



BTCoE

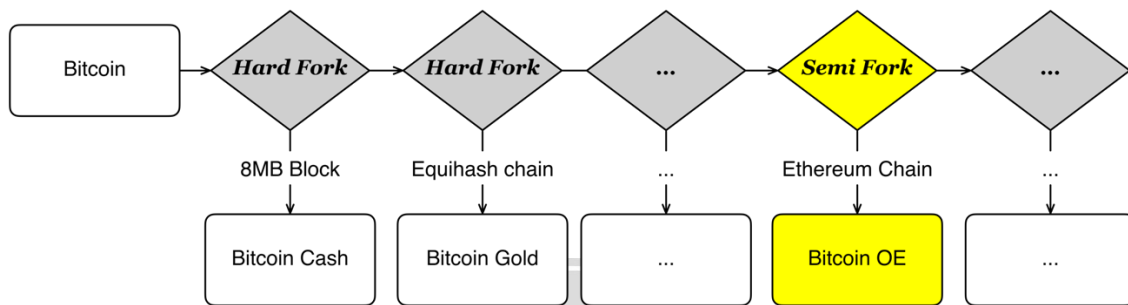
Technical Specifications

A fast, cross-chain semi-fork of bitcoin for micro-payment

Version 3.14

1. Introduction.

Bitcoin over Ethereum (BTCoe) is a cryptocurrency derived from bitcoin via a semi-fork process. Semi-fork is a technique that help us to bring bitcoin balances to ethereum network. BTCoe is also an ERC20 standard token on ethereum network so it benefits all advantages of this platform.



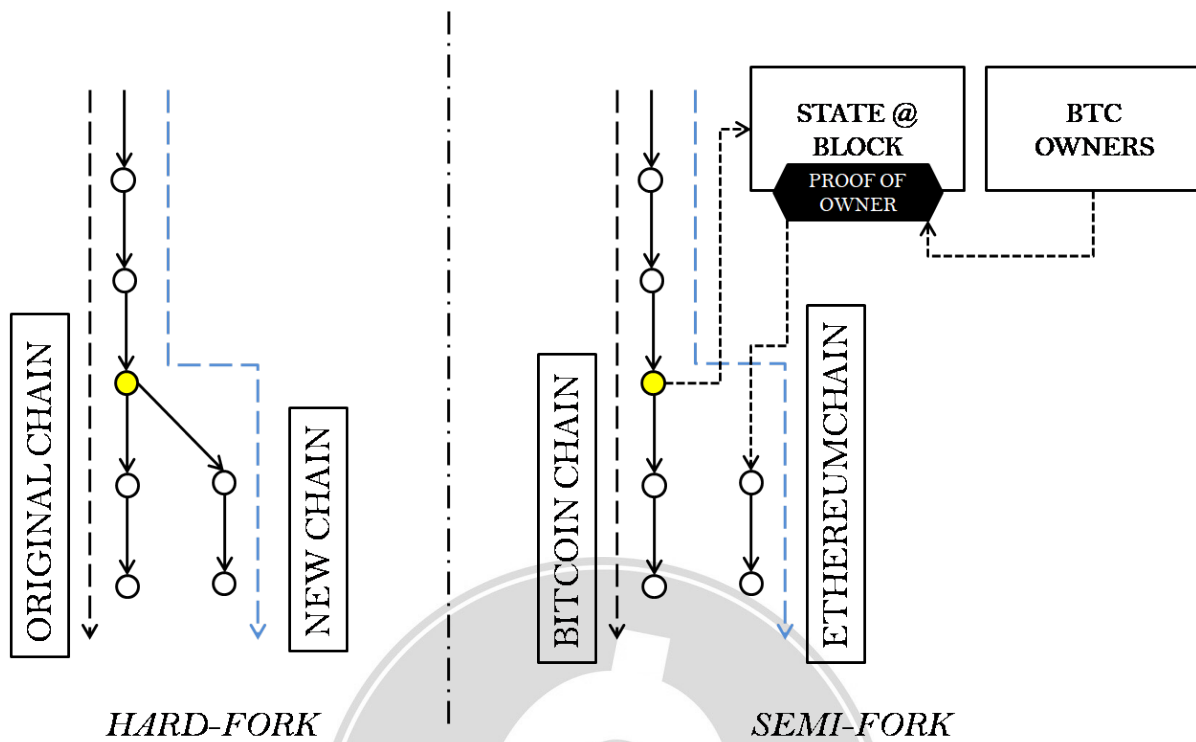
Drawing 1: BTCoe semi-fork process.

2. Technical specifications.

a) BTCoe, a semi-fork of bitcoin.

