BR.
THE BLOCKCHAIN REVIEW

Ethereum White Paper Made Simple

A guide to understanding the Ethereum white paper for people without an advanced degree in computer geekery

CONTENTS

WTF

Like its well-known forerunner, the Bitcoin White Paper, Ethereum's founding document has left most of us regular folk scratching our heads in utter bewilderment ever since its release in 2013. I mean common. WTF is going on, right?

Look at this:

> *The intent of Ethereum is to merge together and improve upon the concepts of scripting, altcoins and on-chain meta-protocols, and allow developers to create arbitrary consensus-based applications that have the scalability, standardization, feature-completeness, ease of development and interoperability offered by these different paradigms all at the same time. Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.*

That's a real excerpt from the Ethereum White Paper.

WTF?!

Yes, WTF indeed. But luckily for you, the Intrepid

Ventures team has heard your distress calls we're here to help. The confusion and frustration ends here.

Who should read this guide?

This guide will break down the Ethereum white paper so that anyone can understand what Ethereum is, how it works and the problems it solves. If you have a general idea about Ethereum but just can't seem to make sense of it all, this guide is for you.

By reading this guide, you will also gain a better understanding of the differences between Ethereum and Bitcoin and a clearer grasp of where Ethereum fits into the emerging blockchain/cryptocurrency story.

This guide is not for people with advanced knowledge of Ethereum nor will it make you an expert. With this in mind, we will be leaving out some of the more hardcore technical elements that are irrelevant to you gaining a fundamental understanding. We will also be expanding on some concepts where needed.

Why should you care?

That's easy. Ethereum has served to realize the broader potential of blockchain technology beyond bitcoin and first-generation decentralized applications. By offering a platform for developers to build any decentralized application, Ethereum opened up a world of unimagined possibilities. If you

want to understand the decentralized applications of today and tomorrow, you will need to get your head around Ethereum.

So if you can digest the central concepts in the Ethereum white paper, the broader decentralized revolution, which involves hundreds of different cryptocurrencies and other types of blockchain based decentralized applications will begin to make a lot more sense.

Prerequisite reading

For this guide to have maximum impact, you will need to have a basic understanding of Bitcoin and Blockchain, the underlying technology that enables it to operate. If you're unfamiliar with Bitcoin and Blockchain, read our Bitcoin White Paper Made Simple guide first.

Background

Since emerging in 2009, Bitcoin and its core operating technology, blockchain, have laid the foundation for a new era of digital peer-to-peer transactions.

But it would be years after the advent of Bitcoin that the true power of blockchain technology would be realized. In late 2013, Vitalik Buterin, an unknown Russian-Canadian programmer involved with Bitcoin and the crypto community released a white paper that changed the game.

According to Vitalik, the Bitcoin community was approaching blockchain technology in the wrong way. He believed that blockchain applications were being designed to do an extremely limited set of operations.

> *I thought [those in the Bitcoin community] weren't approaching the problem in the right way. I thought they were going after individual applications; they were trying to kind of explicitly support each [use case] in a sort of Swiss Army knife protocol.*

Bitcoin, for example, was developed solely to operate as a peer to peer digital currency. Developers were either required to expand the set of functions offered in existing applications (a time-consuming and challenging process) or develop an entirely new platform altogether. An equally time consuming

and expensive endeavor.

To overcome the technological limitations which were ultimately holding back the development of new blockchain-based applications, Vitalik and a small core team developed Ethereum - A Next-Generation Smart Contract and Decentralized Application Platform.

From humble beginnings, Ethereum has grown into a well known and widely used platform. Ether, the native Ethereum currency and Bitcoin's chief rival has dramatically increased in value. The platform has also been responsible for launching hundreds of other cryptocurrencies and decentralized projects in recent years through a new fundraising mechanism called an Initial Coin Offering (ICO).

What is Ethereum?
A next generation blockchain?

Like Bitcoin, Ethereum is a public blockchain network. They both rely on a blockchain to operate.

