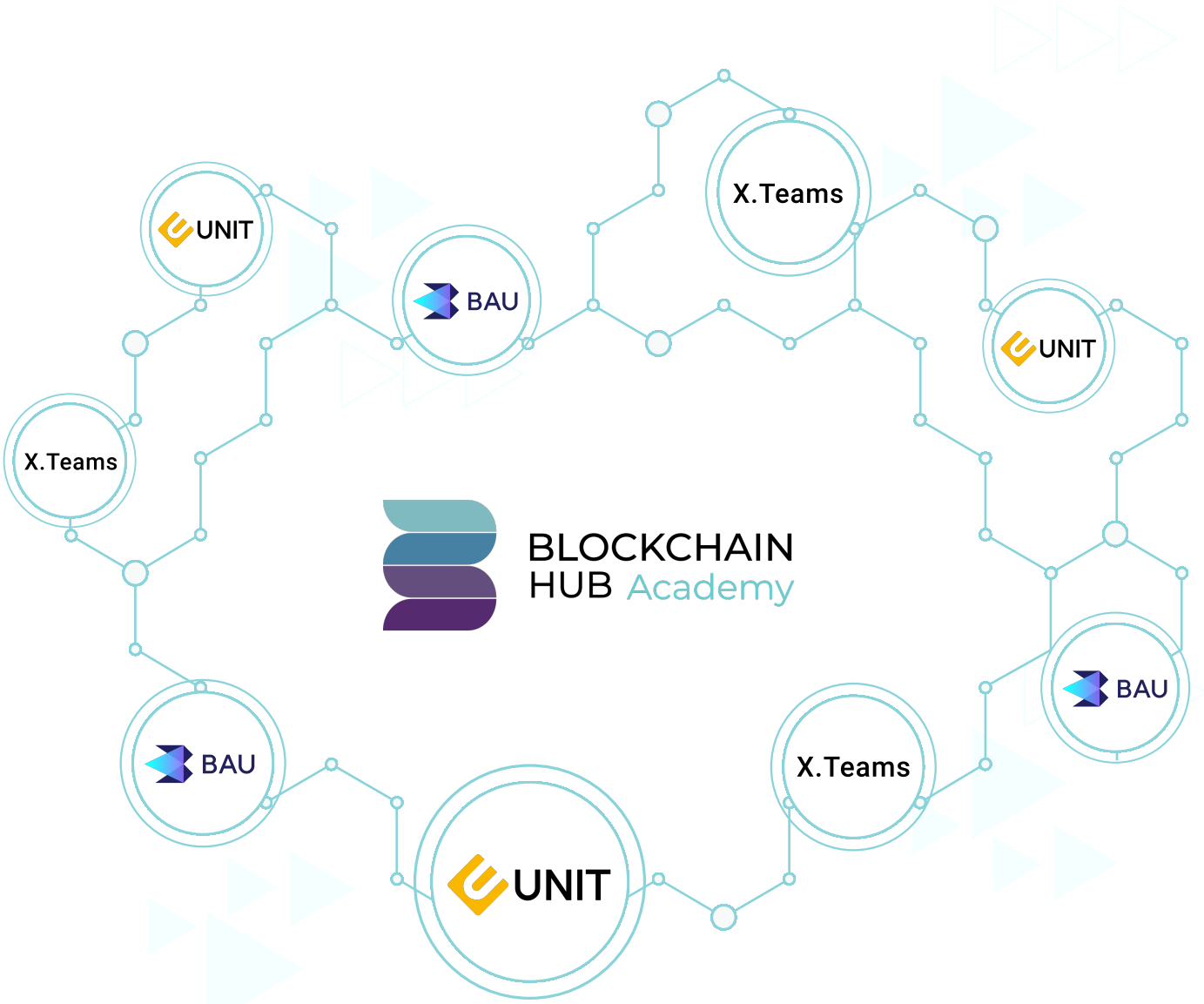
UNIT
BAU
X.Teams
UNIT
X.Teams
BLOCKCHAIN
HUB Academy
BAU
BAU
X.Teams
UNIT

Satoshi way

XBIP: 3
Created: 2019

CONTENTS

Introduction

Hey there,

Well, you passed important part of Satoshi way.It was implementation of the ideas behind original Bitcoin network. Satoshi Nakamoto invented and combined some existing approaches and as result our world got Bitcoin in 2008.

