# CoinMarketCap

# 白書の概要

改訂:9
日付:2018年１２月 19 日
Sergio Demian Lerner 著

## はじめに

2008 年、サトシ・ナカモトなる人物が Bitcoin を作り出して決済に革命をもたらしました。Bitcoin には、Nick Szabo 氏が 1993 年に紹介したコンセプト、いわゆる「スマート・コントラクト」のかなり限定された実装が含まれます。

その時までは、多くの研究が、フルチューリング完全配信プログラムをサポートする新しい暗号通貨の創出に力を注いできました。現在、この目標を達成するために利便性、安全性、決定性に優れた仮想マシンを構築できるという自信が広がっています。

当社は、Bitcoin を世界で主要な暗号通貨にするためには新たな使用事例が必要であり、そのような未来を保証するにはスマート・コントラクト機能の追加が重要になると考えています。当社はこれを念頭に置き、チューリング完全仮想マシンを Bitcoin に組み込むスマート・コントラクト・プラットフォーム、 CMCを作り上げました。 CMCによって、より高速なトランザクションやより優れたスケーラビリティなど、ネットワークに別の強化機能も加わり、新たな使用シナリオを実現することもできます。

CMCは、同じ開発チームにより 2013 年に創出されたチューリング完全仮想通貨であるQixCoin の進化型です。 CMCはほぼ瞬間的な確認による強化された決済体験を提供します。現時点で 300 tps を達成しており、20 秒以内に最多の決済を確定します。なおかつ、Bitcoin と同様のセキュリティ保証に基づいており、SHA-256Dマージマイニングに対応し CMC
は Bitcoin サイドチェーンとして機能します。Bitcoin は CMCブロックチェーンに移管されると、「SmartBitcoin」（SBTC）になります。SmartBitcoin は、 CMC
ブロックチェーンに生存する Bitcoin に相当し、いつでも追加費用なしで（標準 CMC手数料を除く）Bitcoin に変換できます。SBTC は CMCサイドチェーン上で使用されている基本通貨で、ト

ランザクションとコントラクト処理についてマイナー（採掘者）に支払われます。通貨発行は伴いません。SBTC は全て、Bitcoin ブロックチェーンに起因する Bitcoin から生成されます。

CMCは次の分野で Bitcoin を強化します。

- スマート・コントラクトを可能にするチューリング完全 CMC仮想マシン
- （RVM）
- トランザクションの 10 秒以内の平均初期確認
  PoW とバックアップ閾値署名ベースのフェデレーションマイニングを組み合わせた
- 安全なマージマイニング
  ピア・ツー・ピアのゴシップ・ネットワークに埋め込まれた低遅延率の高速リレ
- ー・バックボーン
  サイドチェーンを使用する 2 ウェイ・ペグ（現在はフェデレーテッドペグで、
  Bitcoin の改善に依存する完全自動ペグ）

頭字語:「 CMC」とはルートストック（プラットフォーム）を指し、関連用
語は「 CMCプロトコル」（仕様）および「 CMCリファレンス・ノード」
（参照実装）であり、ネイティブ CMC通貨は「SmartBitcion」を指し、
「SBTC」はSmartBitcoin

通貨のシンボルであり、
「BTC」はビットコイン通貨を指し、「Bitcoin」はビットコインプロトコルを指します。

## CMCが Bitcoin Ecosystem にとって重要な理由とは?

### Bitcoin ステークホルダーと価値の保護の一致

CMCガバナンスの第一の目的は、Bitcoin の主要利害関係者の現在の活動に完全に合致した報酬を創出することによって、彼らと同じ立場で考えることです。
この哲学はコアなアーキテクチャに直接反映されます。このアーキテクチャでは、Bitcoin マイナーがプルーフ・オブ・ワークのブロック検証に必要なハッシング・パワーを提供し、業界のリーダー（Exchanges、Wallets、Payment Processors）が、検証チェックポイントを作り出すフェデレーションを統合し、2 ウェイ・ペグの買い戻しトランザクションに署名します。

その上、マイナー、業界リーダー、Bitcoin / CMCホルダー、コアな開発者が最終的な判断を下す投票システムに基づいて、 CMCはそのプラットフォームに対する改善策を決定します。

以降のパラグラフでは、このイニシアチブがどのように協働するのかを説明します。

### ガバナンス・モデル

コミュニティの各プレーヤーは、Bitcoin 貯蓄を保護するために両替とウェブ・ウォレットのノウハウ、ユーザーのトランザクションの保護を目的とした大規模なマイニング作業を実現するためのマイナーのノウハウなど、コミュニティに最高のサービスを提供するためのノウハウを持っており、ブロックチェーン企業は新たな使用事例に取り入れて夢を実現し、コア開発者は技術面での課題に取り組む方法について技術的な専門知識を持っており、ノード維持者はインフラストラクチャとネットワーク接続性を提供し、ユーザーはシステムの中心に立って信頼性と流動性を提供します。

（Bitcoin 財団など）に提供されます。イーサリアム財団がイーサリアム・コミュニティの代表である場合、機関票はイーサリアム財団に提供される可能性があります。

### Bitcoin マイナーの投資金の保護

2016 年 8 月、Bitcoin マイニング収益性マージンは、25 BTC から 12.5 BTC へのブロック・リワードの分散化により、50%未満へと下落すると思われます。何億ものマイニング・ハードウェアが瞬く間に陳腐化します。これにはおそらく現在市場にあるすべてのマイニング・マシンが含まれます。なぜなら、2017 年よりも前にチップの 2 つの世代（高

速・低電力）が開発され販売される予定になっているためです。現在のマイナーのほぼ全員が各自のハードウェアを交換しておらず、マイニング・ビジネスの終焉に直面することになります。 CMCは、マージ・マイニング能力のおかげで、これらのマイナーに対し、ビジネスを今後少なくとも 4 年間は継続できる機会をもたらします。Bitcoin のマージマイナーたちがゼロという限界費用で両方のコインを採掘できることから、採掘者たちは CMCマイニングによる付加的収入が収益性ギャップに悪影響を及ぼさない限り、Bitcoin を採掘することができます.
加えて、半減期までにマイニングの収益性が減少すると、さらに低コストマイナーへの集中化が生じ、それによって Bitcon のネットワークがさらに脆弱になります。したがって CMCは、収益性のある幅広いマイナーによる Bitcoin の安全性と価値の向上を促す上で重要な役割を果たす可能性があります。

