Cyber-Physical Chain (CPChain) Whitepaper Decentralized Infrastructure for Next Generation Internet of Things

物信チェーンのホワイトペーパー

次世代の物事のインターネットの分散インフラ

物信チェーンのチーム

Cyber-Physical Chain (CPChain) Team

2018 年 1 月 10 日

January 10, 2018

要　約

物信チェーン（Cyber-Physical Chain, CPChain）はブロックチェーン技術を物事のインターネットテクノロジに深く統合し、分散型で信頼できる新世代の分散型IoTシステムを実現し、システムの相互接続および相互運用性のコストを削減し、データのオープンな共有価値を高め、ユーザーのプライバシーとシステムのセキュリティを確保する。CPChainはブロックチェーン技術がIoT業界で直面しているスケーラビリティ、セキュリティ、リアルタイムの問題に焦点を当て、ブロックチェーン-IoT—分散暗号化ストレージとコンピューティングの3つのテクノロジを組み合わせ、新しい世代のIoTアーキテクチャを構築する。物事のインターネットのデータ取得、共有、およびアプリケーションのためのフルプロセスソリューションを確立する。 CPChainは多方参加型のデータ取引や物事のインターネットの大規模なデータに基づいた人工知能の決定シナリオに重点を置いている。多方の信頼を確立し、異種データの相互接続と相互通信を実現し、業界のアプリケーションの問題点を解決し、これに基づき、CPChainプラットフォームに基づいて次世代のデータ共有のための革新的なビジネスモデルを作成する。

目次

1. プロジェクトの背景

1.1 物事のインターネットシステムの集中アーキテクチャがチャレンジに直面する

物事のインターネット（IoT）は情報分野における大きな発展と変化の機会である。高度な情報技術、通信技術、センシング技術、コンピュータ技術を統合してグローバルなダイナミックネットワークインフラストラクチャを構築する。ネットワークはすべてのスマートオブジェクト（RFIDタグ、センサー、スマートフォン、ウェアラブルデバイスなど）を相互接続し、完全な感知、信頼性の高い配送、インテリジェントな処理のために情報とデータを送信し、共有する。現在、物事のインターネットはインテリジェントな輸送、スマートホーム、医療の分野における集中型の技術と運用モデル、すなわち「煙突型」IoTアーキテクチャを採用し、接続コスト、信頼、データ値、ビジネスモデルの共通の問題に直面している。

機器の相互接続コスト。 近年、コンピューティングデバイス、ストレージデバイス、センサーの価格が低下するにつれ、物事のインターネットのデバイスは爆発的な成長を遂げている。IBM 研究院は2020年までに世界で300億以上の接続デバイスが使用されると予測し、既存の物事のインターネットソリューションのコストが高すぎ、ほとんどが「煙突」縦型アーキテクチャであり、すべてのデータセンターは単一のプロジェクト構築に基づいている。システムには独自の管理ツールとデータベースがあり、情報の島を形成している。数百億もの接続デバイスの時代には、このようなアーキテクチャは効率が悪く、時代のニーズを満たすことができない。さらに、IoTデバイスのほとんどが長いライフサイクルを持ち、安物の性質を備えているPCやスマートフォンなどのスマートデバイスに比べて利益がずっと低いため、メーカーは対応するITシステムを長期間維持する必要がある。メンテナンス費用を支えるのに十分な利益がないため、機器メーカは継続することが困難である。

ユーザーデータのプライバシーに関する問題。インターネットは信頼に基づいて構築する必要があり、Snowdenのような一連のイベントでも「信頼できる第三者」は100%信用できないことが証明された。インターネットが大きなデータの時代に入った後、人々はより多くのプライバシーを失った。したがって、物事のインターネットの開発の初期に、個人情報を明らかにせずにユーザがより便利でスマートなサービス

を楽しむことを保証するために、プライバシーを物事のインターネットのインフラストラクチャに統合しなければなわなく、そしてユーザーが実際に自分のデータとその価値を持つことができるようにする。さらに、現在の集中化されたアーキテクチャーで「閉鎖は安全である」というコンセプトは時代遅れであり、ブロックチェーンで代表される新しいテクノロジーは新しい「オープンは安全である」相互接続された物事を構築している。

データ価値の問題。IoTシステムは大量のデータを毎時生成する。これらのデータは商用アプリケーションと科学研究の両方で高い価値がある。たとえば、交通旅行データに基づき、ディープラーニングを使用してより正確で効率的に経路計画アルゴリズムをトレーニングする。医療機関はカメラなどのセンサからのデータを使用して患者の状態をより正確に判定することができ、よりカスタマイズされたケアプランを設計することができる。しかし、「煙突型」の島構造システムでは、大量の交通データが複数の集中プラットフォームの中に保持され、効率的な相互接続や相互運用性を実現することができないため、中小企業はこれらのリソースを使用できず、大学などの機関が高品質のデータを得ることは困難である。これは科学研究の進展を著しく阻害し、データの価値が完全に反映されないことにもつながる。さらに、IoTデバイスの大部分の独自接続は実用的ではなく、複数のデータを包括的に分析するだけで価値が生まれる。データが相互接続できない場合、価値を送信することはできない。

ビジネスモデルの問題。IoTデバイスのネットワーキング、コンピューティング、およびストレージ機能はコストを増加させるが、センサなどの伝統のデバイスでは、ネットワーキングはデバイスの主要機能ではなく、ハードウェアの販売だけではITの長期メンテナンスをサポートできない。現在の集中化されたアーキテクチャでは、ほとんどの製造業者がIoT機器のIT機能システムを完全に利用することができない。ビジネスモデルは単にユーザデータの販売であり、ユーザの権利とプライバシーを侵害する疑いがある。物事のインターネットシステムのさらなる開発と開放とユーザーの安全意識の向上により、現在のビジネスモデルは確かに変化を迎える。

1.2 ブロックチェーン技術が物事のインターネットの新たな発展の可能性をもたらす

新興テクノロジーとしてのブロックチェーンはデータセキュリティとプライバシーの問題を解決する大きな可能性を秘めている。現在、多くの研究者や企業がブロックチェーン技術をますます多くの分野に導入している。その中に、物事のインターネットとブロックチェーンの組み合わせは最も有望な方向の1つである。ブロックチェーン技術は基本的なアーキテクチャを再構築し、現在の集中型「煙突」システムで一連のチャレンジを解決する機会を与えている。

機器の相互接続コストを大幅に削減する

ブロックチェーンテクノロジのコアコンセプトは複数の関係者によって管理されたオープンな分散データベースである分散元帳である。ブロックチェーンに基づいた基本的なIoTデータプラットフォームの構築は「データの島」の問題を効果的に解決することができる。製造者は独自の単一製品用の完全なデータソリューションを作成する必要がなくなり、機器相互接続のコストとITシステムのメンテナンスコストを大幅に削減できる。したがって、ブロックチェーン技術に基づいて構築された分散型ネットワーキングシステムは百億レベルの相互接続されたデバイスデータを格納するのに十分である。

データプライバシーを効果的に保護する

ブロックチェーン技術の最大の利点は分散によってもたらされるプライバシーのセキュリティにある。ユーザーデータを管理する第三者はなく、データセンターには大量のデータが格納されていないため、ハッキングや悪意のある開示のリスクが軽減される。 ブロックチェーンを使用して構築された物事のインターネットは誰も参加でき、完全にオープンで安全であり、すべてのユーザーが自分のデータを管理し、プライバシーと権利を保護できる分散システムである。

