

Whitepaper


Bryllite Platform


Beyond the Game Boundaries

ブリルライト・プラットフォーム：ゲームの境界を越えて



 Bryllite Ltd.

 labs@bryllite.com

 www.bryllite.com

目次

| | |
|--------------------------------------|----|
| ● Introduction | 3 |
| ● ブリルライト・プラットフォームの紹介 | 8 |
| ● ブリルライト合意プロトコル | 18 |
| ● Bryllite Platform Service | 28 |
| ● ブリルライトコインの価値 | 29 |
| ● BRC Crowd-Sales & Token Allocation | 31 |
| ● ロードマップ | 34 |
| ● The Third Impact | 35 |
| ● References | 37 |

Introduction

古い紛争：ゲーム資産の所有権

90年代半ば、本格的にサービスされて巨大なグローバルゲーム市場を形成することに成功したオンラインゲームサービスで、私たちは長い間持続されてきた一つの紛争に対して注目しています。ゲームアイテム等を含むゲーム資産の所有権が開発会社（以下流通会社、サービス会社、1人開発者等の開発主体をすべて含む）に最終的に帰属されなければならないかという問題です。「**ゲーム資産**」にはアカウント、個人情報、ユーザ名/ニックネーム、装備/アイテム、キャラクターレベル/能力値、サイバーキャッシュ、メンバーシップサービス等、ゲーマーが保有することができる有/無形のすべてのコンテンツが含まれます。

多くのゲーマーが自分のアカウント/キャラクターの価値上昇のために多くの時間と努力、金銭を投資しており、開発会社は、このようなゲーマーの献身的な努力によって収益を上げ、会社を維持し、成長させていきます。このような点でゲーマーが現金で購入した有料アイテムについてだけ契約が成立したのではなく、時間と努力をかけて獲得したすべてのゲーム資産についても開発会社とゲーマー間で「**黙示的なゲーム資産の売買契約が成立した**」とみななければなりません。

しかし、ゲーマーはゲームをやめる場合に、これまで投資した費用（時間+努力+金銭）に対していかなる補償も受けることができません。更には、開発会社の問題でゲーム資産データが流失したり、ゲームサービスが一方向的に終了されることになった場合等にも、合理的な補償を期待することは難しいです。これは開発会社から提示する一方的で、不公正な利用規約等により、ゲーム資産の所有権が開発会社に最終的に帰属されているからです。

私たちは、「**黙示的なゲーム内資産の売買契約の成立**」を根拠に、現金で購入したアイテムだけでなく、すべてのゲーム資産がゲーマーにその所有権が最終的に帰属しなければならないと主張します。そして、ブロックチェーン技術を利用して、ゲーマーの資産を安全に守り、ゲーム間の境界を越えて資産を移動したり取引できるようにして、「超連結ゲーム社会 (Hyper Connected Game Society)」エコシステムの構築を目標とする「**ブリルライト・プラットフォーム**」を提案しようと思います。



グローバル・ゲーム資産市場の規模

国内のゲームアイテムの現金取引市場は、10年前に既に1兆ウォン市場に成長し[1]、全体のゲーム市場規模は約11兆ウォンを突破して着実に上昇しています[2]。ゲーム専門市場調査会社のNewZooの2017年報告書[3]によれば、グローバル・ゲーム市場規模は既に1000億ドルを突破し、2020年に1,300億ドルに達すると見込まれており、この傾向を根拠として2023年までに1500億ドルに達すると予想されています。



[図1] 2017グローバルゲーム市場規模及び2020年までの展望、©Newzoo | Global Games Market Report Light

私たちは、全世界の1,000億ドル規模を遥かに超えるゲーム資産をゲーマーに返してあげようとしています。もちろん、それは容易ではない挑戦となり、短い時間内に実現可能なことではないということをよく知っています。

しかし、これは必ず実現する必要がある価値であり、いつかまた誰かがしなければならないことであるため、ブリルライト・プラットフォームを通じて、今、私たちが先頭に立って挑戦を開始しようとしています。

ブロックチェーン技術を眺める私たちの視点

2008年10月、さとしなかもと(匿名の個人あるいはグループ)は、「Bitcoin: A Peer-to-Peer Electronic Cash System」という論文[4]を通じてブロックチェーン基盤のP2P電子貨幣システムを公開しました。ビットコイン(BTC)は遠くない未来に必ず実現する「現金のない社会(Cashless society)」[5]に到達するための一つのアイデアとして提案されました。「二重支出」[6]問題等を解決した偽/変造が「ほぼ」不可能な分散台帳システムで現金のない社会にいく目的地に一歩近づいたと評価されています。

しかし、このような発展にもかかわらず、ビットコインは依然として多くの問題点にさらされています。非常に遅い転送速度や不足する処理容量、高価な手数料の問題などは、技術的な補完を通じて解決可能な問題だとしても、利益に応じて動く中央化された採掘ノードと開発陣営間の合意が難しい点は、ブロックチェーンネットワークの持続的な発展において非常に深刻な問題であります。

より本質的な問題は脱規制、脱中央化という名分で国家の通貨発行権限を否定するアナーキズムに近い哲学にあるかもしれません。正しいか否かを論じるのではなく、国家の経済及び通貨政策などの社会維持機能を否定しながら現実的に生存することができるのかについての疑問をいうのです。「51%の攻撃」[7]に対する防御の論理は、悪意的なノードを前提とした防御の論理ですが、50%を超えるハッシュパワーを投入してネットワークを攻撃した時に利益がより大きい場合はいくらでもあり得ます。例えば、ビットコインキャッシュのような競争暗号通貨陣営でビットコインを崩し、暗号通貨市場の基軸通貨地位を占めたいと願う場合や、ドルやユーロなど、自国貨幣の価値と通貨発行権を守ろうとする米連邦準備制度理事会(FRB)、EU、個別の国家又は個別国家の連合などの場合、50%を超えるハッシュパワーを投入して、ビットコインのブロックチェーンネットワークを崩壊させるのがより大きい利益となりえます。個別の国家又はその連合単位の攻撃者ならば、費用が発生する面倒な方法ではなくても、法的規制や行政措置を通じてブロックチェーンネットワークを簡単に崩壊させることができます。

もちろん、さとしなかもとがビットコインシステムを最初に考案した時に「法定通貨の完全な代替」または「グローバル単一通貨」を念頭に置いていたのではないかもしれませんが、投機ブームの副作用及び各国政府機関の危機感の中で強力な規制に直面しているのが現実です。これはビットコインだけの問題ではなく、脱規制と脱中央化を叫んで法定通貨を代替しようとするすべてのアルトコイン(Alternative Coins)が同時に直面している危機です

そのため、私たちは、ビットコインで「現金のない社会」という価値の志向を排除し、ブロックチェーンの技術そのものに集中しようと思います。ブロックチェーンの技術は、本質的には、全世界に散らばっている数多くのコンピュータで構成された「スーパー・コンピューティング・パワーの分散DBシステム」です。

このシステムの利点を最大限に活用するために、ビットコインという電子貨幣システムが最初に提案され、ビットコインの問題点を補完したり、機能を拡張する数多くのアルトコインが提案されて開発が進められています。ゴーレム(GNT)プロジェクトのようにグラフィック処理(CG)作業、人工知能など、「スーパー・コンピューティング・パワー」が必要な作業に使用者PCの

遊休資源を利用する意味のある試みも続けられています。

私たちは、ブロックチェーン技術の「分散DBシステム」から完全に孤立している個々のゲームを互いに連結することができる大きな可能性を発見し、個々のゲームが互いに共有することができ、互換できるブロックチェーン基盤の分散DBプラット

私たちの問題認識

前で私たちはゲーム資産の所有権がゲーマーにあることを明らかにしました。しかし、大多数の国家でサービスされているゲームは、利用約款を根拠に、ゲーム資産に関する最終的な所有権を開発会社に帰属させています。そのため、ゲームをやめたり、ゲームサービスが終了した場合にも、ゲーマーが支払った費用に対して合理的な補償を期待することは難しいです。

ゲーマーのアカウントや保有する装備/アイテムなどのゲーム資産を他のゲーマーに現金取引等で販売することは暗黙的には認められますが約款違反である場合がほとんどです。法の適用の曖昧さによって法的訴えが難しく、オンライン上のゲーマー資産と現金の取引には、常に詐欺のような危険が潜んでいて、法に訴えることができる場合でも、信頼が担保されていない取引による事故はいつでも発生する可能性があります。信頼が担保されていない相手と (1) **ゲーマーの資産を送信する行為**と (2) **現金を送信する行為**が同時性をもたない取引を行うことは非常に危険なことであり、実際にこれによる事故は頻繁に発生してきました。

このような問題を解決するために、取引当事者の信用を保証し、ゲーマー資産の支払いと現金の支払いを保証する役割をする信頼できる第三者としてアイテム取引仲介所が登場しました[8]。資産取引の安全性は高くなりましたが、仲介所に支払わなければならない高い手数料はそのままゲーマーの負担となっています。

私たちは、この問題を解決するために、ゲーマー資産をブロックチェーン上に保存して移動することができるシステムを考案しています。そして、このようなシステムはブロックチェーン技術の発展を目標としていません。私たちは、現在までブロックチェーンの先駆者たちがみせてくれた意味のある技術的前進を、私たちの目標に合わせて、ゲーム産業に適用することに徹底的に集中します。

現在まで公開された多くのブロックチェーン技術を活用するために多様なプラットフォームについて検討し、次のような問題を確認することができました。

イーサリアム (ETH) プラットフォーム上でトークンやDAppなどの形で実現しているものは、イーサリアムシステムに従属していて機能の拡張に制約がある場合があります。また、取引ごとに発生する高い手数料を耐えなければならず、全世界のすべてのゲーマーが残高を所持したイーサリアム口座を保有しなければならないという点は使用性、接近性の面で非常に大きな問題をもつこととなります。

ビットコインに代表されるプルーフ・オブ・ワーク(Proof-of-Work)方式は、過度なエネルギー浪費と遅い取引確認速度などで、私たちの哲学と目標に合致しない問題点があります。

DASH、EOSなどに代表されるプルーフ・オブ・ステーク(Proof-of-Stake)方式は、後続の参加者の参入障壁が発生し、富の偏りが深刻化する問題などで、すべての開発会社及びゲーマーに公正に参加する機会を提供しようとする私たちの理想に合致しません。

私達は、このような問題認識をもとに、私たちの哲学と目標に合致するBCP(Bryllite Consensus Protocol)合意プロトコルを考案し、これにより私たちの目標を達成していきます。

私たちの目標と未来のゲーム

私たちの目標は「ブロックチェーン技術の発展」のような大げさなものではありません。孤立しているゲーム間の境界を崩して、信頼できるグローバルゲーム資産の統合エコシステムを構築することが究極的なゴールです。

