Table of Contents

Authors

Blockchain Basics: *A Curated Collection* grew out of a community of across ConsenSys who have been writing about blockchain and Ethereum since the founding of ConsenSys. A huge thanks to the entire ConsenSys team for helping develop this guide. The following individuals were especially key in writing, creating, inspiring, and/or editing the content that appears in this book, and they are listed in first name alphabetical order:

Aditi Sriram - Business Strategist, Project Manager, ConsenSys Academy

Akshi Federici - Executive Director of Strategic Projects and ConsenSys Academy Global Lead

Andrew Keys - Co-Founder, ConsenSys Capital

Dr. Christian Lundkvist - Decentralization Generalist, Co-Founder uPort, ConsenSys

Daniel Finley - Lead Developer on MetaMask

Hadrien Charlanes - Founder of VariabL

Ilan Ben-Brith - Technical Program Manager, ConsenSys Academy

John Lilic - Managing Director for Global Business Technology Development, Strategy and Operations, ConsenSys

Joseph Lubin - Co-Founder of Ethereum, CEO of ConsenSys

Jesse Grushack - Co-Founder of Ujo Music

Joseph Chow - Software Developer, ConsenSys

Joshua Crites - Tecchnical Content Developer, ConsenSys Academy

Matt Liston - Founding Member, Gnosis

Mayowa Ojo - Product Designer, ConsenSys Academy

Paul Kohlhaas - Director of Business Development, uPort

R. Tyler Smith - ConsenSys Energy

Rene Nayman - Government Affairs and Policy, ConsenSys

Simon de La Rouviere - Engineer of Societies, ConsenSys

Thomas Hay - Product Manager, ConsenSys Academy

Tori Adams - Leader of US Government Practice, ConsenSys

Will King - Project Manager, ConsenSys

Yunyun Chen - UX Designer, ConsenSys

Blockchain Basics

This guide will help you develop a mental model of blockchain technology in order to help you understand its impact on society and business. By the end of this book you should have basic knowledge of the underpinnings of blockchain technology, specifically the Ethereum blockchain.

This guide does not have to be read start to finish. Rather, it is an index of subjects which you can reference to get an understanding of certain concepts. The blockchain industry is a collaborative one, and as such, this guide will cite materials both internal and external to ConsenSys. We believe these materials are key in pushing the discussion further than the limitations of this book.

Is this guide for me?

This guide is designed for anyone who is looking to wrap their head around blockchain technology, how it works, and how it could affect the world around them.

If you have a more technical background, such as a developer with experience building software, please look out for our coding based offerings, which cover setting up the developer tools and building on top of the Ethereum blockchain.

What this guide is not

This guide is not how to set up a wallet and start buying and trading cryptocurrencies. It does not give you advice on which cryptocurrencies to buy.

Overlapping resources

Because this guide is an introduction to key concepts, there will be times when sections might overlap in content or scope. This guide was written to explain blockchain simply and concisely, so many ideas will be repeated. There are links to additional information to offer different mediums of communication (video, for example) to fit diverse learning styles. It is suggested that a complete beginner read all of the sections of this guide. Going over the topics in multiple sections can be a good review of material and are presented using different examples. However, how you use this guide is up to you, and if you ever encounter a topic you feel you are already familiar with, feel free to skip it and move on.

Updates

Due to the nature of this ever growing and changing space, purchasers of this book will get updates via the publishing platform when they are available. This will allow you to keep up to date about what is going on. We will also include relevant information about in-person or virtual discussions of topics within the book and how those will be facilitated.

How to Ask Questions, Comments, and Raise Concerns

First of all, thank you for wanting to engage with us! One of the things that makes the Ethereum community so wonderful is their willingness to collaborate to make wonderful tools for learning. Interacting with you will help us improve our products.

I found a link that does not work, or a citation that leads to outdated information.

Sadly, times slows for no one. Products break, code does not compile, and our documentation becomes progressively outdated. If you find a citation or link that fits this description, please do the two following things:

First, report the issue on the publishing platform. Second, if you have the time (and want to do a good deed for others who purchased the book) and find where that citation has moved to, you are more than welcome to let us know via this form, and we will push out an updated version of the book to all purchasers periodically.

I want to you to add a page/want you to add more detail.

Please let us know what information you want more detail on. As we hear from readers, we can push updates to this book to include more detail or clarity. We hope you will find this update feature useful, and allow you to continue to engage with the book over time.

I have a question, comment, or a concern

Please fill out this form, which will alert the team of your inquiry and we will respond promptly as we work to address your inquiry.

We are happy to accept all worthwhile submissions! Cheers!

What's the Big Deal?

