイズの多い信頼性の低い通信チャネルへの自然な拡張です。イジングモデルの温度パラメータは、システム内のノイズの量を制御します。この場合、更新規則にランダム性があります。

ゼロ温度では、更新規則は決定論的ですが、温度が上昇するとルールはランダムにな度が無限になると最終的に純粋にランダムになります。初期状態を含めることによって、メッセージ配信の確率的な失敗は、イジングモデルの有限温度によってモデル化することができます。このように、上述のように、ノイズが閾値を下回っている限り、コンセンサスを作ることができます。閾値は、ネットワークコネクティビティの統計を考慮して数値的に計算することができます。

非同期状態の更新は、通信タイムアウトが追加されたときにそのようなノイズによってモデル化することもでき、実装に実用的です。

5.3. プルーフ・オブ・リレイ（PoR）

NKN のコンセンサスは、ノードがネットワーク接続とデータ送信電力に依存すると予想される報酬が得られる、有用なプルーフ・オブ・ワーク（PoW）であるプルーフ・オブ・リレイ（PoR）によって駆動されます。ノードは、データを転送するときに電子署名を追加することによってリレーのワークロードを証明し、コンセンサスアルゴリズムによってシステムによって受け入れられます。

PoR で実行される作業は、より多くのデータ転送のためのリソースを供給することによってネットワーク全体に利益をもたらすので、PoR はリソースは無駄になりません。「マイニング」はデータ伝送レイヤに寄与するものとして再定義され、より多くの報酬を得る唯一の方法はより多くのデータ転送のためのリソースを提供することです。ネットワーク内のノード間の競争は、最終的にシステムを低遅延、高帯域幅のデータ送信ネットワークの方向に駆動します。

PoR は、トークンマイニングとトランザクション検証の両方に使用されます。一方では、トークンはデータ送信のためにノードに報奨される。他方では、取引検証のための予想される報酬は、選挙または難易度調整を通じて PoR に依存することもあります。

詳細なアルゴリズムと経済モデルについては、別のテクニカルイエローペーパー[34]と経済モデル[8]を参照してください。

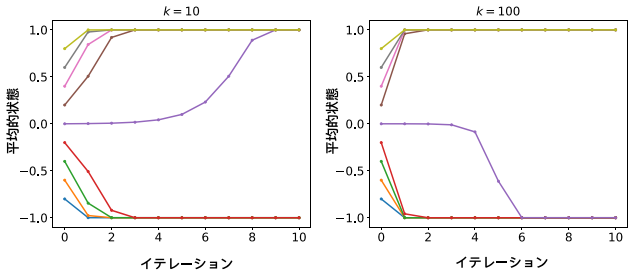

図 12. システムの平均状態は、1 または-1 のいずれかに収束し、どちらもグローバルコンセンサスを表します。MV セル・オートマトンは、1,000,000 ノードのネットワーク内にわずか 10 個の隣接ノードがあっても、わずかなステップで多数ノードの状態であるコンセンサス状態に収束する。近傍の数を増やすと収束が早くなります。ノードのちょうど半分が一方の状態にあり、他方の半分が他方の状態にあるとき、収束状態はいずれか 1 つになり得ることに留意してください。

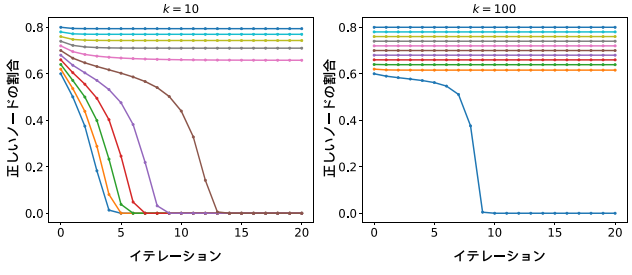

図 13. 状態を更新しない悪意のあるノード（状態-1）の攻撃のもとでの正しいノード（状態 1）の割合。

悪意のあるノードの最初の部分が変更されたときに、システムが間違った状態に崩壊するかどうかの移行があります。

5.4. 潜在的な攻撃

NKN は攻撃防御を考慮して設計されているため、関連する攻撃の種類を検討します。攻撃分析と緩和は、NKN の開発と今後の作業の重要な側面の 1 つで、テクニカル・イエロー・ペーパー[34]に含まれます。