私たちは、このエコシステムを通じて、ゲーマーの資産を安全に保存し、仲介者や手数料なしでも安全な資産取引システムを構築します。また、私たちのシステムはゲームの境界を越えてゲーマーの資産を移動したり、取引することができる機能を提供します。この過程を通じて開発会社に帰属されているゲーマー資産を所有者であるべきゲーマーに返してあげるのです。

私たちを含むほぼすべてのゲーマーは近い未来にVR(仮想現実)基盤のゲームが普遍化することを信じています。AR(増強現実)基盤の「ポケモン・ゴー」ゲームは、空前の大ヒットをなして数多くの垂流作を誕生させました[9]。また、VRとARの利点を取ったMR(融合現実)基盤のゲームも遠くない未来に普遍化されることを容易に予想することができます。

しかし、私達はこのようにゲームのハードウェア的な形態に対する未来を予測しようとしているわけではありません。私たちは、ハードウェア技術の発展とは別途に、「ワールド・オブ・ウォークラフト」で使用されていた私のキャラクターと装備を「グラナドエスパダ」に移してきて使用することができ、今日新規に発売されたVRゲームに私の「オーディション」キャラクターをそのまま移してきて使用することができる未来のゲーム世界を夢見ています。

もちろん、それは現在のレガシー・ゲーム基盤では不可能であり、実現すればゲームの企画段階からブリルライト・プラットフォームに参加することを前提に開発されたゲームが多くなる時のことになるとは思いますが、もしそれが全世界のすべてのゲーマーが望む方向であれば、必ずそうなる私達は信じています。

そのため、現在のレガシー・ゲーム基盤で実現可能な部分から漸進的に構築する作業を黙々と進めていくつもりです。

ブリルライト・プラットフォームの紹介

ブリルライト・プラットフォームはゲーマーの資産を安全に保存して移動することができる機能を提供し、資産取引の同時性を強制して、仲介者がなくても信頼できる取引を可能にさせるプラットフォームです。ゲームサービスの内部DBに保存されていたゲーマーの資産をゲームサービスの外部DB、即ち、ブロックチェーンに保存して、ゲーム間の資産移動が可能になるよう設計されたプラットフォームです。

このような機能の拡張は、レガシー・ゲームシステムとブリルライト・ブロックチェーンをゲームコンテンツレベルで融合するブリルライト・マスターノードとブリルライト・ブリッジサービスを介して可能となります。レガシー・ゲームシステム開発者は、ブリルライト・ブリッジサービスで提供する抽象化されたAPIを利用して、簡単にゲームコンテンツレベルの連動が可能です。

ブリルライトプラットフォームでは、ゲーマーの資産の価値尺度化などのためにブリルライトコイン(BRC)を媒介貨幣として利用し、ブリルライト・プラットフォームと連携されたゲームをプレイするだけでも、誰でも公正で簡単にBRCを獲得することができます。

Features

Decentralized

ゲームサービス提供主体(開発会社、流通会社、サービス会社など)から独立したグローバルゲーマー資産エコシステムを構築し、ゲーマーの資産を安全に守ることができます。

Trustless Game Asset Deal

信頼できる仲介者の存在がなくても安全にゲーム資産を取引することができます。

No Transaction Fee

プラットフォームはBRCの移動及び取引過程でTransaction Feeを要求しません。一般的に、ブロックチェーン上で発生する取引は、DDoS攻撃に対する防御やノード運営目的などで毎取引ごとに一定の手数料を要求しますが、ブリルライト・プラットフォームでは、別途の手数料なしに移動や取引が可能です。

Fastest Transaction

ゲーム資産の移動及び取引速度がどのブロックチェーンより早いです。同じゲームでの取引はすぐに締結され、異種のゲーム

間の取引は、1コンフォームだけで取引が確定されます。

Asset Transfer over Game

異種ゲーム間の資産の移動及び取引が可能です。BRCを含むゲーマーのすべての資産を異種のゲームに移動したり、他のゲーマーと取引することができます。

Smart Contract

プラットフォームは、スマートコントラクト機能を支援し、各開発会社は、この機能を活用して、ゲーマー間の多様な契約形態を支援することができます。例えば、異種ゲーム間のアイテムのオークションや取引システムを実現することができ、紛争の余地のある傭兵システムのようにゲームコンテンツに非定型化された形の多様なゲーマー間の契約にスマートコントラクト機能を活用することができます。開発会社は、スマートコントラクトコードを作成するだけで、既存のゲームシステムの修正なしに完全に新しいゲームコンテンツをリリースすることができるようになります。

Easy to Use

ブリルライトプラットフォームはゲーマーにBRC及びゲーム資産の移動/取引などに関連して追加的な学習を強要しません。ゲーマーは、単にゲームをプレイするだけで、ゲーム画面でBRCが積立されることを確認することができ、同僚にゲームマネーを転送するのと同じ方法でBRCを移動することが可能で、他のゲーマーとアイテムを取引するのと同様の方法で資産を取引することができます。このように簡単な使い方は多くのゲーマーの接近性及び使用性を向上させるのに重要な役割をしましょう。

Device Free

PC Game、Mobile Game、Web Game、Console Gameなどのネットワークが可能な如何なる形のゲームもブリルライトプラットフォームに参加することができ、ゲーマーは保有する端末機の種類に関係なく、誰でもブリルライトプラットフォームに参加することができます。

Open Source

私たちのソースコードはGitHubなどを通じて公開されて開発進捗状況を一目で確認できるようにします。また、誰でも簡単にブリルライトプラットフォームにゲームを連動できるように分かりやすく親切な連動ガイド文書などを提供し、コミュニティを通じたフィードバックに忠実になります。



BRC Specification

ゲーマーはブリルライトプラットフォームに連動されたゲームをプレイするだけでも、ブリルライトコイン(BRC)を獲得することができます。獲得したBRCは、ゲームサービスで提供する有料アイテムなどの購入に使用することができ、他のゲーマーとの資産取引に使用することができます。また、ゲーマーの他のゲーム口座や個人のウォレットに移動することもできます。

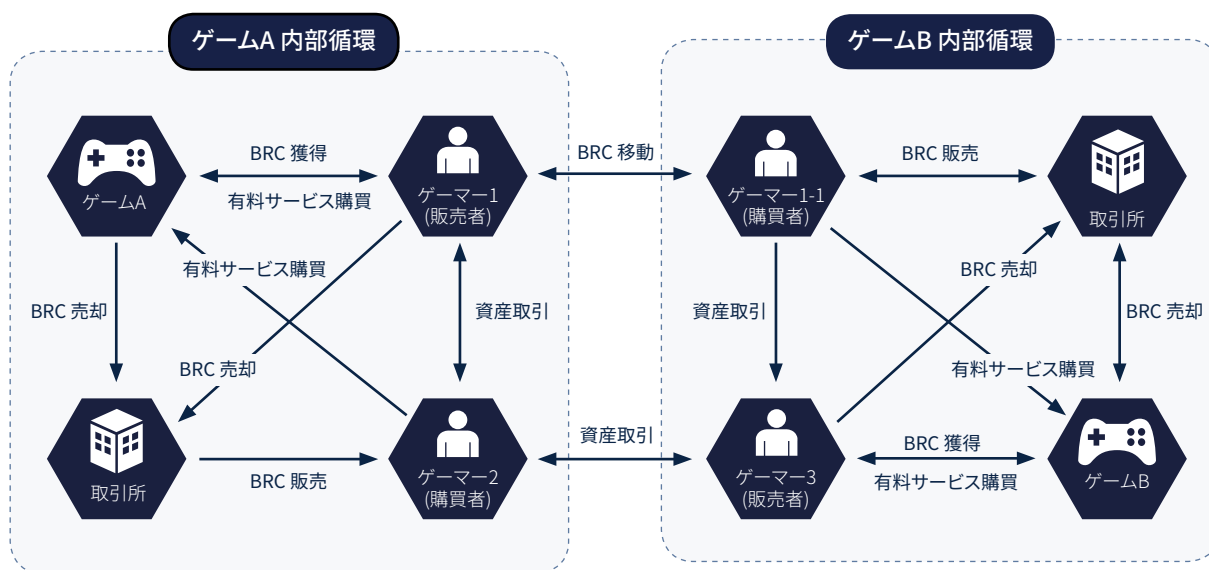
| Bryllite Coin (BRC) 明細票 | | |
|-------------------------|---|---|
| シンボル | BRC | |
| ブロックタイム | 30秒固定 | |
| ブロック補償 | 100 BRC | |
| 半減期 | 約1,000,000ブロックごとに10%ずつ減少。 100 BRC -> 90 BRC -> 80 BRC -> ... -> 20 BRC -> 10 BRC (以後固定) | |
| イベントブロック | 毎日10,000BRCをブロック作りに成功したゲーマーに支給 | |
| BRC 発行量 | 1年 | $\{ 100 \text{ BRC} * (60/30\text{秒}) * 60\text{分} * 24\text{時間} * 365\text{日} \} + (365\text{日} * 10,000 \text{ BRC}) = 108,770,000 \text{ BRC}$ |
| | 2年 | $\{ 90 \text{ BRC} * (60/30\text{秒}) * 60\text{分} * 24\text{時間} * 365\text{日} \} + (365\text{日} * 10,000 \text{ BRC}) = 98,258,000 \text{ BRC}$ |
| | 3年 | $\{ 80 \text{ BRC} * (60/30\text{秒}) * 60\text{分} * 24\text{時間} * 365\text{日} \} + (365\text{日} * 10,000 \text{ BRC}) = 87,746,000 \text{ BRC}$ |
| | (中略) | |
| | 9年 | $\{ 20 \text{ BRC} * (60/30\text{秒}) * 60\text{分} * 24\text{時間} * 365\text{日} \} + (365\text{日} * 10,000 \text{ BRC}) = 24,674,000 \text{ BRC}$ |
| | 10年 | $\{ 10 \text{ BRC} * (60/30\text{秒}) * 60\text{分} * 24\text{時間} * 365\text{日} \} + (365\text{日} * 10,000 \text{ BRC}) = 14,162,000 \text{ BRC}$ |
| | 11年 | $\{ 10 \text{ BRC} * (60/30\text{秒}) * 60\text{分} * 24\text{時間} * 365\text{日} \} + (365\text{日} * 10,000 \text{ BRC}) = 14,162,000 \text{ BRC}$ |
| 備考 | <ul style="list-style-type: none"> - 10年間で約6億BRCが採掘を通じて発行され、以後、毎年約1,400万BRCが持続的に発行 - 採掘過程で開発会社の政策に基づいて0~2%の採掘手数料とコンソーシアム運営費として2%のdevfeeが賦課される | |

