

BUIP077: Enable representative tokens via OP_GROUP on Bitcoin Cash

This BUIP proposes that BU implement the OP_GROUP opcode as described here: <https://medium.com/@g.andrew.stone/bitcoin-scripting-applications-representative-tokens-ece42de81285>, on the Bitcoin Cash blockchain.

This basically adds "native" colored coins to a blockchain. I believe that this additional feature will drive use and therefore adoption of Bitcoin Cash. Today Bitcoin Cash is a payment network. But with the inclusion of representative tokens, the blockchain can be used for asset holding, and the network's functionality will be expanded from payment to exchange.

Specifically this BUIP authorizes us to:

1. Implement OP_GROUP, including all tests etc required to ensure the correctness and safety of the change.
2. Enable this opcode on the BU "nol" network.
3. Work with the Bitcoin Cash community to enable this opcode via hard fork on the Bitcoin Cash blockchain

What is OP_GROUP?

OP_GROUP is a single additional opcode to the Bitcoin scripting language that effectively enables representative tokens (that is, "colored coins") on a blockchain. Unlike all current colored coin proposals and implementations, in the OP_GROUP system the miners validate the colored coins, as part of normal transaction validation. This means that, like bitcoins, invalid colored coin transactions will not appear on the blockchain (all other colored coin proposals can have illegal transactions on the blockchain and therefore rely on every client to validate every colored coin tx). Additionally, the OP_GROUP proposal clearly marks every UTXO with a "color". When you add these two features together, the result is that:

1. A user can't accidentally spend colored coins as normal bitcoin
2. SPV wallets can handle coin colorings with the same ease and security model as Bitcoins

This first version of OP_GROUP colored coins does not contain some of the advanced features that some other colored coins support. But I believe that it contains the key feature needed for colored coins -- enabling SPV wallets. This feature is missing from all other colored coins proposals.

Please read this link for details: <https://medium.com/@g.andrew.stone/bitcoin-scripting-applications-representative-tokens-ece42de81285>

EDIT:

Chris Pacia just wrote a great article describing the system very clearly:

<https://www.yours.org/content/colored-coins-in-bitcoin-cash-b26804e05964/>