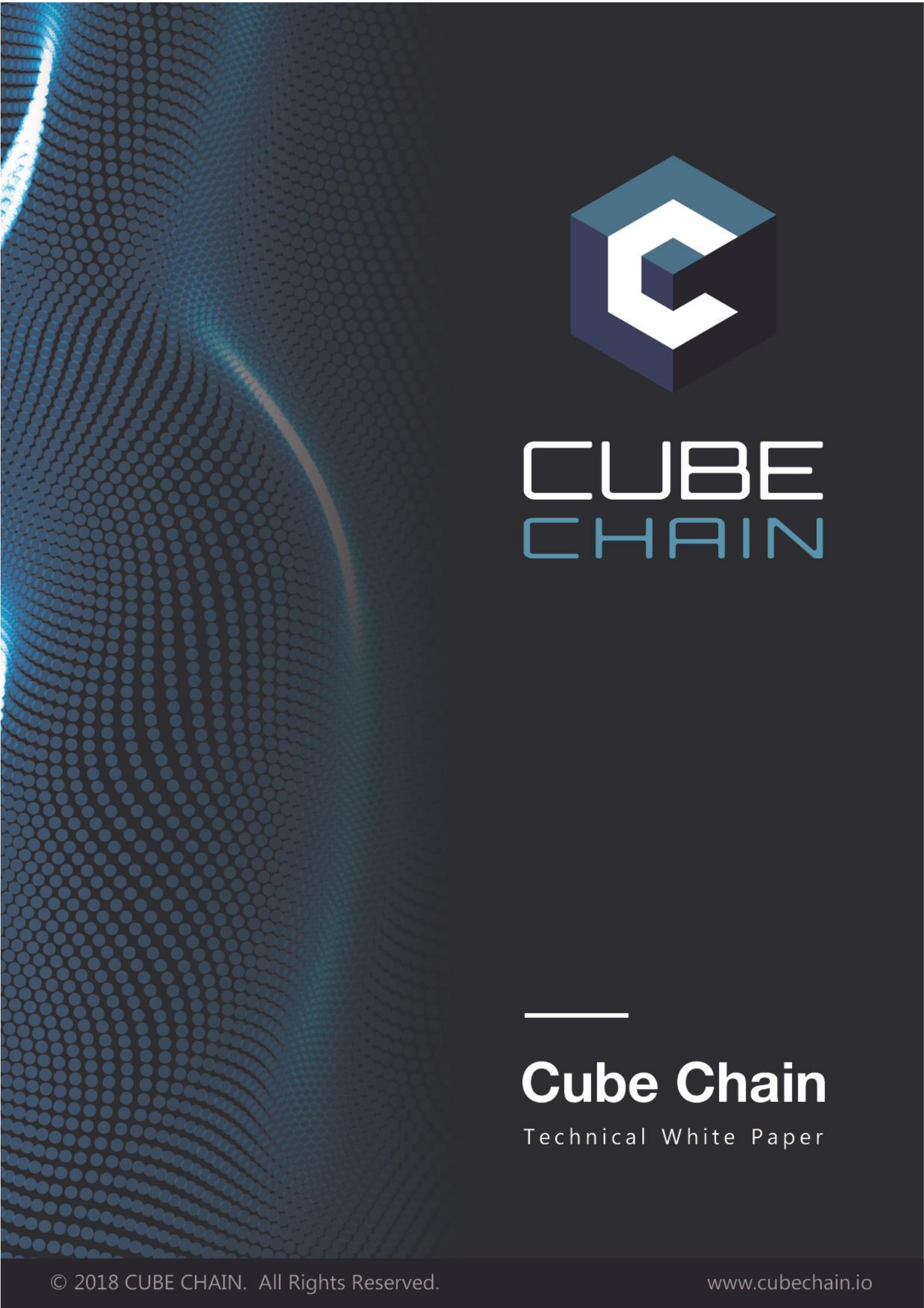


CUBE
CHAIN

Cube Chain

Technical White Paper

www.cubechain.io

Contents

1. 概要

ブロックチェーンは、データを一定の時間単位で集めて、データブロックを生成し、ブロックを暗号化したハッシュ値を使用してデータを検証し、このように記録されるデータを分散サーバに保存するシステムである。そして、暗号化を通じたデータの検証と同じデータを分散保存し、データの信頼と安定性を確保するためのシステムである。

既存の使用されたデータベースに比べてブロックチェーンの利点は、データを時間順に暗号化検証して不可逆的であり、これを P2P 方式で同じデータを共有して保存することで、データを非常に安全に保護して維持することができるという点にある。

多数のユーザーからの信頼を得なければならい暗号通貨技術にブロックチェーンが使用され、今日の暗号貨幣市場の基盤技術として定着する事にはこのような理由がある。ブロックチェーンが暗号化方式と P2P 方式を使用して独自のデータ記録方式を実装して、新しい技術の地平を開いたが、まだ技術的な限界を持っている。ブロックチェーンが既存のデータベースを適切に変換する速度の改善と使用の利便性など、既存のデータベースが持っている技術的な機能が伴われなければならない。ブロックチェーンの技術が持続的に発展して、データベースを置き換えることができるレベルになれば、データを記録して管理する非常に安全な方法で位置づけられるものである。

そのような観点から、キューブチェーンは、ブロックの代わりに、キューブと呼ばれる概念を使用してデータベースの機能要素を拡張していくことができるよう構造化した。したがって公開データベースの安全な使用のために、既存のブロックチェーンが持つ長所をベースに、データベースが持ついくつかの利点を活用できるようにした。キューブチェーンの開発は発展したブロックチェーンの源泉技術を確保して、暗号通貨を発行して公開用データベースを必要とする様々なオンラインサービスを実装する予定だ。

１．２　基本情報

Cube Chain (QUB)

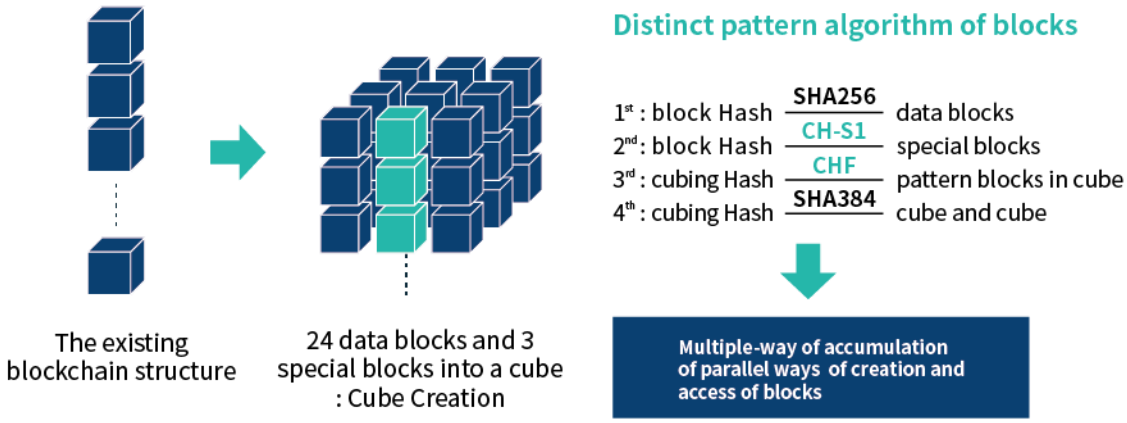
コイン名：Cube Chain
総発行量：120 億枚
アルゴリズム：SHA256,CH-S1,CHF,SHA384
補償方式：POH (Proof of Hybrid: POW+POS)
POS 参加条件：ウォレットに最小限５千枚以上のキューブコイン保有
開発スタート：2017 年 1 月