[表1] BRC 明細票

現代国家が経済政策などのために発行する名目貨幣(Fiat Currency)と同様に、脱中央化を通じて、別途の発行機関が存在しない暗号通貨(Crypto Currency)の通貨政策もやはり非常に重要な要素であり、私たちは、その重要性を非常に真剣に認識しています。初期に間違っ樹立された通貨政策による、需要に比べて過剰であったり不足する通貨量の供給は貨幣の実質的な価値の下落や流動性不足などの問題を引き起こす可能性があり、暗号通貨の性質上、このような通貨政策を再調整することは技術的な問題を別にしても参加主体間の合意が難しいと予想されるため、容易ではないと思います。

私たちは、BRCのブロックタイムを固定して、毎年発行される通貨量を制限することができ、ブロック補償の半減期適用を通じて全体発行通貨量を一定の規模に制御することができます。全体の発行通貨量は2023年まで約1500億ドル規模と予測されているグローバルゲーム資産市場の需要を基準として設計されました。

BRCの循環構造



[図2] BRC循環構造

BRCの循環過程は、上記[図2]のような形で表現することができ、異種ゲーム間の循環が可能であることを表現しています。

BRCの獲得

ゲーマーはブリルライトプラットフォームと連携されたゲームをプレイするだけでもBRCを獲得することができます。この過程で、開発会社のポリシーに基づいて、単純参加者よりゲームの寄与度/達成度が高いゲーマーにより多くの補償を提供するか、活動していない単純な接続者に補償を制限することができます。また、開発会社は、独自のポリシーに基づいて採掘手数料名目で0~2%のBRCを獲得することができます。

BRCの使用先及び資産価値保存の媒介手段

獲得したBRCは、ゲームサービスで提供する有料コンテンツの購入に使用することができ、この取引で発生したBRCの所有権は開発会社に帰属します。開発会社は、獲得したBRCを取引所などを通じて売却して利益を得ることができます。BRCは、ゲーム内で現金と同じ価値を持ちますので、ゲーマー資産を安全に保存することができる優れた手段になります。

BRCの資産価値移動機能及び取引媒介手段

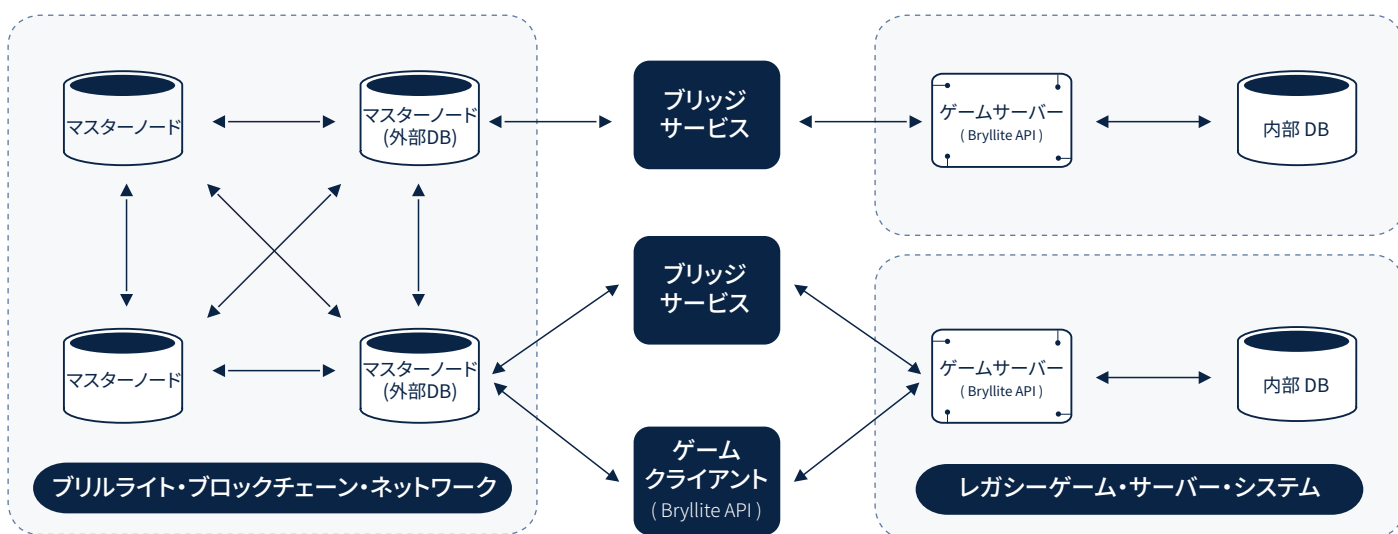
BRCは、ゲーマー間の資産取引の媒介手段として使用することができます。ゲームシステムが提供する取引システム(取引ウ

インドウなど)を利用して、仲介者や手数料なしに信頼できて即時的な資産の取引が可能です。それだけではなく、他のゲームの私の口座や友人の口座、個人ウォレット、取引所など、どこにでもBRCを迅速かつ安全に送金することができます。このプロセスを通じてブリルライトプラットフォームに参加しているすべてのゲームの巨大なデジタルゲーム資産のエコシステムが構築されます。

BRCの購買及び販売

ゲーマーは誰もゲームプレイを通じてBRCを獲得することができますが、時間が資産である現代人タイプの多くのゲーマーは喜んで自分の時間の代わりに金銭を投資してゲームを楽しみたいと願い、また他のゲーマーは、自分のBRCを売却して収益を得ようとすると思います。ゲーマーのこれらの要求は、BRC取引所を通じて満たされることができます。binance、bittrex、poloniexなどのような既存の暗号通貨取引所にBRCを上場することを含め、信頼できて、且つ、安定的な独自の暗号通貨取引所をオープンしてサービスし、取引所サービスはブリルライトプロジェクトとは別途の関連会社を通じて進行されています。

プラットフォーム構造図



[図3] ブリルライトプラットフォーム構造図

ブリルライトプラットフォームは、基本的に[図3]のような形で構成することができます。ブリルライトマスターノードで構成されたブリルライトブロックチェーンネットワークをブリルライトブリッジサービスを利用して、レガシーゲームサーバーシステムと連動する形です。

ブリルライトマスターノードは、ゲーマーのProof of Participationの委任を受け、Concurrent User数に比例してBRCを採掘(ブロック生成)してブロックチェーンを維持し、レガシーゲームシステムの外部DBとして機能します。

ブリルライトブリッジサービスは、レガシーゲームシステムとブリルライトブロックチェーンネットワーク間の連結を担当し、双方向の通信を可能にさせます。これは、レガシーゲームシステムでブロックチェーン上にトランザクションを発生させるだけでなく、異種ゲームで発生したトランザクションなどをブリッジサービスが感知して、ゲームサーバーにイベントの形 (Event-Driven) で即時的な通知が可能であることを意味します。

キプロスネットワーク(Cyprus Network): Federated Local BlockChain

ビットコイン、イーサリアムなどの多くのブロックチェーンネットワークは、慢性的なスケーリング問題に苦しんでおり、シャディン技法やライトニングネットワーク、レイドウンネットワーク、プラズマなどのような多様なオフチェーン処理方式を導入するなど、問題の解決に没頭しています[10]。このようなオフチェーン技術の本質は、ステートチャンネルなどを利用してブロックチェーンの外で多くの取引を処理し、その取引の結果だけをメインチェーンに反映する取引内訳の簡素化形態に要約することができます。ブリルライトプラットフォームは、このようなオフチェーンモデルからインスピレーションを受けて考案されたキプロスネットワークを適用してスケーリング問題を解決することができます。

ブリルライトプラットフォームでのトランザクションは、同じゲーム内部で発生するIn-Game Transaction (Internal Game Transaction) と異種ゲーム間で発生するEx-Game Transaction (External Game Transaction) の2つに大きく区分することができます。

ゲームの性質上、対面した相手との直接的な取引画面等を通じて行われる資産の取引、すなわち、In-Game Transactionは即座に締結され、資産の移動が同時性をもって発生しなければならない必要があります。In-Game Transactionはオフチェーン技術であるキプロスネットワークを利用してすぐ処理し、キプロスネットワークはブリルライトコンソーシアムにより事前に決定された、いくつかのゲームの連合で構成されます。例えば、1000個のゲームがプラットフォームに参加している場合には、必要に応じて、4~5つのゲームで構成されている約200余りのキプロスネットワークを構築することができます。

全体の資産取引の相当部分を占めるものと予想されるIn-Game Transactionをキプロスネットワークを利用して処理することで、ブロックチェーンネットワークのスケーリング問題を解決することができ、ゲームというジャンルの特性が要求する即時的な取引の締結が可能となります。

Ex-Game Transactionは異種ゲーム間の資産移動及び取引が主な目的で、取引の即時的な締結および資産移動を必要としない取引であり、キプロスのネットワークを経由せずに、メインチェーンに直接記録されます。この取引は、1コンフォームで取引が確定されるので、即時的ではありませんが、比較的早い時間内に取引の処理が可能です。

Synchronized Transaction

ブリルライトプラットフォームで資産の取引は、同時性を強制し、仲介者なしでも信頼できる取引ができるように設計されました。レガシーアイテムを含むゲームの資産取引は、各ゲームが提供する取引システムを利用して、資産のatomic swapができるようにします。ゲームで提供される取引画面を通じて二人の取引当事者がすべての取引を承認する場合にのみ、取引が成立され、この取引はIn-Game Transactionであり、締結後すぐ資産の移動が行われます。

レガシーアイテムとBRCの取引を締結する場合、(1) ゲームサーバーからブリッジサービスにBRCの移動を要求します。(2) 要求に対して成功応答を確認した後、レガシーアイテムを取引相手のインベントリに移動処理します。(3) もし要求に対して失敗応答または一定期間成功応答が確認されない場合に取引は失敗に処理され、両方のユーザーの取引画面にはエラーメッセージと一緒に取引失敗を出力します。

Benefit to Gamers

ゲームのBRC獲得

ゲームは複雑なプロセスがなければ、ただのゲームをプレイするだけでも、BRCを獲得することができます。BRCは、ゲームサービスで提供する有料サービスの利用に使用が可能であり、他のゲームとゲーム資産の取引に活用できます。また、BRCを取引所などに売却して利益を得ることができます。

異種ゲーム間の資産移動及び取引可能

ゲームはBRCを利用して、異種ゲーム間の資産移動および取引が可能となり、これはゲームをやめたり、ゲームサービスが終了される場合にも、自分の資産を安全に保管できることを意味します。ブリルライトプラットフォームが提供するオークションシステムを利用して取引対象者を手配し、価格を交渉しなければならない煩わしさから逃れることができます。

