THE KAICOIN WHITE PAPER

ブロックチェーンと文化の融合
通貨に革命をもたらす暗号通貨プラットフォーム

www.kaicoin.io

Initial Ver. 1.0 : 2017-05-01
Last Updated Ver. 1.2 : 2017-08-18

目　　次

1. 概要

カイコインは、韓国投資者協会会員の利益増大を図るとともに、国内外関係会社のコンテンツ決済用に使用する目的で、韓国投資者協会によって投資・開発された。カイコインは、ビットコインやイーサリアムの技術を補完してセキュリティを強化し、処理速度を10倍以上に向上させたもので、特にセキュリティ重視の安全な暗号通貨と評価されている。発行総量が21億枚に制限されており、世界的に普及すればするほどコインの希少性が高まって自然と価値が上昇する。
また、モバイルゲームやオンラインモール、VRコンテンツなどに使用できるようにシステムを構築済みで、カイコインの使用環境は今後、急速に拡大すると予想される。
また、完璧なセキュリティシステムによって収益性を追求し、カイコインやビットコイン、イーサリアムはもちろん、その他世界有数のアルトコインも取引できるように統合取引システムを独自に運用する予定。

2. 背景

ブロックチェーンは、2009年にナカモトサトシによってビットコインの中核技術として誕生した。
ビットコインは二重決済問題を解決するためにブロックチェーンを使用した。これは個人のトランザクションを公に記録する取引台帳で、ブロックチェーンを利用する一番の理由がここにある。その後、ブロックチェーン技術を応用した様々なアルトコインが出現し、これまでに約800種類の暗号通貨が競争しながら世界中で活発に取引されている。
また、コンソーシアムブロックチェーンの導入により、数多くの企業や銀行がこのブロックチェーン技術に投資している。
ブロックチェーンは通貨をはじめ金融商品、サービス、物流情報、財産所有権、知的所有権、身元情報、あらゆるデジタル資産を使用・管理しようとする幅広い層によって研究・開発されている。2014年7月にヴィタリック・ブテリンが考案したイーサリアムは、「任意の状態遷移関数実現に使用できる契約」というスマートコントラクトを提供するブロックチェーンを中核技術としている。このようなスマートコントラクトベースのブロックチェーンの最大目標は、ユーザーがあらゆる種類の契約(プログラム)をブロックチェーンに書き込めるようにすることであり、スマートコントラクトは脱中央集権型市場、通貨取引プラットフォームなどに使用できる。
しかし、ビットコインの問題点—処理速度(決済/送金)が遅いことやブロック容量(1MB)が小さいこと—やイーサリアムのセキュリティ脆弱性(DAO)問題も存在する。
暗号通貨に対する国内外の関心は急速に高まっており、より安全でより便利に使用できるコインが求められている。カイコインはビットコインやイーサリアムの欠点を補って利便性やセキュリティ性が強化され、特に韓国文化を基盤とする電子商取引に重点を置いたブロックチェーン技術に焦点をあて、収益性が確保できるように開発された。

3. GSChainについて

GSChainは組織の間で特定のブロックチェーンを作成して配布できるカスタマイズプラットフォーム。
GSChainは使いやすいパッケージによってプライバシーを保護するとともに規制をかけ、金融圏にブロックチェーン技術を伝播する上で難関とされている問題を解決するところにその目的がある。Bitcoin coreのソフトウェアから派生したGSChainはWindows、Linux、Macサーバーすべてに対応しており、簡単なAPIやコマンドラインインタフェースにも対応している。GSChainの初公開バージョンとGSChainの特徴については後述することにする。

3-1. プライベートブロックチェーン

GSChainはユーザー権限を統合管理して採掘、プライバシー、開放性に関わる問題に解決策を提示する。GSChainの中心目的は次の3つである。

1) ブロックチェーン活動が選ばれた参加者にだけ見えるようにする
2) どのようなトランザクションを許可するか管理方法を導入
3) PoWなどの関連コストをかけることなく安全に採掘可能

ブロックチェーンが私有化される場合、そのブロックチェーンの参加者がブロックの最大サイズを調整できるため、ブロックの拡張問題は簡単に解決される。また、クローズドシステムのため、参加者と関連のあるトランザクションのみ発生する。

暗号通貨はすべて公開鍵暗号方式(public key cryptography)で身元とセキュリティを管理するところから始まる。暗号通貨のユーザーは各自の秘密鍵を任意に作成することができ、他の参加者には絶対に公開してはならない。各秘密鍵には数学的関係のある公開アドレスがあり、これは通貨を受け取ることができる身元証明の役割を果たす。公開アドレスに通貨が送金されたら、秘密鍵がないとその取引を「締結」することはできない。これは秘密鍵でアクセスできる人がその鍵によって保護されている通貨の所有者であることを意味する。