２．キューブチェーンの特徴

まずブロックチェーンの中核であり、暗号化技術用語であるハッシュに対して以下のように説明する。暗号化ハッシュの一種である SHA256 に対する定義である。ハッシュは「特定のデータを象徴する、常に同じ長さのデータに変換する行為」を意味する。ここでは象徴データは、元のデータが少し変わっても確実に変わる特性があり整合性を守るために役立ちます。たとえば、「A」という文字列のハッシュと「B」という文字列のハッシュはわずかなアルファベットが異なるだけなのに、その結果が千差万別ということだ。例えば、代表的なハッシュアルゴリズムである SHA256 はどのような入力値を入れても常に 256bit の他の 64 桁の 16 進数の値を返す。

２．１　キュービング

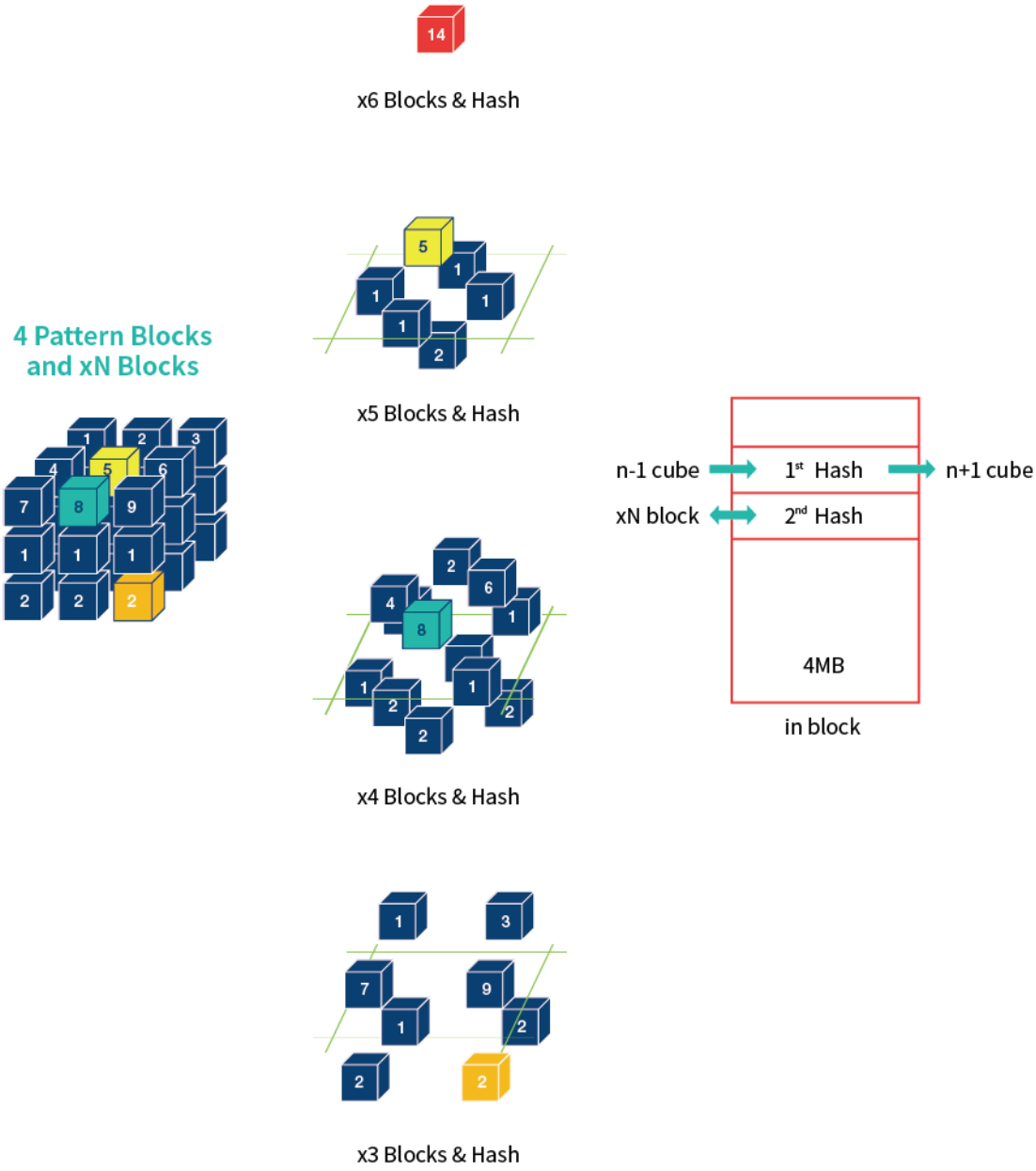
キュービング（キューブ化）は２７個のブロックを集めてブロックの集合体である一つのキューブにするキューブ化技術を意味する。取引履歴を記録した 24 個の一般的なブロックと 3 つの特殊なブロックが合わされ一つのキューブを作成する。単純な Grid 概念ではなく、並列に管理され、同時にブロックが生成される技術である。27 個のブロックが生成されると同時に、キュービング（キューブ化）は行われ生成されたキューブは、もう一つのハッシュ値を作る。その後記録されるすべての帳簿は、持続してキューブを作成し、ハッシュ値は、ブロックとブロックではなく、キューブとキューブを繋ぐ。これは、ブロックが接続され、生じる 1 次暗号化となる。さらに、キューブが接続され生じる 2 次暗号化現象を作り出して、既存のブロックチェーンよりもはるかに強力な暗号化技術のブロックが生成されると同時に、キューブ化は行われ生成されたキューブは、もう一つのハッシュ値を作る。キュービングによりキューブのハッシュ値が作成される事でブロックのハッシュ値と一緒に二重に検証されているデータのシステムを構築することが出来る。



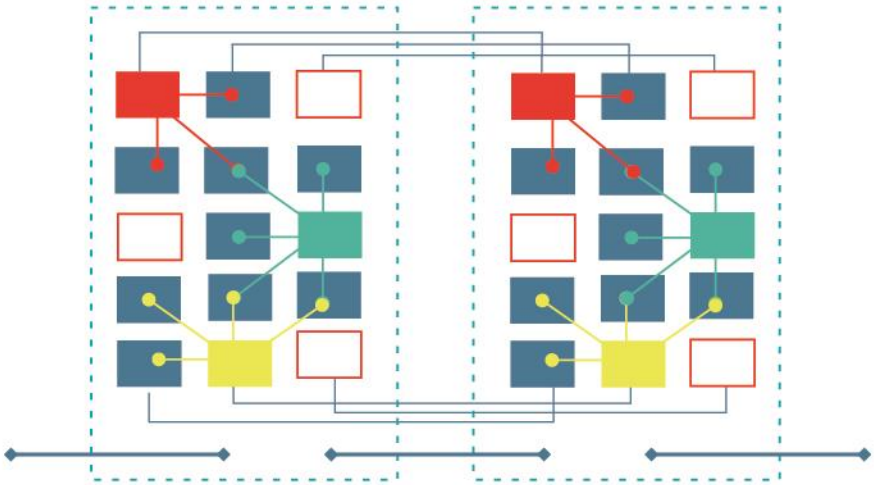
既存の直列の接続構造に起因する速度の低下とスケーラビリティの問題を解決するために、24 個のトランザクションのプールを介して並列構造にデータブロックを迅速かつ安全に生成されたのがキューブチェーンである。トランザクションプールで同時に生成された 24 個のデータブロックがキューブへの積載まで続いて高速で安全な処理が可能である。キュービングと呼ばれる技術を使用して、大量のデータブロックの並列処理を管理し、二重ハッシュ関数とパターンブロック構造を介してブロック間の高速なアクセスが実現できるように設計した。

