BUIP078: Enable Binary Contracts in Bitcoin Cash via OP_DATASIGVERIFY

This BUIP proposes that BU implement the OP_DATASIGVERIFY opcode, and reenable selected string and integer manipulation opcodes as described here: https://medium.com/@g.andrew.stone/...ications-decision-based-spending-8e7b93d7bdb9

OP_DATASIGVERIFY allows a script to validate the signature on arbitrary data using the same ECDSA algorithm (and code) used to validate the signature on Bitcoin transactions. This opcode therefore enables the use of an external "oracle", which is a very important too to enable external information to be imported into a transaction. Once the data is part of a transaction it is useful to be able to manipulate it to check various conditions on that data. This requires the re-enabling of certain opcodes.

I believe that these opcodes were originally disabled when Bitcoin was the only cryptocurrency because the potential of Bitcoin as a simple payment system was too great to risk a setback due to and exploit in an immature code base for a secondary use case. However, now that cryptocurrencies are well established, it is time for some of these seconondary uses cases to be reenabled.

This additional feature will drive use and therefore adoption of Bitcoin Cash.

Specifically this BUIP authorizes us to:

1. Implement OP_DATASIGVERIFY, including all tests etc required to ensure the correctness and safety of the change.
2. Re-enable necessary string and integer opcodes, and clean up any issues with them.
3. Enable these opcodes on the BU "nol" network.
4. Work with the Bitcoin Cash community to enable these opcodes via hard fork on the Bitcoin Cash blockchain

1zerg12nRXZ41Pw4tfCTqgtdiJx6D1We3