April 18, 2017

Israeli Bitcoin Association Statement about Hashrate Attacks

We, the Israeli Bitcoin Association, pursue the goal of maximizing the benefit that Israel's population obtain from the Bitcoin technology - which strongly depends on Bitcoin's worldwide success.

We believe that, as a currency, Bitcoin is subject to the network effect, and that it is strongest when its community and industry, brought together by both ideology and practicality, are united in a single network; and that rifts and separation should be avoided if at all possible.

We also believe that Bitcoin is voluntary money; people use it because they choose to, not because they are coerced. As such, people can also choose to fork Bitcoin's open source code and use an alternative currency with similar underlying principles.

We recognize that there may be different views about what Bitcoin is, and a time may come where those differences cannot be reconciled. It might then be unavoidable to experience a split of the currency into two separate networks, each sharing a blockchain history and - at least temporarily - the Bitcoin brand.

We believe that all these different currencies have a right to coexist peacefully and compete fairly. We oppose any attempt of supporters of one currency to inflict damage on a different currency, in a way which achieves no purpose other than denying others the right to use the currency of their choice.

It saddens us that lately we have heard people planning just such attacks. In particular, in the event of a split of the Bitcoin network to two, both using the same PoW hash function, proponents of the network with majority hashrate might exploit known vulnerabilities of the Bitcoin protocol against the smaller network - such as the well-known >50% attack or a more sophisticated attack commonly known as "selfish mining". By mining malicious blocks in secret (which double-spend or deny service) and releasing them strategically, they can effectively erase blocks mined by the honest network, and render the currency unusable.

We believe such attacks are in stark opposition to Bitcoin's spirit and we condemn anyone who supports them. We invite others to publicly condemn and shun these deplorable, hostile plans.

We believe that in so doing, we can help promote a healthier atmosphere, where would-be attackers realize they would only ostracize themselves by carrying out such an attack - thus allowing an open, decentralized ecosystem where people may choose between alternatives and the best currencies may thrive.