Every bitcoin direct-owners hold private keys for signing their transactions, the signing information proof that the transactions are generated only by the real owners. We use a technique called “proof of owner” in that each bitcoin owner must sign a message containing their ethereum address (address that they want to receive BTCoe) and submit to the verifier by calling a smart contract function. The system then will verify the signed message and deploy an amount of BTCoe corresponding to their bitcoin balance at the semi-fork block.

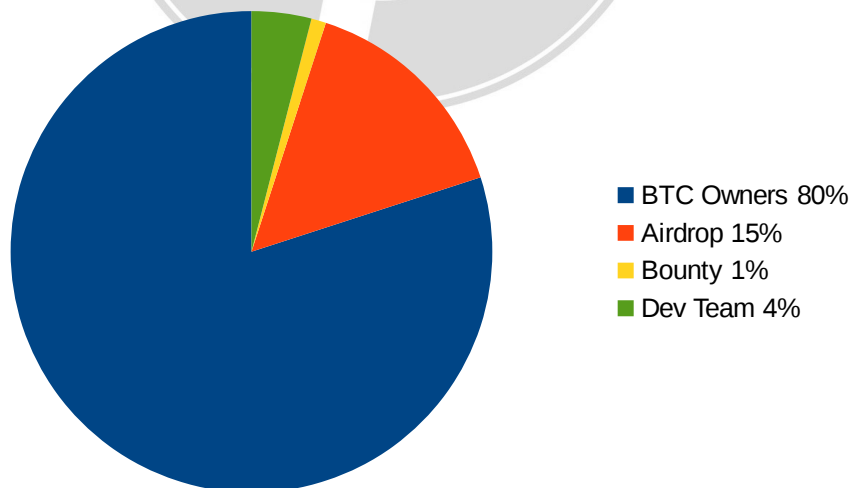
Comparing to traditional hard-fork, our semi-fork is a replay-proof process because your BTC and BTCoe accounts will stay at a completely different chain with different protocol and private key, that mean we does not need to implement any replay attack protection.



Drawing 2: BTCoe semi-fork details

b) BTCoe token distribution.

The following chart show BTCoe token distribution with 96% of total supply belongs to the community.

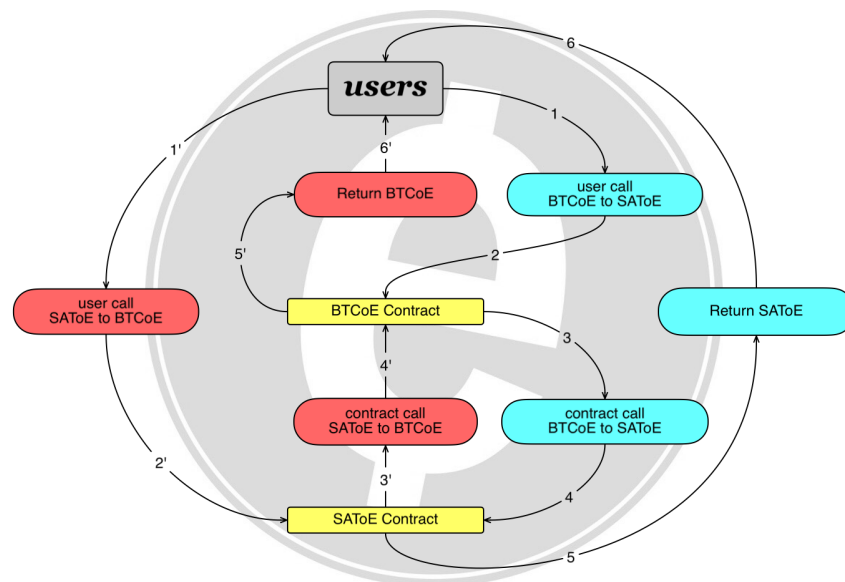


Drawing 3: BTCoe distribution.

c) Satoshi over Ethereum (SAtoE).

We introduce the concept of multi-denomination cryptocurrency that consists of multiple types of token, currently we implemented two types: The first is Bitcoin over Ethereum and the second is Satoshi over Ethereum, they are swappable units that mean coin owners can exchange between BTCoe and SAtoE at any time, $1 \text{ BTCoe} = 10^8 \text{ SAtoE}$. SAtoE contract will provide an easier way for users to make a micro-payment. The maximum supply value of these two tokens is always equal to 21 million BTCoe

(i.e. $\text{CirculatingSupply}^{\text{BTCoe}} + \text{CirculatingSupply}^{\text{SAtoE}} / 10^8 \leq 21000000 \text{ BTCoe}$).