このような暗号方式は通貨に対するアクセス権限を管理し、ユーザーが特定アドレスの秘密鍵を所有しているということを証明するために、メッセージに署名できるようにする。このような特徴から、GSChainはアクセス許可リストに載っているユーザーのみブロックチェーンにアクセスできるように許可するが、2つのブロックチェーンノードが接続するとき、以下のような「ハンドシェイク」プロセスが行われる。

ブロックチェーンのハンドシェイクプロセス

1) 各ノードはアクセス許可リストに公開アドレスで身元を明らかにする。
2) 各ノードはそれぞれが持つ許可リストに相手のアドレスがあるか確認する。
3) 各ノードは相手にチャレンジメッセージ(challenge message)を送る。
4) 各ノードは受け取ったチャレンジメッセージに署名(signature)をして送り返し、自ら提示した公開アドレスに対応する秘密鍵を持っていることを証明する。

いずれか一方のノードで結果が条件を満たさなければ、P2P接続を強制終了する。

権限を公開アドレスに結び付ける原理は、ネットワーク上の他の機能にも応用できる。例えば、送金・受取トランザクションの権限を特定のリストで制限することもできるわけだが、これはトランザクションの内訳に送金人と受取人のアドレスが両方とも明示されるためである。送金人・受取人が多数の場合もあるため、トランザクションに含まれる送金人と受取人の全員が許可リストに載っている場合のみトランザクションが許可される。もちろん、ブロックチェーンを完全に公開して閲覧できるようにし、トランザクション機能のみ制限することもできる。最後に、採掘者がブロックに含めたコインベーストランザクションに署名欄を追加し、GSChain内の採掘を同じように制限できる。これは少数がプライベートブロックチェーンを掌握することができないように中心的な役割を果たす。これについては後述する。

GSChainの権限

GSChainでは、特定のメタデータを含むネットワークトランザクションを使ってあらゆる権限の承認とキャンセルが行われる。「最初(genesis)」のブロック採掘者は、他のユーザーの権限を管理できる管理者権

限を含めて、あらゆる権限を持つことになる。管理者は、トランザクション出力値に含まれるユーザーアドレスや各ユーザーに与えられる権限を明示するメタデータにより、他のユーザーに権限を与える。他のユーザーの管理者権限および採掘権限を変更するときは、制約が追加で適用される。既存の管理者が変更事項について同意するかどうかを票決しなければならず、最小比率以上の同意があって初めて権限の変更が可能となる。このような票決は別のトランザクションによって各管理者が登録し、十分な合意に至ったときに変更事項が反映される。ブロックチェーンの生成初期にいくつかのブロックは「設定段階」を構成するが、このときに管理者1名は前述の票決をスキップすることができる。今後のバージョンではGSChainに独自に権限の承認・キャンセルができる「スーパー管理者」を反映させることもあり得る。

権限の変更内容はトランザクション内のメタデータに保存されるため、ネットワークにあるすべてのノードに速やかに伝播され、現在の状態に対する合意を導き出す。しかし、分散ネットワークなだけに、各ノードが他のトランザクション前後の異なる時期に権限のトランザクションを受け取ることもあり得る。万一、代金支払いトランザクションの有効性がまだ伝播されていない権限の変更で決定される場合、この違いは大問題につながりかねない。あるノードは支払いを受理し、あるノードは拒否することもあり得るためである。

このような違いはブロックチェーン上でトランザクションの確認が行われれば解決し、最終的な順序が固定される。トランザクションがブロックチェーンの順番どおりに「再生」されるため、ブロックにある各トランザクションは直前のユーザー権限に基づいて有効なトランザクションでなければならない。ブロックにあるトランザクションが有効でない場合、ブロック全体が無効処理される。 ブロックが有効であっても、そのブロックのトランザクションに定義された許可リストに採掘者が載っていなければ有効なものとして処理されない。

ただし、アクセス権限の場合はブロックチェーンの内容と無関係なため、このような権限管理システムから除外される。その代わり、特定アドレスの権限が取り消される場合、すべてのノードがハンドシェイクプロセスでそのアドレスを使用したノードとの接続を切る。

便宜上、固定範囲のブロック番号に一時的な権限を制限的に承認することもできる。このような一時的権限によって行われるトランザクションは、指定された範囲にあるブロック番号に対してのみ有効である。権限の変更は、十分な数の管理者がそのユーザーと権限に合うブロック範囲を正確に選んだときにのみ、合意に達したとみなされる。これによってネットワークの透明性を高めると同時に、期間の満了した一時的な権限をひとつひとつ取り消す手間が省ける。

ブロックチェーンがきちんと「プライベート」ネットワークになるために、アドレスはすべてチェーン上で承認され、少なくとも1名の管理者がアドレス所有者の実際の身元を必ず知っていなければならない。しかし、ほとんどの参加者がお互いの身元を知っている必要はない。ブロックチェーンの主要機能の1つがP2P(Peer-to-Peer)トランザクションで、2種類のトークンを交換するケースがある。アドレスの匿名性が保障されれば、トランザクションが行われるときにお互いのことをよく知らなくても取引が可能である。金融機関は数多くのアドレスを取り扱ってこのようなトランザクションを処理するわけだが、各アドレスの所有者は担当者にしかわからない。

