The Blockchain – UC Irvine

Course 1

Contents

[Required Reading: “Blockhain Basics” by D. Drescher 2](#_Toc54796449)

[Module 1 – Foundations of Blockchain and Digital Currencies 3](#_Toc54796450)

[The Internet of Money 3](#_Toc54796451)

[Blockchain Basics 3](#_Toc54796452)

[Vitalik Buterin Interview – Ethereum Co-founder 3](#_Toc54796453)

[Quiz 4](#_Toc54796454)

[Module 2 – The Need for Blockchain 5](#_Toc54796455)

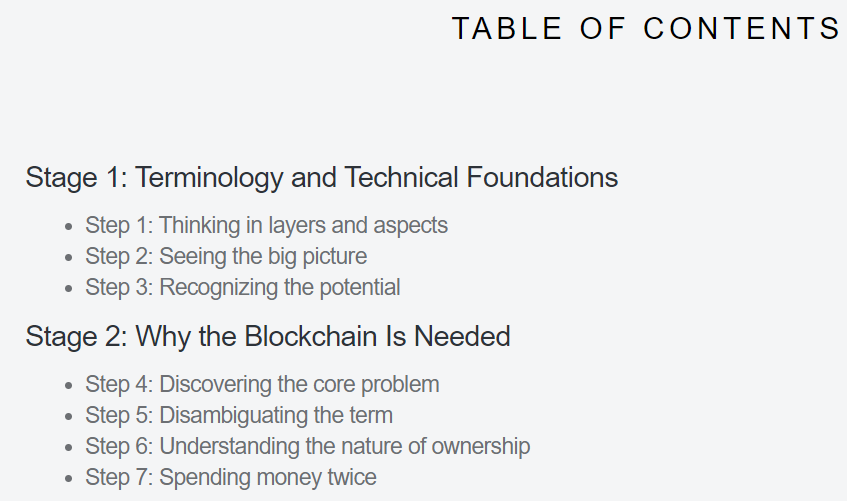
[Blockchain Basics (same as previous module) 5](#_Toc54796456)

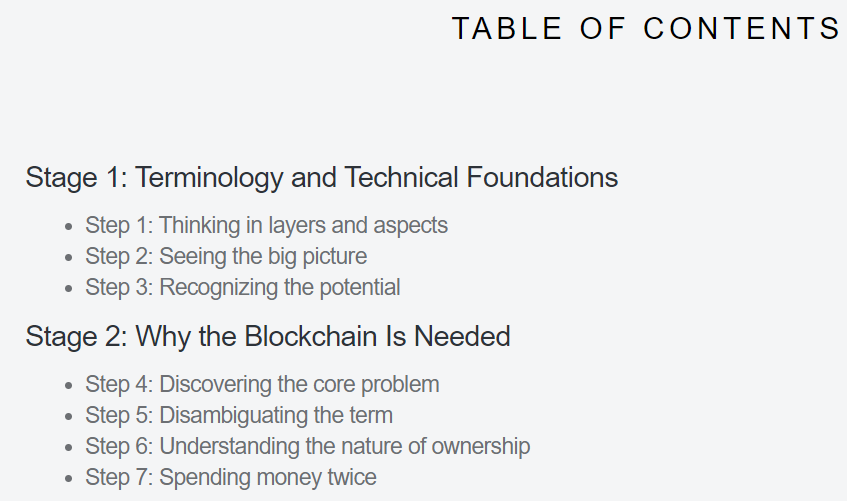
[Round Table Discussion - Blockchain and Digital Currencies 5](#_Toc54796457)