You keep hearing about Bitcoin and cryptocurrencies via the news, social media, and even late night talk shows. Considerable amount of newspaper and magazine space has been dedicated to articles about the rise of cryptocurrencies. There have been profiles of individuals who are movers and shakers in the space - Bitcoin millionaires, crypto-nomads, and people who only use cryptocurrency. Strong opinions on cryptocurrencies are being expressed and there are claims that blockchain will change the world. What is going on here? Did you miss something along the way? How is a person supposed to keep up?

It would be fair to say that Bitcoin’s past has not been the most accessible to the general public. An anonymous individual or group with the name Satoshi Nakamoto self-published a paper in October 2008 to a mailing list describing a peer to peer electronic cash system (referred to as the Bitcoin Whitepaper). As word spread, explanations of Bitcoin's importance have competed with images of upward trending price charts that caused people to be overwhelmingly skeptical or excited about this digital currency. The **blockchain**, which is the name for the technologies that together underpin the cryptocurrency Bitcoin, has begun to get more attention.

What is a blockchain?

A blockchain is a public distributed ledger, in which all who choose to participate in it have autonomy to access it. Simply put, a blockchain is like a spreadsheet anyone can access. Every participant has a copy of the spreadsheet and is responsible for keeping it up to date. This is a purposeful oversimplification, as this guide will show you in later chapters (using a blockchain to store data as if it were a spreadsheet or even a database does not always make sense, and vice versa). However, we are going to temporarily use this analogy to tie blockchain back to a technology you may already know and use.

Like we said, anyone choosing to participate in the blockchain has the autonomy to access it. Some individuals use that autonomy to download the blockchain to their own computer and play a role in maintaining the blockchain. When the blockchain is downloaded and maintained on a computer, it is referred to as a "**node**". Those running a "node" have a copy of the blockchain. This copy is actively updated along with every copy on every other node. The blockchain is maintained collaboratively and does not have a single central entity maintaining the ledger. Edits can only be made to the blockchain with general consensus among the individuals running a node. When consensus is reached, new data is added to the blockchain. Therefore, all participants are recording the agreed upon changes to the blockchain. There were an estimated 11,924 Bitcoin nodes operating on Febuary 1st, 2018 according to Bitnodes.

Data on the blockchain is made secure through the creation of hashes, hexadecimal numbers that are created using the all the data from the blockchain each time a new block is created. Hexadecimal what? For now, let's think of hexadecimal is a base 16 number system - we are much more familiar with the base 10 number system and some may be familiar with base 2 (also known as binary). Hexidecimal numbers look like this: BF35 (48,949 in base 10). Putting data into hexidecimal hashes allows for a high density of information to be encrypted in a consistent format, typically in a hash of a fixed length. This allows for large amounts of data making up the blockchain to be written to a fixed length hash. As the blockchain grows bigger, the number of characters in the hash will always be the same length (the characters themselves change). This is part of a set of rules that makes the blockchain secure - any change to the blockchain will cause a change in the resulting hash, and alert us that the state of the blockchain has changed.

Use cases for the blockchain are now rampant: information about an individual's identity can be stored on the blockchain, banks can record transactions using blockchains, and copyright licenses can be issued via this transparent framework.

The blockchain is engineered to be open to anyone who has a computer terminal and decentralized so there is no single decision-making authority. No central authority holds power to make decisions and enforce rules. An issue with a system that is open and decentralized is that careful consideration must be given to incentivize individuals to not only participate, but behave in a manner that is not detrimental to other users.

Influence on Economic Systems

Digital currency can be thought of as a tool that enables people in different regions and countries to trade with each other without worrying about an exchange rate or transfer fee from one banking system to another. The excitement we have seen around cryptocurrencies comes from their potential to enable easier exchange of value from an entity to any other entity. More individuals would have the opportunity to buy or sell anything from theoretically anyone from nearly anywhere.

What is Ethereum?

Ethereum is an open source, programmable blockchain platform that allows for the development of decentralized applications (or DApps - sometimes stylized as dApps). It was created and conceptualized by Vitalik Buterin. Ethereum runs smart contracts. **Smart**

contracts are pieces of code that allow the Ethereum blockchain to immediately transport or move data without an intermediary. No central authority is required to cause the code in a smart contract to run - the code runs based on the rules contained within it. The "rules" of a smart contract can be thought of as automatically initiated (sanctioned) after the contract is activated.

Ethereum has received significant support from an ecosystem that has formed around it, with existing and new institutions creating DApps, tools, conferences, forums, meetups, and companies to support and accelerate the adoption of this new technology. The Ethereum Foundation developed Ethereum, and retains the role of an open source project aimed at building out improvements to the software, as well as developing protocols. Some enterprises have further supported the adoption of Ethereum by creating the Enterprise Ethereum Alliance.

Decentralized products and solutions built on Ethereum have already hit market. Companies are finding solutions for preventing identity theft, improving crowdfunding, paying musicians more fairly for their work, tracking food from farms to grocery stores, and many other use cases.