1. **二重支払い攻撃**：二重支払い攻撃とは、同じトークンが複数回使われる場合です。古典的なブロックチェーンシステムでは、ノードは、トランザクションシーケンスを確認するためにコンセンサスによる二重支払い攻撃を防ぎます。

2. **シビル攻撃**：シビル攻撃とは、悪意のあるノードが複数のユーザーであることをふりかえるケースです。悪意のあるマイナーは、より多くのコピーを配布して支払いを受けることができます。物理転送は、複数のシビルアイデンティティを作成することによって行われますが、データは 1 回だけ送信されます。

3. **サービス拒否（DoS）攻撃**：オフラインのリソース中心の攻撃は、サービス拒否攻撃（DoS）と呼ばれます。たとえば、攻撃者は特定のアカウントをターゲットにして、アカウント保有者が取引を投稿しないようにすることができます。

4 **サービス品質（QoS）攻撃**：一部の攻撃者は、システムのパフォーマンスを低下させ、潜在的にネットワーク接続とデータ転送の速度を低下させます。

5. **エクリプス攻撃**：攻撃者は P2P 通信ネットワークを制御し、悪意のあるノードとしか通信しないようにノードのネイバーを操作します。エクリプス攻撃に対するネットワークの脆弱性はピアサンプリングアルゴリズムに依存し、ネイバーを慎重に選択することで軽減できます。

6. **利己的なマイニング攻撃**：利己的なマイニング攻撃では、利己的なマイナーは 2 つのブロックチェーンを維持しています。最初は、プライベートブロックチェーンはパブリックブロックチェーンと同じです。プライベート・チェーンの長さがパブリック・チェーンに巻き込まれていない限り、攻撃者はプライベート・チェーンを常にマイニングします。この場合、攻撃者は報酬を得るためにプライベート・チェーンを公開します。他のマイナーがパブリックチェーンよりもプライベートチェーンを採掘する方が効率的である可能性があるため、攻撃は本質的に 51％の攻撃の閾値を下げます。しかし、経済的な攻撃として、マイナーを誘致するために、利己的なマイニング攻撃を事前に発表する必要があります。

7. **不正行為**：悪意のあるマイナーは、大量のデータを送信すると主張できますが、アプレットを使用してオンデマンドでデータを効率的に生成します。アプレットが実際の中継データ量よりも小さい場合、悪意のあるマイナーがブロックボーナスを受け取る可能性が高くなります。

6. 結論

このホワイトペーパーは、NKN システムの構築に向けた明確かつ合理的な道を示しています。この作業は、分散型ネットワーク接続とデータ送信に関する今後の研究の出発点になると考えています。

今後の作業には、セル・オートマトンによるルーティング、セル・オートマトンベースのコンセンサス、プルーフ・オブ・リレイ（PoR）などが含まれますが、これらに限定されません。

NKN は現在のプラットフォームに比べていくつかの利点があります。

まず、NKN は分散アプリケーションを開発するため

の理想的なネットワークプラットフォームです。DApp の開発者は、ビジネスロジックだけでなく、エンドユーザーにとっても自社の製品を成功させるクリエイティブなアイデアや革新に完全に注力することができます。ネットワークインフラの詳細を心配する必要はありません。

第二に、NKN のインセンティブモデルは、より多くの人々がネットワークに参加してネットワーク接続とデータ送信を共有し、強化し、ネットワーク構造全体を変え、巨大な市場を創造することを促します。NKN は、1 兆ドルの通信事業をターゲットにしており、未使用のネットワーキングリソースの共有を促進し、共有ネットワークを拡大し革命を起こし、全員により良いコネクティビティを提供することを目指しています。

