Bo
Blockchain developer, engineer, entrepreneur.
Aug 30, 2017 · 13 min read

Cracking the Ethereum White Paper

"The World Computer"

Hi there,

I'm Bo, I read cryptocurrency white papers so you don't have to.

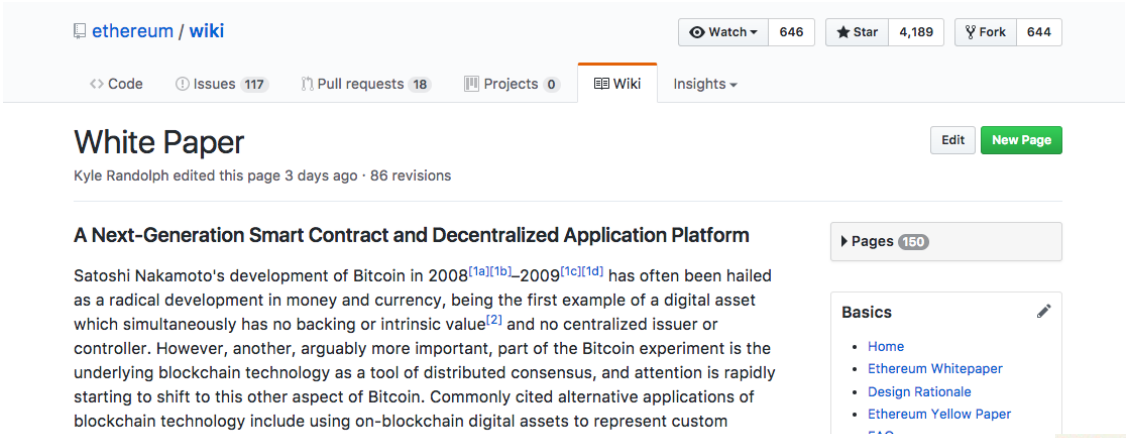
There's just something about reading white papers that turns a lot of people off. If it turns you on, I strongly recommend reading the Ethereum white paper. In it, Vitalik Buterin describes the Bitcoin protocol, it's shortcomings and how Ethereum addresses them as a "next generation smart contract & decentralized application platform".

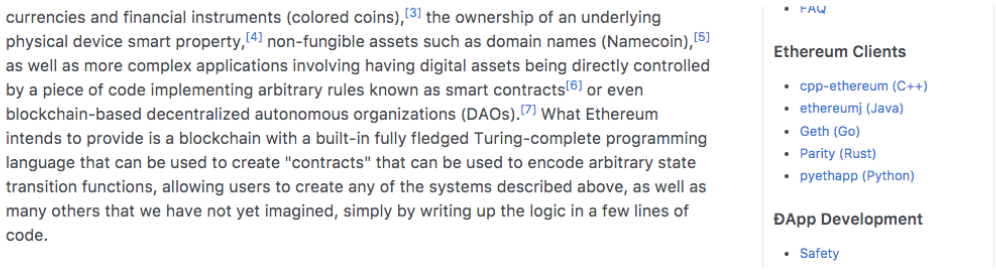
I know it's not immediately obvious how a "smart contract" can help the average person. So before we begin, let's make it so with a brutal oversimplification.

Imagine you have a website that beautifully conveys all your company's information in a precise and well thought out fashion. Now imagine all your customers demand you send them the same information via plain text email. Email is great, but conveying sophisticated information just can't be done via plain text. It would be slow, inefficient and grossly incomplete. The scary part is that you'd happily have done this a few years back before knowing websites were possible.

With cash, you directly express simple transactions i.e. payments, but you require intermediaries such as banks, brokers, and investment managers for more nuanced ones (e.g. your credit card, overdraft limits and investment portfolio). Through smart contracts, you can directly and independently express any of these complicated transactions. In fact, you can be your own investment manager, banker, broker and currency issuer if you choose. Profound as it sounds, this barely scratches the surface of what smart contracts on Ethereum can do.