また現在、Btcoin マイナーは、最小限のコストで開始し、 CMC向けアプリケーションを作成することによって、各自の投資金を保護できるだけでなく全く新しいビジネス機会を開発できます。

**Bitcoin / CMC 2 ウェイ・ペグのセキュリティ**

Bitcoin の主流企業は、Bitcoin ブロックチェーンと CMCブロックチェーン間での資金移行の安全を確保するという基本的な役割を果たすフェデレーションを統合します。その見返りとして、これらの企業は、資金の流入と流出の間の精算によって生じる料金から利益を得ることになります。

**Bitcoin 取引手数料の低下および資産発行の価値の安定化**

Bitcoin の現在の保有者と利用者候補は、主にビットコイン価格の変動性（ボラティリテイ）が原因で、特定の使用事例（いわゆる投資、グローバル決済ネットワークなど）に制限された通貨制度の利用を見てきましたが、次の Bitcoin 半減期に取引手数料が上昇する可能性があることから、この制限は悪化する可能性があります。

CMCは、ほぼ一瞬の取引検証（20 秒）と、価格が不換通貨の価格またはその他の安定商品の価格に固定されている資産発行を提供することで、上記の問題に対して解決を講。取引におけるボラティリテイ・エクスポージャーを低下させると同時にビットコインを準備通貨として維持することで、ビットコインの全体的な価値が上昇します。

**Bitcoin セキュリティ強化**

次の Bitcoin 報酬半減期には、陳腐化したマイニングハードウェアの数億ドルが、個人向けまたはオンラインで安く販売されます。これによって脆弱性の窓が開き、ごくわずかな金を得るために、膨大なハッシング・パワーを購入して 51%の攻撃を実行できるチャンスを攻撃者に与えることになります。さらに、セキュリティの低下はコインの知覚価値に影響を与える可能性があります。 CMCマージマイニングによる Bitcoin マイニングの収益性を向上させることで、Bitcoin ネットワークではハッシュ率の急落を防止できます。

## 低コスト BTC 決済ネットワークとしての CMC

ハードフォークによって Bitcoin ブロックサイズが増大しない場合、次の Bitcoin 報酬半減時に、Bitcoin 取引手数料からの収益が特定の用途に対して高くなる可能性があります。CMCブロックは Bitcoin ブロックよりも多くのトランザクション（取引）を保持できるため、当然ながら CMCはより低い手数料を提示します。取引手数料に関する将来的なシナリオの分析については、次のセクションをご覧ください。

Bitcoin とその取引手数料の将来は不透明です。現在、最大ブロックにおける変更に関する提案が議論を呼んでおり、これが将来の取引手数料に大きな影響を及ぼすと考えられています。将来のシナリオの予測と、成長と分岐の合理的な予測における CMCと Bitcoin の比較を下の表に示してみました。

| パラメータ | Bitcoin | CMC |
|---|---|---|
| サトシの等価において安全性が同程度である場合の確認時間 | 10 分 | 10 秒 |
| 逆転可能性 0.1%に対する最短確認時間 | 20 分（2 ブロック） | 30 秒（3 ブロック） |
| 1 秒当たりの最多取引数 | 3.3 tps<br>（平均サイズ tx の仮定） | 開始時 300 tps<br>1000 tps まで拡張可能 |
| ユーザーによる標準取引に対する現在の平均コスト | 6 セント<br>仮定:<br>- 1.5 tps | 市場価格不可 |
| マイナーによる標準取引に対する現在のコスト | 1 セント<br>仮定:<br>- 高速リレーネットワークの使用<br>- メモリーの UTXO<br>- tx 当たりの処理時間 1 ミリ秒<br>- BTC 平均ブロック報酬 25.2<br><br>5 セント<br>仮定:<br>- 標準リレーネットワークの使用 | 1 セント未満（推定）<br>仮定:<br>- CMC専用ハードウェアスイッチングはなし<br>- CMCトランザクションはほぼなし<br><br>1 セント（推定）<br>- マイナーによる新規ヘッダーのロードを妨害すると処理時間が 10 ミリ秒失われる |
| 2016 年末までの取引手数料 | 1.6 USD<br>仮定:<br>- ブロックサイズを増大させない<br>- BTC/USD レートが変化しない<br>- 同レベルのセキュリティ<br>- 3 tps | 1 セント（推定）<br>仮定:<br>- 3 tps |

上記チャートにおける取引手数料の推定額は、2016 年全体の BTC 価格が約 240 BTC/USD のまま維持されるという根拠のない事実に基づいているので、注意が必要です。この期間中に価格が 10 倍に上昇した場合、取引手数料も上昇し、Bitcoin ブロックチェーンは銀行間取引決済システム（決済ネットワークではない）として存続可能な状態になります。また、オフチェーン決済システムも出現する可能性があり、その場合は安価な決済処理が提

供されますが、同時にネットワークが中央に集中し、その分散的性質が変化することも考えておくことが重要です。

下の表は、2016 年末までの考えられる将来のシナリオを示しており、ネットワーク・ハッシングの難易度が BTC 価格と同じ割合で上がると仮定しています。

| シナリオ | tx からマイナーまでの Bitcoin コ | tx からマイナーまでの CMCコスト |
|---|---|---|
| Bitcoin 価格が 10 倍に上昇 | 16 USD | 2 セント |
| ハードフォークにより TPS が 10 倍に上昇 | 11 セント | 0.2 セント |
| BTC 価格と TPS が 10 倍に上昇 | 1.1 USD | 2 セント |

利用者は、Bitcoin 取引手数料を含めたコストを考えると、取引手数料がより安いプラットフォーム（ CMCなど）に切り替えると考えられます。

## CMC使用事例

CMCプラットフォームは、1993 年に Nick Szabo によって提唱された「チューリング完全」スマート・コントラクトを提供します。同時に、 CMCの VM にはイーサリアム VMとの後方
互換性があることから、 CMCはイーサリアムに従事する開発者たちに対し、 Bitcoin ブロックチェーンの安全性の恩恵を享受する機会を提供します。 CMCの範囲を超え開可
能な潜在的なスマート・コントラクトと使用事例の一覧を以下に記載しています。

**マイクロ決済チャネルおよびハブ・アンド・スポーク・ネットワーク**

マイクロ決済チャネルでは、2 名の当事者が、手数料を毎回の支払時には支払わずチャネルのクローズ時に 1 回支払うだけで、定期決済のコストを低く抑えて安定させることができます。