ゲーム従属から解放

ゲームは通常一時点に一、二種類のゲームだけをプレイします。限られた時間と資源を割愛しなければならないゲームの特性上、様々なゲームを同時に進行することは容易ではありません。ゲームをやめてしまうと、投入した時間と資源をそのまま失うので、プレイするゲームを選ぶ作業から慎重なアプローチを要し、進入したゲームで簡単に抜け出すのが難しくなります。私たちは、これをゲームの「ゲーム従属現象」と呼びます。ブリルライトプラットフォームはゲーム資産をゲームに返してあげて、他のゲームに簡単に移行することができる環境を構築し、ゲームに従属しているゲームを解放してあげます。

イベントブロック補償を通じた収益の極大化

ブリルライトプラットフォームは毎日に該当するブロックをイベントブロックに指定し、そのブロックを見つけることに成功した

ゲーマーに10,000 BRCを支給します。ゲーマーは、ゲームを楽しむだけで毎日宝くじに応募するのと同じであり、当選する幸運を得れば多くの補償と特典を得ることができます。

Benefit to Developers

マーケティング効果の引上げ及びゲームの活性化

ゲームプレイを通じて価値の安定性が確認されるBRCを獲得することができますので、マーケティング効果が爆発的に増加し、多数の新規ゲーマー誘致と休眠アカウントの活性化が可能になり、このようなゲームの活性化は当然、開発会社の売上高の上昇に直結することができます。また、定期的が発生されるイベントブロックは、新しいピークタイムを形成し、開発会社で施行しようとするマーケティングの効率を極大化させることができるようになります。

市場のボリューム拡大による売上高の増加

開発会社はゲーマーのゲームプレイによる採掘補償の一定量を手数料(0-2%)として徴収することができ、コミュニティサービスやオークションサービスなどのようなブリルライトプラットフォームサービス利用料としてBRCを獲得することができます。また、ゲームサービスで有料サービスをゲーマーに提供し、ゲーマーに支給されたBRCを回収することができます。このように獲得したBRCは取引所を通じて売却して売上に連結することができます。ゲーマーの立場からは、一つのゲームで購入した資産を他のゲームに簡単に移動することができますので、有料サービス購入の参入障壁が著しく低くなり、これは全体のゲーム資産市場のパイを育て、開発会社の追加利益の実現に肯定的な効果をもたらします。

連動開発費の支援

初期に参加が決定される開発会社から開始して、ブリルライトICOを介して投資を受けた資金をブリルライトプラットフォーム連動開発費として支援を受けることができます。名目貨幣、BTC、ETH、BRCなどの形で支援が可能であり、開発会社のプラットフォーム参加への負担を大幅に減らすことができます。また、初期の開発資金の確保にも大きな助けになります。1人創業者のような形の開発者にサーバーホスティング費用を支援することもできます。

ゲームコンテンツ開発に集中

すべてのゲーム資産をブリルライトプラットフォームを利用して開発することになる場合、会員管理、アカウント管理、アイテム管理などの多くの管理業務から解放されることができ、ゲームコンテンツの開発により集中できるようになります。

新規ゲームの進入障壁の緩和

ゲーマーのゲーム従属現象により、新規ゲームがぶつかる高い参入障壁はブリルライトプラットフォームに参加することで緩和されます。プラットフォーム参加ゲーマーの誰でも簡単に新規ゲームに触れることができる機会を提供することになるので、新規ゲームのマーケティング費用を大幅に下げ、ゲーム性に優れたゲームが簡単に市場に定着することができる機会を提供します。

開発会社の評判管理

ブリルライトプラットフォームが追求するグローバルゲーム資産のエコシステムに参加することで、ゲーム資産のゲーマー返還、ゲーム間の自由な移動を可能にする次世代ゲーム開発会社のイメージを構築することができ、これは全世界のゲーマーの高い信頼につながり、発売されるゲームタイトルの成功に大きな助けになります。

多数のコイン実使用者の確保が可能

ブリルライトプラットフォームが他の一般的な暗号通貨やゲーム関連暗号通貨と示す多くの違いの一つは、圧倒的多数のBRC実使用者を確保することができるという点です。多くの暗号通貨がICOを介して暗号通貨使用者を確保していますが、ICOを介して参加する使用者数は限りがあり、それも投資収益を得るための取引所取引を除けば、暗号通貨を対人取引に使用する実際の使用者は極めて微々か全くないといえます。

ブリルライトプラットフォームは、すでに累積加入者10億人に達するグローバルゲーム会社と提携(MOU)を締結しており、参加したゲームのすべてのゲーマーをBRCの実使用者として確保することが可能なほぼ唯一のプラットフォームになるでしょう。

Consortium BlockChain

ブリルライトプラットフォームは、グローバルゲームサービス主体(開発会社/流通社/サービス社など)で構成されたコンソーシアムブロックチェーンです。コンソーシアムブロックチェーンは、ビットコインやイーサリアムのように、誰でもネットワークに参加できるパブリックブロックチェーンや、一つの閉鎖された組織内で特定の目的のために使用されるプライベートブロックチェーンとは、その性格を異にし、リップル(XRP)のように許可された複数の組織がコンソーシアムを構成し、ネットワークに参加する形と定義することができます。

そして、我々はリップルのようなコンソーシアムブロックチェーンが熱烈なブロックチェーン信奉者たちから非難されたり攻撃されるのを目撃してきており、その非難と攻撃の主な内容は、「真のブロックチェーンの技術ということができない」とか「多数のユーザーの確保が難しく、持続可能性が落ちるブロックチェーン技術」または「中央化された組織や機関の専横を防ぐことができない」ということでした。

もう一度言いますが、私たちの目標は、「ブロックチェーン技術そのものの向上」や「グローバル単一通貨の出現」などにありません。私たちは、孤立している各ゲームの境界を崩してグローバル単一ゲーム資産のエコシステムを構築することが最終的なゴールだと思います。もし、我々がパブリックブロックチェーンを標榜して、ゲームとは全く無関係な悪意的になれるノードの

参加を許可しなければならないのであれば、果たしてそれが私たちの目標達成にどのように役立つのでしょうか？

ブリルライトプラットフォームは、10億人に達する実ユーザーを確保することができ、また、今後、より多くの実ユーザーを確保することができます。つまり、現在の基準でパブリックとは単語に概念的な誇張を加えた場合、いくつかのパブリックブロックチェーンよりも多くの実ユーザーを確保した、真のパブリックブロックチェーンとまで言えるかもしれません。

ブリルライトプラットフォームに参加しようとする開発会社は、会社の大きさや開発履歴などに関係なく、大規模開発会社、流通会社から個人の開発者に至るまで、誰でも参加することができます。ブリルライトコンソーシアムは、プラットフォームの運営と維持のための目的で存在し、プラットフォーム参加許可などのようなプラットフォーム政策意思決定をする組織ではありません。プラットフォームに関する政策意思決定は、参加しているゲーマーの自律投票 (ONE GAMER ONE VOTE) によって決定され、ブリルライトコンソーシアムは、ゲーマーの自律投票結果を遵守する義務をもつことになります。



ブリルライト合意プロトコル (BCP: Bryllite Consensus Protocol)

補償が存在するブロックチェーン技術で最も重要なノード間合意アルゴリズムは、本質的に、ブロック作成権限、即ち、ブロック補償を誰が持つのかについて合意するプロセスです。

プルーフ・オブ・ワーク方式は、演算力競争で勝利したノードがブロックを作成する権限を持つことになり、これは過度なエネルギー消費競争につながって社会的に大きな副作用を生んでおり、部分的な分岐発生により即時的な取引締結の確認が困難な問題に直面しています。

プルーフ・オブ・ステーク方式は、持分保有量競争で勝利したノードがブロックを作成する権限を持つことになり、このような持分競争は、後続の参加者に参入障壁として作用し、富の偏りが深刻化されて、最終的には、暗号通貨使用者をすべて失う問題に到達するかもしれません。

私たちは、過度な競争は、何らかの形で副作用が現れると信じており、そのため、ノード間の合意における競争の激化要素を完全に削除するか、最小限に抑えることだけが、ほぼ唯一の解決策だと考えています。可能であれば競争の激化要素がないじゃんけんゲームで勝者を決定して合意したほうが良いと思っています。

ブリルライト合意プロトコルは、競争を激化させる要素を排除し、プルーフ・オブ・パーティシペーションを通じて、比較的簡単な方法で、ノード間の合意に至ることができるように設計されました。

合意プロトコル達成目標 (Consensus Protocol Achivement Goal)

ONE GAMER ONE VOTE

システム資源の割り当てや保有持分量などに関係なく、参加したすべてのゲーマーは、公平な権限を持ち、同時接続者数に比例してブロックを作成する権限を持つように合意する必要があります。

一時的な部分フォークの非許容

一時的な部分フォークを許容せず、1コンフォームだけで即座に取引の確定が可能でなければなりません。

Device Free

PC Game、Mobile Game、Tablet Game、Web Game、Console Gameなどのすべての種類の端末での参加が可能でなければなりません。これは合意過程で不必要な演算を除去してはじめて可能となります。

No Transaction Fee

BRCの移動及び取引過程で手数料が発生しないようにしなければなりません。これは、ノードのブロック生成段階で、トランザクションを故意に欠落させても利益がなく、できるだけ多くのトランザクションを含めることが利益的な状況を作ることで可能となります。また、悪意的な目的で不必要に過度なトランザクションを発生させるユーザーに対して適切な制限とペナルティを課す必要があります。

障害が発生したノードが存在しても合意可能

一部のノードでシステムダウン、ネットワーク断絶などの障害が発生した場合や誤作動が発生した場合にも参加しているすべてのノードは、同じ一つのブロックで合意が可能でなければなりません。

非可逆的ブロック生成

ブロックチェーンネットワークの多数が合意して生成されたブロックは、いかなる場合にも戻したりブロックの内容を変更することが不可能でなければなりません。これは一時的な部分フォークを許可しないのと同じ脈絡です。

プルーフ・オブ・パーティシペーション

ゲーム参加に対する証明が可能でなければならず、これにより、多重アカウント作成攻撃 (Sybil Attack) に対する防御が可能です。参加ゲーマーの数に比例してブロックを作成する権限を持つように合意する必要があります。

プルーフ・オブ・パーティシペーション (Proof of Participation)

私たちがプルーフ・オブ・パーティシペーションを通じて実現しようとするものは、ゲーマーがゲームをプレイする間に端末の性能に影響を与えずに、できるだけ多くの参加ゲーマーに公正にBRCを採掘できるようにするものであり、これは、ノードに参加したゲーマーの数に比例してブロック作成権限を持つようにする形で実現されます。

| | 同時接続者 | ブロック生成確立 | ブロック補償 | ゲーマーのブロック当りBRC獲得の期待値 |
|-------|----------|----------|---------|---|
| A ゲーム | 50,000 人 | 50% | 100 BRC | $(100 \text{ BRC} * 50\%) / 50,000 \text{ 名} = 0.001 \text{ BRC}$ |
| B ゲーム | 30,000 人 | 30% | 100 BRC | $(100 \text{ BRC} * 30\%) / 30,000 \text{ 名} = 0.001 \text{ BRC}$ |
| C ゲーム | 20,000 人 | 20% | 100 BRC | $(100 \text{ BRC} * 20\%) / 20,000 \text{ 名} = 0.001 \text{ BRC}$ |