Think about the Internet. You can build lots of different applications on top of it like email, online shopping sites and Facebook.

Well, in a way, blockchain technology is a new type of Internet where you can build lots of different applications. Bitcoin and Ethereum are just two examples.

The major difference between Bitcoin and Ethereum, however, is their purpose. Whereas Bitcoin provides one specific function, peer to peer electronic Bitcoin payments, Ethereum offers a platform that enables developers to build and deploy other decentralized applications. You could, for example, build another Bitcoin type currency on Ethereum.

In a nutshell, Ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications.

As Vitalik states,

> *Rather than being a closed-ended, single-purpose protocol intended for a specific array of applications in data storage, gambling or finance, Ethereum is open-ended by design, and we believe that it is extremely well-suited to serving as a foundational layer for a very large number of both financial and non-financial protocols in the years to come.*

What's a decentralized application?

A decentralized application or Dapp for short, in this context, refers to an application that is built on top of blockchain technology. Bitcoin is a decentralized cryptocurrency application for payments, for example.

Decentralized applications run on a blockchain and benefit from all of its properties like immutability, security, tamper resistance and zero downtime.

Essentially any service could be turned into a decentralized application. The possibilities are endless.

> *Decentralized applications enable services we already have today, like payments, storage, or computing, but without a central operator of those services.*
>
> Adam Ludwin

The Ethereum evolution

Ethereum helped propel the decentralized application movement forward beyond Bitcoin and first-generation decentralized applications.

The start of the paper focuses on the movement toward next-generation decentralized applications or as Vitalik calls it, 'Bitcoin 2.0'. The paper also describes the Bitcoin protocol, its shortcomings and briefly introduces how Ethereum addresses these shortcomings.

What you need to know

In the immediate years following Bitcoin's emergence, new platforms were developed like colored coins, Mastercoin, Bitshares, and Counterparty in an attempt to offer a more advanced set of functions for users. The problem according to Vitalik was that these platforms were still very narrow in focus.

> *Up until this point all of the protocols that have been invented have been specialized, attempting to offer detailed feature sets targeted toward specific industries or applications usually financial in nature.*

While Bitcoin offered one specific application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments, and other Dapps like colored coins, Mastercoin, Bitshares, and Counterparty all offered a set of slightly more extensive features, Vitalik believed

this was not enough.

Although he believed that Bitcoin was indeed revolutionary and capable of its intended task, he thought it was not a particularly good foundation to build any other applications.

Vitalik noted that developers were using three limited approaches to building applications. They were either

- building a new blockchain, or
- using scripting on top of Bitcoin, or
- building a meta-protocol on top of Bitcoin.

These approaches all came with limitations.

> *Building a new blockchain allows for unlimited freedom in building a feature set, but at the cost of development time and bootstrapping effort. Using scripting is easy to implement and standardize, but is very limited in its capabilities, and meta-protocols, while easy, suffer from faults in scalability. With Ethereum, we intend to build a generalized framework that can provide the advantages of all three paradigms at the same time.*

So, herein lies the intent of Ethereum. To merge and improve upon the approaches outlined above thus enabling developers to build consensus based decentralized applications with greater ease.

The mechanics:
How does Ethereum work?

It's easy to claim that Ethereum enables developers to build whatever decentralized applications they want, but how does it actually achieve this?

Well, according to Vitalik Buterin,

> *Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.*

There's a lot to unpack here. Let's take a closer look.

What you need to know

Five main elements enable Ethereum to do what it does. You will need to understand each one, at least on a conceptual level. They include:

- Smart Contracts
- The Ethereum Virtual Machine
- Solidity
- Ether
- Proof of Work

What are Smart contracts?

You've probably heard this term getting thrown around for some time now. A smart contract is just a bunch of code that manages the exchange of anything of value from property and shares to information and money between parties. Smart contracts run on top of the Ethereum blockchain precisely as programmed and become like autonomous agents that execute when previously specified conditions are met.