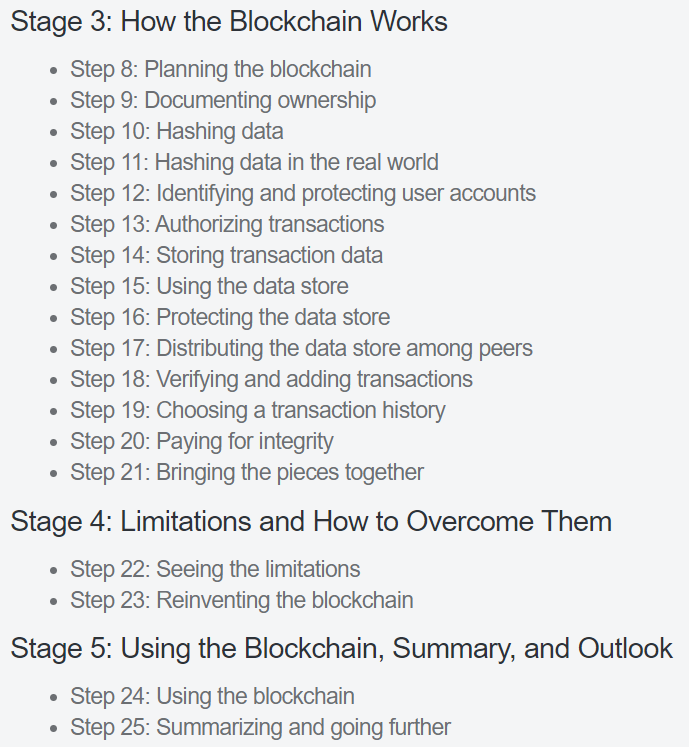
[Round Table Discussion - Blockchain as Protocol 5](#_Toc54796458)

# Required Reading: “Blockhain Basics” by D. Drescher

*This is book is required reading for the course, I will leave the Table of contents here*







# Module 1 – Foundations of Blockchain and Digital Currencies

**Learning Objectives**

* Identify key elements of the software architecture underlying the blockchain.
* Identify the characteristics of digital currencies and their prospect for the future.

### The Internet of Money

Consists in reading chapters 1-3 of “The Internet of Money Volume Two: A collection of talks by Andreas M. Antonopoulos”

https://www.amazon.com/Internet-Money-Andreas-M-Antonopoulos/dp/194791006X/ref=tmm\_pap\_swatch\_0?\_encoding=UTF8&qid=1559232641&sr=8-3

*will skip this, I doubt public talks have any content that I don’t already understand enough of*

### Blockchain Basics

Consists of reading steps 1-5 of Blockchain Basics: A Non-Technical Introduction in 25 Steps

<https://www.amazon.com/Blockchain-Basics-Non-Technical-Introduction-Steps-dp-1484226038/dp/1484226038/ref=mt_paperback?_encoding=UTF8&me=&qid=1559232841>

“This book bridges the gap that exists between purely technical books about the blockchain and purely business-focused books. It does so by explaining both the technical concepts that make up the blockchain and their role in business-relevant applications.”

### Vitalik Buterin Interview – Ethereum Co-founder

Decentralized applications = applications which can run without dependence on any particular or a central third-party.

“For years, I would just do stuff in Excel but then I started programming games and for that I would play myself in C++. Then at some point I discovered Python and JavaScript and I'm like, "Wait, why does anyone even care about C++ if these languages exist. "

*Why does Vitalik prefer Python:*

“I love the syntax and it feels very nice and pretty. It has a lot of features that just make stuff easy that really should be easy, like support for big numbers, support for array literals, just being able to make arrays and make mappings and dictionaries and so forth. Programs that just to work nice and clean and take 10 lines in Python just seemed always be three times harder in things like C++. Then in JavaScript, like it gets not having big numbers and then just like mixing up numbers and strings makes it clear easy to have bugs everywhere. I mean I do wish Python had some more strong typing but otherwise even still it seems like a nice middle ground.”

*How will Blockchain Compete with direct Acylic graphs (DAGS) and Hashgraphs?*

“So first of all, I personally really hate how the word DAG is just been over hyped. So first of all, a blockchain is a kind of DAG. The Ethereum 1.0 chain is a kind of DAG because of how ongoing collision works. Ethereum 2.0 chain will be even more of a DAG because of how you have the shorter chains and they keep on constantly cross-linking with each other. Then even within each one of the chains, every block has many attestations and then get included into the next block. So those are things that we are totally adopting. At the same time, it does seem like there is room for more innovation on the data structure side. But at the same time, it does seem like we are getting closer and closer to understanding what the optimum structures are. A lot of the possibilities for big improvements are things that I think have already been incorporated into quantity Ethereum consensus algorithms.”