ブロックが 1 つのキューブに合わされるとき、4 つのハッシュ関数を使用してセキュリティを強化した。ここで使用されるハッシュ関数は SHA256、CH-S1、CHF、SHA384 で SHA256、SHA384 は公開されたハッシュアルゴリズムである。下の独自開発されたハッシュアルゴリズムについて説明する。CH-S1（CubeHash Special Version1）は、特殊なブロックが作成時にハッシュ関数を作成するときに使用する独自開発されたアルゴリズムであり、CHF（CubeHash Function）は、キュービング過程でパターンブロックにハッシュ関数を作成するときに使用する独自の開発されたアルゴリズムである。

構造分解と説明
キューブチェーンは、複数のブロック積載と並列ブロックを生成し、アクセスして速度を向上させる構造を有する。



キューブを分解すると、上記のような 4 つのブロックパターンが存在する。



各パターンブロックは、直前のキューブの最も近いブロックと接続され、
図の 2nd Hash に xN ブロックのハッシュ値が格納される。
キュビンによるキューブの接続は、直前に生成されたキューブのハッシュ値が図の 1st Hash に保存される事により直前に生成されたキューブと接続される。これにより、各ブロックとブロックが接続され、キューブとキューブが接続される。各パターンに接続されたブロックのハッシュ値は、キューブに保存される。

２．２　インデクシングブロック

インデクシングブロックはブロック全体の膨大なデータを一目瞭然に整理して、検索機能が強化される。インデクシングブロックは全体の取引に含まれているウォレットアドレスごとに取引が行われたキューブの高さ（既存のブロックチェーンのブロック高さ）をまとめたデータブロックである。したがってインデクシングブロックのみで対応されているデータを、より短時間で見つけることができる。たとえば、A というアドレス：20c（20：20 のキューブ、c：3 番目のブロック）、32a、105h、201j、302r キューブブロックの位置、B というアドレス：3b、102v、201s、1001q キューブブロックの位置、C アドレス 5c、34e、56g、234k、456y キューブブロックの位置など、上記のようなすべてのアドレスをアドレス値順に整理した後、該当するブロックの高さをアドレス値に合わせて整理する。検索者が B アドレス内の特定の取引を検索したいとき、Indexing Block 内整理された B アドレスのように、特定の取引を迅速に見つけることができる。インデクシングブロックの目的は、特定のアドレスの履歴を簡単に探して簡単に管理できるようにしてくれる。

[既存のブロックチェーンの方式]

特定のウォレットアドレスの取引履歴検索時にすべてのデータを検索
（すべてのキューブ 1,000 個のキューブの生成時に 1,000x24=24,000 個のブロックを検索）
時間の複雑さ = $O(B \log 2\ I)$

[キューブチェーンの方式]
ウォレットアドレス、キューブの高さとブロックの位置に関する情報だけを持っており、そのデータを持っているブロック全体をスキャンする必要がなく、インデクシングブロックでウォレットアドレスだけを検索すると、そのデータを取得することができる。
時間の複雑さ = $O(\log 2\ I + \log 2\ I)$
例）特定のウォレットアドレスの取引履歴検索時のインデックスブロックだけを検索
（1 つのブロック+1 つのキューブ）

２．３　スタティスティックスブロック

スタティスティックスブロックはブロック全体の統計値をまとめて、応用サービスと各種 API でも迅速なロジックの実装と、さまざまな活用性を提供する。スタティスティックスブロックは非常に高速なデータ処理を実現します。たとえばスタティスティックスブロック内で POS 対象者が 5,000 枚以上であるため、残高 5,000 以上のウォレットアドレスのデータ、残高が多く、ウォレットのトップリスト 1000 個、変形回数が 100 回以上の電子財布のリストを集めておくことができる。他にも使い勝手が多く、統計データを集めておいて、いつでも必要なときにリストをすばやく出力することができる。
これらの統計は、ブロック全体の統計値に整理された内容がない場合は、検索時に多くの時間が必要な部分だが、スタティスティックスブロックを使用すると、短い時間内にサービスの処理が可能である。残高が多く、ウォレットのトップリスト 1000 個、取引履歴が 100 回以上のウォレットリストなど、頻繁に使用される出力データを集めておけば効果的な検索を達成することができる。結果的に、対応するアプリケーションサービスの API を非常に迅速に実装することができる。

例）キューブの高さに応じた POS 対象者検索のための検索ブロック

[既存ブロックチェーン方式]
ブロックの高さ 1,000 ： 1+2+3+ ... +998+999+1,000=500,500x24=12,012,000 ブロック
ブロックの高さ 10,000 ： 1+2+3+ ... +9,998+9,999+10,000=50,005,000x24=1,200,120,000 ブロック
[キューブチェーン方式]
キューブの高さ 1,000 ： 1+1+1+ ... +1+1+1=1,000 ブロック
キューブの高さ 10,000 ： 1+1+1+ ... +1+1+1=10,000 ブロック

キューブが 1,000 個だけ溜まっても取得する必要があるブロックの数は、10,000 倍以上の差がある。リストを整理する過程とその履歴を検索する過程を考慮すると、これより大きな差が生じるものである。現在までに検討している機能は、単一の取引で 1000QUB や 2000QUB 以上が取引されている内容についての統計、残高ランキング 1～1000 などまでの統計は、全体の取引量/全取引回数の統計情報、未承認エスクローの統計である。

２．４　エスクローブロック

エスクロー(escrow)は商取引の際に、売り手と買い手の間に信頼できる中立的な第三者が仲介して金銭や商品を取引することを意味する。取引の安全性を確保するために使用される。具体的には、売り手・買い手・第三者の間では、次のような手順で行われる。バイヤーは第三者に代金を任せる。売り手は第三者への入金を確認して購入者に商品を発送する。バイヤーは送付された商品を確認して第三者に商品が到着したことを知らせる。当初の取引内容と異なる場合は、商品を返送するか、取引を破棄することができる。第三者は、売り手に代金を送金する。売り手は代金を受領する（取引の終了）。仲介する第三者は、一定の手数料を受けることの利益を得ることが一般的なエスクロー取引方式である。

キューブチェーンでのエスクロー取引は、取引の締結がされてももらった財布ですぐに使用することができない状態になって、必ず承認が行われてから使用することができる。一般取引は 24 個のデータに分散して記録されるが、エスクロー取引の際には、エスクローブロックに記録される。

暗号通貨エスクロー問引き時の承認、暗号化キーを作成し取引することができ、承認暗号化キーを送信者と受信者が暗号化キーを使用して承認処理を行うことができる。この時、承認、暗号化キーは、自動生成方式と送信者が作成し送信する方式がある。暗号化キーの承認許可方式でも送信者だけ受け入れられるように、あるいは受信者側で承認できるように、送信者と受信者の両方を可能にする必要が受け入れ可能な方法で処理することができる。また、一定期間後に自動的に承認方式もあるがこの時の承認キーの自動承認を解除しない限り、一定期間後、承認されて、受信者の使用可能な状態になる。この時、自動承認解除をすると、送信の側での承認を可能にする方式に切り替えされ、エスクロー状態許可時まで維持される。そうなれば、受信者は、取引をキャンセルすることはできませんが、送信者が使用することができないため、持続して取引や契約を守るよう要請することができる。

承認キーを許可方式で受信者の承認許可方式は、送信者側ではメールやメッセンジャーなどの通信手段を介して承認キーを渡せばいい。既存のエスクロー取引は仲介がトレーダーの間の中間で取引の役割をした場合、エスクローブロックは仲介がないエスクロー機能が特徴である。もちろんサービスの実装に応じて、従来の方法のように、第三者が中間紹介の役割も可能ですが、直接の当事者間の取引のみエスクローを導入することができるという大きな特徴がある。オンラインショッピングモール、オープンマーケットだけでなく、ショッピングモールがない個人間の直接取引でも簡単かつ安全な取引が行われれるようにする画期的な方法になることができる。