What’s to come?

While Ethereum use cases are plenty, this technology promises something larger than just a few thousand applications. Creators of these blockchain-based applications can tap into new ways to fund the development of the applications. They can also find new ways for their users to interact with the applications themselves. Tokenization allows for the distribution of **tokens -** representations of value or the permission to do some actions within an application. For example, a token could represent an opportunity to play a video game or download a song. These tokens are specific to the application. Tokenizing an application is done on top of the Ethereum blockchain, giving creators of DApps new ways to do business on an open source system.

Think of tokens like keys that allow a user to participate in the system, rather than a stock ownership certificate. The founders of the network keep a percentage of the tokens for themselves and if the network gains popularity, demand for the tokens rise while supply remains constant, making the price of the tokens increase. Founders can now monetize the networks they build by tokenizing their system and increasing the value of the system to the users. Ether (ETH) is the token for Ethereum. Any DApp built on top of Ethereum can also use Ether, or create a new token specific to their application.

An example is tokenizing social networks and current day media platforms. Each platform’s value is designated by its users. As a user, for the first time, it would be possible to purchase a portion of a system and power its entire protocol. While a lot of this is hypothetical, furthering the experimentation and education around blockchain technology gets us a step closer to this kind of future. Decentralized blockchain protocols have the ability to displace centralized internet systems and providers to the point that each user of the internet will ultimately be sovereign.

Principles of Decentralization

We used the word decentralization in "What's the Big Deal", but have not spent too much time defining this concept which is key to blockchain. So what does decentralization mean? In this section we will seek to understand various definitions of decentralization, and how members of the blockchain community have applied that definition to development of the technology. A good way to think about decentralization is to associate the word with a transfer of authority.

There are three main forms of decentralization, or how authority is transferred. Vitalik Buterin, the founder of Ethereum, detailed the following three forms of decentralization in a post on medium account:

> **Architectural (de)centralization** —how many **physical computers** is a system made up of? How many of those computers can it tolerate breaking down at any single time?
>
> **Political (de)centralization** —how many **individuals or organizations** ultimately control the computers that the system is made up of?
>
> **Logical (de)centralization** — does the **interface and data structures** that the system presents and maintains look more like a single monolithic object, or an amorphous swarm? One simple heuristic is: if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?

Let's get specific with an example. The computer or tablet on which you are reading this book was very likely made by a company with a CEO and a board of executives. This company is very likely structured to have business units that take care of various components of building, marketing, and selling the device you are using. The CEO and the board of executives provide direction to the different business units so they can work together to build computers. If the company were to split up, the CEO and board of executives would have to decide (or be incentivized) to split the company up. The individual parts of the company could not decide to do that on their own. If the part of the company that assembles the keyboards decided they no longer wanted to be part of the larger company, they really do not have the choice to break off into another company. According to Vitalik, this means the company is **logically centralized.**

Another example that Vitalik uses is language. For most languages, there is no centralized infrastructure enforcing people to speak in a certain way. While there are best practices and grammar rules that are most typically followed, no centralized authority polices a person’s everyday use of language. Organizations that publish dictionaries do not have direct control over the language. People who speak the language are the ones with control over it. This is how we see language evolve over time, depending on the place and time in which it is spoken and written. An example is how Latin over time evolved into the modern day romance languages of Spanish, French, Italian, Portuguese, Romanian, and Catalan. No central authority decided that Latin should evolve into these languages. In this case, language is something that is **logically decentralized.**

In the case of blockchains, they are **politically decentralized** because no one person has singular control over them. They are also a**rchitecturally decentralized** because there is no infrastructural central point of failure, as each node keeps a copy of the blockchain. But, blockchains are **logically centralized** because the system behaves like one computer despite being spread apart on all the participating nodes in the network.

Why is Decentralization Useful?

Given the characteristics of a blockchain, decentralization (politically and architecturally) allows blockchains to be:

1. Less likely to fail because they rely on many separate components.
2. Harder to attack because the networks are spread across many computers.
3. Harder to overthrow or take advantage of in a way that only a select part of the platform benefits.

If one node stops working, or even 100 nodes, the blockchain survives assuming there is at least one node up and running. This makes the blockchain very resistant to attacks. The blockchain does not stop working even if the power is lost in an entire country. This makes the blockchain very resilient, which can not be said of many of the existing systems on which we associate with the Internet.

Where do we go from here?

The phrase Web 3 is used to indicate that we are going past Web 1.0 (the original protocols of the Internet) and Web 2.0 (the responsive web, which is the Internet as we know it in 2018). But what does this actually mean?