データ価値の配信を実現する

タ共有プロセスに参加する。すべてのユーザーが自分のデータへのアクセスを許可でき、データ・アプリケーションおよびサービス・プロバイダは合法的に大量の貴重なユーザー・データを低コストで取得し、これに基づいてよりインテリジェントなサービスを作成し、データのリアルタイム・フローを通して価値の伝達を実現する。

新しいビジネスモデルを作成する

IoTシステムにおいてのユーザー、IoTデバイス、およびメーカーの役割はブロッ

クチェーンテクノロジによって変化する。現在の集中アーキテクチャとは異なり、ユーザーは新しいIoTシステムでデータ承認メカニズムとデバイスを動的にセットアップできる。 デバイスが単一の機能を実行するだけでなく、単にデバイスを相互接続するだけでなく、デバイスが自発的にやりとりすることも可能になり、メーカーはもはや異なるシステムで数百のITシステムを維持する必要がなくなる。役割の変化はより多くの参加者を引き付け、市場のルールを改革し、新しいビジネスモデルを創造する。

1.3 商用ブロックチェーンシステムのスケーラビリティのボトルネックの問題

ブロックチェーンテクノロジは分散型の信頼性を実現できるが、スケーラビリティは大規模な産業システムでのボトルネックの問題である。既存の大規模なブロックチェーンシステムアーキテクチャでは、高スループットの並行性の高い商用システムの需要をサポートするには十分ではない。

高いデータストレージと計算コスト

ブロックチェーンは多数のノードによって管理される分散データベースである。ストレージと計算のコストは非常に高く、大規模な公的チェーンアプリケーションプラットフォームでは大規模なデータを処理する必要がある。現在のブロックチェーンのストレージコストの下で大規模な公的チェーン・ベースのデータ・プラットフォームには実用的な実現可能性はない。

コンセンサスのメカニズムは非効率的である

現在のブロックチェーンでのPoWに基づくコンセンサスアルゴリズムは多大なリソースを消費するが、多くのアプリケーションシナリオでは、ユーザーは強力なコンピューティングパワーを得る方法がない。さらに、マイニングに基づくすべてのコンセンサスアルゴリズムはトランザクション速度のボトルネックに直面する。 ブロックチェーンシステムのスケーラビリティ問題を解決することが不可能な場合、分散アプリケーションは実際には地面に落ちることはできない。

上記の背景の下、物信チェーン（Cyber-Physical Chain, CPChain）は物事のインターネットとブロックチェーン技術の統合におけるデータとトランザクションのスケーラビリティ、セキュリティ、リアルタイムの問題を解決することに専念している。まず、分散型クラウドストレージシステムとブロックチェーン分散システムの並列分

散アーキテクチャを提案し、大規模なデータストレージと共有のスケーラビリティ問題を解決する。次に、コンピューティングとコミュニケーションを組み合わせた共同最適化設計を提案する。 大規模な公的チェーンのためのハイブリッドコンセンサスプロトコルを開発する。最後に、エッジコンピューティングとハードウェアセキュリティ手法を組み合わせた業界チェーンでは、セキュリティ、リアルタイム、および高性能の並行マシントランザクションを支持するサイドチェーンコンセンサスシステムが設計されている。

２．物信チェーン-並列分散アーキテクチャ

CPChainプラットフォームはIoT（Internet of Things）システムの基本データプラットフォームを構築し、データ取得、ストレージ、共有、アプリケーションのフルプロセスソリューションを提供することに専念している。画期的なブロックチェーンは物事のインターネットシステムの基盤となるテクノロジーに適用され、インターネットのデータの共有やトランザクションのためのインフラを提供する。これに基づいてデータ集約とリアルタイムデータフローアプリケーションは構築され、物事のインターネッのデータの価値を最大化するようにする。

分散型ブロックチェーンシステムでは、ネットワークノード全体が同じトランザクション（データ）上で操作を行う必要があり、計算とストレージの観点から多くの欠点があり、分散型ネットワークシステムの協調能力を十分に発揮することはできない。したがって、「バレル原理」にしか従えなくてスケーラブルがない。CPChainはデータ層と制御層の分離を提案し、システムのスケーラビリティを強化するための並列アーキテクチャを構築する。オープンなデータ共有機能を提供しながらユーザーのプライバシーを保護し、分散ストレージソリューションを使用してクラウドへのユーザーデータを暗号化し、ブロックチェーンのストレージ負担を軽減しながらデータの整合性と正確性を確保する。

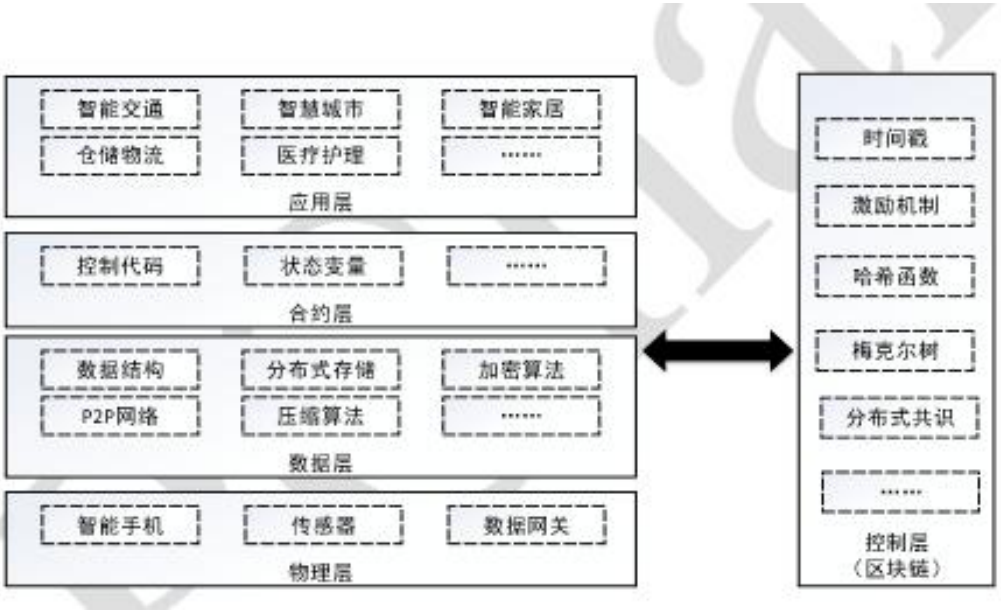


図1. CPChainのシステム階層

图片对照翻译

智能交通　スマートな交通

仓库物流　倉庫物流

智慧城市　スマートと詩

医疗管理　医療看護

应用层　応用層

智能家居　スマート用品

控制代码　制御コード

状态变量　状態変数

合约层　契約レイヤ

数据结构　データ構造

P2P 网络　P2P インタネット圧縮アルゴリズム

分布式存储　分散ストレージ

压缩算法　圧縮アルゴリズム

数据层　データレイヤ

加密算法 暗号化アルゴリズム

智能手机 スマートフォン

传感器 センサー

物理层 データゲートウェイ物理レイヤ

数据网关 データゲートウェイ

时间轴 タイムスタンプ

激励机制 インセンティブメカニズム

哈希函数 ハッシュ関数

梅克尔树 メルクルツリー

分布式共识 分散コンセンサス

控制层 制御レイヤ

（区块链）（ブロックチェーン）

図1は物理レイヤ、データ層、コントラクトレイヤ、アプリケーションレイヤ、およびコントロールレイヤからなるCPChainシステムの階層構造を具体的に示している。ブロックチェーンはデータの相互作用を監督する垂直コントロールレイヤとして機能する。物理層は主にスマートフォン、センサ、データ・ゲートウェイを含み、CPChain IOTデータ収集システムをベースとし、CPChainネットワークに参加するスマートデバイスはブロックチェーンノードを実行するか、ブロックチェーンネットワークと通信する必要がある。同時に分散アプリケーションの運用環境として暗号化、コンセンサスなどの操作を処理する。データ層ーはメインデータを処理し、異なるアプリケーション用に異なるデータ構造と圧縮アルゴリズムを設計し、データの読み取りと書き込みの効率を改善し、元のデータをブロックチェーンにアップロードする必要はなく、ハッシュ値のみをデータの一意の識別子と完全性や正確性の証明としてアップロードする。元のデータはユーザーサイドで暗号化されたあとに分散ハッシュテーブル（Distributed Hash Table,DHT）に保存される。