[表2] ゲーマーのブロック当りBRC獲得の期待値

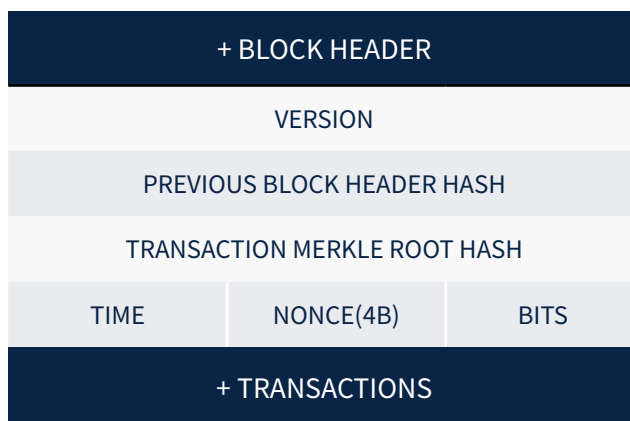
例えば、それぞれ5万人、3万人、2万人の同時接続者を保有しているゲームがあると仮定してみます。この場合、それぞれのゲームが50%、30%、20%の確率でブロック作成補償が支払われると仮定することができます。5万人の同時接続者を保有しているAゲームで参加することが確率的に有利であると考えられますが、[表2]で示すように、それぞれのゲームに参加しているゲーマーのブロックごとのBRC獲得の期待値は0.001 BRCで同じです。私たちは、このような方式の分配がゲーマーに最も合理的かつ公正な方法だと考えています。

Proof of Participationは、ゲームサーバーを介して受信したブロックヘッダにゲーマーがデジタル署名を行う過程で表現されます。したがって、我々は、ゲームプレイに影響を与えることなく、ゲーム参加を証明することができ、参加したすべてのゲーマーに公正にBRCを獲得できる機会を提供することができます。

ブリルライトブロックヘッダとProof of Participation過程

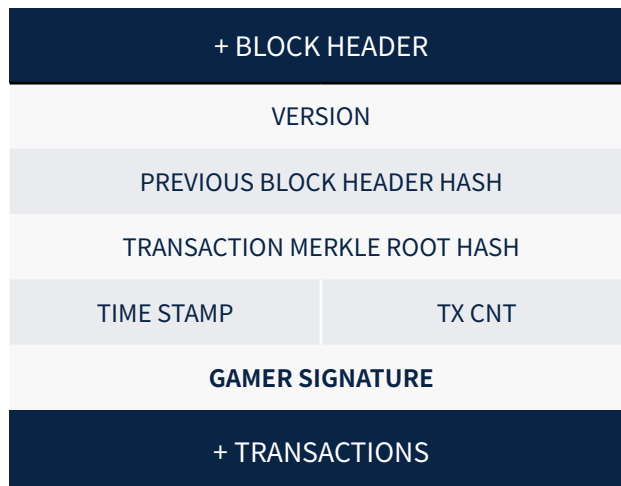
下記の[表3]は、ビットコインで使用されるブロックヘッダを抽象化して図式的に表現した様子です。採掘ノードは、このブロックに含めるトランザクションを整理してモクルツリーを構成し、4バイトのNONCE値を0から約43億まで増加させながら目標の難易度(BITS)を満足する結果値を見つけるまで、ブロックヘッダをSHA256関数でハッシュします。

4バイトのNONCE値は現在の機器の性能や目標の難易度に比べて非常に不足するので、TIME STAMP値を変更したり、トランザクションリストの順序を変更してモクルツリーハッシュ値に変更を与えた後、目標の難易度を満足する結果値を見つけるまで、ブロックヘッダをハッシュする演算を無限反復することになります[11]。



[表3] ビットコインブロックヘッダ構造

私たちは、このような消耗的な演算過程が、私たちの目標を達成するのに何の助けにならないだけでなく、ゲーマーのゲー



[表4] ブリルライトブロックヘッダ構造

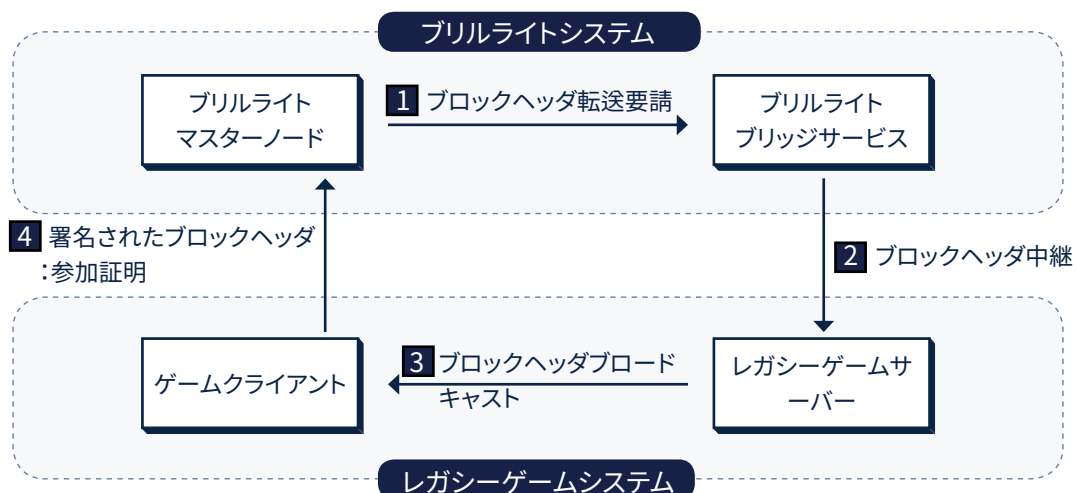
ムプレイに大きな支障をきたすことがあるという点を指摘したいです。

[表4]は、ブリルライトプラットフォームで使用されるブロックヘッダを抽象化して図式で表現した様子です。ビットコインブロックヘッダと比較するとNONCE、BITS項目が除外され、TX CNT (トランザクション数)、GAMER SIGNATURE (ゲーマー署名)の項目が追加されました。ゲーマー署名項目には、ゲーマーの公開鍵(ゲーマー口座)と署名が含まれます。

ブリルライトマスターノードは、このブロックに含めるトランザクションを整理してモジュールを構成し、ゲーマー署名項目を除いたブロックヘッダを完成し、ブリッジサービスを経て、レガシーゲームシステムに送信します。

レガシーゲームシステムは、接続されているすべてのゲームのクライアントにブロックヘッダをブロードキャストします。ゲームクライアントは、このブロックヘッダに自分の秘密鍵で署名したブロックヘッダを最終完成し、ブリルライトマスターノードに転送して参加を証明します。

下記の[図4]は、このような過程を順次的に表現しています。



[図4] ゲーマー署名を利用したブルーフ・オブ・パーティシペーション過程

マスターノードは、自分の数多くのゲーマーから送信を受けた署名されたブロックヘッダの中でハッシュ結果値が最も小さいブロック1個を採択して、他のノードとの合意過程に使用する準備をします。もしブロックヘッダのハッシュ結果値が同じのブロックが存在する場合、GAMER公開鍵の値を特殊演算して1つのブロックを選択します。

それでは他のゲームのノードとじゃんけんゲームをする準備が整いました。

実用的ビザンチン障害許容とブリルライト合意プロトコル (Practical Byzantine Fault Tolerance & Bryllite consensus Protocol)

ビザンチン障害許容 (Byzantine Fault Tolerance) アルゴリズムは伝統的なビザンチン将軍問題を解決するためのアルゴリズムであります[12]。

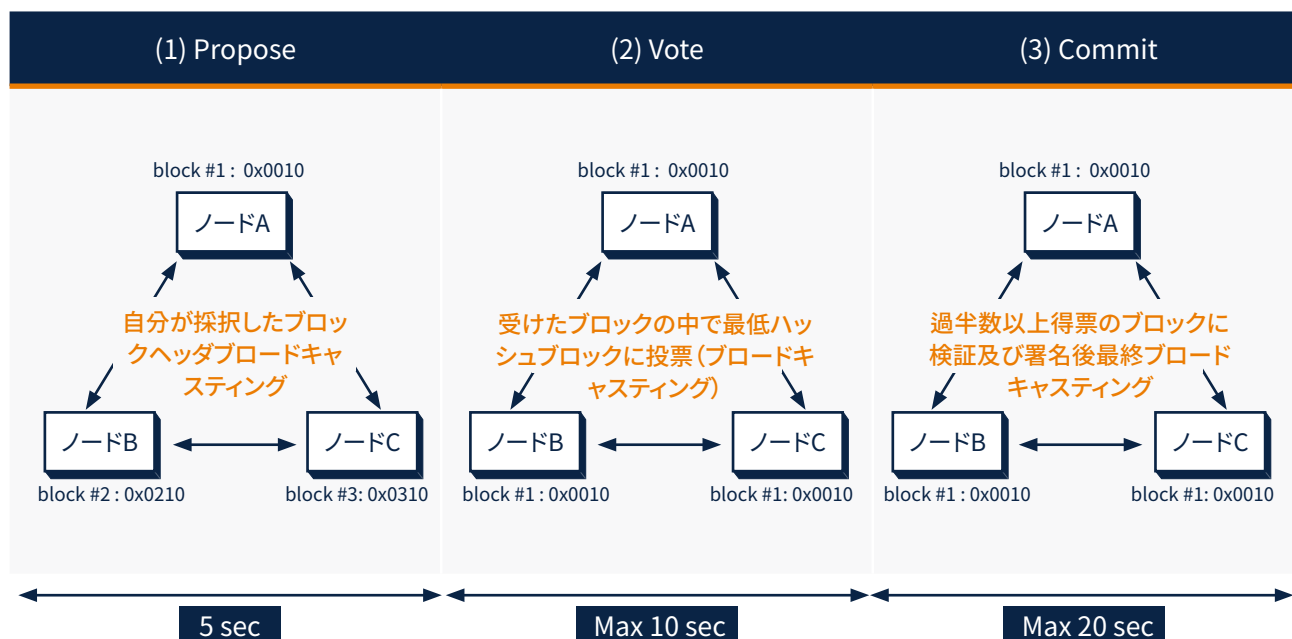
「ビザンチン将軍問題はレスリー・ランポートとショースターク、ピースが共著した1982年の論文で初めて言及された。この論文で、著者らは敵の都市を攻撃しようとするビザンチン帝国軍のいくつかの部隊が、地理的に離れた状態で、各部隊の指揮官が(途中で捕まるかもしれない)メッセンジャーを介して交信しながら攻撃計画を一緒に立てる状況を想定している。この部隊の指揮官の中の一部には裏切り者が混ざり込んでいる可能性があり、裏切り者はルールを忠実に従う忠実な指揮官とは異なり、ルールにとらわれず自由に行動することができる。この時に裏切り者の存在にもかかわらず、忠実な指揮官が同じ攻撃計画を立てるためには、忠実な指揮官の数がどのくらい必要であり、この指揮官がどのような規則に沿って交信しなければならないかに対する問題がビザンチン将軍問題だ。」