ハブ・アンド・スポーク・ネットワークでは、相互信頼を築いていない利用者が、最低限の信頼を築いている第三者とのやり取りに支払チャネルを使用して、低コストの 1 回限りの決済を間接的に行うことができます。 CMCでは、ハブ・アンド・スポーク・ネットワークを最小限の手間で直接実装して、標準的な e ウォレットと自然に連動させることができます。

**ピア・ツー・ピア分散型交換**

CMCは、TierNolan のプロトコルを使用して、ピア・ツー・ピア交換として機能するコントラクトをサポートします。注文控え帳の自動マシンも簡単に作ることができます。このマシンにより、独立ブロックチェーン上に分散型市場を設けて、第三者を関与させることなく仮想アセットを交換できるようになります。

**小売決済システム**

CMCでは日常的な小売決済を目的として BTC をグローバルに採用できます。 Bitcoin の小売用途の主な制約の 1 つが確認時間です（不可逆性の確証まで 10 分～1 時間）。
CMCでは、消費者がわずか数秒の確認時間で Bitcoin セキュリティの恩恵を享受できます。マーチャントはサードパーティのゲートウェイを必要とすることなく、ほぼ瞬時に決済を受諾できるようになります。小売市場でどのプラットフォームでも成功を収められるようにするために重要となるもう 1 つの要素は、大量のトランザクション件数（tps）に対応できることです。 CMCネットワークでは DÉCOR+プロトコルを使用しており、 Bitcoin ブロックチェーンで最大 300 tps（Paypal の 2 倍）を処理できます。

**エスクロー・サービス**

CMCはスマート・エスクロー・サービスの構築を可能にします。このサービスでは、Oracle がトランザクションに署名することで（または署名しないことで）、エスクロー下の資産に接することなくサービスを実行する（または実行しない）ことを決定します。

**仮想アセット生成**

CMCは、Bitcoin ネットワークが保障する仮想アセット（またはアルトコイン）の生成を可

能にします。コントラクトの燃料に価格を設定するための CMCの柔軟性を考えると、これらのアプリケーションは（他のすべてと同様に）、学生から銀行や企業に至るまで利用される可能性があります。

**資産の流動化**

CMCはさらに、実資産に裏打ちされたデジタル・トークンの生成も可能にします。これはREIT、株式、債券またはその他の資産（あるいは先物の利益）のデジタル商品化に用いることが可能です。この特定の使用事例は、従来の金融市場が成長にあたっての運転資本または資本に対する需要を満たしている開発途上諸国の小規模ビジネスに独自のソリューションを供与します。

**分散化送金**

この特定の使用事例は、銀行未利用/ 未実証の人々が食糧や住居目的で家族に送金するのに高額の手数料を支払っている開発途上諸国においてとりわけ重要です。

**IP 保護 / レジストリ**

CMCは、存在証明（PoE）として知られているものを複製できるコントラクトの開発を可能にします。PoE は個人や会社も、Bitcoin ブロックチェーンの安全性に合わせ、特定の文書（あるいは財産権）の存在を証明するのを可能にします。この使用事例は登録のメカニズムの信頼性が低い中南米、アフリカ、アジアの社会ではとりわけ重要です。

**投票制度**

仮想アセットの特殊事例として、 CMCは、極めて安全で透明性の高い選挙を実現するデジタル投票の構築を、最小コストで可能にします。

**マイクロレンディング（少額融資）**

グローバル人口の 50%超が従来型の金融制度にアクセスできていません。こうした信用アクセスの欠如は現在のグローバル社会が直面する経済格差の原因となっています。CMCは、世界の 30 億という最貧困層に信用アクセスを提供できるような、拡張可能なデジタルマイクロレンディング・コントラクトの開発を可能にします。

**サプライチェーンのトレーサビリティ**

CMCはさらに、デジタル・ウォレットが特定の製品やバッチの物理的ロケーションの（デジタル的な）追跡や追尾を行うのを可能にします。こうした種のコントラクトは、とりわけ小売業界、食品産業、ヘルスケア産業において特に有益と考えられます。その他の全ての使用事例として、これは CMCを用いることで、Bitcoin ブロックチェーンの安全性により最小コストで実現できます。

**オンラインの評判 & デジタル・アイデンティティ**

開発途上諸国の主要な問題の 1 つとは、貧困層にとって文書化や ID が不十分であることです。結果、貧困層による投票、医療へのアクセス、犯罪/虐待や酷使の報告、金融支援の

活用が妨げられています。 CMCは極めて低いコストで、Bitcoin ブロックチェーンと同程度に安全なグローバルのデジタル・レジストリの創造を実現します。

**インゲームのグローバル通貨**

多くのマルチプレーヤー・ゲームがプライベート通貨などのインゲーム・エコノミーを採用しています。こうしたゲームの進化に伴い、仮想通貨が法定通貨と同じ程度に利用者にとって有用となり、二次市場ではしばしば取引されています。インフレ、詐欺、オンライン窃盗は利用者の懸念となってきました。また、ゲーム会社は利用者の仮想通貨を委託することで法定およびセキュリティ上のハードルに直面することもあります。グローバル化が進むにつれ、バーチャルゲームも同様であり、プレーヤーは、1 つのゲームで獲得したお金を他のゲームで簡単に消費できないという不便を感じるようになるでしょう。
CMCは、ゲーム内決済として BTC（ CMCに相当）を受け入れることができるようにすることで、あるいは CMCによって保護されているプライベート・デジタル・アセットの創造を可能にすることで、こうした問題を解消できます。 CMC決済は低額のクローズドループ・システムと同様にスピーディとなり得ることから、ゲームエンジンはプレーヤー同士の取引や会社

とプレーヤー間のバーチャル・オファー目的でインゲームの購買システムとして CMCを採用することができます。URL のクリックまたは QR コードのスキャンにより、取引が標準

プレーヤーの外部電子ウォレット・ソフトウェアを使うことで起動可能で、また、ゲーミン

**インターネット賭博および予測市場**

グ会社への委託料の支払にも対応します。

迅速な決済とは迅速な払い出しも意味します。Bitcoin のギャンブル・サイト（SatoshiDice など）は 0 確認やチェーンド・トランザクションを使って登録不要の高速賭博体験を提供しようとしていますが、ギャンブル・サイトにとってはセキュリティ面のリスクが伴います。 CMCはブロック確認を伴うほぼ瞬時の払い出しによって賭博を可能にします。

**フェアプレー**

スマート・コントラクトの導入により、ならびに Mental Poker 等のよく研究された暗号プロトコルと連動して、 CMCは上前をはねる、信頼の置けるサードパーティの要件を伴