Currently, companies like Facebook, Amazon, and Google dominate the Internet. They offer many free or cheap services because they are able to collect valuable data on their users, and find ways to monetize that data. As a user of the modern internet, one is never too sure where their demographic and personal data is being used. Through the implementation of decentralization, also called Web 3, data does not have to be stored in centralized systems. Data can be verified independently and content creators are valued by the quality of their work. Micropayments become a feasible method of being rewarded for value created. Users control how their data is used and accessed over the Internet, and can be paid for the use of their data.

This is all possible through the usage of blockchain protocols which can be operationalized by Ethereum, Bitcoin, etc. Jesse Grushack, the founder of Ujo lays out the problem of users becoming the product for digital advertisers in Web 2.0 and how the Ethereum blockchain can flip this model on it's head, in this article on ConsenSys media, **Welcome to 3.0**.

As you finish reading this section, we want you to come away with the following: Decentralization disintermediates central control of systems. Instead of a single company being responsible for writing information to the blockchain, the responsibility falls to anyone who wants to participate in the system. This is a significant shift in thinking, but an important one to understanding why blockchains are so important - they are both philosophically and technically engineered to be different from the centralized systems we are familiar with.

A Brief History of Blockchain

Although the concept of a blockchain was first fully actualized in Satoshi Nakamoto's Bitcoin Whitepaper, the underlying concepts and technologies draws from years of research across cryptography, computing, and economics. In this section we will uncover some of this history:

We start with the idea of centralization. Centralization, or control by a single authority or entity, is a common and pervasive form of governance. We trust (or lack trust of) central authorities, like banks, governments, and other institutions to maintain order and structure within the space they operate. This trust is not universally earned by every central authority, as there are many examples where the trust given to the authority is broken. Sony employees have had their social security numbers stolen from employee databases, Target customers have had their credit card information stolen, banks have compromised user accounts to thieves, and governments have taken away the rights of their citizens. Centralized technology and data allows for the monopolization of power.

The problems in centralization came to a head in the global financial crisis that occurred in 2008. On October 31, 2008, in the midst of the financial crisis, Satoshi Nakamoto (an alias for a still unidentified individual or group of individuals) published the **Bitcoin Whitepaper**, titled *Bitcoin: A Peer-to-Peer Electronic Cash System*. This paper described a peer-to-peer electronic cash system, Bitcoin, that combines cryptography, computer science, and game theory in its design and implementation. Satoshi’s creation enabled a participant to digitally transact directly with another participant without relying on an intermediary, such a a bank, to process the payments. When we say peer-to-peer, we are essentially describing a transaction from one entity directly to another entity. There is no intermediary the transaction has to pass through. For example, if you schedule a payment via a banking app on your phone to a friend of yours, the actual flow of money goes from an account controlled by your bank to an account controlled by your friend's bank. If you friend does not have a bank account, you could send the money from your bank to a third party, like a money transfer company, where your friend could pick up the money. Even if you withdrew the money from the bank and mailed it to your friend, you would need to have an address to send it to and rely on the speed of your postal service to get the money there safely.

Bitcoin attracted attention for its ability to allow for peer-to-peer transactions without a centralized intermediary. Technologists were drawn to the **blockchain**, the underlying technology on which Bitcoin operates. To remind you, a blockchain is a decentralized ledger that records transactions or activity between two participants permanently with verification.This verification comes in the form of reviewing cryptographic functions and timestamps. Transactions can be verified on multiple computers, which are referred to as nodes. This makes the blockchain decentralized and transparent. Blockchain technology can be uncoupled from the Bitcoin protocol and can be used for many other kinds of cryptocurrencies. It can also be applied to many industry wide use cases, specifically provenance tracking and management, creative rights management, patient records, etc.

With the surge of attention to the Bitcoin codebase and white paper, Vitalik Buterin, a contributor to the community, saw some limitations in the design of Bitcoin and began designing an open source protocol starting in late 2013, now known as **Ethereum.** Ethereum also operates on a blockchain, but it allows for other digital assets to be recorded on the ledger, unlike the Bitcoin blockchain. Released in 2015, the Ethereum protocol allows for programmable instructions, or **smart contracts**, to be built around a set of transactions, which automates many processes. This ability helps make the Ethereum blockchain more malleable than other blockchains. Ethereum blockchains operate with Ether (ETH), the digital token that powers functions and is necessary to run decentralized applications.

In his article **Here Comes the Epoch of Blockchain**, Andrew Keys, Head of Business Development at ConsenSys, lays out the areas of our world that are centralized, why it causes issues, and how blockchain can be a catalyst for change. He emphasizes that the Ethereum blockchain gives users the ability to program interactions with other users - if you do this, I will give you this - opening up new possibilities for people from all over the world to interact with each other. The promise of blockchain that is beginning to be realized is that a blockchain can give anyone the opportunity to interact with anyone else, and not have to trust a central authority in the process. This is incredibly powerful.

Blockchain Basics

So far, we have discussed the impressive implications of blockchain technology. We will now simply and concisely explain how the technology works to make it transparent and immutable across all users.