And smart contracts are only half the story.




currencies and financial instruments (colored coins),[3] the ownership of an underlying physical device smart property,[4] non-fungible assets such as domain names (Namecoin),[5] as well as more complex applications involving having digital assets being directly controlled by a piece of code implementing arbitrary rules known as smart contracts[6] or even blockchain-based decentralized autonomous organizations (DAOs).[7] What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

- FAQ

Ethereum Clients

- cpp-ethereum (C++)
- ethereumj (Java)
- Geth (Go)
- Parity (Rust)
- pyethapp (Python)

ĐApp Development

- Safety

Title: “A Next Generation Smart Contract and Decentralized Application Platform”

Author: Vitalik Buterin

Published: November 2013

Reading duration: ~60 minutes

Readability Score: %

To fully understand the implications of this ambitious project it is important not to overlook the unique circumstances under which Ethereum was born. We’ll need to take a closer look at the Bitcoin protocol and the aftermath of its release—situations that inspired the Ethereum project.

After that, I’ll use the white paper to walk you through Vitalik’s motivations, Ethereum’s quasi-Turing Completeness, the Tragedy of the Commons and the ambitious potential of The World Computer.

What is Ethereum?

Like its predecessor Bitcoin, Ethereum is a protocol (rules for information exchange) and community. Community members transact with the native currency called Ether or “ETH” which is necessary for gas payments—more on gas in a bit.

Naturally, Ethereum inherits the censorship resistant, tamper-proof, economically secure and decentralised nature of Bitcoin’s consensus process. Censorship resistant as transactions can be created and signed offline then issued secretly and remotely. Tamper-proof because each new block (group of transactions) is referentially embedded in every consequent block creating an unbreakable chain of references all the way to the first block. Economically secure because of the negative incentives for nodes, especially miners (those doing the Proof of Work), to game the system. Ethereum builds on these to go a few steps further.

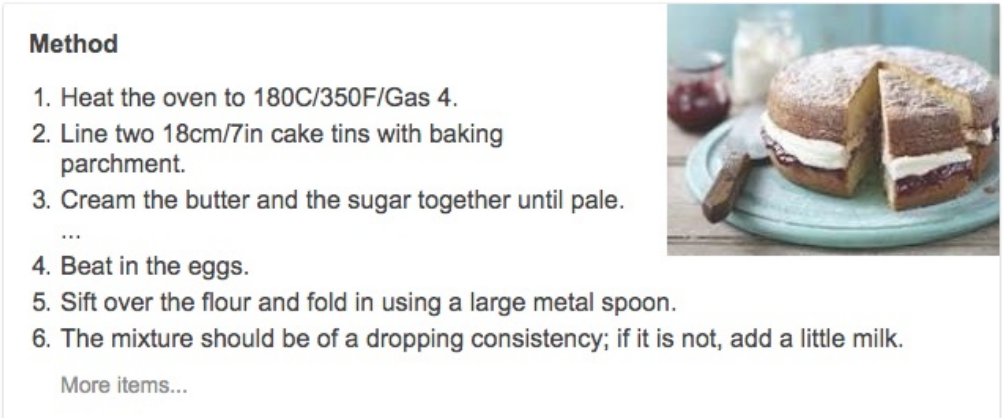
Read more about Bitcoin & blockchain-based platforms in my previous article —Cracking the Bitcoin Whitepaper.

A closer look at Bitcoin

Let’s quickly take a look at one important element of Bitcoin that Ethereum builds upon.

Bitcoin records each of its blocks as a list of transactions. Each transaction is a software

instruction to be executed by nodes (computers) running the Bitcoin protocol. So think of a block as a list of instructions to be executed in order—Just like a you'd execute a cake recipe.



BBC food sponge cake recipe. yum

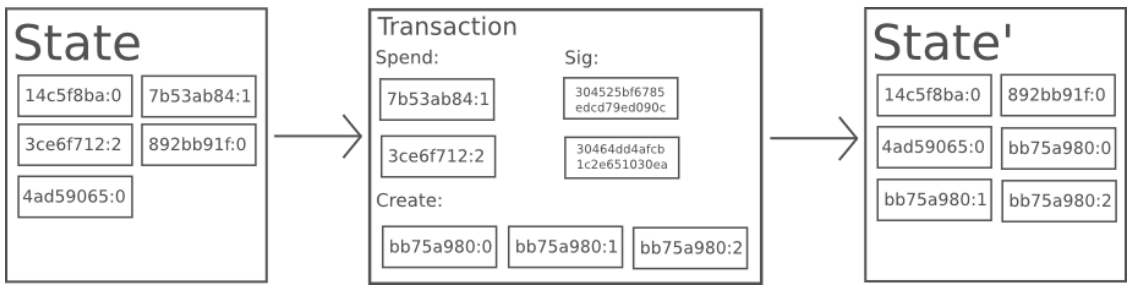
The Bitcoin client understands only one language, so all transactions must be made of instructions from that language. When you spend Bitcoin, your software/website writes this for you! Developers can also write custom contracts for special purposes.