うことなく、カードゲームのオープンで公正なプラットフォームを提供することができます。

基本的な Bitcoin テクノロジーを用いて CMCプラットフォームで開発してプログラミングすることができる事例はたくさんありますが、これらはそのごく一部です。

**Bitcoin**

マイナー（マージマイニング経由）が、これらのコントラクトを実施してその実施に消費

した燃料の大部分から利益を得ているマイナーになろうとしていることに言及することが重要です。

## 技術の概要

CMCプラットフォームは、根本的に
は以下の組み合わせになります。

- チューリング完全リソース説明決定論的仮想マシン（スマート・コントラクト向け）
- 2 ウェイ・ペグ型 Bitcoin サイドチェーン（BTC 建て取引向け）
- 動的ハイブリッド・マージマイニング/連合合意プロトコル（合意の安全性確保を目的とする）、および低遅延ネットワーク（高速決済向け）

### チューリング完全仮想マシン

CMC仮想マシン（RVM）はスマート・コントラクトのプラットフォームの基幹です。スマート・コントラクトは、高い割合のネットワークノードにより同時に履行されます。スマート・コントラクトの実施に伴い、コントラクト間メッセージが処理され、金銭トランザクションの生成、ならびにコントラクト持続メモリの状態の変更につながる可能性があります。RVM はオプコード・レベルで EVM と互換し、イーサリアム・コントラクトが CMC 上で円滑に実行されるようにします。最初のリリース時には、VMは解釈によって実施されています。次回のリリースに向けて、EVM オプコードを Java
のようなバイトコードのサブセットにダイナミックに再標的化することで EVM をエミュレートすることが計画されており、セキュリティ強化とメモリー制約を伴う Java のような VM は新た
な VM（RVM2）になります。これにより、 CMCコード実行がネイティブ・コードに近似するパフォーマンスになります。
主要な特長：

- VMは独立しているがオプコード・レベルでEVMと互換。
- CMCはイーサリアム利用者に対して、Bitcoinネットワークの安全性を利用して各自のプロジェクトを実行できる可能性を提供。
- 高速int32演算と優れたジャスト・イン・タイムのコンパイルを実現する新しいオプトコード（予定）。パフォーマンス向上のため。

### サイドチェーン

サイドチェーンは独立したブロックチェーンであり、決済証明を使用することで、そのネイティブ通貨が自動的に別のブロックチェーン通貨の価値に固定されます。2 つの通貨で自由に、自動で、価格交渉において負担を伴わずに、交換可能な時に 2 ウェイ・ペグが存在します。 CMCでは、SmartBitcoin（SBTC）は 2 ウェイ・ペグで BTC に固定され（厳密には、 CMCの最小計算単位である Rootosh が、Bitcoin の最小計算単位であるSatoshi に固定されます）。

実際、BTC を RTS と交換する場合、1 回のトランザクションにおいてブロックチェーン間で「変換」される通貨はありません。なぜなら Bitcoin では別のブロックチェーンにおけるバランスの信憑性を検証できないためです。変換が生じた際、一部の BTC は Bitocoin にロックされ、 CMCにおいて同量の SBTC のロックが解除されます。SBTC を BTCに戻す必要がある場合、 CMCにおいて SBTC が再度ロックされ、Bitcoin において同量の BTCのロックが解除されます。

## セミ・トラスト・フリーのサイドチェーン

両方のプラットフォームのスマート・コントラクトを使用すれば、完全に信頼されているサードパーティ・フリーの 2 ウェイ・ペグを作ることができます。しかし、現在 Bitcoin はスマート・コントラクトに対応しておらず、外部 SPV プルーフの認証にあたってネイティブ・オプコードにも対応していないことから、 CMCの 2 ウェイ・ペグ・システムの一部はセミ・トラスト・サードパーティ（STTP）群を必要とします。ロックされたBTC を制御できるシングル STTP はありませんが、その大半に BTC 資金をリリースする能力が備わっています。STTP は、ロックされている BTC を一時的に保存し、Bitcoin 利用者への支払を行うときに BTC のロックを解除します。SBTC を Bitcoin に戻す場合、SBTC は CMCにおいてロックされます。

CMCでは、固定資金を保護する STTP はまさにフェデレーションのメンバーです。その理由はフェデレーションのインセンティブが STTP と強く連携しているためです。フェデレーション・メンバーは、大学など高評価のコミュニティ参加者出なければならず、安全なネットワーク・ノードを維持できる技術力も備えていなければなりません。資金のロックと解除は人的介入を伴わず、フェデレーションによって実施されます。そのため、フェデレーション一員になるためには、特に BTC ファンドの放出を決定する要素の正当性に関して、ノードに電力を供給するソフトウェアの適切な挙動を検査する能力が必要になります。当社は、連合検証アルゴリズムを実行してセキュリティをさらに強化する耐タンパー性ハードウェアの作成を計画しています。
Bitcoin がハードフォークとして SPV プルーフ認証にあたっての特殊オプコードまたは拡張性を付加する場合で、新規システムが安全で管理者による承認不要であることが証明されたら、STTP としてのフェデレーションの役割はもはや不要と化し、 CMCチームは変更を実施して CMCを管理者による承認不要のシステムに適応させる場合があります。

**動的ハイブリッド型のマージマイニング/フェデレーション**

当社は、PoW こそが、低コストでブロックチェーンの歴史の上書きを防ぐ唯一のコンセンサス・システムであると確信しています。マイニング向けの価値あるリソースを消費しないその他のすべての合意システムにこの難点が付きまといますが、これらのシステムは評判を信頼し、マイニングへの匿名参加を防止します。その他のすべての合意システムでは、新規利用者は、台帳の認証チェックポイントを見つけるために一連の当事者を信頼する必要があります。

高い確率の PoW 合意はオーファン・ブロックの無駄が少ない断続的なブロックに基づいており、マイナーは、新たなブロックがネットワークによって解消されるたびに、各自のハードウェアマイナーを停止して再始動し、新たなヘッダー・ミッドステートを採掘する必要があります。その結果、大抵の場合、マイニング時間にギャップが生じるか、またはミッドステートの切り替えのためにネットワーク遅延が長くなります。このギャップによってミリ秒が消費されても、Bitcoin マイニングの効率が低下します。そのため CMCでは、DECOR+ブロック報酬共有スキームを採用することで、競争を減少させ、ゆえに CMCベストブロックに切り替えられるようにしています。マイナーは、