コントラクトレイヤはシステム機能の中核であり、スマートコントラクトがブロックチェーン上に配備され、契約ルールを変更することはできないため、シンプルさに基づいて設計し、よりインタラクティブな機能をアプリケーションレイヤに配置する必要がある。アプリケーション層はユーザが契約を交わすためのインタフェースであり、さまざまな要件に応じて異なるアプリケーションを開発することができる。制御層の機能はブロックチェーンによって完成され、初期段階ではスマートコントラクトをサポートするエテリアム（Ethereum）などのパブリックチェーンプラットフォームを使用してプロトタイプシステムの開発を加速する。ブロックチェーン技術に基づく分散システムは伝統の分散システムとは異なる。分散システムでは、コンピューティングとストレージのタスクは冗長である。分散ノードの各ノードは同じデータを格納して同じ計算タスクを実行する必要がある。この種の冗長な記憶と計算は一方では、ブロックチェーンシステムを信頼できる第三者の動作から独立させ、データの完全性を保証し、変更することができず、システムの一貫性を保つ。他方、冗長なデータはまた、システムの負担を増大させ、新しいノードを追加するコストがますます重くなる。

長期的には、このモデルはスケーラブルでなくて持続不可能である。Bitcoinを例にとると、Bitcoinブロックチェーンのサイズは130GBを超えており、新しいノードがデータを同期するのに時間がかかり、そして時間が経つと、新しいノードを入力するのが難しくなる。 冗長性の計算は重要で不可欠であろ、システム状態の一貫性を保証するが、大量の冗長なデータストレージがシステムの負担を増やし、スケーラビリティを持たせない。CPChainは図2に示すように、分散型のメインチェーン、産業チェーンネットワーク、分散型ストレージシステムを有機的に組み合わせている。CPChainプラットフォームの制御層一として、ブロックチェーンはシステムのすべてのデータを保管しなくなり、データの識別と信用証明書のみをアップロードするため、プラットフォームのストレージ負荷が大幅に軽減されるだけでなく、システムの一貫性が保証される。

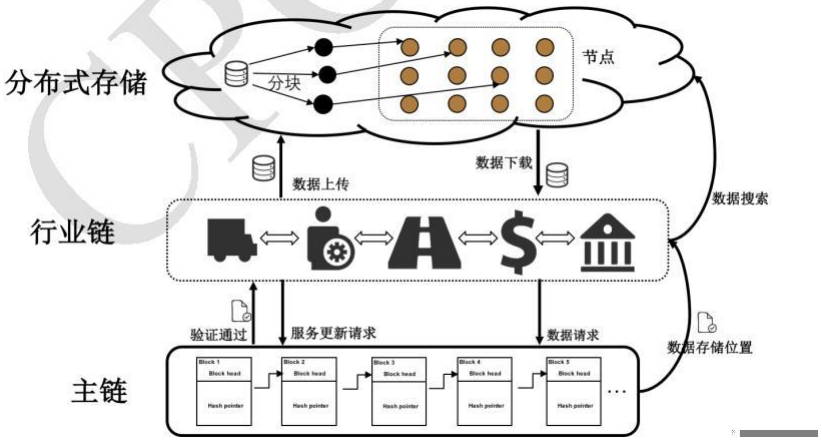


図2. CPChain並列分散アーキテクチャ

分布式存储 分散ストレージ

分块 ブロック

节点 ノード

数据上传 データをアップロードする

数据下载　データをダウンロードする

行业链　　産業チェーン

数据搜索　データの検索

主链　主チェーン

验证通过　検証をパスするパブリックチェー

服务更新请求　サービス更新要求

数据请求　データ請求

数据存储位置　データストレージの位置

CPCain並列分散アーキテクチャでは、分散クラウドストレージレイヤとブロックチェーンレイヤはパラレルに分散された2つの並列分散ネットワークとして機能し、データストレージとコンピューティングタスクを担当する。暗号化された後、ユーザデータはブロックに分割され、各部は異なるストレージノードに入ると同時に、ブロックチェーンネットワークのすべてのノードにハッシュ証明書がアップロードされ、データの検証や権利の確認などの後続の動作が実行される。並列分散アーキテクチャはブロックチェーンから

データ層を取り除く。これにより、ブロックチェーンシステムのセキュリティと分散された性質が維持されるだけでなく、スケーラビリティが向上し、ブロックサイズが大幅に縮小される。 現在の多くのブロックチェーンプラットフォームでは、ブロック容量を増やすなどの容量拡張の問題に直面しているが、ブロック容量を増やすだけでは、ブロックチェーンノードのメンテナンスコストが増加し、ノード数が減り、システムセキュリティが低下する。一定のブロックサイズを持つCPChainのシステムアーキテクチャでは、単一ブロックにパッケージ化できるトランザクションの数が大幅に増加し、プラットフォームのトランザクション処理速度が大幅に向上する。

3. 物信チェーンの重要技術

データ層と制御層を分離するCPCainの並列分散アーキテクチャソリューションはブロック容量を変更することなくトランザクションの速度を大幅に向上させ、システムのスケーラビリティを向上させることができるが、新たなチャレンジに直面する。例えば、データ層を制御層から分離した後、分散ストレージネットワークを構築し、ブロックチェーンとの効率的なやりとりを保証する必要がある。また、データ層が独立している場合は、ブロックチェーン内のデータのプライバシーを破棄し、暗号技術に基づくプライバシー保護方式を設計し、重度の暗号化または準同型の暗号化技術に基づいて構築された暗号化機能はコンピューティングリソースに対して特定の要件を備えているが、ブロックチェーン自体にはコンピューティングリソースとコストが限られており、プライバシーと可用性のバランスを取る必要がある。

大規模なP2Pネットワークでは、大規模なノードとデータの異種性のため、ノードの一貫性とデータの安全なストレージを確保する上で大きなチャレンジがある。POW（Power of Work）コンセンサスプロトコルに基づく現在のブロックチェーン分散ネットワークは拡張性、コンピューティングリソースの浪費、ブロック速度の制限などの問題を抱えている。CPChainシステムはシステムの低スループットと高遅延問題を解決し、データの一貫性とセキュリティを強化するために、動的委員会セキュリティ選定メカニズムを設計するし、二重レベルコンセンサスプロトコルソリューションを採用している。また、CPChainは物事のインターネットの特性を踏襲し、CPChainのメインチェーンを基盤としたクロスチェーンアーキテクチャを採用しており、実用化の多様化に対応した業界指向のサイドチェーンネットワーク機能を提供している。メインチェーンのネットワークは主に物事のインターネットのデータ交換のための高速制御チャネルに使用される。

3.1　並列分散暗号化ストレージと計算

CPChainは並列分散アーキテクチャを採用している。このアーキテクチャでは、図3に示すような物事のインターネットの一般的なデータアップロードと共有プロセスが示されている。CPChainはデータセキュリティ、ネットワークにおける信頼性の高い効率的な共有を実現するために、分散ストレージテクノロジと重い暗号化テクノ