3-2. GSChainでの採掘

GSChainでは身元が確認できる当事者にのみ採掘権を提供し、1名が採掘権を独占できるプライベートブロックチェーンのジレンマを解決している。その解決策は、同じ採掘者が特定の期間内に生成できるブロック数を制限するというものである。

制限をかけるときに必要なパラメーター

mining diversity （*0 ≤ mining diversity ≤ 1* と定義）

パラメーターを活用してブロックの有効性を検証

1) ブロック内のトランザクションに定義されたすべての権限変更を順次適用する。
2) 変更適用後に許可された採掘者の数を数える。
3) 採掘者数と*mining diversity*を掛け、四捨五入して*spacing*値を得る。
4) 当該ブロックの採掘者が前の*spacing*-1ブロックを採掘したことがあれば、そのブロックは無効処理される。

ラウンドロビン(round-robin)スケジュールの適用により、許可された採掘者が有効なブロックを作成するにはローテーションで行わなければならない。*mining diversity*パラメーターは、結託してネットワークを攻撃しようとするであろう許可された採掘者の割合によってスキーム(scheme)の厳格さを決定する。値が1なら、すべての許可された採掘者がローテーションに入り、0なら制限が全くないことを意味する。一般的に値が大きいほどネットワークは安全とみなされているが、1に近すぎると 一部の採掘者が活動していないときにブロックチェーンがフリーズしてしまうこともある。そこで、中間の値として0.75を勧奨する。各ノードはリソースを節約するために、前に採掘した*spacing-1*ブロックのあるチェーンでは採掘しようとしない。

多様性変数で制約をかければ悪意のある活動を予防することができ、通信途絶などによってネットワークが一時的に切れるときも役立つ。このとき、切れたネットワーク区間のノードは他の区間の取引やブロックを参照することができないため、ブロックチェーンが分岐することもある。ネットワークが復旧すると、世界的な合意として分岐したチェーンの中から一番長い枝が選ばれる。このような多様性制限により、一番長い枝に許可された採掘者が集中するようになる。他の区間のチェーンはすぐにフリーズしてしまうためである。

プライベートブロックチェーンの有用性

なぜ、あえて集中データベースではなくプライベートブロックチェーンを使うのか、と疑問に思うかもしれない。集中データベースも受信トランザクションの承諾、紛争解決、データベース状態のクエリー回答などが可能なのにである。この疑問に対する答えを以下の3つにまとめた。

1) ブロックチェーンでは、各参加者が秘密鍵によって自分の資産を完全に管理する。採掘者も、他の参加者の資金でトランザクションを作成することはできない。

2) データベース管理権が多くの参加者に分散しているため、特定の個人や少数集団がトランザクションの有無を単独で判断することはできない。

3) ブロックチェーンは集中データベースシステムより安定している。サーバーが1つなくなったり故障したりしても、ネットワーク全体のトランザクションには影響を及ぼさない。

権限ベースの採掘においてPoWはどうなるか？ビットコインではPoWによって採掘に必要な計算を難しくして(すなわちコストがたくさんかかるようにして)採掘の多様性を保障する。これに対してプライベートブロックチェーンは、はるかに単純な方法で採掘の多様性を保障するため、PoWに必要な作業は形式的なものに過ぎない。実際に、GSChainの最初のバージョン

は各ノードのブロック生成率を規制してランダム化するために依然としてビットコインスタイルのPoWを採用しているが、これはブロックチェーンのセキュリティを目的としているわけではない。

GSChainブロックチェーンでは、トランザクション手数料とブロック報酬が"0"に設定されている。ブロック採掘のコストが 無視できるほど少なければ、採掘者も別の補償は必要なくなり、ブロックチェーンが円滑に機能することによって得られる利益のために採掘をするようになる。その代わりに採掘者がネットワーク参加者から固定年会費を受け取ることもでき、その場合の支払方法はブロックチェーンではなく制度圏内の支払手段によるものとする。ブロックチェーンの唯一の目標がトークン化された資産にトランザクションを提供することであれば、そのネットワークの暗号通貨は単なる技術革新程度で無視することもできる。しかし、トランザクションの希少性が望まれる状況なら、GSChainでも暗号通貨がブロック報酬や最小のトランザクション手数料、取引量などに使用されるように設定できる。このような場合、参加者は暗号通貨を採掘者から購入しなければならず、トークン化された資産などを支払手段とすることができる。

3-3. 多数のブロックチェーン駆動

Bitcoin Coreのようにシングルブロックチェーン対応ではなく、GSChainでは同時にいくつものブロックチェーンを作って作業するということが容易にできる。機関レベルでは、特定の開発者ではなくシステム管理者がプライベートブロックチェーンを作って運営できるという面で非常に有利である。例えば、OracleやSQL Serverなどの関係データベース管理システム(RDBMS)でいくつかのSQLコマンドによってデータベースを作成・使用できるというのと似ている。また、多数のブロックチェーンに対応できることの長所は、サーバーが他のチェーンの活動と接続できるという点である。例を挙げれば、特定のブロックチェーンに資金が入ったとき、他のブロックチェーンに送金するようにもできる。