エスクローブロックには、Double authorization data system（二重承認方式）を導入し、
データを保存する。一般データは、24 個のデータのいずれかの記録が、エスクローデータは別々に保管管理される。エスクローデータは、二重承認が行われる時点で、通常のデータに書き換えられる。

Double authorization data system（二重承認方式）とは、一般的なブロックチェーンを使用した取引の際、行われる電子署名のほか、暗号化キーを追加発行し、承認しなければなら取引可能な方法をいう。エスクローブロックを使用したこの方法は、暗号通貨で取引の締結がされてもウォレットですぐに使用できない状態になり、第三者が中継するエスクローの形ではなく、取引当事者間の取引を保護する機能を付与することができる。ブロックチェーンをベースにしたエスクロー機能である。
また、エスクローブロックは、所有者がパスワードを使用してデータを保護する際に使用することができる。データをオープンされた形で使用するのではなく、暗号化を介して、パスワードを知っているユーザーのみがデータを確認できるようになるのだ。

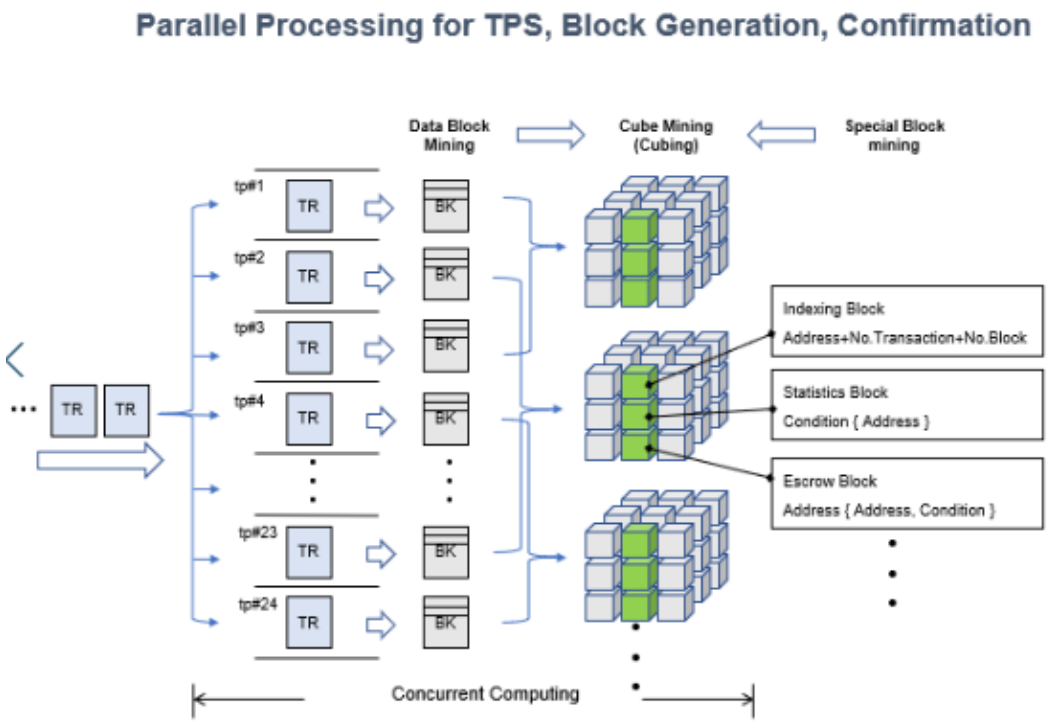
一般ブロックと特殊ブロックのサイズと作成までの所要時間

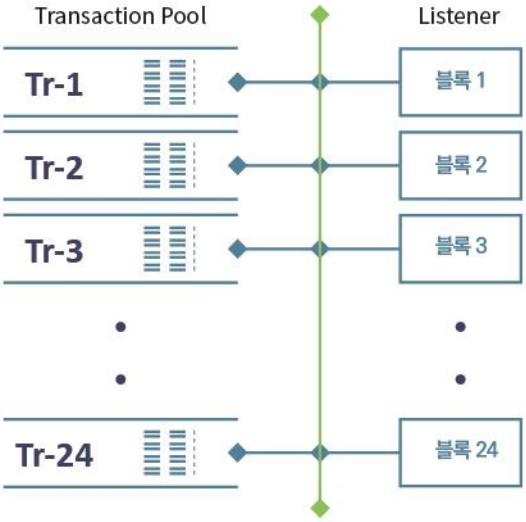
一般ブロック：1 つのブロックは 4MB である。
特殊ブロック：3 つの特別なブロックの容量は可変的であり、キュビンで一般ブロックが作成されるときに生成される。

キューブのサイズ：特殊ブロックは、特定のサイズが決まったわけではないので、α と定める。
1 キューブ=24 ブロック*4+α、すなわち 1 キューブは 96+αMB のサイズを持つ。

トランザクションプールにデータの到着からキューブ生成までの過程

トランザクションプールに取引履歴、またはその他の情報（入力されたデータの種類が複数存在可能、ただしすべてのデータは、ハッシュ（暗号化）処理されたデータの長さとサイズは同じ）が到着すると、トランザクションプールで Tr1～Tr24 までのデータが順次割り当てられて、一般のブロックを生成する。特殊ブロックは、以前のキューブが生成されると同時に、以前のキューブの特別なブロックがコピーされ、優先的に生成される。





各ブロックは、各 4MB の最大サイズを持つが、場合によっては 4MB 以下の場合もある。4MB 以下のサイズを持つ場合には、トランザクションプールにデータが入ってくる順序は、ブロックの順序入り、1 件のトランザクションが 1 つのブロックに割り当てられ、このような方法で並列処理が行われる。採掘者 24 のブロックのうちのリソースが許す限りで重複して選択し、採掘に参加することができる。
例えば、24 個の一般的なブロックの採掘選択で 2,3 番目のブロックを選択して採掘することができ、特殊なブロックも選択して採掘することができる。

２．５　POH（Proof of POW+POS Hybrid）

POW+ POS Hybrid 方式を採用してマイナーのネットワークへの参加を誘導しながら、電力の無駄を減らす。POW と POS 混用時 POS を計算して支給するために時間がかかる欠点があるが、Statistics Block 統計機能で計算の欠点をなくし、POW と POS の割合を確定した。

POS 参加条件は、ウォレットに少なくとも 5,000 枚以上の Cube Chain コインを保有する必要があり、条件に合致する対象者に残高の比率に応じたコインの報酬支払いをする。POH は POW と POS を組み合わせた方法で、POW はプロトコル（コンピュータ間で情報を送受信するときの通信方法に関する規則と約束）であり、プログラム関数である。これ Proof-of-Work の略で作業証明方式を意味する。 POW は、多くのハッシュ（Hash）を保有している人がコインを得ることができるブロックをより多く発見することができるシステムを意味する。サービス拒否攻撃とネットワーク上でのスパムのようなサービスの乱用など処理時間を必要とするサービス要求に、いくつかの作業を必要とすることで、やめさせる経済的な手段である。現在「採掘」が可能なすべてのコインは POW であり、現在最も普及している方法であり、市場も大きく、インフラが継続的に拡大しているコインはほとんど POW 方式である。ビットコイン、ライトコインなどのアルゴリズムを緩めコインを報酬として得る概念のすべてのコインは、全て POW 方式である。 暗号通貨が POW のビットコインからだったので、現在の主流は、当然 POW 方式であり、市場の規模は、POW が POS より圧倒的に大きい。

POS は、POW の最大問題点である、「採掘に入る多くの費用と維持費（電力の使用、機器の購入費）の節約」、「ハッシュの独占によるセキュリティ上の問題」を解決しようと作られた方式である。POS の場合、インターネットが接続された PC1 台あれば、すべての準備が終わって、より良い CPU より良い GPU のように、もはや機器の追加が必要ない。コインを得る方法は、各コインごとに得られた方式、量は異なるが、基本的に POS は持っているコインの量が多ければ多いほど、より多くのコインを継続的に得ることになる（利子のような概念）。