CMCブロックが見つかるたびに自分のハードウェアを切り替えている場合、完全CMCブロック報酬の獲得を目指して競争することになります。マイナーが、遅く切り替え、過去のブロ

ック・チップの採掘を継続する場合は、アンクルを作成してブロック報酬の共有を獲得できます。これらのどの場合もマイナーが完全に孤立することはありません。DECOR+によりアンクルに対して報酬が支払われ、GHOST ルールによって、アンクルが通常のブロックとしてカウントされ、ベストチェーンの安全が確保されます。そのため BTC マイニングの効率が最大限に引き出されます。

CMCハッシュ・パワーが総 BTC ハッシュ・パワーの 50%を下回ることがあります。その場合、ネットワークは 51%攻撃に弱い状態のままになり、残りのハッシュ・パワーは既存の CMCハッシュ・パワーの 2 倍になります。

このような状況を防ぐために、 CMCには PoW マイン・ブロック向けにフェデレーション・チェックポイントが設けられています。フェデレーション・チェックポイントはフェデレーション・メンバーによって署名され、クライアントはその署名の大多数を使用すると、どれがベスト・チェーン化を見極めることができます。 CMCにはさらにラストリゾート・プロトコルもあります。これにより、マイニング・パワーが
Bitcoin ハッシュ・パワーの5%を下回った場合、フェデレーションは署名済みブロックを作ることができます。初期の段階では、Roostock ハッシュ・パワーが、ベスト・チェーンに見られる最高
BTC ハッシュ難易度の 66%を超え、ブロックで支払われた手数料がビットコイン・ブロックの平均報酬と同額またはそれ以上になった場合、クライアントはフェデレーション・チェックポイントの使用を停止します。
CMCプラットフォームは、コミュニティから称賛されている有名なメンバーで構成されるフェデレーションとともに開始されます。各メンバーはチェックポイント署
名スキームの公開キーで識別されています。フェデレーションは、投票システムを使用し埋め込んでいるメンバーを追加または排除できます。ただしこれらの措置には高い割合のメンバー票が必要です。

CMC創業者の狙いは、 CMCネットワークによるマージマイニングの奨励です。ただし、 CMCはマージマイニング不足に強く、不足発生時にはネットワークの安全を
確保するためにフェデレーションが自動で投入されます。

主要な特長：

- マイニング報酬の 1 日満期。
- フェデレーション・メンバー・チェックポイント
- ブートストラップ期間のコード埋め込み型チェックポイント。
- マージ・マイニングにより期待される Bitcoin マイニングの効率性の喪失なし（ミッドステート・スイッチングでは 0.1%未満、遅延スイッチングでは 0%）

## 迅速な決済と待ち時間が短いネットワーク

CMCはより優れた決済ネットワークになることを目的としています。高速決
済を実現するために、いくつかのソリューションが開発されています。

- 競争のないブロック選定の使用（Hyperledger、Ripple、閉ループシステムなど）
- ハブ・アンド・スポーク・ネットワークの使用（Bitcoin ライトニング・ネットワークなど）

- 高 PoW ブロックレートの使用

ハブ・アンド・スポーク・ネットワークでは、新たに集中ノードが追加され、全く異なる新しい決済モデルにクライアント・ウォレットを導入する必要があります。したがってこの代替策は CMCに簡単に実装できますが、これは高速決済用のネイティブシス
ではありません。 CMCは DECOR+および FastBlock5 プロトコルを採用していますが、これらは採掘の集中化を対象とするインセンティブを生成しない 10 秒という平均ブロックレートの実現を可能にします。 CMCはセルフィッシュ・マイニングを受け付けず、インセンティブに対応しています。

主要な特長：

- 10 秒のブロック間隔
- 2 段階ブロック伝搬（2SBP）プロトコル
- プッシュ・ミッシング・トランザクション（PMT）プロトコル
- セルフィッシュ採掘の防止とブロックレートの低減にあたっての最終競合ブロックの完全ネットワーク増殖。
- 遅延トランザクション包摂ヒューリスティック（DTI）。トランザクションがすでにネットワークの各ノードのプールに存在しているため、各マイナーのブロック・トランザクション・キューでトランザクションを 5 秒間遅延させることで、高速で実行可能なブロック検証を可能にします。
- タイムクリティカルの優先事項を伴うブロック・ヘッダー拡散にあたっての新規ネットワーク・コマンド。
- ブロック・ヘッダーの伝搬直後にブロック・トランザクション・ハッシュ・リストを拡散させるための新規ネットワークコマンド。
- 未検証ブロックでのマイニングのヒューリスティック（MUB）。フォールバックが 5 秒間である未検証トランザクションを伴うブロック・ヘッダーでのマイニング。
- ブロックヘッダーには、トランザクションがない時にフラグが付きます（コインベースを除く）。
- 接続プロトコル別の 2 つの優先ストリーム（2PSC）。メッセージスライスを含む新たなメッセージ移行レイヤーで、明確な優先順位によって 2 つの並列セッションを許容します。このレイヤーにより、ブロック・ヘッダーを高優先度セッションで送信し、低優先度セッションで転送されていたメッセージをすべて中断できます。
- ローカル・ルート最適化プロトコル（LRO）。ピア優先度に基づくローカル最適ブロック・ルーティング。ピア優先度に基づくローカル最適トランザクション・ルーティング
- DECOR+プロトコル（競合ブロック間のリワード共有）。
- GHOST プロトコル（チェーン加重）。

## CMC特長比較

CMCを他のブロックチェーンと比較し、 CMCが分散化を損なうことなく、本質的により良い技術的選択を提示することを示します。分散化はフルノード・インスタンスの実行コストの逆数として算定されます。

