



Regarding the debate over the hard fork in the Bitcoin blockchain, I have always maintained a neutral position, avoiding supporting one side or the other based on political ideals. As CEO of bitFlyer, Inc., running an exchange demands objectivity as does the position of representative director of the Japan Blockchain Association, thus, decided it was best to avoid taking a stance.

Many stakeholders may be unaware of the result of both technical analysis of the extended consensus algorithm, of which Proof of Work is a part, and the implications of a dynamic hard fork and potential blockchain reorganization driven by economic interest. But beyond this awareness, each stakeholder's code of conduct can have an impact of the largest effect on the stability of the entire Bitcoin ecosystem. I have friends on both sides, but I believe that continuing this conflict for an extended period of time will have negative repercussions for all stakeholders.

Today, bitFlyer, Inc. is declaring an official stance, but only in the interest of customer protection and to send a strong message of support for the continuation of the Bitcoin ecosystem. For the sake of the future of Bitcoin, I hope that this instability is resolved as rapidly as possible.

Yuzo Kano, CEO
bitFlyer, Inc.



March 27, 2017

bitFlyer, Inc.

Our Perspective on the Bitcoin Hard Fork

Currently, the possibility of a hard fork in the Bitcoin blockchain is being debated. With this hard fork, it's possible that the current Bitcoin blockchain will branch into two—one branch remaining as Bitcoin Core (a continuation of the current Bitcoin model, hereafter referred to as BCC) and another with a variable block size that will be called Bitcoin Unlimited (hereafter referred to as BU). At the heart of this debate is an attempt to improve the throughput of the Bitcoin network in face of the nearing current maximum amount a block can store.

In our view, regardless of the details of the hard fork, a branching of the blockchain that may result in the coexistence of multiple virtual currencies must be avoided for the entire Bitcoin ecosystem.

In the Proof of Work system adopted by Bitcoin, hashing power plays an essential role in record verification. Concretely speaking, as was pointed out in Nakamoto's white paper, even if a branch occurred in the blockchain, both blockchains would converge on the blockchain that is supported by the strongest hashing power.

Based on that principle, if hashing power is distributed after a branch and an imbalance in hashing power occurs between post-branch blockchains, blockchains that are supported by weaker hashing power will be exposed to the risk of being invalidated, which would result in the sudden disappearance of customer assets.

Accordingly, **we are strongly against the coexistence of multiple blockchains that would result from a hard fork.**

We also believe that there is room for improvement in the current BU specification. Under the current specification, the probability of temporary branches of a blockchain increases. Additionally, it's currently impossible to predict the maximum block length of these temporary branches.

Up until now, due to the fact that Bitcoin transactions require six confirmations, the possibility of a transaction being overturned has been extremely small and it is

generally safe to think that a transaction is final. However, under the current BU specification, one must wait for a larger number of confirmations before the transaction is confirmed. As a result, it may in fact take much longer to confirm Bitcoin transactions in order to make deposits, and send or receive coins to secure the operations.

In light of the possible result of a hard fork, we wish to make the following promises to our customers:

- Our customers' assets will be protected. If a BU hard fork occurs, the amount of Bitcoin held before the fork will be the same in both BU and BCC after the fork.
- If a fork occurs, we may need to establish a time period during which no Bitcoin operations, no Bitcoin deposits, and no sending or receiving of Bitcoin may be processed.
- We understand how to protect against replay attacks that are a current cause for concern. We are committed to providing, and have already started preparing, countermeasures against these attacks.
- We will continue to analyze and research the specifications and implications of BU to minimize the risk to our customers to the greatest extent possible.

Since 2009, the Bitcoin ecosystem has been supported by many users who wish to see it continue to grow while maintaining long-term stability. We at bitFlyer are committed, as fellow participants, to continuously contributing to this community to the best of our abilities.

Should any new developments occur, we will provide updates in subsequent releases as time and circumstances allow.

Contact Information

Midori Kanemitsu, PR Manager, bitFlyer, Inc.

107-0052 Tokyo, Minato-ku, Akasaka 3-5-5 Strong Akasaka Bldg., 6F

HP : <https://bitflyer.jp>

mail : info@bitflyer.jp