If you totally followed Satoshi way, this point represents the moment, when Satoshi disappeared and further development and support fell on the community only. There was a lot of issues, one of them is scalability. The bitcoin scalability problem refers to the discussion concerning the limits on the amount of transactions the bitcoin network can process.

In 2015, Pieter Wuille introduced a new feature to bitcoin called Segregated Witness, also known by it's abbreviated name, Segwit. Basically, Segregated Witness moves the proof of ownership from the scriptSig part of the transaction to a new part called the witness of the input. It was not only solving the scalability problem as general. It also helped to avoid transaction malleability issue and allowed to build off-chain protocols. SegWit was mentioned in the set of BIP’s.

This week we will continue to improve Pitcoin network. It includes basic features from Satoshi and one crucial feature from community.

PART 00: Enhance basic Pitcoin mining

In this section you have to enhance mining of Pitcoin network and prepare it for the further automated interaction between personal full nodes and each others.

Add difficulty calculation. It means additional parameters for block and calculation of that parameters in blockchain. Take into consideration bits, target and difficulty params. Also, please provide web route /getDifficulty in API. This will be used for the getting information about current Pitcoin network difficulty

Add timestamp validation. During the block validation process (when node receives new mined block), timestamp have to be carefully validated. You can decrease validation to 3 previous blocks.

Automated mining. Please provide process for the further automated network interaction between nodes. Thin process includes:
Receiving blocks. It happens when block is mined and broadcasted to the other nodes (add corresponding web route like /block/receive in full node API for receiving new block)
Validate new mined and received block
If validation is successful, add block to chain
Start new mining. You can remove manual initialization of mining with cli and start mine after the newly valid block add to chain

Supply and halving. Please add total supply of pitcoins to your blockchain. This is the value from original Bitcoin network (in bitcoins, not in satoshis). Also, coinbase reward starts from 50, like in Bitcoin. In addition, please add halving mechanism (every 5 blocks). Don’t forget validate this values during the mining process.

PART 01: P2WPKH

This part is about scalability and major actions, which have happened in summer 2017. You can read some articles and stories about this big drama, SegWit soft fork. Also, you can get more detailed information in corresponding BIP's about SegWit improvement. According to the P2PKH mechanism from previous week, please implement P2WPKH transaction. This is a parallel task, don't remove your P2PKH logic.

In your wallet add bech32 addresses. When you call swnew in wallet cli, the wallet mechanism has to generate new bech32 address from your private key and store to file swaddress

Build P2WPKH transaction for Bitcoin testnet. For the not so hard implementation you can use transaction between bech32 addresses. It helps to avoid more complicated structure like P2WPKH-P2SH, wrapper for backward compatibility. This is the new transaction standard. This script is based on P2PKH with some differences.

Also, please update wallet for the building and broadcasting transaction to the network (Pitcoin or Bitcoin testnet, it will be below). Your new commands in wallet cli for SegWit usage must start with sw prefix, like swbroadcast … and take parameters like in P2PKH transaction.
Don't forget about new serializer (please don't crash your previous logic with P2PKH).

PART 02: Task with asterisk

Satoshi way is a really hard way...This task can bring you additional points. Implementation of P2WPKH means you will broadcast your transaction to the original Bitcoin testnet. If you want to broadcast it to the Pitcoin network, you must implement this feature:

Make P2WPKH Script in Pitcoin network. You have to update block header and add additional parameters to the block. Don’t forget about witness data, wtxid merkle root and other delicious things. Block validation should be updated also.

PART 03: Tests

All parts of the ecosystem and newly created features should be covered with tests. At this stage it is proposed to continue the test coverage.

Provide test coverage of newly created use cases - mining process, bech32 addresses, P2WPKH transaction.

PART 04: Estimation

If you do not have time to implement all the tasks from 3 weeks, please move consistently. You will have the opportunity to pass the peer-review of the previous weeks again. Just keep in mind, the amount of points will be slightly less than the completed on time tasks.