The blockchain is a digital ledger that operates via a network of computers. Data added to the blockchain is visible to everyone participating. When a transaction is carried out on the blockchain, it is added to a cryptographically encoded "block" with all the other transactions that occurred in the last ten minutes (for the Bitcoin network) and shared with the entire network of computers. Members of the network with participating computers, otherwise known as **miners**, compete to solve these cryptographic puzzles to validate the transaction. The first miner to decode the puzzle receives a small reward from the network for their work. The puzzle is difficult to solve, so in order to solve the puzzle fast enough to receive the reward, a miner will use powerful computers. When Bitcoin was first launched, it was possible to use a laptop purchased in a store for mining. That is no longer the case.

This ‘validation’ is in the form of reviewing cryptographic inputs, outputs and a timestamp, which then allows validated blocks to be linked to older validated blocks. This forms a chain of blocks that show every transaction made on the blockchain. This chain is updated and is made accessible to every member on the platform. This decentralized quality allows for transparency and immutability - that anyone on the platform has the ability to view any data added to the network.

Hashing and Public Key Cryptography

A blockchain uses hash functions in order to create an immutable record of what is written to it, as well as to create "digital signatures". A hash function is a digital mechanism that is used to compress data into a specific format. The hashing algorithm used by the Bitcoin blockchain is SHA-256. In this hash, the hashed data is always 256 bits long. The Ethereum blockchain uses a hashing algorithm called Ethash. A hash created using Ethash will look like:

```
0xb846300e188829d1b819389b31cef3b9cfaf335082ee66f830a875f1c1beb396
```

The above hash is from block 5000171 mined at Jan-30-2018 02:20:28 PM +UTC on the Ethereum blockchain. More data on this block can be found at Etherscan.

This hashed data is used on the blockchain to indicate value and the links between each specific blocks. In addition to hashing, the blockchain relies on public key cryptography to encode information securely - the digital signatures we referred to in the above paragraph. Specifically, participants on the blockchain have a private code - called private keys - that allow them to access their information which is encoded with a public code - called a public key. The public and private key are related, but a malicious actor cannot derive the private key from the visible public key. Private keys are not meant to be shared since a private key is used unlock its associated public key. These keys sign transactions on the blockchain.

Yunyun Chen of ConsenSys created an excellent visual explaining hashing in Guide: Hashing and how it is a part of public key cryptography in Guide: An Introduction to Encryption.

Hashing and public key cryptography work hand in hand to maintain consensus in the system. Through consensus, the entire system has common knowledge of the happenings on the platform and any action is recorded and made available for the platform to view. This solves the issue of a trustless system with intermediaries because now, participants on the blockchain have constant verification on the platform. The process of miners verifying actions on the blockchain is known as **proof of work**. Mining ensures that the constant state of the ledger has transactions that are all true. This prevents attacks and false information from perpetuating within the system, ensuring lasting validity.

Public vs Private Blockchains

As we learned in Principles of Decentralization, there are different types of decentralization. Due to the transparency of a blockchain and the need to involve a community of computers in syncing the blokchain, companies and governments have introduced the idea of private blockchains. This section will explore the differences between public and private blockchains and what types of problems each are suited to solve.

Differences between public vs. private blockchains boil down to the participants of the network. Public blockchains allow anyone to take part in block creation as long as they adhere to the network's protocol. Private blockchains only grant the power of block creation to a set number of participants. Public blockchains maintain protocol specification and decentralization with consensus algorithms like **proof of work**, while private blockchains could have a single entity responsible for syncing the blockchain.

We see that enterprises are adopting the idea of private blockchains more quickly than they are public blockchains. Private blockchains alleviate concerns that business have around privacy and the ability of a blockchain to be able to handle the requirements of their business. We will explore conceptual differences between public and private blockchains, but if you are interested in deeper technical differences you can read more on Vitalik Buterin's personal blog.

Private Blockchains

While public blockchains are typically advertised as completely decentralized, private blockchains have more tightly controlled permissions while still maintaining the decentralization principles that classic blockchains provide users with.

Given the nature of a private blockchain, attacks are often minimized considering that all validators are known to the network. Private blockchains also benefit from having the capability to blacklist certain users. Additionally, the predetermined controllers of the network can very easily make changes to the blockchain if needed. Due to the smaller number of contributors to the network, prices of transactions are often cheaper and they process faster and faults within the network are more easily rectified.

Public Blockchains

While it may seem like private blockchains are the better choice between the two, public blockchains have many benefits. Because of the large volume of participants on the public blockchain, participants are often protected from engaging in activities on the blockchain that they have no authority to do. Public blockchains are also open and benefit from gaining a variety of participants. We believe that adding more participants adds more value to the public blockchain, as each participant increases opportunities for peer-to-peer interactions and innovations to arise. Bitcoin and Ethereum both have a public blockchain (referred to as Bticoin mainnet and Ethereum mainnet) that anyone can participate in.