ロジおよび準同型暗号化テクノロジを創造的に組み合わせ、効率的なデータアクセス制御メカニズムを実現する。以下には主に2つの側面から詳細に説明する。

DHTベースの分散暗号化ストレージ

IoTデータの分散ストレージプロセスを図4に示す。システムはデータ層と制御層を分離し、すべての生データはローカルで暗号化され、所有者が署名し、パーティショニングの後、ホストが元のデータを知ることができないように、分散ハッシュテーブルメソッドは異なるノードに格納される。同時に、データのハッシュ値はデータの完全性と正確性のためのクレデンシャルとデータの識別としてブロックチェーンに格納される。CPChainの第1段階では、システムプロトタイプ開発とアプリケーションテストを加速するために、Ethereumがメインチェーンとして選択された。ブロックチェーンはデータアクセス制御に行われ、データの所有者がデータを格納すると、ブロックチェーンは各データレコードのアクセス権を格納する。これはデータ識別子を含むトランザクションを送信することで実行できる。ユーザーがデータを検索したい場合は、データへのアクセスを得るために、データのアイデンティティを取得できるという証拠を提供する必要がある。システム内の悪意のあるノード場合、それはアクセスを無視することができるが、データは暗号化され、DHTでは、各ノードはデータのランダムな部分だけを保存するため、悪意のあるノードは影響が限られている。すべてのデータはユーザー側で暗号化されているため、効果的なデータ認証アクセスメカニズムを設計してデータ共有を実現する必要がある。伝統的な分散ハッシュテーブルはデータのkey-valueのペアしか保持しないが、これはCPChainプラットフォームでは不十分である。したがって、データ層では、CPChainはデータ暗号化計算に使用されるキーを組み合わせ、キーとデータブロックの間の対応関係を記録し、改良された分散ハッシュテーブル法を提案する。

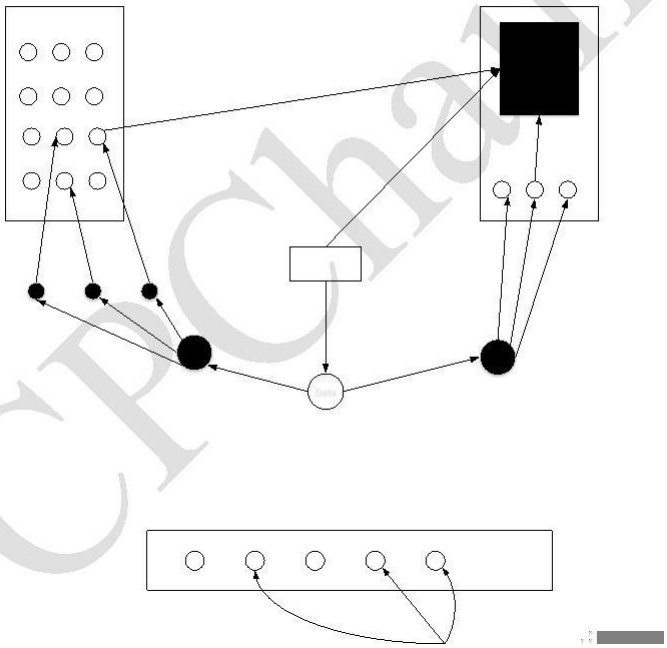


図3. CPChainの一般的な物事のインターネットのデータのアップロードと共有

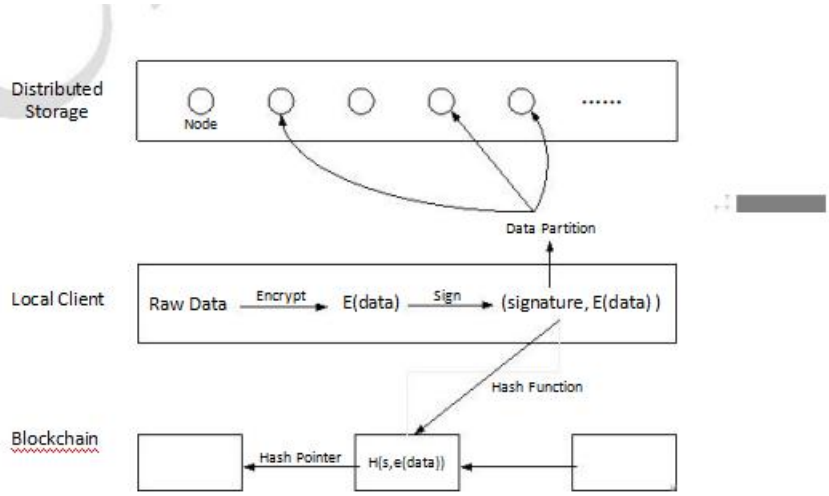


図4.データ分散ストレージプロセス

データの暗号化と復号化はコンピューティングリソースの一定量を消費し、毎日物事のインターネットのシステムによって生成された莫大な量のデータに直面し、各データレコードを個別に暗号化することは間違いなく計算資源の浪費である。したがって、さまざまなタイプの物事のインターネットデータに対してデータセキュリティと処理効率のニーズを同時に満たす適切なデータ構造と暗号化メカニズムを設計する必要がある。CPChainプラットフォームは生成されたデータを時系列順に整列して

チェーン構造に編成すると同時に、期間Tを設定し、1サイクル内のデータをブロック化し、暗号化間隔eとアップロード間隔uを選択することにより、 ブロックチェーンレコードはブロック全体のデータの完全性と信頼性を保証する。暗号化コンピューティングに基づくデータ共有とアプリケーションであるCPChainプラットフォームはブロックチェーンからデータ層を取り除き、データのセキュリティとプライバシーを確保するため、元のデータはすべてユーザー側で暗号化されている。データは第三者には見えないため、暗号化されたデータの計算や共有の実装方法は並列分散アーキテクチャが直面する主なチャレンジである。公開鍵暗号方式では、受信者の公開鍵を使用してデータを暗号化する必要があるため、分散型暗号ストレージを導入した後は、ブロックチェーンプラットフォームで採用されている公開鍵暗号システムは適用されなくなる。図5に示すように、しか達成できない。CPChainプラットフォームでは、図6に示すように、データが一度暗号化されてアップロードされ、複数の用途に使用されることが期待されている。 したがって、CPChainプラットフォームはより安全で効率的なデータ共有とサービスを実現するために、再暗号化と準同型暗号化技術を深くて研究して開発し、暗号化技術とブロックチェーン技術を深くて統合する。