POS という名前のように、全体のコインの多くの株式（Stake）を保有している人が追加で発行されるコインの多くの数量を持って行くが、POW は「ハッシュ」は、これらの機能をしたら、POS は保有している「コイン」の量この基準となる。だから POS 方式には、セキュリティのために大規模なハッシュが必要としておらず、各個人がコインを保持して、ウォレットを連動させておくだけで、強いセキュリティの壁を作り出すことができるのだ。 また、発売初期に大量のコインが短期間に発行され減っていく POW とは違って、いつも一定の量が少しずつ発行されるので、価格が大幅に上昇または下落する場合が少ないという利点がある。また、採掘に消費される大量の採掘機が要らないので、より多くの人が簡単にコインを接し、使用することができる。しかし、価格の上昇幅が大きくないため、「大量の資金」が流入されなかったという点（現在保持する必要は少ないため）、「資金」の多い人が簡単に独占することができる点、株式を通じた利点が POW より少ない点、初期コインの流布が公平していない点などの理由が弱点に存在する。

キューブチェーンは POW と POS 比率が 7：3 で開始され、時間の流れにより POS 割合が高くなって、最終的には、POS のみ維持されるようにした。初期の POW を高め、ネットワークが安定的に構築されるようし POS を高めながら、ネットワークリソースと電力の無駄を削減する方法を使用した。
POW と POS 混用時 POS を計算して支給するために時間がかかる欠点があるが、キューブチェーンの Statistics Block を利用すれば、毎回繰り返して計算する非効率性を大幅に削減することができる。初期には、採掘が生態系を造成する役割をするので、POW の割合が高いが、資源の浪費の問題が深刻で、競争を通じた非効率性が増大するという問題があって、POW を最初には高く持っていくが、段々と割合を調整して POS のみ可能にする。POW と POS の利点を時間的に配分して、適正な利点をとるようにする。

３．暗号化技術

３．１　ウォレットの生成

ウォレットの生成で最も多く使用される方法は、非対称型（公開キー、個人キー）暗号化方式である。非対称暗号化方式は、二つのキーをペアで持ち、一つのキーで暗号化すると他のキーで復号化することができる。二つのキーの中の公開キーは、ウォレットの生成時に、ウォレットアドレスとして使用され、もう一つは個人キーで伝送時にパスワードとして使用される。キューブチェーンはウォレットのアドレスとパスワードの生成で非対称型の暗号化方式（Asymmetric Cryptographic Technique）である RSA（Rivest Shamir Adleman）アルゴリズムを使用する。

３．２　デジタル署名

ウォレットを介して伝送すると、デジタル署名の過程を経ることになるが、この時、暗号化方式は、対称暗号化方式（Symmetric cryptographic technique）である AES256 を使用する。 ウォレットアドレスとパスワードを生成する RSA Algorithm の非対称型暗号化方式は、キーを公開しても、ハッキングすることができないパスワード配信の問題を解決したが、速度が遅い欠点がある。だからキーの交換上の難しさがありますが、暗号化と復号化の速度が速い利点がある AES256 方式と混合して RSA の欠点を保護するようにする。データのサイズが小さい場合は、RSA で生成された公開キーと個人キーを使用して、デジタル署名暗号化キーを生成するデータの暗号化処理方式が効率的ではない。しかし、データのサイズが大きくなるほどその効率ははるかに増大する。

３．３　ブロックハッシュ関数

ハッシュ関数は、データを固定された一定の長さのハッシュ値に変換して出力する関数である。この変形されたデータは、元のデータを復元する復号化はされず、データの整合性を検証したり、パスワードを認証するために使用する。ブロックチェーンでは、n 番目のブロックのハッシュ値は、n-1 番目のブロックのハッシュ値と接続される。

キューブチェーンでは、そのブロック内の 27 個の各ブロックのハッシュ値を作るが、この時のデータブロックに使用されるハッシュ関数は、SHA-256 を使用する。 特殊ブロックは、通常のデータブロックよりもデータが徐々にさらに増加するため、従来のハッシュ関数とは違う他のハッシュ関数が使うべきで、それは独自開発された CH-S1 関数を使用する。既存のハッシュ関数を使用時に深刻な速度低下が起こることがあります。これらの速度の低下を防止するために、既存の他のデータの抽出/圧縮過程でハッシュ処理速度を飛躍的に高めた CH-S1 ハッシュ関数を使用する。

３．４　キュービングハッシュ関数

キュービングを行うとき、暗号化方式は、独自に開発した CHF-Algorism（Cubing Hash Function Algorithm）を使用する。キューブ内 27 個のブロックは、各ブロックの位置に応じて、隣接するブロックがそれぞれ異なっている。 六面体の各面の位置に基づいて角に位置するブロック 8 個、中心部に位置ブロック 6 個、中心を取り巻くブロック 12 個、キューブの真ん中のブロック 1 個で構成されている。4 つの区分に応じて使用するハッシュ関数も異なるが、それぞれ CH-B3、CH-B4、CH-B5、CH-B6 と命名する。 前の CH（Cubing Hash）はキュービングハッシュ関数を意味し、後の B（Block）は、あるブロックからキューブ内の隣接ブロックの数を意味する。

キュービングハッシュ関数は、隣接するブロックのハッシュ値を利用して、別のハッシュ値を生成します。このようにして、27 個のブロックのそれぞれのハッシュ値を得る。キュービングハッシュ値がブロックハッシュ値と他の特徴は、ブロックデータをベースにしたものではなく関連したブロック

のハッシュ値に基づいたという点である。キュービングハッシュ値を通して、現在のブロックとブロック全体を検証し、27 ブロックが個別にチェーン関係を作って検証する。キューブ内の位置の値を使用して、互いのブロックを検証するようになり、この時一つのブロックだけ違っても、全体の値が違ってくる。

３．５　キューブハッシュ関数

キュービングで得られた２７個のブロックのすべてのハッシュ値と以前キューブのハッシュ値を含んで現在キューブのハッシュ値を生成する。キューブのハッシュ値を作るのに SHA-384 関数を使用する。

４．特殊ブロック生成プロセス

４．１　特殊ブロックの設定

キューブチェーンではデータだけを持って動く事ではなくデータ領域と特殊機能のデータを区分して拡張出来るように設計した。暗号通貨の為には３つの特殊ブロックを設定しましたが、アプリケーションの開発の為には特殊ブロックを別途に設定して使用可能し、これはゼネシスファイル設定を通じて可能である。特殊ブロックはコアーを設置する時、設定だけで使用出来るようにしたし、これを通じて多様な分野に易しく適用出来るように設計された。キューブチェーンでは多様に定義された特殊ブロックを用意しましたし、今後継続的に追加する予定である。

４．２　特殊ブロックの種類

特殊ブロックには Indexing Block, Statistics Block, Escrow Block, Format Block, Edit Block などがある。この中、３個のブロックについては前述したので省略する。

Format Block（フォーマットブロック）

Format Block はデータブロックに記録されるデータフォーマットが柔軟性のある様に変化が必要の場合使用される。フォーマットを決定する情報を変更すれば Format Block はデータの有効性検査を自動に進めて、これを通して間違ったデータが格納されるのを防止し使用者とプログラムのエラーを防止する。データの形式に対するデータのみ保管するだけで、使用者が使う一般データは使用されない。