| 項目 | Bitcoin | Ethereum | Factom | Counterparty | CMC |
|---|---|---|---|---|---|
| 平均確認時間 | 10 分 | 12 秒（GHOST） | 1 分（フェデレーション・サーバー） | 10 分 | 10 秒（DECOR+GHOST） |
| セキュリティ閾値（セルフィッシュ・マイニングに起因） | ~30% | 30%～50% | ~30% | ~30% | 50%（DECOR+GHOST） |
| チューリング完全スマート・コントラクト | なし | あり | あり | 予定 | あり |
| Bitcoin への価値の付加 | - | なし | なし | なし | あり（マージ・マイニング） |
| Bitcoin との統合 | - | なし | オーバーレイ・プロトコル | オーバーレイ・プロトコル | サイドチェーン |
| 確率的検証と不正証明によるスケーラビリティ | なし | なし | なし | なし | あり |
| SPV クライアント | あり | あり | なし | なし | あり |
| ブロック・リレーのバックボーン | あり | なし | あり | あり | あり |
| ユーザー定義アクセス構造向けのネイティブサポート | あり | なし | あり | なし | あり |
| ユーザー定義署名スキーム向けのネイティブサポート | なし | なし | なし | なし | あり |
| ハードウェア・ウォレット簡易統合 | なし | あり | なし | なし | あり |
| 安全保障 | SHA256D マイナー | Ethash マイナー | SHA256D マイナー + フェデレーション | SHA256D マイナー | SHA256D マージマイナー + フェデレーション |
| 機密トランザクション | なし | コントラクト経由 | 外部プログラム経由 | なし | AppeCoin プロトコルを用いたネイティブ・サポートを予定 |
| 固有トランザクション ID | なし（malleab.） | あり | なし | なし | あり |
| スケーラビリティ[tps] | 3～24 | 無制限 | 無制限 | 3～24 | 開始時 300 |
| ネイティブ・トークン | BTC | ETH | FACTOID | XCP | 2 ウェイ・ペグ経由の BTC |

## 即時決済テクノロジーのプレビュー

Bitcoin の創造は PoW ブロックチェーン・ベースの仮想通貨を対象とするより低いインターバルに向けての競争でした。まずは 10 分インターバルの Bitcoin が登場し、次に 2.5 分インターバルを採用した LiteCoin、1 分の DogeCoin、30 秒の QuarkCoin、12 秒の Ethereum が登場しました。新たな暗号通貨はそれぞれ少しずつインターバルが短くなってはいますが、この短縮化の意味するものを認識しているデザイナーは非常に少ないのが現状です。ブロック・インターバルが暗号通貨ネットワークの安定性と能力にどう影響するのかを理解するには、いくつかの因子を考慮しておく必要があります。何よりも、短い確認インターバルの実現性に影響を及ぼす最重要因子は、生成される陳腐化したブロックの数です。陳腐化したブロックの発生率に影響を与えるその他の因子は主に 2 つあります。ブロック伝搬プロトコルと、トップマイナーからトップマイナーへのブロック伝搬時間です。 CMCについて、当社はこれらの因子を慎重に解析してシミュレーションを実施し、ネットワークのパフォーマンス、ユーザビリティ、セキュリティを検証してきました。このセクションでは、陳腐化したブロックの発生率を抑えるために CMCが採用している新しいプロトコルについて検討します。

### DECOR+ プロトコル

Bitcoin においては、2 人以上の採掘者が同じ高さでブロックを解いた場合、明らかな利害相反が存在します。競合する各マイナーは自分のブロックがベストチェーン・チップとして残りのマイナーに選ばれるようにしたいと考え、残りのマイナーたちは全般的に、どれが選ばれるかは気に留めないでしょう。しかしながら、残りの正直なマイナーとユーザーは全員、誰もが同じブロックチップを選ぶことを希望すると思われます。そうすることでブロックが逆転する可能性が低くなるためです。対立するマイナーたちはこの理想的なソリューションによって同じ親を選ぶよう促され、DECOR+によって、一点に集中した選択のために適切な経済的誘因が設定されます。マイナー間の相互作用を強化する必要はありません。DECOR+は以下のように、対立の解消を経済面から刺激する報酬共有戦略です。

1. 全当事者が同じブロックチェーン・ステートの情報にアクセスする際、その対立は決定論的に解消されます。
2. 選択した解消策は、対立するマイナーもそれ以外のマイナーも含めて全員の収益を最大化できる策です。
3. 対立の解消には時間はかかりません。

### ブロック伝搬プロトコル

Bitcoin と Ethereum は、ブロックに含まれるすべてのトランザクションにロック・ヘッダーを詰め込むことで、各ブロックを前進させます。この戦略では、分析が非常に簡単になる一方で、ブロック伝搬レガシーについてもバンド幅の利用（2 倍になる）についてもうまくいかないことが分かっています。Bitcoin マイナーは高速リレー・ネットワークを利用してこの問題を部分的に解決しました。これは、圧縮形態でブロックをリレーする集中化バックボーンで、1 名のユーザーによって維持されます。 CMCはネットワークトポロジに埋め込まれた高速リレー・ネットワークとともに生まれました。その低遅延特性はネットワーク・トポロジーから発生し、集中化を必要としません。

### 2 段階ブロック伝搬（2SBP）

CMCブロックは 2 つの段階において送られます。第 1 段階ではブロック・ヘッダーのみが送られます。第 2 段階ではそのブロックに含まれるトランザクションのハッシュのリストが送られます。2SBP を利用すると、チャネル容量が 2 倍になるため、各ブロックにより多くのトランザクションを保存することができるようになります。各ノードは、ブロック・ヘッダーと、そのブロック・ヘッダーに関連するトランザクション・ハッシュ・リストを受信すると、完全検証のためにそのブロックの再構築を試みます。

### プッシュ・ミッシング・トランザクション（PMT）

各ノードはそのピアによって公表されたトランザクションのハッシュを保存するので、マイナーも、各ピアのプールで不足していることが分かっているブロックに含まれているトランザクションをすぐに送ります。これにより、追加のトランザクションの要求を目的とした 2 つ目のインタラクションのニーズが完全になくなります。不足しているトランザクションをピアから要請される前に送ることが、2SBP プロトコルの第 3 段階になります。

### 遅延トランザクション包摂ヒューリスティック（DTI）

マイナーは、数秒戻る前に受け取ったトランザクションのみを包摂します。このことから、ブロックが採掘される前にピアがすでにトランザクションを受け取っている可能性が高くなると断言できます。ここで注意したいのは、トランザクションの遅延はマイナーにとって最大の関心事であることです。この遅延によってブロック検証時間が短縮されるので、競合するブロックの機会が減少するためです。この最適化は、未検証ブロックでのマイニングのヒューリスティック（MUB）がネットワーク内で有効である場合には不要です。

### ブロック・ヘッダーの即時伝搬（IBHP）

最新ブロックのブロック・ヘッダーが受領されると、トランザクションの確認またはブロックの妥当性確認の前に、ノードによってそのブロック・ヘッダーが転送されます。転送時にはブロックの PoW と高さのみを確認します。これによりヘッダーを 1 秒未満でネットワークに拡散できます。

### 接続プロトコル別の 2 つの優先ストリーム（2PSC）

各ネットワーク接続は、異なる 2 つの優先度を持つ 2 つの論理的双方向ストリームで構成されます。低優先度ストリームで低優先度メッセージが送信されている場合であっても、ブロック・ヘッダーの即時送信には高優先度ストリームが使用されます。

