



今回、5月のNYAにおいて合意された「SegWit2x」の「2x」部分（ブロックサイズの2倍への引き上げ）の適用が延期されたことは合理的な判断で、ビットコイン・エコシステムの恒久的な存続において重要な意思決定だと考えています。

当初はマイナーのハッシュパワーのみで新しい仕様が決められると考えられていたビットコイン・エコシステムは、実はマイナー以外のユーザー、開発者、ウォレット提供企業、取引所といったステークホルダーの合意がない状況で仕様変更を行うと、非常に不安定で大きな混乱を生み出す可能性があることが判明しました。仮にリプレイアタックに向けた対策がなされない状況でハッシュパワーが均衡した2つのチェーンが存在したとすると、常にどちらかのチェーンがReorgのリスクに晒されて顧客資産の保護が図れません。これは取引所の立場としては絶対に許容することができない状況です。ブロックチェーンが安定して存在することはビットコイン・エコシステム存続の絶対条件です。

当時対立する意見により分岐の危機を迎えていたビットコイン・コミュニティ内の「妥協案」として提案されたのがNYAで、当社はこれに署名いたしました。そして、NYAによって混乱なくSegWitが無事アクティベートされました。次にブロックサイズを2倍にする「2x」の適用の前にビットコイン・エコシステムを取り巻く状況が大きく変化し、「SegWit2x」の意義について議論が起きました。ビットコインの非中央集権的な側面は非常に民主的であり、多くの人が未来の社会システムとして応用の可能性を期待しています。一方で紛争が起きた時の解決手段がないことも露呈しました。それはユーザーが急増し続ける中、ブロックチェーンの負荷をどのように軽減するのかといったスケーリングの課題が未だに解決に至っていないことから明らかです。

非中央集権型システムであるビットコインのブロックチェーン技術は、PoWを用いた合意形成アルゴリズムによりビザンチン将軍問題を解決しました。しかし皮肉にも、そのアルゴリズムやプロトコルの仕様変更に関する意思決定は、プログラムの外で行われ各ステークホルダーの理念や利害を反映し政治的に決定されています。引き続き非中央集権型社会システムにおける合意形成プロセスへの挑戦は続きますが、大きなイノベーションであるビットコイン・エコシステムおよびブロックチェーン技術の発展に微力ながら貢献できればと考えています。

株式会社 bitFlyer
代表取締役 加納 裕三

SegWit2x 延期声明に対する見解と対応方針について

SegWit2x によるビットコインのブロック高 494,784 に予定されていたハードフォークについて、SegWit2x プロジェクトの開発者を含む 6 人により延期声明*1 が発表されました。当社は当該声明に賛同いたします。

ビットコイン・エコシステムにおいて、コンセンサスを得る方法を変更するには、マイナー、ユーザー、開発者、ウォレット提供企業、取引所といったステークホルダーの合意が必要になります。この合意が無い状態でのブロックチェーンの分岐は、ビットコイン・エコシステムを不安定にし、混乱をもたらします。分岐により発生するチェーンに Reorg*2 やリプレイアタックに向けた対策*3 がなされない場合、どちらかのチェーンもしくは両方のチェーンの資産の価値が失われる、すなわちお客様の資産が突然失われる可能性があります。当社は、ハードフォークの内容がいかなるものであったとしても、上記のような合意が無い、あるいはお客様資産の保護に向けて十分に対策がなされていない分岐は、ビットコイン・エコシステムのために絶対に避けるべきであると考えています。

NYA*4 は、まず SegWit そして続く「2x」と合意がとれたハードフォークを促すために締結されたものでした。SegWit については混乱なくハードフォークができたものの、続く「2x」については現時点でステークホルダーの合意がとれておらず、ビットコイン・エコシステムを不安定にする可能性が高いと思われます。当社は、今回の延期声明に賛同することにより合意のとれていないハードフォークを避け、ビットコイン・エコシステムの安定に寄与することができると考えています。

【当社サービスにおける対応方針*5】

今回の延期声明を受け、当社はビットコインのブロック高 494,784 前後においてもビットコインのお預入・ご送付サービス等を一時停止する予定はございません。ビットコイン決済等を含む当社の全サービスが通常通りご利用いただけます。当社は引き続き SegWit2x の開発の進捗やハッシュパワーの状況等、取り巻く環境変化を分析し、対応方針の検討を行います。

【当社の取組について】

当社は 2017 年 5 月時点において、ビットコインのブロックチェーンにおける送金手数料高騰問題を解決するため、かつビットコイン・エコシステムの安定化のために、SegWit をアクティベートすることが重要であると考えました。混乱無く 8 月に SegWit がアクティベートされトランザクション処理能力を向上させることが可能になりました。当社は仮想通貨交換事業者で唯一 P2WSH を実装するなど、SegWit の利用推進およびビットコイン送付手数料を減額しユーザー利便性の向上に寄与しています。

2009 年以降多くのユーザーに支えられてきたビットコイン・エコシステムが、今後も安定的に存続し発展することを強く望みます。当社もコミュニティの一参加者として、継続的にできる限りの貢献を行っていきます。

*1 SegWit2x のハードフォーク延期声明について、詳細は下記リンク先をご参照ください。
<https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html>

*2 Reorg とは、短いチェーンが長いチェーンに再編成され、短いチェーンに含まれた承認済みトランザクションが無効になることを指します。

*3 リプレイアタックに向けた対策が実装されない場合は、分岐後に片方のチェーンでのコインの送付において意図せずもう片方のチェーンでもコインが送付されてしまう可能性があります。

*4 New York Agreement の略称。2017 年 5 月 23 日にマイナー・取引所等が SegWit2x 推進について合意しました。詳細は下記リンク先をご参照ください。
<https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77>

*5 本対応方針は 2017 年 11 月 9 日現在の状況に基づくものであり今後のビットコイン・エコシステムの状況変化によっては当社の対応も変わりうるものをご了承ください。対応に変更があった場合は改めてご連絡させていただきます。

お問い合わせ先

株式会社 bitFlyer 広報担当 金光 碧

〒107-6208 東京都港区赤坂 9-7-1 ミッドタウン・タワー 8F

HP: <https://bitflyer.com> Contact: <https://bitflyer.com/ContactPage>