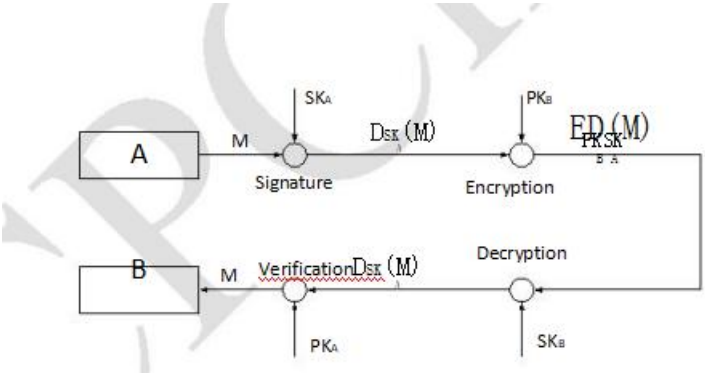


図5.公開鍵暗号システム

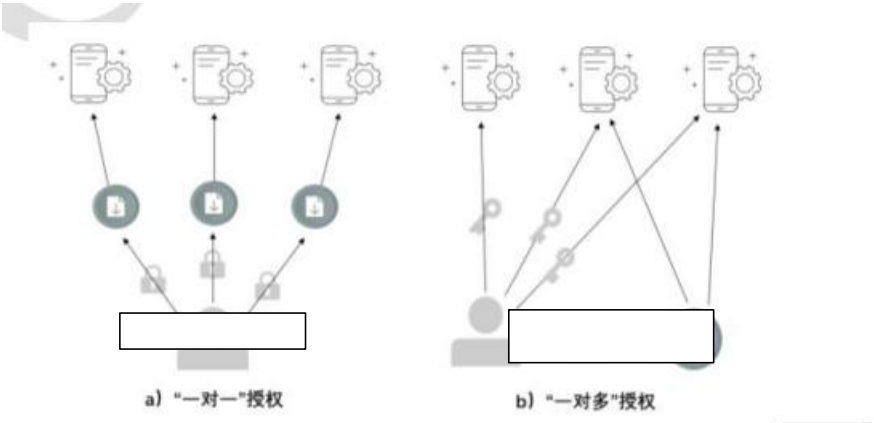


図6.公開鍵の暗号化「1対1」の許可とCPChainの暗号化「1対多の許可」

一度の暗号化によって複数の許可を実現するために、CPChainは再暗号化技術に基づいて対称暗号化と非対称暗号化のセットを構築した。ユーザが各暗号化区間を暗号化する際には、対称暗号鍵が使用される。すなわち、同一の鍵が暗号化および復号に使用され、暗号化されたデータブロックと鍵との対応が改善されたDHTに記録される。データのセキュリティを向上させるために、暗号化キーは暗号化間隔ごとに更新する必要がある。非対称暗号化に基づく再暗号化システムは暗号化データによって使用される鍵を送信するために使用され、データの許可が単一の暗号化間隔に限定されることを保証することができる。

複数の暗号化技術は並列分散アーキテクチャの下でデータ共有の問題を部分的に解決できるが、そのデータはスマートな契約の下で見えるため、特定のセキュリティとプライバシーの問題に直面している。このため、CPChainは分散暗号化マッチングや検索などの暗号化されたデータの下で計算機能やアプリケーション機能を実現するための準同型暗号化技術を導入し、ユーザープライバシーの保護を強化する。

3.2　大規模な公的チェーンのハイブリッドコンセンサスプロトコル

大規模な物信チェーンシステムでは、大規模なネットワークと物事のインターネットの大量のデータ量のため、一貫したノード状態と分散データ記憶を達成するために多くのチャレンジに直面している。CPChainシステムはスケーラブルなパフォーマンスを備えたハイブリッドコンセンサスプロトコルを開発し、動的委員会選挙メカニズムを提案し、POWコンセンサスプロトコルに基づく元のシステムのスケーラビリティ問題を克服する。

メインチェーン構造の主なコアの問題はどのノードがデータ収集を完了し、パッケージングをブロックし、ブロックデータのセキュリティと一貫性を保証するかを決定することである。伝統の分散フォールトトレラントアルゴリズム、例えばPBFT、Zyzzyvaなど、ノード間の一貫性を保証するために通信の性能（communication-bounded）に依存する。しかし、アルゴリズムのセキュリティを保証するための通信方法の依存度が高く、システムのスケーラビリティが悪く、ノード数が増えた場合、そのパフォーマンスは急速に低下する。ノード数が一定のしきい値を超えると、システムは使用できないになる。小規模での信頼性と可用性のために、伝

統のビザンチンフォールトトレランスアルゴリズムはプライベートおよびアライアンスチェーン環境に適している。この問題を解決するために、CPChainシステムの中心的な解決策は動的な委員会のセキュリティ選挙メカニズムを設計し、ブロックデータの収集とブロックのパッケージ化とチェーンを完了するための信頼できる委員会を選出することである。

二重コンセンサス

CPChainは伝統のビザンチンフォールトトレランスアルゴリズムを大規模な公開チェーンシナリオに適用することはできず、POWや他のコンセンサスプロトコルは計算資源の浪費により効率が悪いため、CPChainの主なコンセンサス効率を向上させる委員会ベースの二重コンセンサスプロトコルを提案している。第1ラウンドのコンセンサスでは、ラウンドでのノードのレベルを決定するために一定の固定ラウンド（ブロックが追加されるたびに、ラウンドと呼ばれる）でローカル選択アルゴリズムを実行し、計算結果が高いレベルである場合は、ノードにラウンドのアカウンティング権限があることを意味する。第2ラウンドのコンセンサスで、主に、ブロックのパッケージ、検証、およびネットワーク全体のブロードキャストを完了する。コンセンサスプロセスを図7に示す。

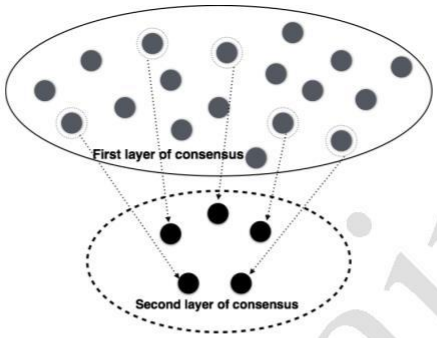


図7. CPChainメインチェーンの二重コンセンサスアーキテクチャ

評判評価モデルに基づく委員会選挙と動的更新

CPChainメインチェーンのコンセンサスプロトコルを実装する上での主な困難は、1. P2Pネットワーク内のネットワーク全体のアイデンティティ2.委員会設立後の相互の識別3.ノードのレベルは偽造できないのを保証することである。上記の問題に対して、CPChainシステムはノード評判モデルを使用してノードの信頼性を評価し、ノードの信頼性に基づいて信頼できる計算を実行し、委員会を選出する。その後、グループ内でコンセンサスを実施するための委員会を通じ、ブロックデータの収集、パッケージング、およびチェーンの実装を実現する。

選挙プロセスでは、確率分布の確率のランダム性が均等に分布し、選挙プロセスのランダム性が高まり、悪意のあるノードがネットワーク全体の行動を制御するための累積評判攻撃を実行することを防ぐ。さらに、ランダム性を高めることによって、信頼性の低い一部のノードがブロックのパッキングと検証に参加し、一部のネガティブノードに対するインセンティブを高めることができる。

コンセンサス協定がtラウンド継続された後、再選が行われる。 ブロックを追加する過程で、高度なノードダウンや悪意のある行為があった場合、信用度の値は罰せられ、信用度の値が一定の閾値hより低い場合は、委員会から削除され、委員会はブロック内の情報を変更し、図8に示すように、次のラウンドの始めに、対応する数のノードを動的に選挙して委員に加わることができるようにする。

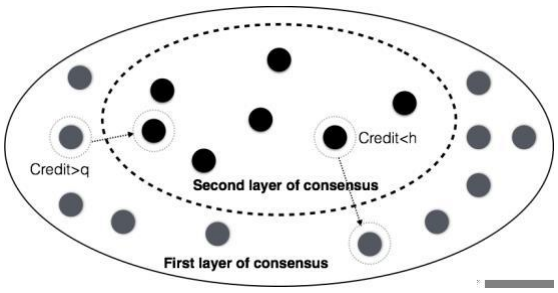


図8. CPChainメインチェーンの委員会メンバーの動的調整

3.3 高度にリアルタイムのサイドチェーンネットワーク

CPChain は物事のインターネットシステムの基本的なデータプラットフォームであり、そのメインチェーンはインターネットの普遍的なデータ制御層である。しかし、物事のインターネットの異なる垂直アプリケーションは異なる性能要件を有する。厳密なリアルタイム性能を必要とする典型的なアプリケーションには、無人車両のリアルタイム制御および車隊の調整が含まれる。そのようなアプリケーションでは、物事