So if a block is a cake recipe, then what's the cake? This is something we call the "state". In the case of Bitcoin, this state is just a list of "coins" available for use. Each coin has an owner and an amount. So all nodes have identical state (an identical list of available coins) and each new block is a set of instructions on how to edit the state by deleting & adding coins.

An owner spends a coin by referencing it in a transaction. So a basic transaction looks something like this attestation:

"I, **User X**, own this **unspent** coin [proof: **signed** coin reference showing coin is part of state/list] so please **delete** it and **output** a new coin (into the state/list) owned by and signed for **User Y**".

The above transaction deletes the old coin and produces a new coin that User Y can now reference in a later transaction. Remember, each block is a list of such transactions with varying degrees of complexity. Hence each block produces a new state. Vitalik thus describes Bitcoin as a "state transition system" and proposes a new system and a new method to perform the transitions. We'll explore the power of this new transition system after taking a look at why it was proposed in the first place.



Example Bitcoin state transition diagram from the Ethereum white paper

Finally, a "coin" is known as an Unspent Transaction Output or **UTXO**. Don't let any Bitcoiners catch you calling it a coin! Each of these UTXOs can have multiple input signatures (previous owners), multiple outputs (current owners) and an arbitrary number of Bitcoin. So "coin", implying a fixed amount with one owner is a pretty poor analogy…

Vitalik's Motivations

Vitalik, creator of Ethereum, has been described as many things—"genius alien" being my favourite and probably the most accurate. He describes the moment he thought of Ethereum as "too good to be true" but for others in the community, it probably was no surprise. The guy was already a main player in Bitcoin by 2013 having authored a Bitcoin code library, contributed to Bitcoin's core development and co-founded Bitcoin magazine. Naturally, he had already exposed himself to a wealth of research in mathematics, cryptography and economics—because that's just what 19-year-olds did in 2013?!

Vitalik's research brought him to the conclusion that several applications for some kind of shared identical database had already been established and were waiting for a sound infrastructure to be built upon. Why not use the blockchain?

In the white paper, he cites at least three new applications trying to do just that. Namecoin, coloured coins and meta-coins. All of which either exist on the Bitcoin blockchain—difficult to do—or bootstrap an independent blockchain—darn difficult to do. Plus it looks like most future applications will be too small to warrant their own blockchains.

> *"Additionally, we predict that the set of applications for decentralized consensus technology will follow a power law distribution where the vast majority of applications would be too small to warrant their own blockchain, and we note that there exist large classes of decentralized applications, particularly decentralized autonomous organizations, that need to interact with each other."*

Say we stick with option A—build applications on Bitcoin. We need to build an application by creating special transactions on the network. Remember how we described a transaction as an attestation that deletes a coin to produce a new one? Let's try creating a more complex attestation.

"I, **User X**, own this **unspent** coin [proof: **signed** coin reference] so please **delete** it and **output** a new coin owned by and signed for **User Y** at time **10/08/2019** if presidential candidate **Z** wins the election".

You may recognise this as a bet. Unfortunately, this is much easier to articulate in words than in Bitcoin's language. Good luck translating. Here lies the problem and as it turns

out, this problem is also a feature—but more on that soon.

The problem is that Bitcoin's language makes it difficult to describe complex transactions. Also, Bitcoin blocks are capped at 1Mb. Therefore, users will pay higher fees to incentivise miners to include their transactions sooner. Since a transaction can't be bigger than a block (transaction size is capped too anyway), the higher the demand for block space, the more users will pay for space to issue larger (and more complex) transactions. Transactions also cannot reference other transactions meaning they hold only their own information—they are siloed.