> *Contracts in Ethereum should not be seen as something that should be "fulfilled" or "complied with"; rather, they are more like "autonomous agents" that live inside of the Ethereum execution environment (EVM), always executing a specific piece of code when "poked" by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables.*

In Bitcoin, for example, users can only make a simple demand like - send one bitcoin from Alice to Bob. In Ethereum, however, it's possible to create a contract that says send one ether to bob if the date is 25th October 2017 and Bob's current balance is more than 20 ether.

The cool thing about smart contracts is that they self-execute exactly as designed by their creators once certain conditions are met. And this is just a simple

example. Creating a smart contract with infinitely more complicated conditions is possible as well.

A smart contract, could, for example, facilitate the automatic transfer of ownership of a property after a number of critical conditions are met. All of this without any human involvement. Crazy!

That all sounds pretty impressive, right? But how does Ethereum enable smart contracts to run and execute?

The Ethereum Virtual Machine

Smart contracts are powered by the Ethereum Virtual Machine (EVM) and by Ether. The EVM includes a Turing complete scripting language which means that it can solve any computation problem.

The EVM turns Ethereum into a programmable blockchain, keeping all the smart contracts running on time and coordinating them with the rest of the network. In doing so, the EVM enables the development of potentially thousands of different applications all on the Ethereum platform.

What is Solidity?

Ethereum has its own programmable language called "Solidity" which is similar to JavaScript. It enables developers to write programs (smart contracts) on Ethereum and is designed to enhance the Ethereum Virtual Machine (EVM).

What is Ether?

In the Ethereum blockchain, instead of mining for bitcoins, miners work for Ether. Ether is a necessary element for operating the Ethereum network.

It's like a fuel that provides an incentive to ensure developers write quality applications and the network runs smoothly. Beyond a fuel that enables decentralized applications to run, Ether is also a tradeable cryptocurrency.

In Ethereum, Ether is used by developers to pay for transaction fees for services and storage on the network. Every computation on the platform as a result of a transaction has a fee, and the more you need to store the more is paid.

This is because computations and file storage place a strain on the network. So, fees are there to discourage developers from excessively using the network. Without fees to drive user's actions, the Ethereum network simply couldn't function. So, think of Ether like the crypto-fuel that powers the Ethereum network.

How are ethers created, who needs them, and is the supply unlimited?

Ether gets issued at a constant rate through the block mining process. This rate along with the total supply of Ether was decided during the 2014 presale.

- 60 million Ethers were purchased by in the 2014 crowdfunding campaign.
- Another 12 million went to the Ethereum Foundation.
- Supply is not infinite. A maximum of 18 million Ether are mined per year.
- Every 12 seconds, 5 ethers (ETH) are given to the miners that verify transactions on the network.

Developers who build decentralized applications (Dapps) on the Ethereum platform, as well as users who want to interact with smart contracts, will need Ether.

Proof of Work (PoW) - Reaching consensus on Ethereum

For a decentralized system like Ethereum to operate without any central intermediary, there needs to be a way for the network to agree about which transaction records are valid to deter any abuse of service attacks like spamming.

Like the Bitcoin network, Ethereum relies on Proof of Work protocol to reach consensus about which transaction records are the real deal. This is set to

change to a Proof of Stake (PoS) algorithm called Casper, but don't worry about that for now.

Proof of Work aka mining is performed to facilitate transactions on the Ethereum blockchain and discourage bad actors from spamming the network by sending out fraudulent or illegitimate transactions. It requires miners (members in the network with high levels of computing power) to prove that a specified amount work has been completed.

This involves miners solving complex mathematical puzzles that are difficult to solve yet easy to verify. The process demands lots of expensive computational effort (lots of hardware equipment and electricity usage) as miners use expensive computer equipment to repeatedly and rapidly guess answers to a mathematical puzzle until someone wins.

Because these mathematical puzzles require so much work to solve, fraudulent transactions become infeasible. They are just not worth it!