- https://ko.wikipedia.org/wiki/비잔티움_장애_허용, ビザンチン将軍問題

プルーフ・オブ・ワークとプルーフ・オブ・ステーク方式は、すべてビザンチン将軍問題を解決するための証明方法であり、それぞれの目標に合わせて、比較的に動作しているということが出来ますが、私たちの哲学と目標に符合しないため、「実用的ビザンチン障害許容」モデルをベースとして実現するブリルライト合意プロトコルを介して、ビザンチン将軍問題を解決していきたいと思います。私たちが借用したい実用的ビザンチン障害許容モデルはMIT Computer ScienceのMiguel CastroとBarbara Liskovによって考案されたアルゴリズムであります[13]。

ブリルライト合意プロトコルの基本的なコンセプトは、実用的ビザンチン障害許容モデルのように参加しているノードが3回のブロードキャストを通じてビザンチンノードや誤作動しているノードが存在しても過半数を超えている正常なノードが動作している場合、最終的に同じ一つの正常なブロックに合意することができることを保証するという事です。

それでは、プルーフ・オブ・パーティシペーションを通じて採択したブロックを利用して、じゃんけんゲームを進行してみましょう。



[図5] ブリルライト合意プロトコル動作方式

[図5]は、(1)提案(Propose)、(2)投票(Vote)、(3)決定(Commit)の3段階で構成されたブリルライト合意過程を表現したものです。各段階は、一定の待機時間が存在し、待機時間を超過して送信されるパケットは無効として処理されます。合意の過程では、約100バイト内外のブロックヘッダのみを送信して合意を試み、Commit段階で取引内訳が含まれた最終ブロック情報を共有することになります。参加しているすべてのノードは、最終ブロック情報を受信した後、ブロックを検証することになります。もし、この段階での検証に失敗した場合、今回のブロックの合意は無効化され、そのブロックを提案したノードにペナルティを課すこととなります。

(1) Propose Step

提案段階では、それぞれのノードがゲーマーのプルーフ・オブ・パーティシペーションを通じて採択したブロック候補を他のノードにブロードキャストして提案することになります。[図2]の(1) Propose段階で、ノードA、B、Cはそれぞれ0x0010、0x0210、0x0310のハッシュ結果値を持つブロックヘッダを候補として選定して参加しているすべてのノードに伝播します。それぞれのノードは、待機時間が終了する時点で、ブロックヘッダのハッシュ結果値が最も小さいブロック一つを再度選択します。

もし、この時、ブロックヘッダのハッシュ結果値が同一のブロックが存在する場合、(1) TX CNTの値が大きいか、(2) TIME STAMPの値が速いか、(3) GAMER公開鍵の特殊演算を介して一つのブロックを採択します。提案段階が終了した時点で、ほとんどのノードが同じブロック候補を選択するようになります。

(2) Vote Step

投票段階は、提案段階を経て再度選択した一つのブロックについて多数決を通じて確認する過程です。[図2]の(2)Vote段階で、それぞれのノードがハッシュ結果値が最も小さいblock#1:0x0010のブロックを選択していることを知ることができます。

投票段階で、各ノードは、自身が保有しているハッシュ結果値が最も小さいブロックを参加しているすべてのノードに伝播して、参加ノードの1/2を超える同意を得たブロックを最終的に選定することになります。この過程で、当該ブロックを提案したノードは、自分のブロックに投票したノードにブロックの取引内訳を含む全体のブロックデータを転送することができます。

もし、1/2を超える同意を得たブロックが存在しない場合、今回のラウンドは無効化され、新しいラウンドを開始します。

(3) Commit Step

決定段階は、投票段階を通じて選定したブロックを検証してブロックチェーンに連結するブロックを最終的に決定する過程です。投票段階を経て、当該ブロックを提案したノードと当該ブロックに投票したノードは、取引内訳を含む全体のブロックデータを持っています。決定段階では、ブロック全体のデータを保有しているノードが保有していないノードにブロックデータを伝播して、すべてのノードがこのブロックの無欠性を検証します。

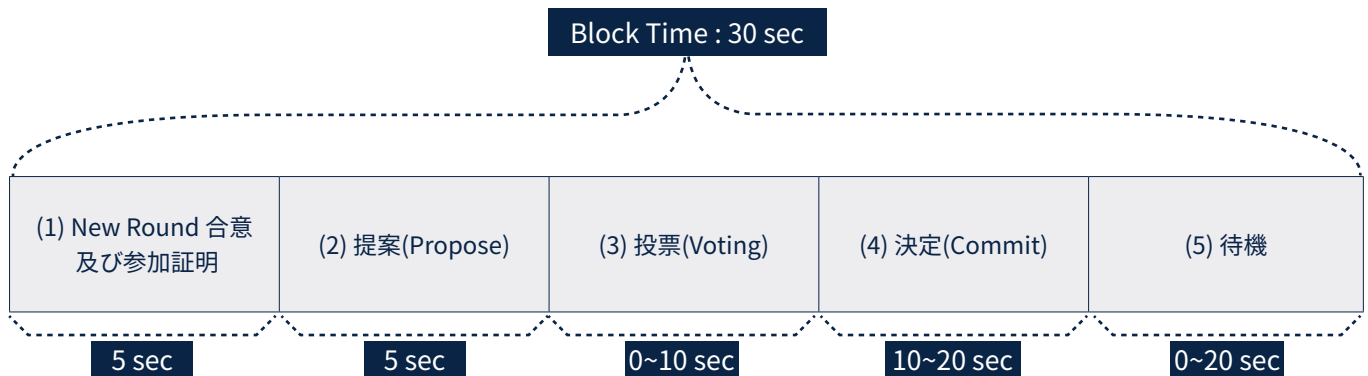
ブロックの無欠性が確認される場合、検証者ノードの署名を含めたブロックヘッダを参加しているすべてのノードに伝播します。この過程で、参加しているノードの1/2を超えて検証が確認されたブロックは最終的にブロックチェーンに登録され、この時点から取引内訳の確定が可能となります。

もし、当該ブロックの無欠性の検証が失敗した場合、今回のブロックの合意は無効化され、当該ブロックを提案したノードは、一定期間の参加を制限されるなどのペナルティが課せられます。

ブリルライト合意プロトコルは提案、投票、決定の3つのステップを経て、1/2を超えるノードが正常に動作する限り参加しているすべてのノードは、常に同一のブロックを合意の下で保持することができようになり、このブロックの内容は、非可逆的であり、偽造/変造が不可能になります。

ブリルライト合意プロトコルの全般的な流れ

ブリルライト合意プロトコルは、大きくプルーフ・オブ・パーティシペーションと合意過程の二つに構成され、合意過程は提案、投票、決定の3段階で構成されています。下記の[図3]は、新しいブロック生成の開始段階から最終的にブロック生成が完了するまでの過程を所要時間とともに表現しています。



[図6] ブリルライト合意プロトコルの全般的な過程

プルーフ・オブ・パーティシペーション段階には、マスターノード間の新しいブロック生成が開始されることを合意する過程が含まれています。以前のブロックの生成を完了したか、以前のブロックの合意に失敗して無効化された場合、ノードは、新しいブロックの開始をブロードキャストして1/2を超えるブロック開始メッセージを受信した時点から新しいブロックを作成 (New Round) が開始され、以後、プルーフ・オブ・パーティシペーションを通じてゲーマーから完成されたブロックヘッダ情報を収集します。このプロセスは、5秒の義務待機時間を持ち、New Round合意にかかった時間が含まれます。制限時間を超えて受信されるゲーマーのブロックヘッダ情報は破棄され、当該ゲーマーは今回のブロック生成の参加に含まれません。

提案段階では、ノードがゲーマーから収集したブロックヘッダの中のハッシュ値が最も小さいブロックヘッダを一つ選択して、参加しているすべてのノードにブロードキャストします。この過程も5秒の義務待機時間を持ち、制限時間を超えて受信されるブロックヘッダ情報は破棄されます。

投票の段階では、提案段階から受信したブロックヘッダの中でハッシュ値が最も小さいブロックヘッダに投票し、そのブロックヘッダをネットワークにブロードキャストする形で行われます。特定のブロックヘッダが1/2を超える得票をした時点で投票段階は終了して決定段階に進むことができます。このプロセスは、最大10秒の制限時間があり、10秒以内に1/2を超えて得票したブロックがない場合、今回のラウンドは、合意失敗とみなされ、再びブロックの作成を開始します。

決定段階は、投票段階で選択したブロックの検証段階であり、投票段階の所要時間に応じて、最大20秒の制限時間が与えられます。もし、投票段階で1秒がかかったのであれば決定段階は、19秒の制限時間を持つようになり、10秒がかかった場合、10秒の制限時間を持つようになります。制限時間内に過半数を超える検証完了メッセージを受けないことができれば、今回

のラウンドは合意失敗とみなされ、再びブロック生成段階を開始します。

決定段階で制限時間内にブロック作成合意に成功しても、次のラウンドをすぐに開始せずに、30秒のブロックタイムまで待機した後、次のラウンドを開始することができます。もし、投票段階で1秒をつかい、決定段階で5秒を使った場合、最終ブロックタイム30秒まで、約14秒を待機した後、次のラウンドの開始を合意することができます。このプロセスによって、ブロックタイムは常に30秒に固定されるようになります。

Well-Known Block Chain Issue

51% Attack & Double Spending Issue

51%攻撃は、ネットワークの50%を超えるハッシュパワーや持分を保有するノードが二重支出を誘発させてブロックチェーンの信頼を崩壊させ、ブロックチェーンネットワークそのものを破壊することもできる攻撃です。プルーフ・オブ・ワーク方式とプルーフ・オブ・ステーク方式は、すべて50%を超える能力をネットワークを崩壊させるのに使用しないという弱い信仰に基づいていますが、先に述べた複数の外部環境要因などにより、発生可能性が完全に排除されるわけではありません。