### 未検証ブロックでのマイニングのヒューリスティック（MUB）

固定インターバル中は、トランザクションがまだ不足していても、ノードによってヘッダー上の空のブロックのマイニングを開始できます。そのインターバルの後、ノードによっ

てそれ以前に採掘されていたブロックについてはすべてマイニング（採掘）が再開されます。上記の空のブロックによって、バンド幅とブロックチェーン・ストレージの使用の効果が減退しますが、シミュレーションによると、DBI を使用した場合、生成された空ブロックの数、空ブロックの保管に必要なスペース、TPS の減少が低下することが分かっています。

### ローカル・ルート最適化プロトコル（LRO）

陳腐化したブロックの数を削減するには、内部マイナー移送遅延を低下させることが重要です。 CMCネットワークは、内部マイナー遅延が低下し、マイナー間のトラフィックの優先度が設定されるように動的に最適化されています。言い換えれば、 CMCでは高速リレー・ネットワークをピア・ネットワークに埋め込み、地理位置情報と最適なローカル・ルートによってゴシップ・プロトコルを強化します。内部マイナー・ブロック転送パスはブロック伝搬用のクリティカル・パスであるため、ピア・ネットワークに対して極めて重要です。このクリティカル・パスのピア・ネットワークにおける非マイナー・ネットワーク・ノードの存在によって、陳腐化したブロックの発生率が上昇する傾向にあります。クリティカル・パスの非マイナー・ノード（エンドユーザー・ノードやモニタリング・ノードなど）だけが、マイナーを弱い匿名化ホップとしてのみ機能するようにできます。ローカル・ノード決定のみからクリティカル・パスを作成するには、LRO プロトコルを使ってノードの優先順位を設定します。このプロトコルによって、有向非巡回グラフ（DAC）が CMCネットワークのランダム・トポロジーに動的に埋め込まれます。はマイナーを最適に結合します。

### Bitcoinイニング・ネットワークの再使用

集中マイニング・ネットワークには大規模なマイニング・プールがあり、生成されるステート・ブロックの数が完全な分散マイニング・トポロジーよりもはるかに少ない傾向にあります。そのため高速決済に関しては、SHA-256D PoW ベースの暗号通貨は、ASIC フレンドリーではない PoW ベースの暗号通貨よりも優れています。

### ネットワークのリアル・トポロジー

Bitcoin は、ネットワークはランダム・グラフに類似しており、一定の平均的な出次数と入次数があることを想定したデザインとなっています。これは現実とは程遠いとはいえ、ネットワーク・ノードは、地理的クラスターが形成されないように局所的な決定を下します（少なくともアウトバウンド接続に対して）。これはブロック伝搬の支援に最適なトポロジーではありません。ブロック伝搬の最適なトポロジーとは、トップ・マイナー間の直接的な結びつきを促進する、またはトップ・マイナー間でのブロックのルーティングを高速化することで、トップ・マイナーを強化するものです。また、陳腐化したブロックの数を激減させるには、マイナー間の直接的なバックボーンも役立ちます。これは攻撃からの回復力を強化するために Bitcoin に対して提案されています。 CMCでは LRO ヒューリスティクスを使用して動的マイナーのバックボーンを構築します。マイナー間認証のコスト、マイナーのプライバシー、IP アドレスの開示、関連する可能性のある DoS 攻撃は発生させません。

## PoW 機能の検証時間

SHA-256 は評価を非常に高速で行うので、Bitcoin PoW 検証に時間はかかりません。一方、スクリプト PoW では、選択するパラメータによって（GPU または ASIC の「レジスタンス」）、評価時間が 3～30 ミリ秒になります。ネットワークをスパムや DoS 攻撃から保護するために、各ノードはブロック・ヘッダーを再転送する前にブロック PoW を検証する必要があります。したがって、検証遅延時間は、マイナー間のブロック・クリティカル・パス内のホップ数の分だけ倍増します。

## クライアント・ネットワーキング・スタック

ブロック・ヘッダーがノードに届いたら、ネットワーク内で陳腐化したブロックが生成されにくくするために、そのノードをできるだけ早く転送するのが最善です。つまり、他のノード・アクティビティを全て一時停止または停止させるべきなのです。 CMCは、優先度が低い処理を即座に取り消して再試行を許可できるように設計されています。即時転送を可能にするために、トランザクション検証処理やその他のハウスキーピング活動（チェーン再編など）において、クライアント・ネットワーキング・スタックによりクライアントがブロックされません。これは、マルチスレッディングを許可してスレッドの優先順位を動的に割り当て、ブロック・ヘッダーを受けたスレッドを強化する CMCクライアントによって実現されます。

## ブロック・オーバーヘッド

大半の暗号通貨のブロック・ヘッダーは小さい（-100 バイト）ので、（ブロック全体のサイズと比較して）ヘッダー・サイズによって著しいオーバーヘッドが生じることはありません。 CMCヘッダーは大きめですが、低レベルネットワーク MTU は一般的に 1500 バイトでこのブロック・ヘッダーサイズを大きく上回るため、このブロック・ヘッダー・オーバーヘッドが伝搬時間に目立った悪影響を及ぼすことはありません。

## シミュレーション

当社はこの目的のために特別に構築した離散イベントシミュレーションを用いて、ブロック伝搬のシミュレーションを行いました。シミュレーターは、少数のトップマイナー間の相互作用についてシミュレーションを行い、マイナー間のホップ距離がネットワーク内のノード間の平均距離に近い状態で、ランダム・グラフにおいて各マイナーを検証します。トップマイナーにとってしっかりと結びついていることが得策であるため、これが最悪のケースではない場合であっても、マイナーのパフォーマンスが平均以下ではないと想定します。シミュレーションを行うイベントとは、位置のうちの 1 か所におけるブロックの生成と、他のマイナーの位置のそれぞれに対するブロックの伝搬です。その結果、シミュレーションを行った CMCでは、5 ブロック・インターバルと 300 TPS（現在のブロック・インターバルは 10 秒）でした。20.35 秒が経過する前に成功確率 99.98%（失敗確率 0.02%）でトランザクションが承認されていることは、特に重要な結果です。この失敗確率は、置換フォークに削除済みトランザクションも含まれている可能性を考慮したものではないため、実際にはかなり低くなることがあります。