のインターネットにおけるデバイスノード間の協力と効率的な作業を完了するために、CPChain はリアルタイム制御シグナリングの安全な通信と相互作用をサポートする必要がある。データのやりとりがメインチェーンを通じて完了していれば、大きな遅延に直面し、さまざまなアプリケーションのリアルタイム要件を保証することはできない。物信チェーンは典型的なアプリケーションシナリオを選択し、高周波、細粒度、高セキュリティ、リアルタイムなどのマシンデータトランザクションのニーズを満たす軽量のサイドチェーンコンセンサスプロトコルを開発する。具体的には、CPChain はさまざまな種類のアプリケーションの情報対話遅延の要件が満たされ、サイドチェーンネットワークの高いリアルタイム性と高いセキュリティを実現することを保証するために、図 9 に示すように業界チェーンのエッジ計算とハードウェアセキュリティ方法に基づいてサイドチェーンコンセンサスシステムを設計する。

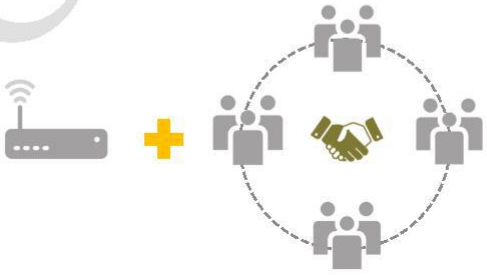


図9.ハードウェアアクセラレーションに基づく無差別協力モデル

データゲートウェイと組み込み暗号化アルゴリズム

物事のインターネットにおける各センサによって収集されたデータの不均質性のために、センサ自体はしばしば計算能力を持たないか、または計算能力が極端に制限される。センサデータ処理および認知関連計算が各センサノード上に配置されれば、より多くの遅延をもたらし、アプリケーション要件を満たすことができない。物事のインターネットに配備されたゲートウェイデバイスはセンサノードよりも強力なハ

ードウェアサポートを備えているため、より高速なコンピューティング機能を提供することができ、デバイスの電力は制限されない。したがって、物事のインターネットに配備されたデータゲートウェイを使用することにより、データ処理と暗号化計算のためにセンサデータがエッジゲートウェイに集約されるが、一方でデータ処理による計算遅延が減少し、他方、物事のインターネットにおける各センサノードの計算負荷が軽減され、その作業時間が延長される。

産業チェーンコンセンサスアルゴリズムインセンティブとセキュリティメカニズム

物事のインターネットシステムはMeshネットワークまたは無線Ad Hocネットワークで構成され、その無線通信技術はIEEE802.11pおよびNB-IoTを含む。したがって、物事のインターネットの機械取引に関するコンセンサスは無線ネットワークシステムの特性を最大限に活用し、コンセンサスプロセスをネットワーク通信プロトコルに組み込み、コンセンサスプロセスにおける情報交換がデータレイヤを必要とせず、下位レイヤ通信レイヤのみを介して完了することができ、プロセスの遅延を低減する。さらに、機械取引の同時並行性、リアルタイム性、セキュリティ要件を考慮すると、物信チェーンは進化的ゲーム理論に基づく効率的な協力およびインセンティブメカニズムを開発し、例えばDAG（Directed Acyclic Graph,DAG）に基づくデータ構造の利他主義的なインセンティブメカニズムにより、CPChainサイドチェーン上のアプリケーションがより効率的に、より速く、より安全になる。

4.物信チェーンの典型的な適用シナリオ

一般的な物事のインタネットのデータの取得、ストレージ、共有およびアプリケーションプラットフォームとして、物信チェーンはインテリジェントな輸送、スマートな製造、スマート都市や他の産業システムで広く使用することができる。図10に示すように、交通情報を例にとれば、物信チェーンは個人的なナビゲーションの最適化、支援された運転、交通派遣の最適化、およびのための全プロセス解決策を提供することができる。

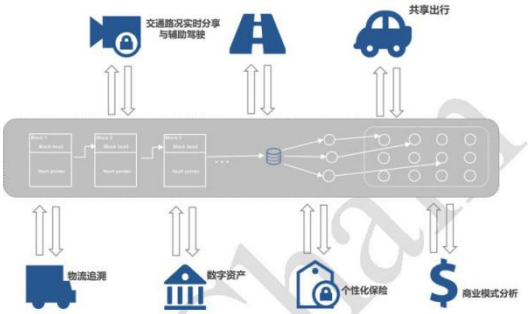


図10. CPChainに基づく典型的なIoTアプリケーションのシナリオ

交通路况实时分享与辅助驾驶 トラフィックのリアルタイムな共有と運転支援

共享出行 共有交通

物流追溯 物流トレーサビリティ

数字资产 デジタル資産

个性化保险 カスタマイズされた保険

商业模式分析 ビジネスモデル分析

4.1 データ共有ベースのアプリケーション

物事のインターネットのデータ共有

大きなデータの時代に、データの価値はよく知られている。 CPChainによって生成された膨大なデータも非常に高い価値を持ち、CPChainはブロックチェーン技術によってすべてのデータをユーザーに依頼し、大企業によるデータの独占を避けてユ

ーザーを支配することができる。

多数のIoTデバイスおよびユーザインタラクションによって生成されるデータはビジネスおよび科学研究分野において極めて高い価値を有する。人工知能の発達により、特に中小企業や大学などの科学研究機関にとって、高品質なデータが非常に重要である。物事のインタネットのデータプラットフォームCPChainのインターネットを開くことにより、大量の実データを低コストで取得することができ、これにより技術の進歩が大きく促進される。現在、研究機関は深い学習モデルの訓練を効果的に実施するために大規模な企業と協力したり、大企業のオープンなデータやオープンプラットフォームに依存する必要がある。実際、大企業によって習得された多数のデータはユーザーから得られるが、ユーザーは自分のデータを制御することはできない。CPChainプラットフォームに基づくデータ市場はこの状況を変え、図11に示すように、CPChainデータ市場では、ユーザーは異なる組織やサービス・プロバイダーに自分のデータを許可し、データのプライバシーと権利を保護することができる。ユーザーにとって、データ共有によって奨励を得ることができ、多数の実際の信頼できるユーザーデータを集めてより大きな商業価値を生み出すことができる。

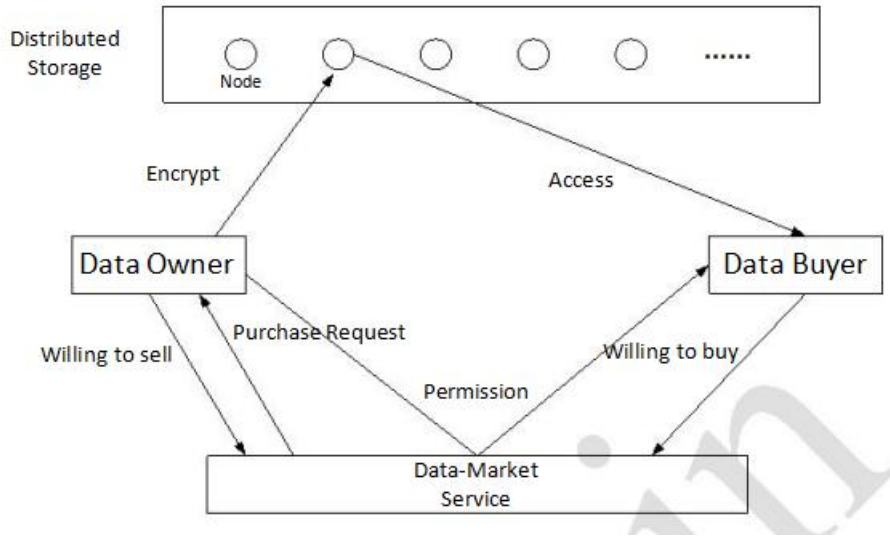
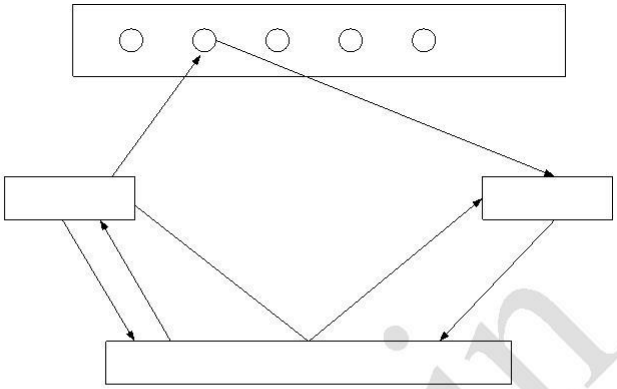