Edit Block（エディットブロック）

Edit Block は既存データを修正する目的に使用する。ブロックチェーンの非可逆性は長所であり、同時に短所でもある。暗号通貨では必須的な部分であるが他の応用サービスではデータの修正が必要な場合もある。この為 Edit Block を設定して修正事項を易しく反映と管理が可能である。
修正するデータを Edit Block に入れて、本来のデータを参照する時 Edit Block にあるデータを反映して提供する方式である。ブロックチェーンのデータが単純に取引履歴としてのデータだけでなく、修正および削除が可能に参照値を連結または切る事によりデータの修正が可能になる。但し、特殊ブロックの中 Format Block と Edit Block はプライベートブロックチェーンを導入しようとする機関か企業を対象にするものである。

２４個のブロックの中、２個のブロックが特殊ブロックに転換されることにより、２２個のデータブロックが残ることになる。実際にブロックチェーンのデータを修正する形ではなく、修正されるデー

タにブロックデータを追加して、参照するデータの領域位置を変更する事に理解出来る。すなわち、既存データの修正ではなく、サービスかアプリケーションで使用可能なデータに変換する事を意味する。Edit Block と Format Block はキューブチェーンコインの発行とは関連なく、サービスの要請により追加される選択事項の特殊ブロックである。

４．３　特集ブロックが生成される過程

特殊ブロックはデータブロックに基いて再加工されたデータ又は反映されるデータである。必須の特殊ブロックとして選ばれる３つの特殊ブロックはデータブロックの再加工データとも言える。特集ブロックが生成されるたまには以前データブロックの存在が必要である。したがって最初の１つ目のキューブでは空いているデータで生成される。

特殊ブロックは２番目キューブから生成される。特殊ブロックの生成時点は直前のキューブの生成が完了されると同時に生成され始め、現在キューブに含まれるデータブロックらが生成完了される時点に含まれてキュービングが行われる。このようなプロセスは特殊ブロックの生成時間のせいで発生するキュービングの遅延時間をあらかじめ防ぐ防止するためである。

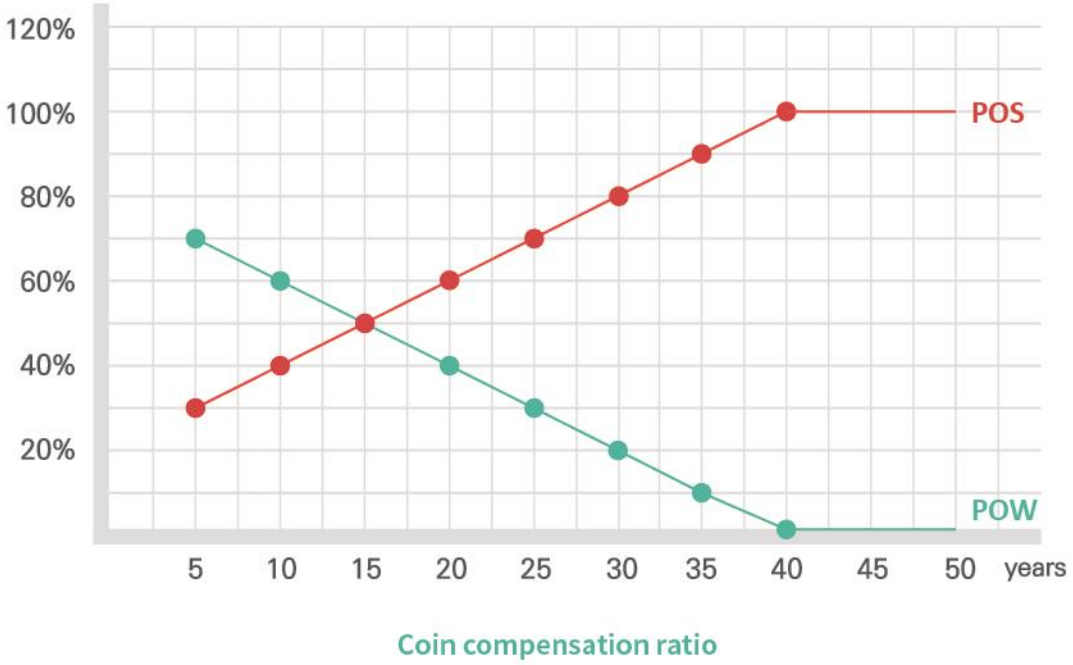
特殊ブロックは直前の特殊ブロックデータから抽出された内容と以前データブロックの内容を追加して累積データを反映する。

すなわち、ｎ番目の特殊ブロックはｎ－１番目のキューブまでのデータを格納している。ｎ－１番目のキューブが完成される時点からｎ－２番目キューブのデータを格納した特殊ブロックとｎ－１番目データを合わせて作られはじめ、ｎ番目のキュービングが成し遂げる時、データブロックと有機的な関係を形成するようになる。特殊ブロックはキューブが生成されキューブとキューブがチェーン化が成し遂げる時間の間に生成されることで機能的な部分は拡張されるが、これにより遅延される時間はない。また、特殊ブロックの暗号化は自体開発したＣＨ－Ｓ１関数を利用してデータ量に比べて非常に速い速度でハッシュ値が得られる。

５．合意方式

５．１　ＰＯＨ（Proof of POW+POS hybrid）

キューブチェーンの基本採掘方式はＰＯＷで作業証明に参加したノードにコイン補償を行う。しかしＰＯＷの過度なネットワーク資源浪費と激しい競争による難易度の上昇問題を解決するためにＰＯＳの補償方式を結合したＰＯＨ（Proof of POW+POS hybrid）方式を採択した。
キューブチェーンだけのＰＯＨ方式はＰＯＷとＰＯＳを同時に進めながら、段々ＰＯＳの比率が上昇する。これはＰＯＷによる採掘の産業化を防止して、ネットワーク資源浪費を防ぐのを目標にする。



ＰＯＷ採掘は３つの方式で参加出来るし、データブロックの生成、特殊ブロックの生成、キュービング作業時に各項目別に選択して参加出来る。

５．２　ＰＯＷ補償方式

作業証明に参加したノードはキューブ毎に支給された補償が計算されて支払われる。
作業の重複で参加する場合、重複で計算されて支払われるし、項目別には合計されて支払われる。

- データブロックを生成時、ハッシュ値に追加された任意値を捜し出す演算を行る事により補償する。この時２４個のデータブロックに対して補償が支給されるし、複数参加時、複数で支払われる。
- 特殊ブロックは生成される時、ハッシュ値の検証に必要な演算を行う事により補償する。
- キュービングの過程でキュービングに使用される暗号化関数を検証する演算を行う事により補償する。

- 一般ブロック２４個、特殊ブロック３個、キュービング１個に構成され、別に補償支給されるし、重複参加時重複に支払われる。

５．３　データブロックの採掘過程

- ブロックのタイムスタンプと、そのノードの難易度を確認する。
- ブロックのタイムスタンプが前のブロックのタイムスタンプと比較して有効範囲を確認する。
- ブロックに含まれるデータや取引についてのリストを作る。
- ブロックヘッダのツリー構造を確認して有効性を確認する。
- 以前キューブでブロックのハッシュ値を繋げて 1 次ハッシュ値を作る。
- 以前キューブのパターンブロックを利用して、2 次ハッシュ値を作る。
- ブロックを生成し、ノードにブロックデータを知らせる。

５．４　特殊ブロックの採掘過程

特殊ブロックの採掘は、キューブチェーンだけが持つことができる採掘方式である。

- 特殊ブロックのタイムスタンプを確認し、その特殊なブロックのヘッダを確認する。
- データブロックで特殊ブロックに追加されるデータを抽出する。
- データの数を項目別小計と総計を計算する。
- この計算のためのモクルツリーを作成して確認して有効性を確認する。
- 以前キューブでは、ブロックのハッシュ値を接続して、1 次ハッシュ値を作る。
- 以前キューブのパターンブロックを利用して、2 次ハッシュ値を作る。
- 以前の特殊ブロックに追加されるデータを入れる。
- ブロックを生成し、ノードにブロックデータを知らせる。