GSChainでは、ユーザーが以下の内容を含めてあらゆるブロックチェーンのパラメータを設定ファイルに定義できる。

1. チェーンプロトコル	プライベートブロックチェーンまたは純粋なビットコインに近い
2. ブロックの目標時間	例：1分
3. 有効な権限の種類	例：誰でもアクセス可能、一部の人のみ送受信可能
4. 採掘の多様性 (mining diversity)	例：0.75
5. 管理者や採掘者を追加・除去するときに必要な合意レベル、このような事項が強制されない設定段階の期間	プライベートブロックチェーンのみ該当
6. 採掘報酬	例：1ブロック当たり50ネイティブ通貨、 21万ブロックごとに半減するように設定
7. P2P接続のためのIPポートとJSON-RPC API	例：8571, 8570
8. 許可するトランザクションの種類	例：pay-to-address, pay-to-multisig, pay-to-script-hash

9. 最大ブロックサイズ	例：1MB
10. 1トランザクションあたりの最大メタデータサイズ	例：4096バイト

1つのサーバーで複数のブロックチェーンが利用でき、ブロックチェーンごとにそれぞれ名前と設定ファイルがある。新しいブロックチェーンを作るには2つの設定が必要。

1) ユーザーはチェーン名を選択する。そうするとGSChainはデフォルト設定を含む設定ファイルを作成する。このファイルは変更可能だが、一般的にはデフォルト設定のままで構わない。

2) ブロックチェーンを起動するとGSChainが最初のブロックを採掘し、その作成者にすべてのユーザー権限が与えられる。このとき、最初のブロックの細部事項とそのブロックチェーンパラメータのハッシュが設定ファイルに埋め込まれ、のちに誤って変更されるのを防ぐ。

GSChainのプロセス

初めて起動するとき、ブロックチェーンは単一ノードで起動する。新しいノードを追加するには、次の3つのパラメータを使って別のコンピューターでGSChainを起動する。(1) ブロックチェーン名 (2) IPポート番号 (3) 既存ノードのIPアドレス
便宜上、この情報は「ノードアドレス」という形式にまとめて使用される。例：
gschain@127.0.0.1:0000
ネットワークがプライベートでノードにまだアクセス権限が与えられていないため、初めは新規ノードがネットワークにアクセスできない。GSChainは新しいノードが自己生成した公開アドレスを含むメッセージを表示する。このアドレスは管理者に送らなければならない。管理者は簡単なコマンドでトランザクションを作成し、そのアドレスにアクセス権限を与える。これで新規ノードがアクセスできるようになり、アクセスするとブロックチェーンの特性が定義された設定ファイルを自動的にダウンロードする。それ以降同じブロックチェーンにアクセスするときはチェーン名のみ必要で、ノード間のハンドシェイクプロセスによって同じパラメータの使用が保証される。

GSChainの改善事項

今後改善の必要があるのは、ブロックチェーンが実行中のときに信頼できる管理者が発行した特定トランザクションを通して一部のパラメータが変更できるようにすることである。例えば、ネットワーク使用量が増加するにつれて最大ブロックサイズを大きくし、予想されるトランザクション量に対応することができる。このような変更を行うときは、ネットワーク上にある各ノードの計算能力も考慮しなければならない。

3-4. 複数通貨のブロックチェーン

CoinSparkやCounterpartyなどのトークン化プロトコルを使用すれば、ビットコインのネイティブ通貨と並行してビットコインブロックチェーンで第三者の資産を発行し、取引できることはすでに言及した。このようなテクニックは、GSChainで作成したプライベートブロックチェーンでも変更を加えることなく同じように使用できる。しかし、プライベートプロトコルを使用するブロックチェーンでは、第三者の資産をサポートする機能をチェーンのルールに反映させることで改善できる。

ビットコインでは各トランザクションの結果値に含まれるビットコインの数量を取引ごとに符号化する。出力

値に符号化された合計ビットコインより入力値に反映されたビットコインのほうが多い場合、その取引はネットワークで無効処理され、ブロックチェーンに確認することも伝播することもない。 ネットワークの全ノードが未使用のトランザクション出力値にあるビットコインを追跡するため、このような検証が可能である。したがって、ユーザーは、ネットワークまたはブロックチェーンで処理されるトランザクションに符号化されたビットコイン数量について、その正確さを信頼することができる。そのため軽量(“simple payment verification”)のウォレットでネットワークと安全に取引することができ、ブロックチェーン全体をユーザーのパソコンに保存する必要はない。