現在のシステムと比較すると、NKN ブロックチェーンプラットフォームは、ピアツーピアのデータ送信と接続に適しています。その間、この自己インセンティブモデルは、より多くのノードがネットワークに参加し、フラットなネットワーク構造を構築し、マルチパスルーティングを実装し、新しい世代のネットワーク送信構造を作成するよう促します。

NKN は、インフラストラクチャの革新の視点から、ビットコインとイーサリアムのブロック化されたコンピューティングパワーと、IPFS と Filecoin ブロックチェーン化されたストレージの後で、インターネットインフラストラクチャの 3 番目の、おそらく最後の柱をブロックチェーン化して、ブロックチェーンのエコシステムに革命を起こします。ブロックチェーン革命の他の 2 つの柱を補完する NKN は、自己進化し、自己インセンティブし、高度にスケーラブルな次世代の分散型ネットワークになります。

NKN は、次世代ネットワークを他の分野に提供する一般的なネットワーク層インフラストラクチャの戦略的な探究と革新です。すべての個人、およびすべての業界がデジタル世界で最大の可能性を達成するためには、信頼性が高く安全で分散化されたインターネットが不可欠です。NKN は、インターネットをより効率的かつ持続可能かつ安全にするために、完全に分散されたピアツーピアシステムを達成するための巨大な可能性を提供します。

現在のネットワークは、すべての情報とアプリケーションにユニバーサルな接続とアクセスを提供するために非常に非効率的です。それは、すでに所有しているネットワークに常にパッチを当てるのではなく、本当に必要なネットワークを再構築するときです。さぁ、未来のインターネットを構築しましょう。

[1] Stephen Wolfram. Statistical mechanics of cellular automata. Reviews of modern physics, 55(3):601, 1983.

[2] Stephen Wolfram. A new kind of science, volume 5. Wolfram media Champaign, 2002.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 2014.

[5] Juan Benet. Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561, 2014.

[6] Protocol Labs. Filecoin: A decentralized storage network, 2017.

[7] Federal Communications Commission. Restoring internet freedom, 2017.

[8] NKN. NKN Economic Model and Roadmap. nkn.org, 2018.

[9] NEO. Neo white paper: A distributed network for the smart economy, 2017.

[10] Xin-She Yang and Young ZL Yang. Cellular automata networks. Proceedings of Unconventional Computing, pages 280{302, 2007.

[11] Carsten Marr, Mark Muller-Linow, and Marc-Thorsten H□utt. Regularizing capacity of metabolic networks. Physical Review E, 75(4):041917, 2007.

[12] Fan Chung and Linyuan Lu. The diameter of sparse random graphs. Advances in Applied Mathematics, 26(4):257{279, 2001.

[13] Ali Mohammad Saghiri and Mohammad Reza Meybodi. A closed asynchronous dynamic model of cellular learning automata and its application to peer-to-peer networks. Genetic Programming and Evolvable Machines, 18(3):313{349, 2017.

[14] David Vorick and Luke Champine. Sia: simple decentralized storage, 2014.

[15] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. Storj a peer-to-peer cloud storage network. 2014.

[16] John Von Neumann. The general and logical theory of automata. Cerebral mechanisms in behavior, 1(41):1{2, 1951.

[17] John Von Neumann, Arthur W Burks, et al. Theory of self-reproducing automata. IEEE Transactions on Neural Networks, 5(1):3{14, 1966.

[18] David MD Smith, Jukka-Pekka Onnela, Chiu Fan Lee, Mark D Fricker, and Neil F Johnson. Network automata: Coupling structure and function in dynamic networks. Advances in Complex Systems, 14(03):317{339, 2011.

[19] B Chopard and M Droz. Cellular automata. Springer, 1998.

[20] Matthew Cook. Universality in elementary cellular automata. Complex systems, 15(1):1{40, 2004.

[21] John Conway. The game of life. Scientifc American, 223(4):4, 1970.