Consortium Blockchains

Another kind of blockchain network to consider is a consortium blockchain. The consensus mechanisms of this blockchain are controlled by a limited set of nodes. The right to access the blockchain can either be restricted to the predetermined set of nodes or to the public (or to a mix of these rights). Considering these possibilities, consortium blockchains can be thought of as partially decentralized.

If you would like to read more on public and private blockchains, we recommend reading **Public and Private Blockchains: Enemies or Allies? Why the Enterprise Ethereum Alliance will prove the latter** by R. Tyler Smith, and we found the following quote quite relevant:

> One thing that blockchains do extremely well is allow entities who do not trust one another to collaborate in a meaningful way. This is one reason people see so much potential in this immature technology.
>
> So it stands to reason that eventually we will begin to see large scale deployments of the technology attempting to do exactly that, connect groups such as businesses, governments, churches, and the like. Public blockchains can already make this claim, however they currently fall short of particular requirements such as privacy and scalability. Private blockchains can provide solutions for these short falls and enable greater privacy and transaction throughput because all the nodes are strictly controlled. However, there is a trade-off, they do so at the cost of their ability to connect any and all to the network.

All three types of blockchains currently exist. For the rest of this book we will consider public blockchains, but it is important to recognize that many organizations are attempting to use blockchain technology to fit their specific use cases.

Connecting Blockchains Together

The blockchain ecosystem is exploding. There are 1,491 cryptocurrencies listed on coinmarketcap.com at the time of writing. Many of these currencies share an underlying blockchain infrastructure, but many are deployed on their own blockchain with unique features. Implementing different blockchain protocols offers particular benefits for users of the system, so various blockchains are created to suit their creators goals.

Variety in design creates a healthy, scalable, and resilient ecosystem, but creates its own problems. Disparate blockchains are isolated environments and transferring value between them is difficult. We currently rely on centralized exchanges which can be slow and expensive. Creating programmatic connections between blockchains to ease transfer of value is an important factor for mass adoption of these systems. In this chapter we explore several approaches in connecting blockchains, such as pegs and relay blockchains.

The Two Way Peg

A **two way peg** allows users of a blockchain to deposit the native cryptocurrency of a blockchain and receive the cryptocurrency of another blockchain on the other network. A classic example of this system is BTC Relay, which acts as a peg between Bitcoin (BTC) and Ethereum (ETH). Holders of bitcoin can send BTC to a Bitcoin address, thereby releasing a certain amount of ETH on their behalf on the Ethereum blockchain. This enables Bitcoin holders to access functionality built on the Ethereum blockchain.

An Internet of Blockchains

The two way peg is a step in the right direction in terms of enabling cross chain functionality, but the goal is to achieve greater interoperability, analogous to the internet in the sense that it is a network of networks. The current blockchain landscape is similar to the web in 1994 - we couldn’t imagine social networks, e-commerce or pervasive video conferencing and look where we are almost 25 years later. Designing systems that can scale as effectively as the internet is important for the future of the blockchain technology.

Paul Kohlhass writes in his **Introduction to Polkadot and Parachains**:

> "A future of multiple blockchain networks is increasingly likely. A Web 3.0 architecture of buzzing public blockchains, private consortium ledgers, anonymous zero knowledge proof chains and all the countless applications running on top of each of them. Not one chain to rule them all, but a world of diversity where individual chains serve specific use cases and specifications.”

Each blockchain has advantages and disadvantages. An internet of blockchains would allow us to transfer value between blockchains to take advantage of specific features relevant to specific applications, regardless of which network holds each stakeholders assets.

If Bitcoin truly emerges at “the gold of the internet” the network will continue to hold massive amounts of value, but with potentially high transactions fees and longer block times it may not be ideal for applications requiring microtransactions. Another blockchain might be better suited for this application.

Additionally, the programmability of Ethereum makes it valuable for applications requiring smart contracts, but if we want additional privacy we might want to conduct transactions on a different network that enables greater privacy, like Zcash. If each blockchain has huge utility, they can do even more when connected.

There are several projects that aim to tackle this enormous challenge. Polkadot facilitates authenticated transaction between blockchains using a central relay chain with parachains and bridges to external blockchains. The project Cosmos is a team working on hub (called the Cosmos Hub) connected to other blockchains via an inter-blockchain communication protocol. Cosmos is planning their main network launch for the end of February 2018.

Inter-chain operability is an important area of research in the blockchain space and could help lead to improvements regarding scalability, consensus and privacy.

The Ethereum Blockchain

Now that you have a basic grasp of blockchain, let's dive into the specifics of one of the fastest growing blockchain platforms on which to build decentralized applications.