Drawing 4: BTCoe and SAtoE interoperation.

SAtoE contract will cooperate with BTCoe as a single instance to provide a mechanism for exchanging between them. SAtoE token can be further split into $\mu\text{SAtoE} = 1/10^6 \text{ SAtoE}$, imagine you can pay some μSAtoE for each page you read on a website, that's really a very small payment and it costs zero fee, zero confirmation time. It can also be used for many IoT projects, for example, you can build a middle service for controlling IoT devices in which user transfer μSAtoE as a

command for those devices. It is cheap enough for paying some μ SAToe as a command code to do something.

SAToe is a micro-payment ready coin derived from μ Raiden, a robust framework to implement instant and free pay-per-use payment channel technology in commercial applications.

d) Technical comparisons.

	BTC Bitcoin	BCH Bitcoin Cash	BTG Bitcoin Gold	BTCD Bitcoin Dark	BTCoe Bitcoin OE
					
Block time	10 Minutes	10 Minutes	10 Minutes	60 Seconds	15 Seconds
Consensus	PoW	PoW	PoW	PoS/PoW	PoW/PoS
Scaling	Lightning Network	8MB Block	Segwit		Lightning, Sharding, Plasma
BTC Fork		✓	✓		✓
Privacy				zkSNARK*	zkSNARK**
Max supply	21 Million	21 Million	TBA	22 Million	21 Million
2 Denominations					✓
Minting	SHA256	SHA256	EquiHash	SHA256, PoS	Airdrop
Micro-payment ready					✓

* Komodo swap; ** To be implemented.

e) Important dates.

- Up to 210K BTCoe will be distributed via a bounty program for about 500 first contributed users. If you are reading this document, **the bounty program was already started.**
- The first airdrop program will begin on **Ethereum block #4574200 (~18-November)** with total 2.1 milion BTCoe will be distributed.

- We will do a semi-fork of bitcoin chain on **Bitcoin block #496330 (~30-November)**, bitcoin owner can claim their BTCoe from **15-December** with the ratio 1:1
- SAToe contract will be deployed in **mid-December**.
- **Feb-2018**: The second airdrop and faucet program for ETH owner will begin.

3. BTCoe bounty and airdrop program.

a) Bounty program.

We will distribute up to 1% of BTCoe total supply to users who contributed to our first step marketing. Bounty coins to these users will consist of two parts:

- Contributors who share our official announcement on the Bitcointalk forum to their Facebook and/or Twitter page as a public post.
- Contributors who helped us to translate this document to their language.

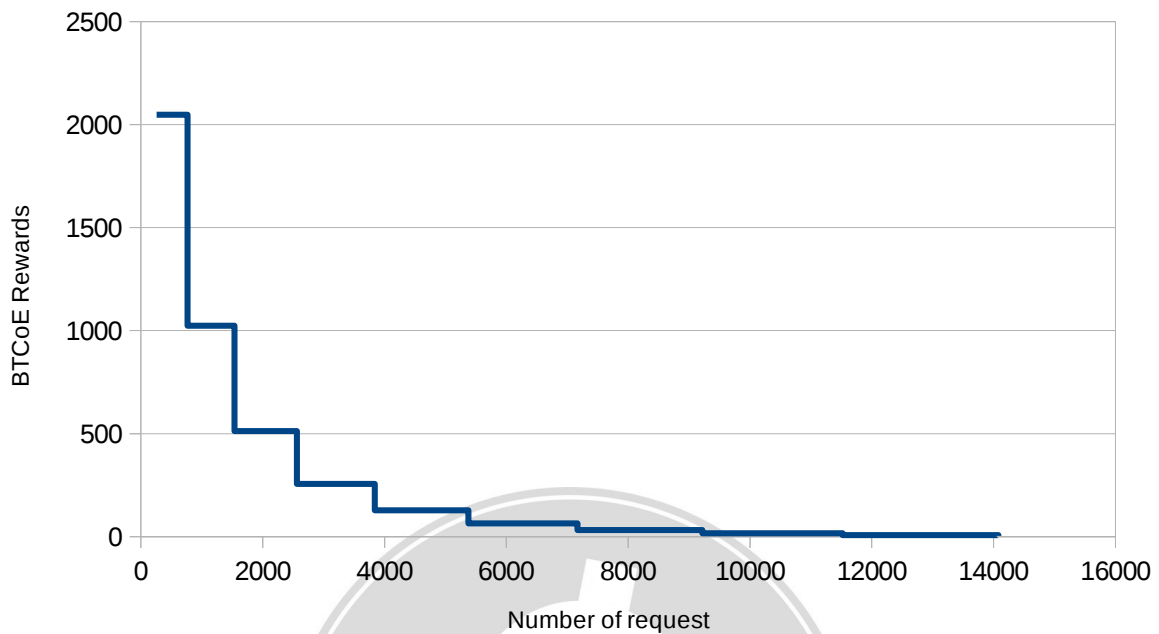
The distribution is based on a first-come-first-serve basis so please send us the information include your ETH address via our bounty form as soon as possible to receive your reward coins. Each accepted social share will receive **500 BTCoe (max 300 users)**, each user translated this document to a new language will receive **4000 BTCoe (max 15 users)**. Thank you for your contributions!

b) First airdrop program.

