September 23, 2020
bitFlyer, Inc.

The current status of Ethereum Classic (ETC) and our policy going forward

We are writing to inform you of the current status of Ethereum Classic (ETC) and our policy going forward.

ETC has been experiencing a series of reorgs since a 51% attack that occurred on the ETC blockchain in early August. The blockchain remained unstable with another 51% attack occurring at the end of August.

Ethereum Classic Labs (a major developer of the ETC network) has published their response, including their cooperation with a law firm to take legal action against those responsible for the 51% attack that occurred in early August (https://kobrekim.com/news/kobre-and-kim-etc-labs-pursue-ethereum-classic-blockchain-attackers). Additionally, it is believed that this attack was facilitated by the hash rental market which can be used to anonymously rent enough hash power to perform this kind of attack. Ethereum Classic Labs has also announced their support for regulations on hash rental (https://medium.com/ethereum-classic-labs/ethereum-classic-labs-to-pursue-enforcement-and-regulation-of-hash-rental-platforms-cfbe90b62a2a).

In response to these attacks, we have increased the number of confirmations required for ETC withdrawals and suspended ETC deposits as of September 15. Since we have consistently required a high number of confirmations, customer assets have not been affected by these attacks.

With security and customer asset protections as our top priorities, we will take the appropriate measures and publish any relevant information as we follow announcements from Ethereum Classic Labs and any blockchain security improvement protocols from the community.

51% attack

A 51% attack can happen when a malicious individual or group of miners who control over 50% of the network's computing power (hashrate). This would allow them to perform actions such as preventing new transaction confirmations, cancel or deny others' transactions, reverse current transactions (double spend), or monopolize mining new blocks to take all of the rewards for themselves. There is currently no effective countermeasure for a 51% attack.

More information on 51% attacks can be found here.

Reorg

A reorg refers to an event where the details of transactions on a blockchain are rewritten. Under normal circumstances, deposit and withdrawal transaction requests between external addresses and our addresses are sequentially confirmed and added to blocks. However, a reorg would prevent these transactions from being confirmed because the block for them to be recorded in could not be specified.

Confirmation

A transaction is "confirmed" when it is included in a new block. Transactions that have not yet been incorporated into blocks are considered unconfirmed. If the transaction belongs to a block, it is considered confirmed. As new blocks are added after the block to which the transaction belongs, it is confirmed further.
For transactions with low commissions, it can take time to get included in the block and they may remain unconfirmed for a long time.

More information on confirmations can be found here.

We appreciate your continued support.

Media Inquiries

PR team, bitFlyer, Inc.

Midtown Tower, 9-7-1 Akasaka, Minato-ku, Tokyo 107-6233

HP: https://bitflyer.com/en-jp Contact: https://bitflyer.com/en-jp/Contact