Ethereum is often described as the ‘world computer’. What does that mean exactly? Ethereum is a platform on which anyone can build decentralized applications, where every program and action is universally accessible and verifiable because everything happens on the global Ethereum blockchain (mainnet). The feature of Ethereum that makes it so extensible is that it is a programmable blockchain. It is similar to a programmable distributed ledger, where everyone agrees to run the same applications with the same data. It is not just a ledger, but global, shared data processing protocol. Hence, the idea of a world computer.

The main Ethereum blockchain is permissionless, meaning anyone can join the network. There are a few caveats to this, but basically, as long as you have an internet connection and follow the protocol, you can participate. Every participant running the protocol is a node in the network and executes and records the same activity. An action on the network is called a transaction. Transactions are grouped into blocks. Only one block can be added at a time and mathematical proofs verify the order of the blocks. This keeps the ‘distributed spreadsheet' in sync.

Every participant in the network processing every transaction results in a system that is expensive to maintain and change. To reduce spam and disincentivize valueless transactions, every operation on the network costs **gas.** Gas is the fuel of the Ethereum network. It is required to cause any modification to the blockchain. Users can choose how much to pay for gas for each transaction - the more they are willing to pay, the faster their transaction is likely to be processed by the network. At the time of this writing (February 1st 2018) the average cost of a transaction converts to rougly $1.30 USD. Gas is paid for with Ether (ETH), the native token of the Ethereum blockchain, which is explained in more depth in the Consensus section below.

Operating on the main Ethereum means that a user will be exchanging value for the services provided by miners. For those who do not want to spend any money, there are several public test networks that essentially follow the same protocol as the main network (mainnet), but are free to use. These test networks are useful for developing and testing applications for Ethereum, but do not have the same reliability or security as the main network so they should not be trusted to handle real value. The test networks are called Ropsten, Rinkeby and Kovan.

Public or Private Networks using Ethereum

The Ethereum main network is a public network that is open to anyone, but it is possible to run an Ethereum network in a private consortium as well (as previously discussed). A closed network allows for certain advantages like faster processing and private transactions as the participants in the network are known. JP Morgan is developing a permissioned, enterprise ready blockchain platform based on Ethereum called **Quorum**.

Smart Contracts

The programs that run on the Ethereum blockchain are called **smart contracts**. Smart contracts digitally facilitate, verify or enforce arrangements between multiple parties where the blockchain plays the role of the intermediary - the blockchain is acknowledged as the source of truth to settle disputes. This can lower costs associated with making agreements and settling disputes, and reduce or eliminate opportunities for deceitful actions among participants in a contract. While this is technically feasible on the Bitcoin blockchain, the protocols of the Ethereum blockchain were designed to allow for smart contracts.

Consensus

Currently, agreement on the state and the security of the Ethereum blockchain is maintained by a mechanism called **proof of work**. This mechanism rewards miners that help update the current state of the blockchain with Ether. Ether, a cryptocurrency, the unit of value on the Ethereum blockchain. It is the token for Ethereum.

Maintaining the network through proof of work is expensive and vulnerable to certain kinds of exploitation. There are plans to migrate Ethereum from a proof of work consensus mechanism to **proof of stake.** Proof of stake allows holders of Ether to stake a large amount of Ether as collateral for the opportunity to extend the blockchain. Honest actors in this system are rewarded with a small amount of Ether and dishonest actors are punished by losing the Ether they staked. The implementation of proof of stake planned for Ethereum is called Casper.

Learning More

If you'd like to learn more, Dan Finley, project lead at Metamask (an internet browser extension for interacting with the Ethereum blockchain), gives a succinct technical overview of how Ethereum and blockchains work at the opening talks of the IPFS Ethererum Hackathon in **Intro to How Ethereum Works**.

Ethereum Limitations

While there is a lot of excitement surrounding Ethereum and its future, it's important to stay realistic about the current state of affairs and the amount of hard work still needed for success. In this section we will touch several areas of concern about the state of Ethereum outlined by Vitalk.

The following list is expanded from a Reddit post by Vitalik Buterin from mid-2017**.**

Scalability

First and most importantly, Ethereum as it exists today will not scale to serve the needs of the projects that are currently being built on it, let alone handle future projects. The current design of the system requires that individual nodes must process every transaction on the entire network. This provides security and verifiability to the system, but severely limits the scalability.

At the time of this writing (January 9th, 2018) Ethereum reached peak transaction volume on January 4th, processing an average of 15.6 transactions per second.To compare, Facebook processes around 175,000 requests per second - Ethereum at its peak performance runs more than 10,000 times slower than Facebook. With the explosion of projects and tokens using the network, demand is sure to continue to increase in the near future.

Thankfully there is active research and support for solving this problem. Vitalk announced “Ethereum scalability research and development subsidy programs” in the domains of **sharding** and layer-2 systems like **Plasma**, State channels and Raiden.