*Advice for new blockchain developers*

“I would say if you're just entering the blockchain industry and first of all, it's important to just get a good idea of what the status quo is in terms of what people are working on, what things are possible at layer 1, what things are possible at layer 2, what things are possible from the point of view of applications, where researchers going. Part of the question also depends on what you see your personal specialty being. So are you a mathematician or a cryptographer, are you a kind of low-level developer, are you someone who is interested in working on things directly related to empowering people in Uganda, are you interested in solving user experience problems for millions of regular people and their space in the community for people of all types? But depending on that, you might have different focuses on whether you want to end up learning the finer grains details of how a zk-SNARK works versus the trying to understand more from a economic and business standpoints like what things the blockchains enable that were not possible without it. If you're doing that, then it's important to try to get your own good understanding of that so you can try to figure out what kind of blockchain application makes more sense more from first principles.”

### Quiz

“In Blockchain Basics, Daniel Drescher describes blockchain as a software system made up of two layers; application and implementation. The application layer is responsible for the user facing components, and the implementation layer refers to everything that brings the application to life, like protocols and code.”

# Module 2 – The Need for Blockchain

### Blockchain Basics (same as previous module)

*Consists of reading steps 1-5 of Blockchain Basics: A Non-Technical Introduction in 25 Steps*

### Round Table Discussion - Blockchain and Digital Currencies

*Nothing all that worthy of note-taking*

### Round Table Discussion - Blockchain as Protocol

*Nothing all that worthy of note-taking*

# Module 3 - Peer-to-Peer Software Systems, Trust, and Integrity

**Learning Objectives**

* Identify the characteristics of a peer-to-peer system.
* Identify the main functional aspects of the blockchain.

### Blockchain Basics (same as previous module)

*Consists of reading steps 1-5 of Blockchain Basics: A Non-Technical Introduction in 25 Steps*

*The most interesting part is the beginning of the video, the transcprit of that part is here:*

“Well, yeah. I think what we mentioned right from the start was more of a open source technology. We didn't mention the private blockchains and the reason for them to be out there and existing. Probably, it's again coming because the industry is very young and the enterprise still has specific needs that are not satisfied by decentralized. Probably, right now, the most concerning one is related to privacy and security. So that's why you would have Hyperledger and other things like that, which basically is a technology you can host it somewhat privately and use it or recently a couple of big-name companies they announced their own blockchains, they're going to support it. Even if you take the same Ethereum, Amazon is supporting running in AWS calls privately Ethereum network. It means it doesn't have to be public. So decentralization is one concept. Running it privately is a little bit differently. It can still be decentralized because they'll be running on AWS or any other Cloud provider in a decentralized way. They'll be talking to each other agreeing on consensus and so on. The whole difference is just to not be public, which means that it will be hosting some specialized solutions for that. The only thing that the concept of the blockchain provides is this distributed database for traceability. Where you have the transactions and then you read them and do whatever. In case of Ethereum, you also have a place where we can store business logic called Smart Contacts, but it's just a more fancy name for writing business logic for your business.”

“Yes, it doesn't satisfy still the full-scale of questions for the enterprises like making a basic HTTP request, which is cutting out a lot of use cases for the businesses and there are a lot more but still it's a way to do it on a distributed ledger. You have the possibility to execute code. So decentralized, centralized at the same time, so that's like one, they're different. The centralized, for example, can be Google, Amazon, Azure, and OpenShift or any other Cloud providers. Then you have the decentralized, which is the Ethereum. So we talk about the concept centralized and decentralized. Then there is still decentralized but private and which is can be the same open source technology running private Clouds, where you will not probably care much because if it's running in a private usual network, then you would not care so much about consensus being one. We would care about attacks because it's a controlled environment. So it's still decentralized but private. At the same time, it's becoming centralized because its running in one place. Nobody has access to it except one specific entity. So all these concepts they're really shifting into each other, depends how you look and what problem you're solving. It also depends, when you're talking about enterprise solutions versus completely public solutions like [inaudible] network. Yes. They have different requirements for, basically, attack factors, the different potential vulnerabilities that their network might have. Yeah. Right. Yes. So exactly for that reason there are other chain or technology provider for the next generation of blockchains, like Dispatch US and others. Who will allow a hybrid between what the private blockchain controlled environment will be running and the public technology stack to be run publicly and it will provide services from both sides. It'll be secure and encrypted at the same time it will be decentralized. So it's not actually centralized, running in a private data center, run publicly by everyone. Just you can keep different types of data and allow access based on encryption and all sorts of mechanisms for security, authorization, authentication and all that stuff. So this is something that doesn't exist yet, but it will be something normal in the next year or two.”

*Went over the Byzantine problem and double spending*

*Went over private and public keys and signatures*