Blockchain Notes

Josh Snider

March 24, 2018

1 Introduction

These are my notes from reading the *Blockchain Applications A Hands-On Approach* book by Arshdeep Bahga and Vijay Madisetti. A major goal of reading this book, is to write a blog post based on it, either as a review of the book or as a summary of topics it discusses.

1.1 Book Contents

The book starts with an overview of the blockchain and some application templates that can be done with it. It then goes to talk about Ethereum, including how to set up a development environment for it. It then goes to talk about services that can be built on the blockchain such as smart contracts, decentralized applications, mining, whisper, and swarm, before wrapping up with an overview of some more advanced topics involving the blockchain. The book requires minimal understanding of the blockchain on the part of the reader, but assumes a competency with programming. There's a companion website at blockchain-book.com that has downloadable copies of the source code used in the book.

1.2 About the Authors

Both of the authors are academics, Vijay's a professor and Arshdeep's a researcher. This book is actually part of a *Hands-On Approach* series which has already covered cloud computing and big data.

2 Blockchain Basics

The main idea behind the blockchain is to create a platform for handling transactions that doesn't depend on a central hub like banks. The first cryptocurrency using a blockchain was Bitcoin which was introduced in 2008 by Satoshi Nakamoto. Without a central authority, there needs to be a new way to prevent people from spending the same money more than once, the Bitcoin solution requires two things, every transaction being announced publically and a system for agreeing on the order of transactions. This ledger works as a chain of blocks or "blockchain" if you will. The process by which blocks are added is called "mining", it involves a node in the network collected the new transactions and then stamping its block with a proof-of-work. In order to incentivize "mining", blockchains routinely award money to the node who mines the block that gets added to the chain.

In 2013, Vitalik Buterin proposed a new type of blockchain network called Ethereum. The main idea is to have a single-programmable blockchain that could be shared by multiple applications as opposed to different cryptocurrencies having different blockchains. Each application takes the form of a "smart contract". Gavin Wood was the first to create a functional implementation of Ethereum in 2014 which included the programming language Solidity.

Each block has four fields, a timestamp, the hash of the previous block, the hash of the block itself (called a *nonce* value), and the hash of the root of the Merkle tree containing the transactions. This means the the block technically does not contain the transactions it has.

So, what are the core features of the block chain?

1. **Immutability** - Once a transaction is recorded in a block, it can't be deleted or altered unless a majority of nodes are conspiring to do so.
2. **No Central Authority** - This reduces the need for transaction fees and speeds up settlement times. Also, makes it impossible to regulate what people spend money on.
3. **Secure and Transparent** - Transactions are final unless a majority of miners collude to change them. The entire process by which blockchains run are largely specified in publically accessible white papers and implemented by open-source programs run by the public.
4. **Privacy** - While all of the transactions are recorded publically, the private key for each party is kept secret and there's no link between the public key and the identity of the transactors.
5. **Scalable and Available** - The blockchain is replicated amongst nodes to ensure, that even as they leave and join the network the blockchain is preserved.

3 Example Smart Contract

Let's consider an escrow contract between two people. The buyer deposits money in an escrow account, the seller then gives the buyer the item, and the escrow account releases the payment to the seller. This can be done in Solidity as a smart contract quite easily. I'm not going to rehash the example completely, but the key points are that contract accounts are different from user accounts, that distributed apps can be used to make nice interfaces to contracts, and that interactions with the contract are validated by miners on the blockchain.

4 A Blockchain Stack

Blockchain is good at maintaining all the transactions in a network, but it's not particularly good at storing large volumes of data or peer-to-peer messaging. That is Ethereum works as a decentralized computing network, but we need something else for decentralized storage, and decentralized messaging. The book recommends Swarm and Whisper respectively.

4.1 Decentralized Computing - Ethereum

Ethereum uses a virtual machine for its execution environment. This environment is called the Ethereum Virtual Machine (EVM), having each node in the network run the same calculation is not efficient, but is necessary to maintain consensus. Ethereum has two forms of accounts, one called Externally Owned Accounts for normal users and contract accounts whose behavior is controlled by associated contract code. You might be worried that letting people compute on the blockchain would bog it down with endless calculations, fortunately there is a solution. Senders are charged a gas fee which increases the more effort their transaction takes. Running on a virtual machine means that the programming language used can be anything as long as it can be compiled to the EVM bytecode.

4.2 Decentralized Storage - Swarm

Decentralized storage and content distribution network, works as a redundant store of Dapp code. Being peer-to-peer means it lacks a single point-of-failure and makes it resistant to DDoS

4.3 Decentralized Messaging - Whisper

Transient messages between Dapps, which works by subscribing to topics.

5 Blockchain Applications

Everyone loves technology, but only useful technology becomes as popular as blockchain. What are some of the fields that can use blockchain?

- FinTech
- IoT
- Industrial and Manufacturing
- Assets and Inventory
- Energy
- Supply Chain
- Records and Identity
- Healthcare

6 Conclusion

Write your conclusion here.