[22] Albert-Laszlo Barabasi and Reka Albert. Emergence of scaling in random networks. science, 286(5439):509{512, 1999.

[23] Arati Baliga. Understanding blockchain consensus models. Technical report, Tech. rep., Persistent Systems Ltd, Tech. Rep, 2017.

[24] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3):382{401, 1982.

[25] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), 20(4):398{461, 2002.

[26] Pavel Vasin. Blackcoins proof-of-stake protocol v2. URL: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper. pdf, 2014.

[27] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19, 2012.

[28] BitShares. Delegated proof-of-stake consensus,

2013.

[29] Ernst Ising. Beitrag zur theorie des ferromagnetismus. Zeitschrift f⊠ur Physik, 31(1):253{258, 1925.

[30] Mark McCann and Nicholas Pippenger. Fault tolerance in cellular automata at high fault rates. Journal of Computer and System Sciences, 74(5):910{918, 2008.

[31] Ludek Zaloudek and Lukas Sekanina. Increasing faulttolerance in cellular automata-based systems. In International Conference on Unconventional Computation, pages 234{245. Springer, 2011.

[32] Ilir Capuni and Peter Gacs. A turing machine resisting isolated bursts of faults. In International Conference on Current Trends in Theory and Practice of Computer Science, pages 165{176. Springer, 2012.

[33] Lars Onsager. Crystal statistics. i. a two-dimensional model with an order-disorder transition. Physical Review, 65(3-4):117, 1944.

[34] NKN. NKN Yellow Paper. nkn.org, 2018.

[35] Benoit B Mandelbrot. The fractal geometry of nature, volume 173. WH freeman New York, 1983.

[36] Michael Abd-El-Malek, Gregory R Ganger, Garth R Goodson, Michael K Reiter, and Jay J Wylie. Faultscalable byzantine fault-tolerant services. ACM SIGOPS Operating Systems Review, 39(5):59{74, 2005.

[37] Kevin Driscoll, Brendan Hall, Michael Paulitsch, Phil Zumsteg, and Hakan Sivencrona. The real byzantine generals. In Digital Avionics Systems Conference, 2004. DASC 04. The 23rd, volume 2, pages 6{D. IEEE, 2004.

[38] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Annual International Cryptology Conference, pages 139{147. Springer, 1992.

[39] Adam Back. A partial hash collision based postage scheme (1997). URL http://www. hashcash.org/papers/announce.txt, 2016.

[40] Vitalik Buterin. What proof of stake is and why it matters. Bitcoin Magazine, August, 26, 2013.

[41] Rodney J Baxter. Exactly solved models in statistical mechanics. Elsevier, 2016.

[42] Catarina Cosme, JM Viana Parente Lopes, and Jo~ao Penedones. Conformal symmetry of the critical 3d ising model inside a sphere. Journal of High Energy Physics, 2015(8):22, 2015.

[43] Bertrand Delamotte, Matthieu Tissier, and Nicolas Wschebor. Scale invariance implies conformal invariance for the three-dimensional ising model. Physical Review E, 93(1):012144, 2016.

[44] Sheer El-Showk, Miguel F Paulos, David Poland, Slava Rychkov, David Simmons-Dun, and Alessandro Vichi. 15 Solving the 3d ising model with the conformal bootstrap. Physical Review D, 86(2):025022, 2012.

[45] Leemon Baird. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. Technical report, Swirlds Tech Report SWIRLDS-TR-2016-01, available online, http://www. swirlds. com/developerresources/whitepapers, 2016.

[46] Arnab Mitra, Anirban Kundu, Matangini Chattopadhyay, and Samiran Chattopadhyay. A novel design with cellular automata for system-under-test in distributed computing. Journal of Convergence Information Technology, 9(6):55, 2014.

[47] Steven Janke and Matthew Whitehead. Practical fault tolerant 2d cellular automata.

[48] Yoshihiko Kayama. Complex networks derived from cellular automata. arXiv preprint arXiv:1009.4509, 2010.