図11. CPChainに基づくデータ共有

パーソナライズされた自動車保険

現在の保険プランでは、自動車保険のカスタマイズレベルは非常に低く、初心者でも経験豊富なドライバーであろうと、購入オプションはあまり変わらない。経験豊富なドライバーはしばしば数年後に一度は危険を起こせず、そのコストパフォーマン

スは高くない。 保険会社にとっては、適切なデータのサポートがなく、異なる運転手の運転習慣を判断することは難しいため、リスクとメリットは包括的にしか考慮できない。異なる自動車保険商品を異なる運転者にカスタマイズするために自動車保険商品を設計することはコストが高くて実用的ではない。



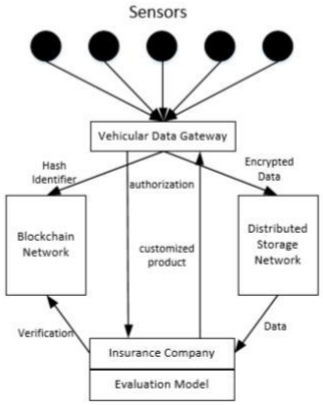


図12. CPChainに基づくパーソナライズされた自動車保険

CPChain 物事のインターネットデータプラットフォームは大量の車両データを収集し、各車両のデータをモデリングおよび分析することにより、運転者の運転スタイルを十分に評価することができる。これらの結果を通じて、保険会社は図12に示すように、より正確に各ドライバーの危険を起こす確率を計算し、より人間化したカスタム車両保険を設計することができる。CPChainデータプラットフォームと組み合わ

せたセンサー技術の進歩により、無人化の損害賠償請求が実現できる。事故後、搭載されているセンサーやロードカメラなどと組み合わせ、事故の責任と車両の損害に分けることができる。保険会社は事故後のクレームリンクをブロックチェインスマート契約で自動的に入ることができ、多くの時間と人員を節約する。

4.2 物信チェーンのサイドチェーンネットワークに基づくリアルタイムデータの応用

交通共有

共有のアプリケーションでは、乗客、ドライバー、共有交通サービス契約の3者が参加する。図13に示すように、CPChainの交通チェーンのリアルタイム通信システムに基づき、ドライバーと乗客は自らの情報を暗号化し、それを車両連動ネットワークにブロードキャストする。同時に、高速で安全なサイドチェーンコンセンサスアルゴリズムにより、迅速な整合と安全な取引を実現する。共有交通サービスはブロックチェーン内のスマートな契約として展開され、ドライバーと乗客に関する情報にアクセスし、バッファ内に一時的にデータを格納し、契約内のマッチングアルゴリズムにより、乗客のために一致する車両を見つけることができる。

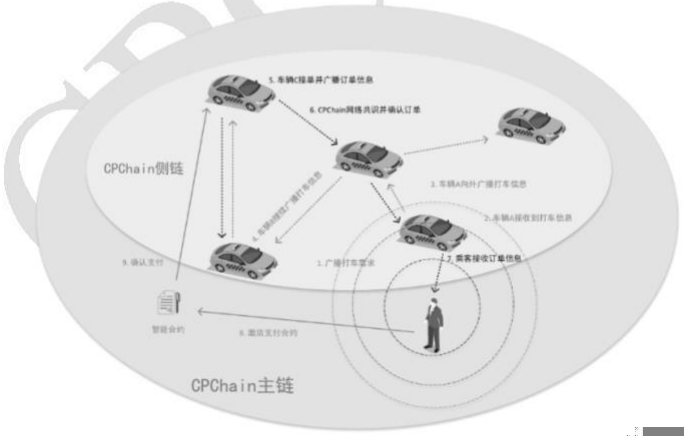


図13. CPChainに基づく共有交通アプリケーション

交通状況のリアルタイム共有と運転支援

現在、Baidu MapsとGaode Mapsなどの地図アプリケーションはリアルタイムの交通データを提供することができるが、CPCainプラットフォームなどの交通データプラットフォームが不足しているため、リアルタイムのデータ取得コストが高くなる。道路の状況を検出するための伝統の方法としては、道路の占有率、交通量、車速などの交通状況を検出するために主に使用される主な道路に、センスコイル、スピードレーダー、ビデオ監視ツールを設置している。

自動車のインテリジェンスの向上とセンサー技術の進歩とCPChainサイドチェーンデータのリアルタイム共有と相まって、より効率的なリアルタイム交通データ共有アプリケーションを構築することができる。車両は各センサデータをリアルタイムでCPCainプラットフォームにアップロードして報酬を得る。リアルタイムデータ共有アプリケーションはデータを収集して分析し、必要な車両に提供する。車両は線路の渋滞や緊急事故のより適切な理解に先立って情報を得ることができる。無人車両の場合、リアルタイムの交通情報を運転戦略に追加し、より良い制御ソリューションとリアルタイム調整を得ることができる。

無人車隊制御

無人車両制御プロセスでは、クラスターはトラフィック環境をインテリジェントに識別して検査し、クラスターメンバーの現在の移動状況を判断し、システムのバッテリー寿命を知り、安全なインテリジェントクラスター制御を実現するために、リアルタイムで信頼できる安全なメッセージ転送を渡す必要がある。無人車両制御システムはCPChainデータ（モーションステータス、位置、地形などの主要情報を含む）に基づいている。車両はクラスタメンバーのリアルタイムステータス情報を取得することができ、無人車両制御の通信コストと計算コストを削減できる。リアルタイムで、信頼性があり、完全な無人クラスターフリート状態情報に基づき、クラスター制御アルゴリズムを最適化することができる。クラスタ車両はクラスタ車両の追加や退避な

どの問題に対応し、迅速に関連情報を取得するために、システムの柔軟性と再構成能力を向上させることができる。それは無人のチームの自律性と悪意のある攻撃環境におけるセキュリティ制御機能を向上させる。