To ensure the anonymity of airdrop receivers, instead of distributing coins via a registration, we send it to you via a contract function. Airdrop coins are free, but you must pay for ethereum network transaction fee and processing fee (0.02 ETH). This processing fee was calculated carefully to avoid spamming over our contract and we only allow each ETH address to join this airdrop one time only.

You can join the airdrop-1 by sending 0.02 ETH to BTCoe contract, it will then resend BTCoe to your address. We do not accept any transaction below this amount or above 0.03 ETH, in those cases, your ETH will be returned to your address.

Airdrop-1 rewards start at 2048 BTCoe per request for first 256 users and decreasing to 4 BTCoe as you can see in the chart, max about 2.1 million of BTCoe will be distributed by this airdrop.



Drawing 5: Airdrop-1 distribution.

$$\text{SumAirdrop 1} = \sum (\text{HalvingCount} * \text{BTCoeReward}) = \sum_{i=1}^{10} \left(256i * \frac{2048}{2^{i-1}} \right)$$

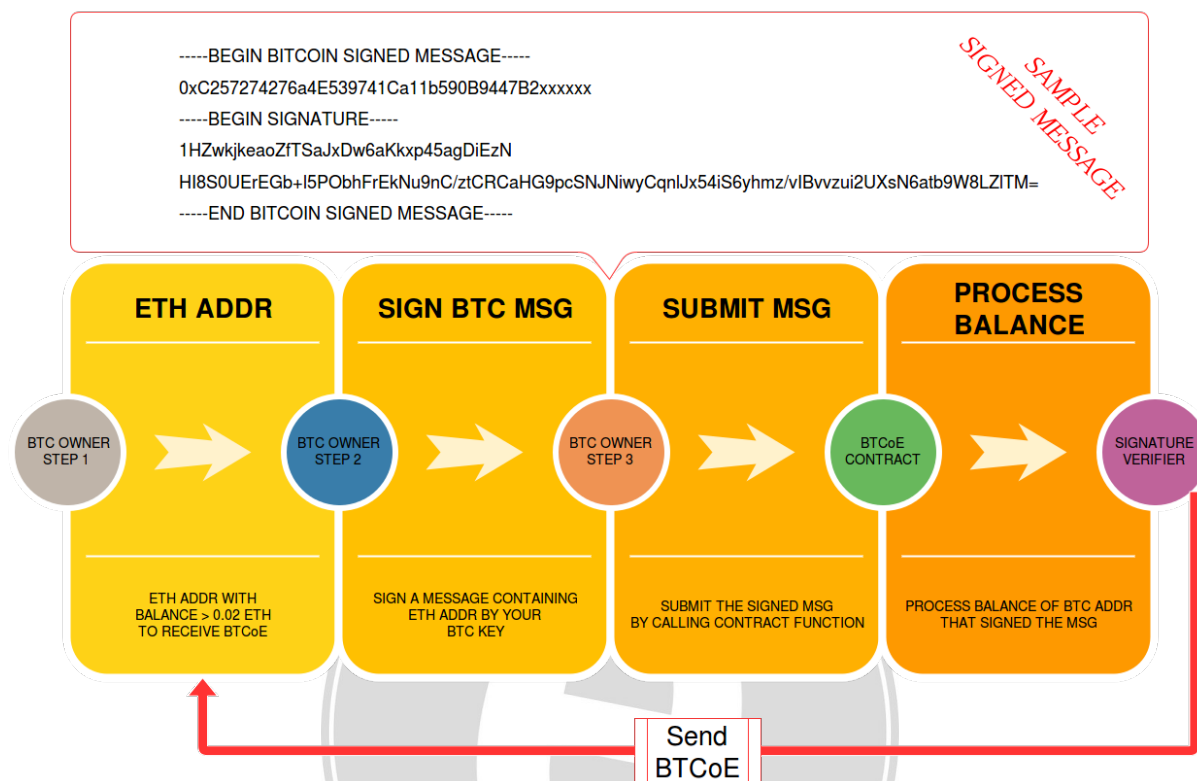
c) Second airdrop program.