トークン化の問題点

ビットコインで資産をトークン化する場合に問題となる点は、外部資産をエンコードするメタデータがビットコイン自体を検証するネットワークレベルの検証プロセスを経ないことである。例えば、ABCという銀行がドルを象徴するトークンを発行したと仮定してみよう。悪意のあるユーザーは、出力値に100 ABC ドルがあるというメタデータを含むトランザクションを作ることができる。実際にはそのトランザクションの入力値にABC ドルがなかったのにである。このようなトランザクションはビットコインネットワークで有効なものとして処理され、ブロックチェーンでも確認することができる。その理由は、第一にビットコインノードがこのメタデータを読めないためであり、第二にはビットコインノードがABCドルを追跡しないためである。

したがって、トークン化資産は、ビットコインブロックチェーンでビットコインのネイティブ通貨に比べて二流国民の扱いを受ける。トークン化資産の存在有無は、そのトークンを初めて作成したトランザクションからトークンに影響を与えるすべてのトランザクションを見ないとわからない。これは「フォワード(forwards)」方式で効率的に計算できる。新しいトランザクションが入ってくるたびに検討すればいいのである。しかし、そのようにしても全体的なネットワークノードが必要で、トークン化プロトコルを軽量ウォレットと使うには不適切である。

GSChainはこのような問題を解決するために、あらゆる資産の識別子(identifier)と数量を各トランザクションの出力値に符号化する。このとき、ビットコインスクリプト言語が提供する拡張子(extension)を使用する。そうすればトランザクションの検証ルールが拡大し、トランザクションの出力値にある全資産の総量が入力値と等しいか検証できるようになる。入出力値が等しくなければならないという要求事項は、ビットコイン自体の要求事項より厳格である。ビットコインの場合、出力値が入力値より小さければ有効なものとして処理され、このときその差額は採掘手数料となる。もちろん、このような方式を使用する前に、そのブロックチェーンが特殊メタデータを含む最初のトランザクションによって新しい資産を作れるように許可しなければならない。GSChainでは、このような最初のトランザクションがブロックチェーンのどこで作られたかによって新規資産に識別子を自動的に割り当て、ユーザーが定義した固有識別子と一緒に使用される。

GSChainの権限システムは、資産作成権を管理するために使用することもできる。また、今後のバージョンには資産別権限を導入する可能性もあり、これによって資産別に管理者と許可された送り主・受取人を設定できるようになる。簡潔さのためにGSChainの最初のバージョンには含まれない機能だが、すでに反映されたルールに少しの拡張を行うことで簡単に追加することができる。

3-5. ビットコインとプライベートブロックチェーンの切り替え

1990年代にインターネットの使用量が急増したとき、何百万人もの人々が新しいパラダイムに触れた。企業はこのような革新技術を内部的に活用したかったが、当時は多くの企業がインターネットを主なコミュニケーション手段として活用するにはプライバシー保護や信頼性、容量の面で不十分であると評価した。したがって、多くの企業は組織内ネットワーク「イントラネット」を構築した。インターネットと同じインフラや技術を使用しながら、企業で完全に管理できる技術だった。
約20年が過ぎた今、インターネットは大容量の情報を世界中に安定して送信できるネットワークとして根付

いた。これによって多くの企業がVPNを活用するようになった。VPNはインターネットを基本技術としているが、組織の通信内容を暗号化するため、公共通信網を通して送信されてもセキュリティを維持することができる。VPNを通してインターネットの規模の経済を享受しつつ、データが外部に漏れるリスクを回避しているのである。

ビットコインブロックチェーンとプライベートブロックチェーンの間でも、似たようなプロセスが行われている。企業の立場からすれば、ビットコインネットワークはまだ未開拓の分野で、容量も限られており長期的なトランザクションコストを予測することもできない。何よりも、ビットコインの採掘は不特定多数がコントロールしており、そのほとんどは企業に反する思想を持っていたり、法的制度が整っていない国に住んでいたりする。したがって、金融機関などにとっては、今後10年間に関して言えば、このような技術を使用するのにプライベートブロックチェーンのほうが魅力的に映るだろう。今から20年後にビットコインや他のブロックチェーンが毎月数十億件のトランザクションを非常に安く処理し、実体の確かな大企業が採掘をコントロールしているという状況になれば、その時はビットコインが金融機関の取引にも魅力的なプラットフォームになるかもしれない。VPNのように薄い暗号化層を使って機関の活動をほとんどのネットワーク参加者に対して隠すこともできる。

GSChainの設計は、多くの面でプライベートブロックチェーンとビットコインブロックチェーン間の双方向切り替えができるようにすることを目的としている。下記5)の機能によって資産のトークン化とメッセージングを使用するアプリケーションがある場合、コード変更を最小限にした状態でビットコインとプライベートブロックチェーン間の切り替えが可能である。