5. 物信チェーン開発ロードマップ

図14. CPChainの開発ロードマップ

项目启动 プロジェクトを開始する

白皮书发布 ホワイトペーパーリリース

架构梳理 フレームワークグルーミング

定位关键技术 キーテクノロジーのターゲット設定

Demo 测试 デモテスト

描写技术白皮书 テクニカルホワイトペーパーの作成

建立完整框架 完全なフレームワークを確立する

设定开发路线 開発ルートを設定する

核心技术开发 コア技術研究

相关专利申请 関連する特許出願

建立开源社区 オープンソースコミュニティを構築する

CPChain 平台 V1.0 版本发布 Cpchain プラットフォーム v1.0 リリース

核心技术模块开发 コア技術モジュール開発

代码逐步开源 コードは徐々にオープンソースされる

发布beta测试版 ベータ版をリリースする

批量产业解决方案落地 バッチ産業用ソリューションが上陸する

开发示例应用 サンプルアプリケーションを開発する

吸引更多企业与开发人员加入 より多くのビジネスと開発者を引き付ける

CPChain 平台 V2.0 版本发布 Cpchain プラットフォーム v2.0 リリース

物联网安全数据网关 IoT セキュリティデータゲートウェイ

行业链共识协议开源 業界連合コンセンサス契約オープンソース

典型物联网行业应用 業界の一般的なインターネットアプリケーション

CPChain は複雑なシステムアーキテクチャーを持ち、多くのテクノロジーを含んでいる。システムアーキテクチャーはシステムの開発中に徐々に進化する。

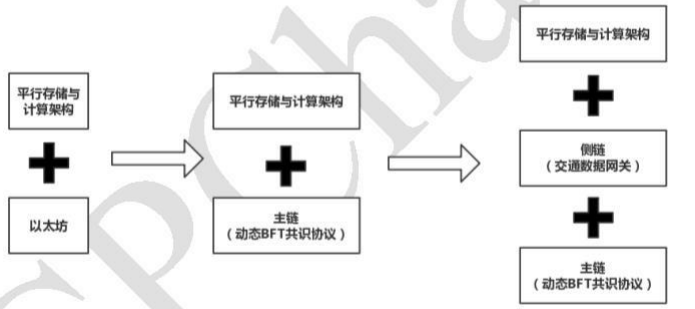


図15. CPChainシステムアーキテクチャの進化

平行存储与计算架构 並列ストレージとコンピューティングアーキテクチャ

以太坊 エテリアム

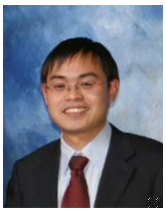
主链（动态bft共识协议）メインチェーン（動的bftコンセンサスプロトコル）

侧链（交通数据网关）サイドチェーン

（トラフィックデータゲートウェイ）

6. 物信チェーン開発チーム

物信チェーンの研究チームは国際化されたナレッジ･ストラクチャードで若手のチームである。創立チームのメンバーには、大学、物事のインターネット業界、財務・証券会社、商業業務から出身する。



龍承念博士、物信チェーンの創始者/チーフ・サイエンティスト
研究方向：物事のインターネット、ブロックチェーンに基づく分散スマートシステム

趙滨博士、物信チェーンの創設者
以前はAlcatel-Lucent上海ベルで働いていた、2015年以来、有名な国内証券会社の研究開発担当者を務め、物事のインターネット研究および通信の開発で12年以上の経験と豊富な研究開発チームを管理する経験を持ち、上海ベルを代表してさまざまな国内外の物事のインターネットの標準を制定する仕事を関与した。

史青偉、物信チェーンの共同設立者
ブロックチェーンとデジタル通貨の初期参加者、業界メディアの共有ファイナンスの創設者、そしてコアチェーンのHPB共同スポンサー、多くのプロジェクト準備と投資に参加した。

7.物信チェーンの経済モデルとシステム利用

CPCはCPChainの元の資産であり、CPCainの価値の起源はCPCainのデジタル経済活動を簡便に表現し測定することができるということである。CPChainの価値は2つのポイントに基づいている。まず、CPChainを使用するには一定量のCPCが必要であり、次にCPCを保持するのはCPChainコミュニティガバナンスに参加することができる。

1）CPCトークンの合計金額は10億であり、メインオンライン回線で1回生成される。

2）CPCの通常ノード（非DAPPアプリケーションノード）は一定量のデータを格納して交易する権利あり、指定されたストレージ容量およびトランザクション数を超えたり、頻繁に送信したりすれば、ユーザーはCPCを支払って追加ストレージとコンピューティングリソースを取得する。

3）DAPPアプリケーション開発者はネットワークとコンピューティングリソースのバランスを取るために、アプリケーションが占有するリソースに基づいて対応するトークンを保持する必要がある。トークンが不十分である場合は、リースすることができる。

4）DAPPアプリケーションによって生成されたトランザクションに対して、DAPP開発者はトランザクション料金を負担し、レンタル料を提供するサービスプロバイダにレンタル料金を支払う。

CPChain基金会は様々なスマート契約の開発者やサービスプロバイダーからCPCを収集し、様々なビジネススマート契約の運用を保証するためにスマート契約の運用に必要なGASに支払う。収集されたCPC収益の大部分はノードとして奨励を受け、ノードプロバイダに支払われる。残りの部分は基金会のその後の日常業務、ビジネス促進、技術開発に使用される。

エンドユーザー企業のニーズに基づき、アプリケーション開発プロバイダーはスマート契約サービスをさらに開発および処理し、エンタープライズ顧客またはエンドユーザー企業にアプリケーション製品を提供し、企業収益としてCPCを受け取る。エ

ンドユーザーはエンタープライズ製品とサービスを取るためにCPCを支払うことができる。

8. 物信チェーンのトークン配布計画

CPChainには合計10億トークンが発行されており、そのうち40%は海外のコミュニティや機関の資金調達に使用されている。

比率	配布計画	詳細
40%	海外コミュニティと機構投資	海外のコミュニティがCPChainの将来の発展にとって重要な力となり、これらの投資は海外のコミュニティの建設に使用される。機関投資家は構築された物信チェーンのエコシステムにおいての企業と物信チェーンの早期準備に寄与する者を指す。これらの投資者は将来のCPChainトークン（CPC）のビジネス活動においての使用に焦点を当てる。
25%	創業チーム、開発チーム、コンサルタント	創業チームと開発チームはプロジェクトの開発中に人力、技術、リソース、資材の面で貢献したため、CPCainトークン（CPC）をリターンとして使用し、ロックアップ期間は3年で、毎年バッチでリリースされる。
35%	コミュニティガバナンス	チームの継続的な運営と発展を維持し、ビジネス推進のための適切な産業を選択し、産業における戦略的な展開、プロジェクトのサポート、トークン交換を行い、産業アプリケーションの技術を真にビジネスランディングに活用する。

9. 物信チェーンの資金使用予算

日常運営	35%	当初のチーム給与、専門家と開発者の募集、技術特許と知的財産保護、営業基盤と市場支出など
技術開発	35%	技術研究開発、技術交流および共有、定期的な出版、同盟の創設または参加、コンミュニティインセンティブなど
ビジネス開発	20%	基金会の拡大運営と着陸のための一連のビジネスチャネル協力などを維持する
生態投資	10%	ブロックチェーン新しい技術と新しいチームへの投資

10. 物信チェーンのコミュニティガバナンス

CPChainのガバナンスはCPC保有者会議、意思決定委員会、実行委員会の3段階ガバナンス構造を採用している。

CPCの保有者会議は所有者が事前設定されたコードルールを通じてコミュニティのガバナンスに参加することを可能にする。意思決定委員会はCPC保有者会議を担当し、実行委員会は実施を担当する。実行委員会はCPChainプロジェクトの日常業務を担当し、戦略的投資センター、財務管理センター、運営管理センター、コミュニティサービスセンター、イノベーション管理センターを含むいくつかの管理センターを持ち、対応する事業部門が業務を遂行するよう指導する。

CPChainチームはCPChainガバナンスの主体であるシンガポールの基盤を確立し、CPCain技術の開発とアプリケーション開発の管理を担当し、CPC保有者の権益を保護し、CPChainブランドの推進を担当している

11. 物信チェーンの初期投資家