５．５　キュービングの採掘過程

キュービング採掘は、キューブ化というユニークな方法のデータ構造のための演算で採掘する。
キュービング採掘過程は次の通りである。

- 以前キューブのタイムスタンプを確認して、27 個のブロックのハッシュ値を確認する。
- キューブのタイムスタンプが、以前のキューブのタイムスタンプと比較して有効範囲であることを確認する。
- 27 個のブロックのハッシュ値と、キューブ内の位置の値に応じた有効性を確認する。
- 27 個のブロックをパターンブロックにハッシュ値を作る。
- 以前キューブハッシュ値と 27 個のブロックのハッシュ値を利用して、キューブのハッシュ値を作る。
- キューブを作成して、ノードに伝播する。

５．６　採掘方式の多様化

キューブチェーンは採掘方式が多様なだけでなく方式による採掘の効率性と難易度が異なって反映された。POW は、キューブチェーンが初期にネットワーク構成を円滑にする目的のために使用される、さまざまな参加者が参加できるように参加範囲を広げた。採掘業者から一般ユーザーは財布を介して

ノードに参加して採掘することもできる。キュービング採掘に必要な演算は、キュービンに使用された関数をデコードするチップやハードウェア機器を開発して演算効率を高める計画である。このようにすると、低コストで高効率の採掘が実現されると同時に無限過熱競争の採掘装置に投資されている非効率性を克服することができる。

５．７　POS 補償方式

POH は POW の採掘方式と POS の補償方式が結合したキューブチェーンのみの参加方式である。
キューブチェーンでは、ノードの参加と関係なく、以前のブロック基準で 5,000 枚以上のキューブチェーン（QUB）残高保有者に保有量に比例して支給する。ただし、POS 参加申請は採掘プログラムを通じて行うことができ、参加数量と採掘ブロックを決定しなければならない。参加数量は参加期間中に伝送不可能になり、伝送しようとするときは、参加数を除いて伝送することができる。　支給時期は、現在のブロックが生成される起点に支給し、支給量は、全体の数量比を保持数量の比率を計算して支給する。キューブチェーンの Statistics Block でブロックごとに POS 対象者の保有量を保存するので、すぐに補償量を計算して、それぞれのウォレットアドレスに送信することができる。

６．ウォレットサービス

キューブチェーンは活用性高く便利なブロックチェーンサービスを目指す。そのために基本的なサービスを提供し、キューブチェーンを最大限に活用し、アプリケーションやサービスの開発に集中することができる環境を提供する。

６．１　ウォレットの提供

キューブチェーンウォレットは、キューブチェーンを利用した変形と履歴管理などのサービスをサポートする。キューブチェーンウォレットは、基本的な伝送、取引内訳照会サービスのほか、様々な特徴的なウォレットのサービスを提供する。第 4 次産業革命をリードする新たな金融サービスとしては、アプリケーション利用時、活用性が高くユーザーの利便性を加えたサービスを追加したキューブチェーン財布だけのアイデンティティを見せてくれる。

ウォレットアドレスのドメインサービス

ウォレットドメインサービスは、一度に覚え難いウォレットアドレスをユーザーが覚えやすい特定の財布の名前でマッチングしてくれるサービスである。特定の IP アドレスを指定されたドメインのアドレスに接続させるように、ユーザが指定したウォレットのドメインアドレスに特定のウォレットのアドレスを接続させて利便性を向上させる。ウォレットドメインでは、個人が使用する携帯電話番号や電子メールアドレスを使用することができ、覚えやすいアドレスを使用することにより、ユーザーまたは振込をする相手がウォレットのドメインアドレスを簡単に記憶し、入力することができるように手伝ってくれる。

例）CWxhQRgBrqZUbj6fj1ftprurb2U9yAFMhu の形式を持つキューブチェーンアドレス
　Abc.com（大文字小文字を区別しない）のような単純な文字列をユーザが任意選定して、複雑なウォレットアドレスを代わりにして、キューブチェーンウォレットで使用することができる。その後、Abc.com を知らせコイン転送を受けることができるようになる。

ウォレットグルップ化サービス

一つの財布に複数の財布を指定された形でまとめるグループ化サービスは、代表ウォレットアドレスは公開せずに、接続されたウォレットアドレスだけ露出させる形のサービスである。ユーザーが一つのウォレットで、複数の接続されたウォレットアドレスを管理することができ、目的に応じた多数のウォレットを開設または分類することができる。グループサービスを利用して、自動振替サービスや接続されたウォレットアドレスを便利で簡単に管理することができる。

自動振り込みサービス

口座振込サービスは、ユーザーが自分の設定した振込条件（受取人、入金ウォレットアドレス、金額、周期など）に応じて、特定のウォレットのアドレスに定期的に送金してくれるサービスである。口座振替サービスを利用する場合、別に受取人に告知をしなくても、指定した日時にユーザーのウォレットから指定金額を引き落として受取人に一括入金し、その内訳を通知することができる。

ウォレットメッセージ伝達サービス

ウォレットを使用するユーザーを対象に、取引後、確認メッセージまたはサービス要求に関するメッセージを伝えることができる機能である。伝送完了メッセージ、または間違った取引の返還要求などの用途に使用可能であり、メッセージは、アプリケーションの通知サービス、SMS、E-mail などの用途に活用される。

６．２　キューブチェーン活用基盤サービス

キューブチェーン活用基盤サービスは、ブロックチェーンベースのキューブチェーン技術を様々な分野のビジネスモデルとして使用できるようにサービスプラットフォームを構築、展開されているサービスである。このような目的は、企業や個人がキューブチェーンを活用して、幅広いキューブチェーンの生態系を作成する開発環境を形成し、さらに拡張された 2 次のキューブチェーンアプリケーション開発のための基礎を提供する。キューブチェーンを活用したベースのサービスは、ビジネスモデルを直接適用することができる完成された形で発展させ行くものであり、これをテンプレートアプリの形で別途配布する予定である。

キューブチェーン個人情報認証サービス

汎用的に個人の電子メールや携帯電話の番号、ピン番号などをキューブチェーンに保存して使用することができる個人認証サービスである。ユーザーは、キューブチェーンに保存された本人の個人情報を、Web やアプリケーション上に提供することができる。キューブチェーンに保存された個人情報は保護されたデータに基づいて本人認証時のみオープンされることにより第三者に公開されなく、個人情報を提供しようとする用途に安全に連動させることができる。

キューブチェーンメッセージ配信サービス

P2P でのサービスが行われるという点で、既存のメッセージ配信サービスと差別される。送受信されたメッセージデータは、キューブチェーンに転送されて保存される。メッセージングデータは、後順位に保存されるので、ユーザーは、データ転送遅延なくサービスを利用することができる。キューブチェーンに分散保存されたデータは、プライバシー機能が適用され、認証者のみオープンされているメッセージに変換させることができる。プライバシー保存機能は、第三者に公開またはハッキング遭わない保護障壁として、ユーザーが安全なチャットサービスを利用できるようにする。また、API を介してチャットルームの開設、参加者の設定、参加者会話の内容を伝えすることで活用性を増大をさ