1) GSChainはビットコインネットワークの公式クライアントであるBitcoin Coreの派生バージョンをもとに作られた。コード変更はローカライズされ、将来のビットコイン改善に対応できるようにした。
2) GSChainはビットコインのプロトコル、トランザクション、ブロックチェーンアーキテクチャーをほぼそのまま使用する。唯一の違いは、2つのノードが最初にアクセスするときに行われるハンドシェイクプロセスである。その他の特徴については、メタデータを使い、トランザクションやブロックの検証ルールに変更を加えて反映させた。
3) GSChainのインタフェース(コマンドライン、API)は、新しいコマンドが提供する追加機能によってBitcoin Coreのインタフェースと完全に互換性がある。
4) GSChainは、per-blockchain設定ファイルにある簡単なプロトコルの設定1つで一般のビットコインネットワーク(またはビットコイン類似ネットワーク)においてノードの役割が果たせる。
5) GSChainの複数通貨やメッセージ機能は、ビットコインのトランザクションを改善するためのCoinSparkプロトコルと非常によく似ている。

4. カイコインの適用技術

4-1. ブロックチェーン方式

特定の団体または組織による先占や独占を防ぐため、先行採掘に関する情報や社会還元の有無を透明に明示してスタートし、Public BlockChain方式で誰でも採掘に参加できるようにして報酬を共有する。これによってコンピューティングパワーを利用した暗号通貨システムのセキュリティはより一層強化される。
パブリックブロックチェーンは「許可不要台帳(Permissionless Ledger)」とも呼ばれている。したがって、誰でも許可なしにブロックチェーンのデータを読み、書き、検証できる。カイコインもこの方式をとっている。また、誰でもブロックチェーンをダウンロードして何が書かれているか閲覧したり、暗号署名を利用して記録に参加したりできる。
参加者はどのようなデータが入力されるかを投票で決める。ノード数ではなく、投入したコンピューティングパワーに比例して投票権を与える一般的な方式がある。しかし、カイコインはこのような方式でmining

diversityによってコンピューティングパワーの強いノードが独占できないようにしている。したがって、最大限多くのノードが採掘に成功できるように助ける。

4-2. ブロックタイムとブロックサイズ

最初のユーザー(3000人～4000人)を確保したコインでスタートするため、トランザクション速度とセキュリティが最も重要な問題となる。したがって、ブロックサイズを最小4Kbyteから最大2048Kbyteまで動的に割り当て、効率的にノードの処理速度を上げて安定したトランザクション速度を保障することができる。
また、ブロックタイムを60秒に指定して平均60秒以内にハッシュされたブロックヘッダ値をつなぐ(chaining)ことができるため、10分という既存ビットコインのブロックタイムより10倍早いadvanced SHA256のハッシュ技法が経験できる。
この2つは我々の追求する次世代ブロックチェーン通貨の最も重要なイシューであるトランザクションが不発だったり、トランザクション自体が遅れたりする現象を防ぐことができ、既存のビットコインのような安定性を保障することができる。
現在盛んに話題となっている最大ブロックサイズに関しては、最も効率的だという意見が集まっている2048Kbyteに定め、過去にブロックサイズのせいで一度に多くのトランザクションをブロックに記録できなかった問題を解決した。

4-3. マルチシグネチャスクリプト

Pay to Script Hash(P2SH)は同時に2つの署名が必要な方式の暗号化を使いやすくしたもの。P2SHの場合、複雑なロックスクリプトは暗号化されたHash値をデジタル指紋で代替することができ、トランザクションサイズを小さくできるメリットを含めてシステムの内部的に効率の良いトランザクション構造を選択できる。

4-4. 半減期

半減期を1年とした場合に100年間採掘できる公開採掘システムを提供する。ブロックタイムを1分とした場合、3年間で約1,576,800のブロックが作られると予想される。これは採掘者により良い採掘環境を保障するためで、最初の発行量21億を考慮してみると、採掘の機会と難易度、その期間を十分に提供できなければ、セキュリティに責任を負うブロックチェーンのエコシステムを安定的に流通させられないと判断するためである。
我々はより良い採掘環境を作ることがブロックチェーン技術の本来の目的を忠実に果たすことになると信じている。

4-5. カイコインの技術仕様

- ハッシュアルゴリズム(Hash Algorithm) : advanced SHA256
- 総発行量 : 21億カイコイン
- 発行方式 : 採掘(Mining)
- ブロックタイム :60秒
- ブロックサイズ : 2048Kbyte

5. カイコインについて

5.1. 目的

カイコインは暗号通貨市場に害を及ぼしてきた既存の古い環境を改善したいというカイ協会会員の願いが動機となって開発された。カイコインは安全・迅速・透明に使用したいというユーザーのニーズに積極的に対応している暗号通貨で、特にadvanced SHA256方式によってビットコインの短所である決済の遅延やセキュリティ問題を改善して誕生した。特に、カイコインに使用されるブロックチェーンは電子商取引に焦点を当てて開発され、ユーザーに多くの利便性と経済的メリットを同時に提供する。
カイ協会の最終目標である系列会社10,000社間の相互有機的かつ協力的なネットワークづくりに向け、

カイコインは決済手段としての役割を忠実に果たす必要十分な媒介になるだろう。
カイコインを韓国だけではなく全世界で通用する電子商取引中心のグローバルな暗号通貨にする ことを目指している。
日常的に様々なシーンで活用できるブロックチェーンベースのシステムを構築するとともに、韓国の特色あるコンテンツと文化を融合させて社会・文化の発展に貢献し、さらには国際的に通用する仮想通貨としての認識を広める。