Vitalik would later argue that these properties made it difficult (not impossible) to create the applications that had been waiting patiently for Blockchain technology to arrive.

> *"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 an alternative framework that provides even larger gains in ease of development as well as even stronger light client properties, while at the same time allowing applications to share an economic environment and blockchain security."*

Vitalik proposed updates to the Bitcoin protocol, but they were met with much opposition. And rightly so! Making complex untested protocol changes to Bitcoin is like changing the engine of a moving car—it might end badly.

Vitalik then went off to research, propose & eventually create Ethereum alongside other brilliant minds such as Gavin Wood & Joseph Lubin, present CEOs of Parity Tech & ConsenSys.

Ethereum's quasi-Turing Completeness

> *"The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of tradeoffs" … "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."*

The most significant difference between Ethereum and most other blockchains is its language. It is Turing Complete. In a non-technical nutshell, this means a short transaction describes either a simple or complex series of operations. It's not possible to tell which one by looking at the transaction's size. Remember Bitcoin users will pay

more on average for larger transactions? Well, this effect means attackers can't issue complex transactions to slow down the blockchain. Because Bitcoin's language is not Turing Complete (intentionally), transaction size grows with complexity. So a cap on transaction size will thwart attackers (to an extent) and hopefully prevent excessive waste of blockchain processing effort. This inherent vulnerability of complexity is the most obvious "tradeoff" between Bitcoin and Ethereum.

Pay attention, because this point is important.

Bitcoin limits the power of smart contract developers to protect the blockchain from developer error & attackers—a common pattern in programming platforms. It's not obvious to me that Satoshi Nakamoto invented Bitcoin for much other than storing and transferring value, so it seems like the right choice. Why let developers wreak havoc?

Ethereum hands over the power (most, not all) to developers. Again a smart choice, given the purpose of the platform, but with great power comes great responsibility. And as we saw with the Parity hack & the DAO hack, the developers using this nascent technology still have much to learn about the platform. This isn't news, fortunately. Ethereum has been around for only three years so it might be a while before developer best practices are tried and tested.

Best practices might thwart contract attackers, but not spammers who try to slow down the blockchain with complex transactions. We will see how placing a new limit on complexity in the Turing Complete environment avoids this tragedy of the commons.

The Tragedy of the Commons

Before looking at how Ethereum solves this potential abuse of the shared blockchain resource, let's quickly recap. Every computer on the blockchain runs through the transactions (instructions) in each block to identically modify the state of its own copy of the blockchain.

Large transactions in a non-Turing Complete language (Bitcoin) imply more processing power required from the computers carrying out the transactions. Bitcoin limits the transaction and block size meaning this is not a problem.

Ethereum's language is Turing Complete so an attacker can issue a tiny and seemingly harmless transaction that takes an infinite amount of time to execute. Fortunately, Ethereum protects its blockchain from misuse through gas payments.

Gas

To issue a transaction, one must pay gas—an amount of gas proportional to the computational effort required to execute it. Miners (nodes that assemble blocks) will reject any transaction that does not pay enough gas as fees, keeping the insufficient gas for themselves.

Here's an analogy that helped me get my head around this one. You call a cab, and on the phone, you get to specify the meter rate (how much you'll pay per minute) and your limit (how much cash you'll bring with you). If the meter reaches your limit before you

limit (how much cash you're bring with you). If the meter reaches your limit before you arrive, the cab driver kicks you out, takes all your cash and teleports you back to your starting point. The meter rate is called the gas price and the limit is the gas limit. Fortunately, if you're a regular user, your wallet software will estimate the gas for you. Attackers, however, might find that they make no progress and run out of gas rather quickly.

Separating gas from ETH prevents gas from being subject to price fluctuations. You can't buy or sell gas as it has only one purpose. Also, every possible instruction (each opcode!) has a predefined and constant gas cost. This means the same transaction will always cost the same gas. However, the conversion rate between ETH and gas can fluctuate with the price of ETH to keep fees stable or to allow miners cherry-pick transactions when there is pressure on them to process more and faster. The latter is an unfortunate consequence of the transaction fees solution to the Tragedy of the commons. Research into better alternatives is ongoing!