せることができる。

キューブチェーンファイルの保存サービス

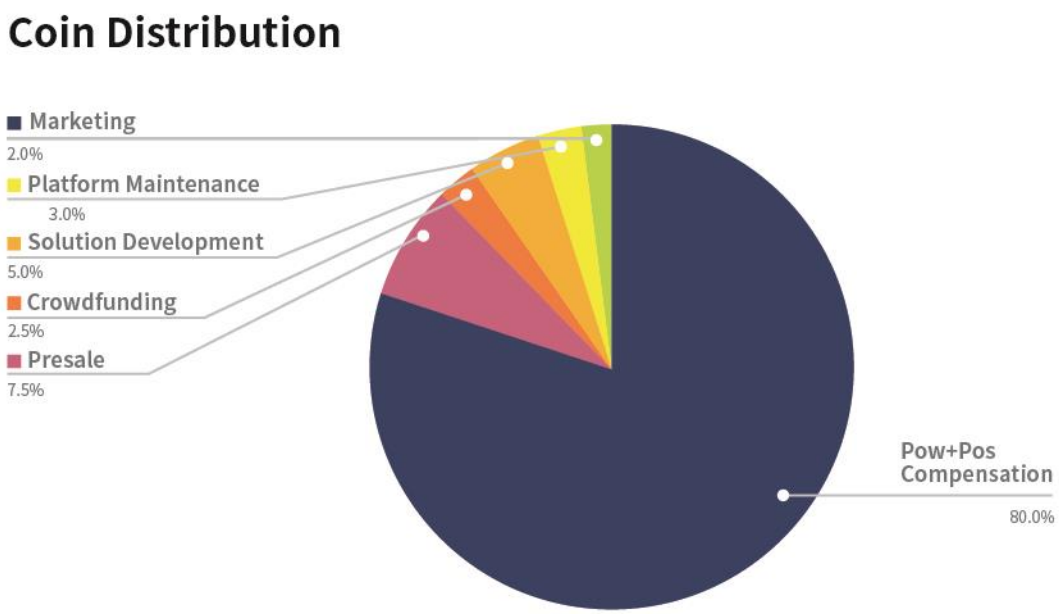
キューブチェーンファイルの保存サービスを使用すると、ユーザーが特定のファイルをキューブチェーンを利用して分散保存して、特定のファイルを公共の目的のために使用したり、公認されたファイルに登録することができる。文書ファイルや画像ファイルを登録するサービスは、ユーザーが重要なファイルを安全に保管することができる。テンプレートアプリやアプリケーションと連動するサービスを介してファイルの活用性を高めることもできる。

キューブチェーンデータベースサービス

キューブチェーンのデータベースサービスは、ブロックチェーンのデータをデータベースのように活用性高く使用するためのサービスである。キューブチェーンの Edit Block と Format Block を使用して、データを構造化させて管理することができる利点を提供する。データを管理することを標準の SQL ステートメントを介して保存、変更、削除が可能なように API を提供する。また、リレーショナル DB でキューブチェーンデータのキューブの作成毎のデータを送信連動させる機能を提供する。

７．キューブチェーンの発行数量

７．１　キューブチェーンの配分



７．２　POH 比率

キューブチェーンは 50 年間にわたり、合計 120 億枚のコインを発行し、5 年ごとに POW と POS の割合が調整される。

区分	5 年間 キューブチェーン 補償数量	POW ： POS 比率	5 年間 POW 補償数量	5 年間 POS 補償数量
~5 年	960, 008, 400	7:3	672, 005, 880	288, 002, 520
5~10 年	960, 008, 400	6:4	576, 005, 040	384, 003, 360
10~15 年	960, 008, 400	5:5	480, 004, 200	480, 004, 200
15~20 年	960, 008, 400	4:6	384, 003, 360	576, 005, 040
20~25 年	960, 008, 400	3:7	288, 002, 520	672, 005, 880
25~30 年	960, 008, 400	2:8	192, 001, 680	768, 006, 720
30~35 年	960, 008, 400	1:9	96, 000, 840	864, 007, 560
35~40 年	960, 008, 400	0:10	-	960, 008, 400
40~45 年	960, 008, 400	0:10	-	960, 008, 400
45~50 年	960, 008, 400	0:10	-	960, 008, 400

８．キューブチェーンの技術活用

８．１　RPC サーバー

キューブチェーンに参加したノードは、RPC サーバーとして使用することができる。RPC サーバーで利用する場合、リモートで関数を実行することができますので、キューブチェーンを活用して、遠隔地からのノードを制御することができる。キューブチェーンネットワークを構成しているノードで RPC サーバーを使用して、キューブチェーンに参加していない PC やサーバーを介してキューブチェーンのデータを参照して、またはノードを制御することができる。遠隔地の制限設定や機能の範囲設定も可能で、遠隔地の制御が可能である。

８．２　API

キューブチェーン RPC サーバーとの API を作って提供することで、遠隔地から簡単にノードの管理が可能にする。RPC サーバーの API の伝達と応答の両方基本的に JSON 形式を使用する。詳細 API ドキュメントは、今後のキューブチェーン進行時、別途オープンする予定だ。API の使用コマンドと簡単な例は、以下の通りである。

rpc_ver ： RPC サーバーの現在のバージョン情報を求めています。

```
curl -X POST --data '{"callno":100,"com":"rpc_ver","vars":{},rmsg:"
サーバーのバージョン確認要求"}'
```

network_info ： サーバーのネットワーク参加形態と参加ノードと活性化の状態に関する情報を求めています。

```
curl -X POST --data '{"callno":100,"com":"network_info","vars":{},rmsg:"ネットワーク情報確認要請"}'
```

p2p_info ： p2p 関連情報を求めています。

```
curl -X POST --data '{"callno":100,"com":"p2p_info","vars":{},rmsg:"peer to peer 情報"}'
```

cube_pow ： POW 参加するかどうかについての情報を得ることができる。

```
curl -X POST --data '{"callno":100,"com":"cube_pow","vars":{},rmsg:"POW 状況確認"}'
```

cube_pos ： 渡されたウォレットアドレスの POS 該当要否についての情報を得ることができる。

```
curl -X POST --data '{"callno":100,"com":"cube_pos",
"vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"POS 状況確認"}'
```

cube_height ： 現在進行チェーンの高さ、すなわち、現在までのキューブの数を求める。

```
curl -X POST --data '{"callno":100,"com":"cube_height","vars":{},rmsg:"
チェーンの数を確認 "}'
```

cube_balance ： 渡された財布アドレスの残高を確認する。

```
curl -X POST --data
'{"callno":100,"com":"cube_balance","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"ウォレットの残高確認"}'
```

cube_transaction_count ： 渡されたウォレットアドレスの取引回数を確認する。

```
curl -X POST --data
'{"callno":100,"com":"cube_transaction_count","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"ウォレットの取引回数を確認"}'
```

cube_transaction_list ： 取引のハッシュ値、すなわち取引 ID を抽出する。特定のアドレスの取引内訳や、特定のキューブの高さの取引履歴を見つけることができる。

```
curl -X POST --data
'{"callno":100,"com":"cube_transaction_list","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"取引の詳細送信"}'
```

cube_transaction_detail ： 取引のハッシュ値の履歴情報を伝達する。

```
curl -X POST --data
'{"callno":100,"com":"cube_transaction_detail","vars":{"tr_hash":"6e8dd67c5d32be8058bb8eb970870f072445675058bb8eb97f"},rmsg:"取引やデータ転送"}'
```

cube_transaction ： 渡された財布アドレス間の取引を進行する。

```
curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","amount":1.2,"fee":0.0001},rmsg:"取引やデータ転送"}'
```

cube_transaction_data ： 特定のデータをキューブチェーンに上げる。

```
curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","data":{"no":1,"id":"cubechain","chapter":"cubechain_api","book_name":"キューブチェーン白書"}},rmsg:"一般データ転送 "}'
```

９．結論

ブロックチェーンの技術は、4 次産業革命をリードする基盤技術として位置づけするために発展している。暗号通貨市場だけでなく、全産業にわたってデータの自由な共有と安全性を同時に確保する技術で普及される日が遠くない。キューブチェーンは、既存のブロックチェーンの短所を補完してブロックチェーン技術の発展に寄与しようとする。キューブチェーンが 4 次産業革命の先導的役割をことを期待すると同時に、様々な分野に広く活用なることを願う。