## 安全なマージマイニング

マージマイニングという技法は、Bitcoin の採掘者たちが同時に、ほぼゼロの限界費用で他の仮想通貨を採掘するのを可能にします。Bitcoin の採掘に用いられる同じ採掘インフラとセットアップが同時に CMCを採掘するのに再利用されます。つまり CMCが追加のトランザクション手数料を支払うので、マージ・マイニングのインセンティブが高くなるのです。ただしこれは、風説の流布や並列チェーンを利用したネットワーク攻撃にかかるコストは、非マージ暗号通貨の攻撃にかかるコストを下回ることも意味します。 CMCは、ブートストラップの初期段階で攻撃を防ぐためにいくつかの保護対策を備えています。

- フェデレーション・チェックポイント: CMCクライアントはフェデレーション・メンバーが署名したチェックポイントを期待します。フェデレーションには、交換、お よびプラットフォームの成功に関与する硬度に安全なその他の当事者が含まれます。ノードでは、Sybil 攻撃の検出と利用者への周知を目的としてフェデレーション・チェックポイントが使用されます。

- 採掘されたコインの成熟度: 採掘された各コインには 24 時間の成熟時間が設けられており、これは Bitcoin の時間よりもやや長めです。コイン成熟度が増すと、風説の流布の攻撃に対するインセンティブが減ります。

- ソースコードに埋め込まれたチェックポイント

## トランザクションのプライバシー

CMC自体、Bitcoin より優れたトランザクション・プライバシーを提供せず、ハンドルネームに依存します。にもかかわらず、 CMCの VM はチューリング完全であることから、ハンドルネーム技術（例：CoinJoin や AppeCoin）はサードパーティの認証を伴うことなく、安全に実施可能です。

## セキュリティ

マージマイニングはアルトコインではあまり広く利用されてきませんでした。Bitcoin の大規模なマイニングプールでは、暗号通貨のブートストラップの初期段階で、攻撃率 51%の新規暗号通貨を妨害できるためです。 CMCは、プラットフォームのブートストラップを行い上記リスクを激減させることができる安全な手段として、フェデレーション・チェックポイントを実装しています。さらに、 CMCは Bitcoin ハッシュ・パワーの 30%に相当するハッシュ・パワーを下限として発売される予定です。 CMCファンデーションはネットワークの健全性を監視し、アラート・システムを使用して、利用者に通知し、ロールバック攻撃からネットワークを守ります。

## スケーラビリティ

CMCは現状として、Bitcoin よりはるかに拡張可能です。 CMC決済には標準的な Bitcoin 決済のサイズの 5 分の 1 が必要で、時間インターバル当たりのブロック・ペイロードが

Bitcoin の 8 倍高くなります。さらに CMCは利用者が選択できる署名スキームとして、ECDSA、Schnorr、Ed25519 を提供します。最後のスキームのパフォーマンスは通常、Bitcoin ECDSA 曲線の数倍になります。

全ての条件が同じであれば、 CMCのバンド幅消費率は Btcoin よりも平均で 50%少なくなります。これは、ブロックにはトランザクションデータではなく既知のトランザクションの参照のみが含まれるためです。確率的検証と不正証明を用いればストレージとバンド幅の利用をさらに縮減できます。

### 確率的検証と不正証明

完全ノードの所有コストは、暗号通貨の集中度に影響を与える主な要因です。コストが高くなれば集中度も高くなります。しかしながら私たちは、分散におけるマキシマリスト・ポジションは、暗号通貨はグローバル決済ネットワークになり得ないことを暗示していると考えています。両方の目的が相反しているのです。ブロック・チェーンのサイズ限界は大半の個人利用者が確実に参加できるほど低いため、Bitcoin は硬度に分散化されたネットワークを常に提供しています。これによって CMCサイドチェーンは、Bitcoin を超えてスケーラビリティを増強すると同時に、通貨管理の集中化の予防策として Bitcoin ネットワークを保有できます。

当社は、第三者信頼度、ネットワーク・ノード信頼度、自己検証の間の得失評価（トレードオフ）は可能と考えており、利用者を招いて利用者が快適と感じる比率を探ります。 CMCプラットフォームでは、ノードによる完全ブロックチェーンのサブセットの保管と妥当性確認が可能で、ノード・コストの削減につながります。これは確率的検証と不正証明によって実現されます。確率的検証とは、（部分的）ノードによって検証するブロックがランダムに選択されるテクニックで、残りのブロックについては条件を満たしている限り受け入れます。ある程度の時間が経過していること、一部の確認ブロックが追加されていること、ネットワーク接続性が適切であること、有効な不正証明ブロードキャなしがオプションで一部の正式なチェックポイントがブロードキャストされていることが条件になります。不正証明とは、「不正」というフラグが付けられているブロックです。ノードによって不正証明が受領されると、同じ高さのブロックが局所的に受け入れられているか（妥当性は未確認）が確認され、受け入れられている場合はそのブロックの妥当性確認が行われます。そのブロックが無効である場合は、ローカルのベスト・チェーンが適切に再編成されます。不正証明はプルーフ・オブ・ワークも伴うため、「不正」フラグ付き不正証明のブロードキャストにかかるコストは高くなります。ピアから「不正」フラグ付き不正証明を受領したノードによって、不正なピアが禁止されます。必要に応じて、ノードにより、安価な DoS による感染 IP の使用を防止するためにピアからの初期プルーフ・オブ・ワークが要求されます。マイナー（PoW とフェデレーションの両方）はフルノードでなければならず、ブロックデータを隠し持っている（ただしヘッダーをブロードキャストしている）攻撃者のブロックを即座に切り捨てるので、ベストチェーンはその攻撃者から影響を受けません。

## 総括

CMCは 4 年に渡ってブロックチェーン技術に改良を重ねており、暗号通貨エコシステムによって、プログラム可能なお金と決済の最高機能を駆使しながら Bitcoin（通貨）の価値を

引き上げることができるようになります。
世界中の開発者たちが、世界一安全なネットワークにおいて安いトランザクション費用で稼働する、個人向けと法人向けの分散型ソリューションを創造して、多様なニーズに対応できるようになります。

Bitcoin マイナーはスマート・コントラクト市場に参入できるようになり、マイニング業界に大きな価値が付加され、長期にわたる持続可能性が保証されるようになります。

CMCはより広範なマイナー基盤の構築に貢献し、Bitcoin ネットワークのセキュリティを強化します。

CMCは分散型で即効性のある安価な金融システムの開発を実現し、銀行を利用らず我々の世界で経済的には十分に機能していない 30 億人のために、金融包摂と機会を構築します。

**CMCコアチーム**