That's not all

Ethereum also introduces better accounting. Most blockchain wallets keep track of all UTXOs that belong to a user (think counting coins in a purse), while Ethereum wallets can simply look up an account balance stored and updated by the blockchain (think checking your bank balance). In Ethereum, this list of accounts is its state.

Ethereum's blocks include not only this list of accounts and associated information, but also a record of transactions made (similar to Bitcoin) and a list of receipts created by those transactions. Each of these lists is updated with every finalised block, producing a dense audit trail useful for external verification.

Vitalik later explains how Ethereum also takes steps to further prevent mining centralization through Application Specific Integrated Chip (ASIC) resistant mining and an enhanced consensus protocol. To get a handle on those, you'll need to have a look at the paper yourself!

The World Computer

By using Ethereum, you pseudonymously pay the decentralised and arbitrary owners of computing power to execute instructions on an immutable, uncensorable and fully secure database of information shared with the entire network. Full anonymity is also on the way with the introduction of zero knowledge proofs.

So using Ethereum might sound familiar to you. To me, it sounds like the current internet—Where I pay the owners of cloud services or bandwidth (Godaddy, AWS & BT) to serve customers or browse websites. Sites where I inadvertently give up private information as an identifiable and censorable customer of a usually centralised platform. I do this in exchange for access to siloed and un-auditable information over several insecure networks ripe for snooping and identity theft. But now I can say bye to most of the above.

One could say that's an unfair comparison. Cyber-security and distributed systems were not as well researched and understood when the internet was first conceived at CERN

not as well researched and understood when the internet was first conceived at CERN. In fact, the immense body of knowledge that is Cryptoeconomics has only begun to take hold. It would be arrogant of us to assume that we've figured it all out and that Ethereum will be the last iteration of the internet. That being said, I have no doubt it will be the next.

So what is Ethereum really? In my previous article, I explained that Bitcoin acts as a trusted store of and means of transmitting value. I like to think of Ethereum as a means of transmitting value but also a trusted store for complex and **shared** interactive information and software. Understanding it is tough, but the reward might just be worth your time.

That is exactly why early-adopters are rushing to figure out what killer applications can be built on this magic box. The first killer app was meta-coins—several new currencies have been built on top of Ethereum with minimal effort. The next killer app is Initial Coin Offerings (ICOs)—a decentralised crowdfunding methodology that has resulted in an estimated $1.3bn in ETH invested in prospective companies… And probably some scammers too. Remittance, decentralised storage and decentralised casinos are on the radar too; even decentralised social travel! But I'm most excited about owning my identity online with uPort. That one's been a long time coming for me.

Ethereum was built to support these cryptocurrencies, but it looks like it might also be able to support other blockchains as Joseph Poon recently proposed with plasma. This along with Ethereum's upgrade to Metropolis and impending transition to Proof of Stake might just provide an unprecedented boost in both scale and speed on the network. These much-appreciated upgrades will be the backbone for the decentralised protocols for projects such as server-less cloud hosting being led by the Ethereum Foundation.

As you can see, the Ethereum community is moving at a breakneck speed just three plus years after the technology's inception and there's no sign of slowing down. I'm pretty confident this technology will change the world as we know it soon enough. Not because I think it has magical powers, no. But because of the levels of raw talent and mental horsepower devoted to it. Ethereum attracted some of the best possible minds from the beginning. People like Gavin Wood, Joseph Lubin, Nick Johnson and many others are working hard to build a community of Ethereum users, developers, participants and leaders in the space. Whole companies have been built to improve Ethereum and aid its evolution and ensure it stays on track so we can build the new internet on top of it.

You must realise by now that blockchain is much bigger than just currency. Like Andreas Antonopoulos said—Currency is only the first application. So don't worry about the price of ETH or whether or not there's a crypto-bubble. Invest in your knowledge of the space so you can contribute. And get ready for the decentralised web!

Find me on twitter @bo_ogunlana to let me know what projects excite you most and what white paper to crack next.

Thanks for reading and remember to share.

Thanks to Corey Petty.

Ethereum Blockchain Smart Contracts Cryptocurrency Bitcoin