Our second airdrop (airdrop-2) program will begin in Feb-2018 which will transfer the rest of 15% airdrop (~1 million BTCoe) to ETH owners base on the number of ETH on their account at that time, we will provide the exact block number one week before it starts. For this stage, we will distribute coins by SAToE instead of BTCoe and the users do not need to do anything to receive coins.

We also implement a faucet delivering SAToE to the users who want to test a payment or develop their own payment channel.

4. Claim BTCoe for bitcoin owners.

a) Overall work flow.



Drawing 6: The overall process of claiming BTCoe for BTC owners.

b) Detailed steps to claim your BTCoe.

- **Step 1: Prepair an ETH address with balance >0.02 ETH.**
- **Step 2: Use your BTC wallet to sign a message containing the ETH address from step 1. Please note that the message must be signed by the BTC address that you want to claim. The message must be generated in a correct format as you can see in this sample, replace three red line with your real information.**

```

-----BEGIN BITCOIN SIGNED MESSAGE-----
ETH ADDRESS (Step 1)
-----BEGIN SIGNATURE-----
BITCOIN ADDRESS (Step 2)
BITCOIN SIGNATURE (Step 2)
-----END BITCOIN SIGNED MESSAGE-----

```


Almost every BTC cold wallet have the message signing function, but may be in a different format. Please reformat it as the above sample.

You can recheck the message format by using <http://btcoe.org/checkmsg/> that perform two tests: Entire message format and signature verification. You are responsible for the ETH and BTC address correctness.

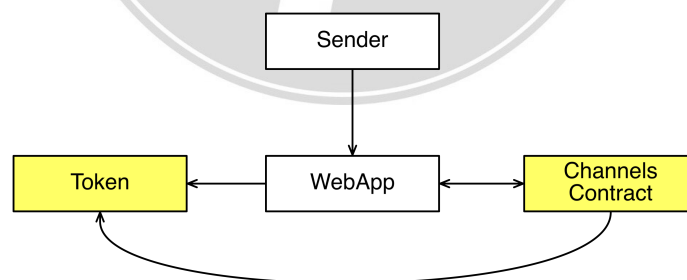
- **Step 3: Call a contract function to submit the signed message.** To do this, your ethereum wallet must support interacting with smart contract. Just as another contract call, we must add the contract address together with its ABI to the wallet and then call the contract function.

In our case, just call the contract function **ClaimBTC("fullSignature")** where fullSignature is your signed message above. Please also check on your favorite chain explorer to ensure that the contract function is executed successfully.

5. Satoshi oE micro-payment.

a) Micro-Raiden interactions.

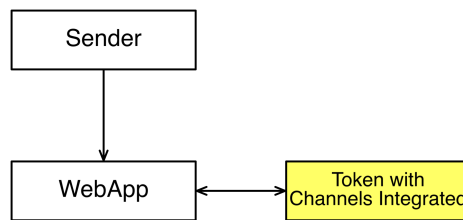
The μ Raiden channel contract is designed independence with the token contract so it very easy to combine with any ETH token to perform micro-payment. The overall interactions of μ Raiden can be seen as the following chart:



Drawing 7: Micro-Raiden Interaction

b) SAToE integrated micro-payment.

We integrated μ Raiden into SAToE contract to make micro-payment even easier, it also offers a lower transaction fee for channel opening and closing. The SAToE contract is currently under development, it will be deployed in mid-December so the swapping functions of BTCoe are not available until there.

Drawing 8: SAToE with μ Raiden Integrated

6. Our policies.

- a) **We do not make an ICO**, so the 0.02 ETH fee is not the price to sell these coins, that fee is for the anti - spam purpose and for the return transaction fee.
- b) **We only allow each ETH address to join first airdrop one time**, if you make a second transaction, your ETH will be returned and you will lose your transaction fee. In addition, we do not allow sending ETH from a contract address.
- c) This is the community oriented/driven project and you are welcomed to make a contribution. Just email us: satoe@btcoe.org.
- d) The second airdrop distribution will depend on your ETH balance regardless you have joined the first airdrop or not.
- e) On the second airdrop we will distribute SAToE instead of BTCoe.
- f) Coins can be exchanged between BTCoe and SAToE at any time by calling a contract function.

7. Conclusions

Our team is working hard to make the first BTC-ETH semi-fork possible. BTCoe is not only a token run on top of Ethereum network, but also offers many unique functions specifically designed for micro-payment such as a dual – denomination design, μ Raiden integrated. We hope that it will become a great cryptocurrency for all types of application over the Internet!