5.2. 活用プラットフォーム

情報通信技術の急速な進歩により、過去のやり方では競争で生き残るのが難しくなっている。このような時代的要求に対応してプラットフォームベースが誕生し、現在では企業の成否を左右する要因となっている。
暗号通貨市場におけるプラットフォームベースの礎は、ヴィタリック・ブテリンが2015年に開発したイーサリアムが最初である。単に通貨としての機能を備えているだけのビットコインとは概念上の違いがあり、これからの第4次産業革命の時代においては、イーサリアムのようなプラットフォームベースの通貨が主流になるだろう。

カイコインもプラットフォームベースの暗号通貨であり、これによって韓国投資者協会はビジネス分野と社会貢献分野で様々な活動を展開していく。

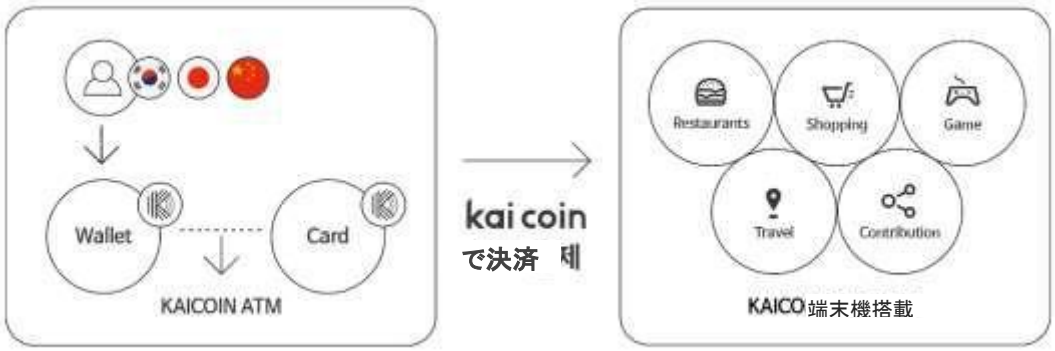
社会	- ブロックチェーン技術の共有による社会インフラの拡大 - 社会貢献プラットフォームの構築による非営利活動の支援およびNGO団体への透明な経済的支援
文化	- K-Cultureコンテンツによって中国や日本向けにマーケティングプラットフォームを構築済み - 分散システムを活用したVRコンテンツやモバイル動画ナビゲーションの使用を拡大 - 飲食店、ベーカリー、旅行会社、病院などオフライン加盟店の確保 - 国内外オンラインモールへの支援を拡大 - オンラインゲーム内アイテム取引の支援
経済	- KAICOIN統合取引所KAIREXの構築 - 現金自動預け払い機(ATM)でのKAICOIN活用 - 国際取引所へのKAICOIN登録

5.3. 詳細情報

- 通貨名 : KAICOIN (カイコイン)
- 通貨単位 :KAI
- プレセール期間 : (GMT+9) 2017年9月1日午後12時から2017年10月31日午後11時59分
- 1トークン当たり価格 : 1,500 KAI = 1 ETH
- 最低購入量 : 150 KAI = 0.1 ETHから可能
- 総供給量 :200,000,000
- 取引可能な通貨 : ETH
- ボーナス : 週ごとに支給
  (～1週目20%、～2週目15%、～3週目10%、～4週目5%、5週目から0%)

総供給量 **2,100,000,000**	公開採掘量	1,000,000,000
	先行採掘量	**1,100,000,000**
先行採掘量 **1,100,000,000**	韓国でのプレセール	600,000,000
	ICO	**200,000,000**
	社会寄付	100,000,000
	投資者保有	100,000,000
	その他	100,000,000

5.4. 使用環境



5.4.1. ゲーム

ゲームを通して得られる2つのメリットは、ストレス解消と関連能力の向上である。ストレス解消の面では模擬競争、代理満足、創作などが挙げられ、関連能力向上の面では集中力向上(囲碁)や手続き記憶の向上(老年層)などに役立つ。
カイコインはこのようなゲームの決済にも使用され、国内外の状況からみて高い需要が予想される。

5.4.2. オンラインモール

オンラインショッピングとは、インターネットやパソコン通信、モバイル機器などを利用して商品を検索し、注文する行為のことをいう。代金の決済はクレジットカードやモバイル決済で行われる。このようなオンラインショッピングは情報通信の発展やインターネットユーザー数の増加、便利さなどから急激な増加傾向にあるものの、個人情報の流出や決済システムの不安定さといった問題点を抱えているため、次第に暗号通貨が新しい決済手段として進化している。
カイコインは、二重決済や決済者の個人情報露出、過剰な手数料などの問題が指摘されている既存の決済システムに代わるソリューションとして期待される。

