Fork Bitcoin

In this section we'll be creating our own blockchain application. We will be using the source code from Bitcoin Core. The software is a result of hundreds of developers over nearly a decade. Bitcoin Core contains many optimizations regarding decentralized networking, Denial of Service (DoS) prevention measures, as well as sync performance enhancements. In addition, Bitcoin Core is open source with an MIT license, so we are allowed to use the code free of charge. Learning foundational principles from this code repository will give you a solid foundation for blockchain application design.

Considerations

There are some considerations to make when creating a blockchain application. These customizations are meant to be educational, the actual customizations you make should take into account the tradeoffs. For example, hashpower on other networks can be used to attack smaller, newer networks, and this must be taken into account. There is more to blockchain than just the code and technology, the number and diversity of users (especially mining hashpower) will determine the balance of power and possibility of attacks.

Install Dependencies

```
$ sudo apt-get update
$ sudo apt-get install software-properties-common libssl-dev libevent-dev libboost-system-dev libboost-filesystem-dev libboost-chrono-dev libboost-test-dev libboost-thread-dev -y
$ sudo add-apt-repository ppa:bitcoin/bitcoin -y
$ sudo apt-get update
$ sudo apt-get install libdb4.8-dev libdb4.8++-dev -y
```

Setup

First, we need to fork the Bitcoin repository, so, go to https://github.com/bitcoin/bitcoin and click Fork at the top right. Once you've forked it, you can click clone to get the address. For me I'll clone the forked repo using:

```
$ git clone https://github.com/jbaczuk/bitcoin.git && cd bitcoin
```

Next, let's add the bitcoin repo as an upstream remote so we can pull updates later:

```
$ git remote add upstream https://github.com/bitcoin/bitcoin
```

Then, we will branch off of the latest release, let's call it `1.0`:

```
$ git checkout v0.17.0.1
$ git checkout -b 1.0
```

Now let's make sure we can build the project, and that we have all of the dependencies we need:

```
$ ./autogen.sh
$ ./configure
$ sudo make
```

Customizations

To customize our blockchain, we are going to make the following changes:

Branding

- Rename the project
- Change address prefixes

Networking

- Message prefix bytes
- RPC and P2P ports
- Seeds

Consensus Rules

- Coin Distribution
    - Max supply
    - Block rewards
    - Subsidy halving interval
- Block size
- Block time
- Activate BIPs
- Checkpoint data
- Genesis block
- Difficulty retargeting interval

Standards

- OP_RETURN data limit

Advanced Customizations

Coin Distribution

- Premine