私たちは、ブリルライト合意プロトコルを介して、一時的部分フォークを許可しない非可逆的ブロック生成に合意して、二重支出問題を根本的に排除することができます。これは、特定のゲームが50%を超えるゲーマーを確保する場合にも、ブロックチェーンネットワークを依然として信頼できることを意味します。

Sybil Attack

ビットコインは「ONE CPU ONE VOTE」というコンセプトでスタートしたが、現実的には、ASICデバイスの普遍化のため目的の達成が困難なつと見なければなりません。私たちは、ブリルライトプラットフォームを介して「ONE GAMER ONE VOTE」という私たちの哲学を貫きたいと思います。

ブリルライトプラットフォームでブロック補償は、多数の同時接続ゲーマーを確保したゲームに高い確率で提供されます。ゲーマーは虚偽のアカウントを大量に生成するなどの方法でブロック作成補償を非正常的に獲得しようとする形のアビューズ誘惑を強く感じることができます。

このような多重アカウント攻撃は、ゲームへのプルーフ・オブ・パーティシペーションを通じて解決され、ゲームの性質上、今後発生する可能性のある様々な形態のSybil Attackに対してもプルーフ・オブ・パーティシペーション方法をより改善、補完して、

持続的な技術的対応が可能です。これはコンソーシアムブロックチェーンが持つ長所であり、プラットフォームの維持に必要であると判断される場合、コンソーシアムの政策的な介入でも問題を解決できる場合があります。

私たちは、なるべくこのような攻撃などから自由になれるように、善意が確認されている開発会社を対象に提携の努力を注ぐつもりです。

DDoS Attack

BRCの取引と移動過程には手数料がないので、ブリルライトネットワークを麻痺させる目的などで大量のトランザクションを発生させる攻撃に備えなければなりません。ブリルライトプラットフォームは、各ゲーマーの口座に対して一つのブロックに含まれるトランザクションの数に適切な制限を置くつもりであり、制限を超えて、悪意的なトランザクションの発生が感知された場合には、当該口座はネットワークから排除されて所有しているBRCは没収されます。

Nothing at Stake Issue

多重アカウント攻撃やDDoS攻撃を敢行するなど、悪意的な行為はブリルライトプラットフォームで感知することができ、このような行為の主体に対してブロックチェーンネットワーク排除とBRC没収など強力な制裁を通じて悪意的な行為を根本的に排除します。



Bryllite Platform Service : “Beyond the Game Boundaries”

ブリルライトプラットフォームを介してゲーム間の境界があいまいになって、すべてのゲームが信頼して共有することができる1つの外部DBを構築することによって、私たちが想像できるよりも多くの新しいサービスが可能になります。ブリルライトプラットフォームが成熟される過程で、我々は全世界のすべてのゲーマーと開発会社などから提案される、斬新で優れたアイデアを持続的に議論して発展させていくことができるでしょう。

私たちは、このような可能性を今まさに開始する段階で次のようなサービスをまず提示したいと思います。

Community Support over Game

私たちは、ブリルライトプラットフォームを介してゲームの境界を超えるコミュニティ機能を提供することができます。既存ゲームのギルドやクランなどのコミュニティシステムは、当該ゲームに従属しているサブコンテンツに過ぎませんが、ブリルライトプラットフォームのコミュニティ支援は、ゲーム間の境界を超えるコミュニティ統合資産管理システム、掲示板及びメールボックスなどを含む様々なメッセージングシステム、国籍を問わない民主的な投票システムなどを可能にします。これらのコミュニティ支援機能により、民主的に選出された役員が運営する、スポンサーから完全に独立したe-sportsプロチームのような形の球団運営が可能になるかもしれません。収益を目標とするコミュニティではなくても、現実で形成された繋がりに基づいた知人とゲームの種類を問わずにプライベートギルドを運営することもできるでしょう。

Auction System

私たちは、ブリルライトプラットフォームを介してゲームの境界を超えるオークション機能を提供することができます。ブリルライトプラットフォームは、全世界のすべてのゲーム及びゲーマーが共有する1つの巨大なオークション市場を形成することができます。これにより、ゲーマーは、ゲーム資産の販売者または購入者を探し回る手間から解放されることができ、妥当な価格のための駆け引きから自由になることができます。

ゲーマーが売り物として登録したアイテムなどを全世界のすべてのゲーマーが落札を受けることができる巨大な単一のオークション市場の存在は、接続したサーバー群など、多くの環境要因によるゲーム資産価値の不均衡問題を解消します。ゲーマーは他のゲームで売り物として登録された装備などを落札受けるとすぐに、自分のインベントリに支給を受けることができるようになります。

これらのオークションシステムは、ゲームサービスと結合されたThird-Partyサービス形態で提供されることがあります。

ブリルライトコインの価値

多数の実使用者を確保した最初の暗号通貨

伝統的に貨幣の相対価値は、需要と供給の論理によって決定されるということが出来ます。当該貨幣を使用しようとする需要（ユーザー及び使用先）と発行量が出会う地点が貨幣の相対価値とすることが出来ます。

しかし、現在までの暗号通貨は未来の可能性というバラ色の希望が投機的な価値上昇を呼んできただけであり、実際的な需要、即ち、ユーザーと使用先を確保できていない場合がほとんどです。

ブリルライトプラットフォームは、すでに累積加入者10億人に達するグローバルゲームとの提携（MOU）を締結し、プラットフォームが成長するにつれて全世界の数多くのゲーマーを持続的にBRCの実ユーザーとして確保することが可能です。全世界の数多くのゲーマーを実ユーザーに確保し、グローバルゲーム資産市場を使用先として確保することが可能なBRCは価値安定的な暗号通貨の現実的な代案となるはずで

価値安全性

BRCの価値は結局、開発会社から提供する有料サービスとBRCの交換比率で決定され、これは開発会社でBRCの価値を策定することになるということを意味します。私たちは、ブリルライト・プラットフォーム・メインネットがローチングされる時点で1 BRC=1 USD程度の価値に策定して開発会社の価値設定を誘導します。これにより、貨幣としての基本機能である価値安定性を維持し、急激な価格変動を抑制します。

サービス競争を通じた漸進的な価値上昇

BRCは、ゲーム内のコンテンツの使用先により価格が安定化されています。多くの開発会社が参加しているブリルライトエコシステムでは、BRCを販売して収益を拡大しようとする開発会社間の競争が自然に広がるしかありません。BRCの価値策定が異なる、多数のゲームが競争になる場合、需要と供給の市場論理に基づいてBRCの価値を高く策定したゲームの方にBRCが漸進的に吸収されて価値の上昇に帰結されるでしょう。これは長期的な視点の投資価値の側面で肯定的な効果をもたらします。

半減期を通じたBRC発行量の減少

ブリルライトプラットフォームを介して10年間で約6億BRCを発行し、以後、毎年約1,400万BRCが固定発行されます。毎年ブロック補償が10%ずつ減少するので、時間が経つにつれ、希少性の原理によってBRCの漸進的な価値上昇を期待することができます。

プラットフォームサービス利用料の一部の消却

コミュニティサービス及びオークションシステムなどのようなブリルライトプラットフォームサービスは、継続的に拡大され、サービス利用時にゲーマーに一定額の利用料を課すことができます。利用料として賦課される手数料の一部を開発会社の分として支給し、残りは消却して、BRCコインのインフレを抑制することができます。約10年目から定期的に発行される1400万BRCまたは、それ以上のBRCがプラットフォーム利用料として消却されると予想することができ、市場に流通している全体通貨量が固定される効果でBRCコインの価値が安定的に維持されるようにします。

オフラインコンテンツ利用機能

私たちは、ゲームサービス内のデジタルコンテンツ決済のほかにもゲームと連携されたキャラクター商品のように、様々なオフラインコンテンツに使用可能な個人ウォレット(ウェブウォレット/モバイルウォレットなど)をサービスします。それと同時に、使用先の拡大にも私たちのすべてのマーケティング力量を集中させます。オフライン使用先の拡張による需要拡大はBRCの価値が一步より上昇するのに大きな滋養分になるでしょう。



BRC Crowd-Sales & Token Allocation

トークン販売概要

ブリルライトプラットフォームを維持して稼働する核心であるBRCは、ゲームプレイを通じた採掘以外にもICO (Initial Coin Offering) 方式のトークン事前販売 (Presales) を介して取得することができます。ICOで販売されるトークンはERC20トークンの形で提供され、今後、ブリルライトプラットフォームメインネットがローミングされた時に1:1の割合でBRCと交換されます。

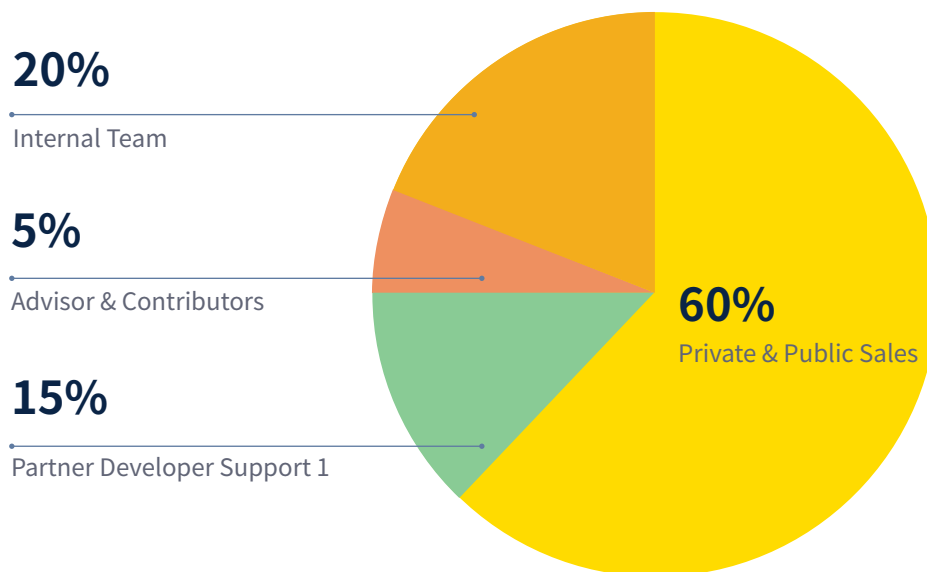
| | |
|-----------------|---|
| トークン発行量 | 1,000,000,000 |
| 目標販売額(Hard Cap) | USD 100,000,000 |
| 最小販売額(Soft Cap) | USD 10,000,000 (最小販売額に満たない場合には募金された投資金は投資者に全額返還されて事業は終了します。) |
| 参加手段 | BTC, BCH, ETH, ETC, XRP, ADA, and PLC |