Only blocks that contain the answer to the complex mathematical problem will be accepted and added to the Ethereum blockchain. This occurs every 15 seconds, on average.

Miners that successfully solve the PoW puzzle receive a reward of Ether. As Ethereum does not have a central issuer of Ethers, this is also how new Ethers are created.

What can Ethereum be used for?

Until the advent of Ethereum, it was challenging to develop new Dapps. But thanks to Ethereum, developers can build and deploy all sorts of decentralized services.

While it seems like the only actual real use case to date has been issuing ICO's deployed with Ethereum smart contracts, there are potentially thousands of other applications that could disrupt hundreds of industries like finance, academia, real estate, insurance, healthcare and the public sector.

While we will only include a few examples in this guide, this is just the beginning. Potentially, any intermediary type service in the real world today could be redesigned using Ethereum.

The white paper splits use cases into three main categories.

- Financial applications - "This includes sub-currencies, financial derivatives, hedging contracts, savings wallets, wills, and ultimately even some classes of full-scale employment contracts."
- Semi-financial applications - "where money is involved but there is also a heavy non-monetary side to what is being done; a perfect example is self-enforcing bounties for solutions to computational problems."
- Non financial applications - "applications such as online voting and decentralized governance that are not financial at all."

Token Systems

These have many applications such as

- Sub-currencies representing assets such as USD, gold, company stocks
- Individual tokens representing smart property, secure unforgeable coupons, and even
- Token systems with no ties to conventional value at all, used as point systems for incentivization (reward systems)

Financial Derivatives

The trading of financial derivatives is currently quite an involved process with paper and computer document based contracts being sent back and forth between parties. Ethereum smart contracts automate the processes involved in derivatives trading by automatically executing the terms of a contract when certain conditions are met. With blockchain enabled smart contracts derivative trading far more secure and efficient.

Identity and Reputation systems

Identity creation and management applications can enable individuals or governments to manage digital identities with unprecedented privacy and safety. They can also increase the control individuals have over their identities. Imagine - digital identities, passports, e-residency, birth certificates, wedding certificates and more stored on a blockchain instead

of company or government servers.

Decentralized File Storage

Decentralized cloud storage networks that enable users to transfer and share data without reliance on a third-party storage provider. By removing the central controls, many of the traditional problems like data failures and outages, security and privacy breaches and high user costs can be avoided. Users also gain control over their data.

Decentralized Autonomous Organization (DAO)

Ethereum can potentially be used to build all sorts of different decentralized applications. This one might just be the craziest of them all.

Even an entire organization can be decentralized.

Welcome to the world of decentralized autonomous organizations (DAOs). A DAO is a decentralized organization that has no leader and is purely run by smart contract code. Instead of the rules and enforcement of these rules being carried out by people, rules are determined and enforced by code. There is no need for employees to govern or documents or any centralized control. DAO's leverage smart contracts on the Ethereum blockchain so that anyone, anywhere in the world can be empowered to participate. In exchange for their early help, participants receive DAO tokens

which represent ownership in the DAO and the right to vote on proposals for the funding of Ethereum blockchain applications.

How is a DAO created?

In a nutshell, the process is as follows. A group of people writes a bunch of code (smart contracts) that will run the organization. There is an initial funding period where people purchase tokens that represent ownership - ICO, Initial Coin Offering. After funding, the DAO begins to operate, and proposals are made and voted on about how the money should get spent.

You made it

Congratulations, that's it, you've reached the end! We hope this guide has provided the clarity you need to move forward with your learning.

You should now have a solid conceptual understanding of Ethereum and its important place in the evolution of blockchain based decentralized applications. The future is exciting. Maybe you can develop a Dapp on Ethereum that will change the world.

BR.

About Blockchain Review

The Blockchain Review provides curated insights from industry insiders on cryptocurrency and blockchain technology, and how it's impacting business and society. Find simple and easy to understand advice for founders, developers, and investors, on how to startup, grow, and succeed in a changing world shaped by emerging technology and innovation.

Visit www.blockchainreview.io