5.4.3. オン・オフライン加盟店

加盟店とは、1つの事業連盟に属しているお店のことで、フランチャイズとも呼ばれる。加盟とは店舗と会社の間で結ばれる営業的な契約であり、加盟店は会社からブランドの知名度による収益創出や経営サポートなどが期待できる。
こうした加盟店の数は爆発的に増加しており、今も増え続けている。カイコインは有名ブランドを保有している会社と協力し、全国の加盟店で決済手段として使用できるように働きかけていく。

5.4.4. モバイルサービス

- カイコインウォレット
  カイコインを受け取ってアカウントを管理できる電子財布
- KAIREX取引所
  カイコインや他の仮想通貨の取引ができる取引所サービス
- 寄付・その他
  国内外のカイコイン加盟店を検索してプレゼントや後援・寄付ができるサービス

6. ロードマップ

1次 **(～2017年9月)**	- カイコイン開発 - カイコイン寄付約定締結 - 韓国でのプレセール(ICO) - グローバルプレセール(ICO) - カイコインウォレットリリース
2次 **(2017年10～12月)**	- カイコイン取引所KAIREX設立 - 国際取引所に登録 - ベンダーや決済代行業者との提携拡大
3次 **(2018年)**	- カイコインとカードの融合 - ATMとの連携およびコインでの簡便な決済に使用 - カイコイン使用の日常化
4次 **(2019年)**	- 中国や日本向けの決済システムに対応 - オフライン加盟店10,000店以上の確保 - 旅行産業を中心に対応拡大 - 中国・日本人観光客に特化した利便性の提供
5次 **(2020年～)**	- 東南アジア・欧州市場への進出を模索 - 国内外で活用度の高い代表的な仮想通貨としての認識定着

7. 開発会社および提携会社

7-1. 韓国投資者協会

韓国投資者協会は2010年12月に設立された。非営利団体として経済教育、投資教育、エンジェル投資クラブを支援し、パートナー会社との協力による株式寄付運動および10万人の健全な投資者養成を目指している。
韓国投資者協会の事業は大きく次の4つに分けられる。

1) 金融教育事業
財産管理アカデミーの様々な金融教育プログラムによって会員に資産管理や投資の教育、青少年に経済教育のサービスを提供している。

2) 投資クラブ育成事業
エンジェルクラブの設立・運営を支援し、投資価値のある企業を発掘して会員に投資できる機会を提供することによって会員の効率的な資産管理を助ける事業。

3) 株式寄付事業
共に生きる社会の一員として企業活動の社会的責任を果たすべく、革新的な社会貢献事業「株式寄付運動」に参加する7,000社の資産寄付協力企業ネットワークを作る事業。

4) IT関連デジタル産業への投資・運営事業
協会は、第4次産業革命の時代に求められる新しい暗号通貨とそれにふさわしい決済システムに対応するため、電子商取引に必要な安全性、迅速性、収益性を考慮して協会の傘下にカイコイン事業本部を設立し、カイコインを開発することになった。
カイコインは韓国投資者協会や会員のみならず、下記に示す協会のパートナー会社によっても使用されることとなり、ゆくゆくは世界的なゲーム会社やオンラインモール、有名ブランドを取り扱う加盟店などで決済手段として使用される見通し。
暗号通貨の特性上、コインの量は限られているのに需要が増えることによってコインの通貨としての価値は上昇する。そのため、カイコインを保有する会員には相当な金銭的メリットがあると予想される。

7-2. 提携会社

KAii	WHITE STONE	Allreve	INCAPO
WOWZONE	PICK:LE 日本	PICK:LE 中国	(株)ビット＆パーソン
AllStarWORLD	ローズ＆ビーメディカル	味来屋 プルコギ専門店	クンムルチャムチマグロ専門店

※ ホームページがない提携会社は一覧から除いた。

※ 新たな提携会社に関する詳しい情報はホームページに表記。

- KAii :http://www.kaii.or.kr/default/mindex.php
- Allreve :http://www.allreve.com/mshop/main.asp
- WOWZONE : http://wowzone.co.kr/mshop/main.asp
- PICK:LE 日本 :http://ameblo.jp/pickle-japan
- PICK:LE 中国： http://weibo.com/u/5888766483?is_hot=1
- AllStarWORLD :http://www.allstarworld.co.kr
- ローズ＆ビーメディカル： http://www.rosenbee.com

8. 結論
韓国投資者協会傘下のカイコイン事業本部は、ビットコインの通貨価値的機能とイーサリアムの幅広いプラットフォームベースの活用による進化した暗号通貨の開発に向けて邁進してきた。合理的なアルゴリズムと実用的なブロックチェーンをベースに電子商取引分野、特にゲームやeコマースの決済に特化して技術を開発した。
カイコイン開発チームは、ブロックチェーン技術によって得られるセキュリティ性や無欠性を活用して日常の様々なシーンで利用できるブロックチェーンベースのシステムを構築した。
韓国のコンテンツと文化を融合させて社会・文化の発展に貢献し、国際的に通用する仮想通貨を目指す。