[表5] ブリルライトトークン販売概要

Token Allocation

ブリルライトトークンは、合計10億個が発行され、この中の6億個のブリルライトトークンがICOを通じて事前販売されます。

15%のトークンは、パートナー開発会社との連動費用などで支援され、5%のトークンは、ブリルライトプラットフォームの成功のために活動した諮問団及び寄与者などに支給されます。また、20%のトークンは、コア開発チーム及び内部開発チームの分として割り当てられており、このうちの一部は、予備費とBRC流動性管理用に割り当てられており、今後予備費の支出項目がなく、BRCの流動性不足現象が発生しなければBRC価値安定化のために消却されることがあります。



[図7] ブリルライトトークン割当

トークン販売日程と細部内訳

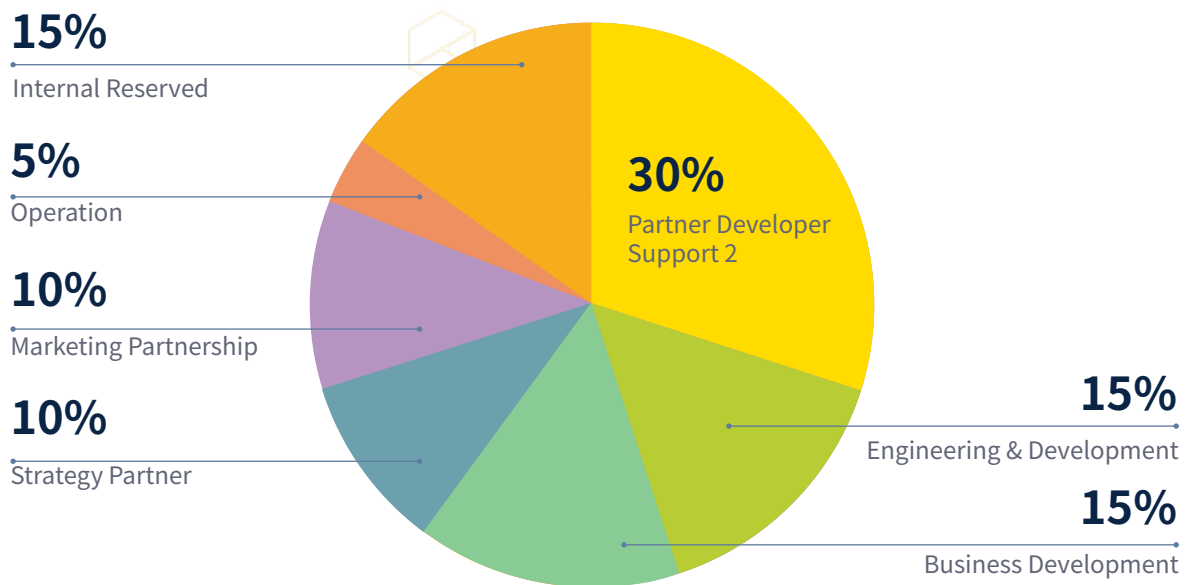
ブリルライトトークン販売は、3つの形態で行われ、日程に基づいてPrivate PresaleとPublic Presale、Public Saleとして行われます。もし、Presale段階で目標販売額を達成する場合、Public Saleは行われません。

| Token Sales Details | | | |
|---------------------|---------------------------------------|---------------------------------------|-----------------|
| トークン発行量 | 1,000,000,000 (事前販売量 600,000,000) | | |
| 段階 | Private Presale | Public Presale | Public Sale |
| セール期間 | 4月16日 ~ 6月30日 | | 7月9日 ~ 7月27日 |
| 参加手段 | BTC, BCH, ETH, ETC, XRP, ADA, and PLC | BTC, BCH, ETH, ETC, XRP, ADA, and PLC | ETH only |
| 参加者 | 戦略的パートナー | 機関等の公認投資者 | KYC認証完了された個人投資者 |
| ロック期間 | 2ヶ月 | 1ヶ月 | なし |
| 最小参加 | USD 100,000以上 | USD 20,000以上 | USD 1,000以上 |
| 予想販売価格 | USD 0.2 | | |

[表6] トークンセール細部内訳

トークン販売収入の使用計画(Use of Proceeds)

ブリルライトトークン販売を通じて得られた収益は、基本的にブリルライトプラットフォームの成功的な構築のために使用されます。ブリルライトプラットフォーム及び各種Third-Partyサービスの開発及び運営コストと、提携開発会社との連動開発費支援などに使われ、一部はブリルライトプラットフォームの成功的な開発のために開発チームと諮問団、寄与者への補償として支給されることがあります。また、グローバルゲーム会社との提携のためのマーケティング費用などで使用することができます。



[図8] トークン販売収入の使用計画

ロードマップ

2018

● The Beginning of Bryllite

2018 Q3

- Bryllite Core Development (Bryllite Master Node / Observer Node, Excluded Light-weight Node)
- ブリルライトトークン取引所上場

2018 Q4

- Bryllite Bridge Service Development
- Bryllite Server/Client API Development
- Bryllite Platform Test-Net Launching

2019

● The Dawn of Bryllite

2019 Q1

- Cyprus Network Implementation
- Bryllite Platform Main-Net Development
- Partner Developer Game Integration Reference

2019 Q2

- Bryllite Platform Main-Net Launching
- ブリルライトトークンをBRCに転換
- 主要取引所にBRC上場

● The Sunrise of Bryllite

2019 Q3

- Legacy Game Asset Converting Development
- Bryllite Light-weight Node Development (Gamer Personal Wallet Support, PC/Mobile/Web)

2019 Q4

- Smart Contract Support

2020

● The Brilliant Sunlight

2020 Q1

- Bryllite Platform Service Development: Auction System

2020 Q2

- Bryllite Platform Service Development: Community System

2020 Q3

- Extended Bryllite Platform Service Development

“The Third Impact”

「私たちは常に未来のゲーム文化を先導してきており、ブリルライトプラットフォームを介して、将来のゲーム文化の‘The3rd Impact’を先頭からリードしていきます。」

- ブリルライトLtd. 代表 金ユラ

私たちは、目の前の収益よりは、ゲームの価値を志向し、現在の価値だけではなく、ゲーム文化の未来を見つめたいと思います。(株)ハンビットソフトは、90年代後半から始まったPC部屋熱風の主役であり、これを土台に新しいゲーム文化を韓国だけでなく、全世界に知らせました。また、第1期e-sports協会会長社として国内外e-sportsの発展に貢献し、新しいスポーツ文化の土台を準備し、(株)T3エンターテインメントは、グローバル累積加入者7億人を超えるゲームをサービスしてe-sportsのアジアンゲーム正式種目採択のために努力してきました。

今、私たちは、ゲーム文化の巨大な「The 3rd Impact」を準備しています。私たちの新しい挑戦はゲーム資産を所有者であって当然のゲーマーに戻してあげて、孤立されたゲーム間の境界を崩し、「超連結ゲーム社会(Hyper Connected Game Society)」に進むことを目標とします。「超連結ゲーム社会」という新しいゲーム文化を通じて、ゲーマーは従属されたゲームから解放されることができ、簡単なゲーム間の往来で無限な自由を享受することができるでしょう。

ここ20年間、グローバルゲーム業界の一軸を担当してきた立場から、このような目標を達成して、理想を貫徹することが非常に容易ではない挑戦になるという点は、誰よりもよく知っています。しかし、この挑戦の難しさについてよく理解しているので、むしろ誰よりもよく準備して熱烈的に開発に臨むことができると自負しています。私たちは、過去の数多くの挑戦を乗り越えてきた経験があり、継続的に新しいゲーム文化を作って認められてきました。これらの勝利の記憶は、ブリルライトプラットフォームが成功することができる根底になり、長い間蓄積された私たちだけのノウハウは新たな挑戦に大きな力になってくれるでしょう。

ブリルライトプラットフォームは、全世界のすべてのゲーマーとの約束であり、現在の私たちがあるまで、数多くのゲーマーが見せてくれた情熱と献身的努力に対する小さなお返しでもあります。そのため、私たちの目標が達成されるその瞬間まで挑戦を止めずに喜んで楽しい気持ちで準備してゲーマーの権利とゲーム資産の価値を守ることができるように努めます。また、多様な経路を通じて持続的にブリルライトプラットフォームの技術的、論理的整合性について検証し、問題の指摘に対して開かれた姿勢で謙虚に収容することを恐れたり、怠けなつもりです。

変化の開始は、過去から当たり前のように思われて来た多くのものについて疑問を抱き、なぜ当たり前のように思われてきたのかについて質問することから始まるのだと信じています。私たちは、これまでゲーム業界で当たり前のようにされてきた様々な問題に絶えず問題提起をして来ました。これからその答えを見つけるためにもう一歩進もうとしています。

全世界の全てのゲーマーに感謝と敬意を...

Fin.



References

- [1] 韓国ゲーム産業開発院, “オンラインゲームアイテム現金取引深層実態調査”, May 2006, http://www.kocca.kr/knowledge/research/_icsFiles/afieldfile/2010/05/02/69855.pdf
- [2] 韓国コンテンツ振興院, “2017 大韓民国ゲーム白書”, Dec 2017, <http://www.kocca.kr/cop/bbs/view/B0000146/1834974.do>
- [3] (C)Newzoo, “Newzoo Global Games Market Report 2017”, Jun 2017, <https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2017-light-version/>
- [4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Oct 2008, <https://bitcoin.org/bitcoin.pdf>
- [5] wikipedia, “Cashless society”, Feb 2018, https://en.wikipedia.org/wiki/Cashless_society
- [6] wikipedia, “Double-spending”, Mar 2018, <https://en.wikipedia.org/wiki/Double-spending>
- [7] bitcoin.org, “51% Attack, Majority Hash Rate Attack”, <https://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do>
- [8] 自由企業院 大学市場経済講座 キム・ヨンジュ, “1兆5千億 地下市場を堂々と世界の外に連れ出す。‘Itembay’ キム・チヒョン会長”, Mar 2016, <http://lecture.cfe.org/info/bbsDetail.php?cid=13113&idx=42943>
- [9] Naverゲーム委員会ソーシャルメディア記者団 ‘무아유지향’, “ARゲーム市場を調べる”, Jun 2017, <http://m.post.naver.com/viewer/postView.nhn?volumeNo=8252598&memberNo=793124>
- [10] blockgeeks.com, “Blockchain Scalability: When, Where, How?”, <https://blockgeeks.com/guides/blockchain-scalability/>
- [11] Bitcoin Developer Reference, “Block Headers”, <https://bitcoin.org/en/developer-reference#block-headers>
- [12] wikipedia, “ビザンチン・フォールトトレラント性”, Aug 2017, <https://ja.wikipedia.org/wiki/ビザンチン将軍問題>
- [13] Miguel Castro & Barbara Liskov, MIT Laboratory for Computer Science, “Practical Byzantine Fault Tolerance”, Feb 1999, https://www.usenix.org/legacy/events/osdi99/full_papers/castro/castro_html/castro.html