Sharding is a scaling solution for Ethereum that would eliminate the need for every Ethereum node to process every transaction on the network. The proposition is to limit certain nodes' processing requirements to a subset of the total processing requirements of the system, with each node processing a shard of the whole and then facilitating communication between shards.

Plasma also reduces the total processing requirements of nodes in the network. It is a scaling solution that consists of a system of smart contracts that will run on the main Ethereum blockchain. The main blockchain only stores small amounts of verified data from "child" blockchains, each of which are required to maintain their own integrity. Implementing many "child" chains would greatly expand the storage and computing potential of the entire network.

Proof of Work Consensus

Proof of work, the mechanism by which Ethereum is maintains system consensus and security, uses a lot of energy. As of December 2017, Ethereum was consuming just over 11 TWh of electricity. That works out to be enough energy to power 1.7 US homes per transaction.

Additionally proof of work is vulnerable to certain types of network attacks whose threats can be mitigated or eliminated by switching to a different consensus mechanism, such as proof of stake.

Fortunately there is ongoing research in this domain as well and there is a roadmap for migrating Ethereum from proof of work to proof of stake. The planned Ethereum implementation of proof of stake is called **Casper.**

Privacy (or lack thereof)

There is a lack of privacy on Ethereum. As a public ledger where data is visible to everyone, there are plenty of reasons to keep any sensitive information off of the blockchain. Nevertheless, there are many applications where making private data accessible on the blockchain would be beneficial - consider applications handling financial data or systems dealing with medical records. There needs to be a way that people can conceal data while still allowing it be used reliably in transactions on the blockchain.

Ethereum took a step closer to achieving this with the Byzantium network upgrade that took place in October of 2017. The Byzantium upgrade included support for **zk-SNARKS** which allow for verifying correctness of computation without revealing the contents of computation. This can technology can be used to meaningfully use sensitive data in smart contracts while maintaining privacy.

Risk of theft or loss

Your private keys are the only way to access your account. This means that if you lose your key or someone who shouldn't gets ahold of it, you are out of luck, there are no fail-safes and no one can help you. The finality of this is unfamiliar to the average computer user and will likely cause many unhappy users as the technology gains greater adoption.

Trusting applications

Contracts on Ethereum are being trusted to hold greater and greater amounts of value. Most of us trust that contracts that we send our ether to are secure without ever glancing at the code, but there are scammers and hackers out there and honest mistakes happen.

Realistically, it will not be possible for Ethereum users to validate and verify smart contracts before they start interacting with them. Users place trust in application developers that the program is going to do what they say it is going to do, but still bugs persist and hackers get in.

There is currently work being done to programmatically verify that contracts on the blockchain are 100% bug free. Using formal verification, auditors will be able to put a stamp of approval that a smart contract is free of bugs. Issues of honesty and trust will remain, but reducing the number of accidental losses will be a big win for the ecosystem.

A Further Discussion of Smart Contracts

Smart contracts are a key underpinning of blockchain technology. This is a chapter seeks to further illuminate what they are.

Smart Contracts Are Not Automatic

Smart contracts can be thought of as self-executing pieces of code, but it's important to note some nuances. When smart contracts operate on a blockchain, they must be initiated with an initial fee. Smart contracts do not run unless they are initiated. When they are initiated, they all run at the same time on all machines participating in the network. Given that all the computers are running at the same time, they come to consensus on the results of the code.

How Smart Contracts Payout

Since smart contracts run on specific blockchains, they pay out in the underlying cryptocurrency. For example, smart contracts written on the Ethereum blockchain would payout in ETH. Smart contracts cannot make payments or transactions in fiat currencies since fiat currencies are issued and stored at centralized institutions and not in distributed platforms. Smart contracts are only able to issue fiat payments when fiat money is also put on a blockchain platform. This is why regulation efforts play a big role in this space.

Smart Contracts and Legally Enforceabitlity

At this point in time, smart contracts are not legally enforceable. Smart contracts can eventually represent legal arrangements, but for now there are a lot of regulation efforts to aid in the adoption of this technology.

Applications and Smart Contracts

Smart contracts can operate with a variety of other technology including Internet of Things (IoT) devices, banking services and systems, assets, and even identities. This versatile technology can truly apply to many use cases and can be programmed to work with a range of industries.

Are Smart Contracts Actually Contracts?

Yes and no. Smart contracts are in a way an agreement but they have the functionality to show a participant whether certain requirements and conditions were met. Smart contracts also have the capability to ‘digitally lock’ an asset if the pre-set requirement or conditions are not met.

Tokens and Crowdfunding

Adapted from A Token-Powered Future on Ethereum - ConsenSys, Simon de La Rouviere and Ashley Taylor, 2015

The recent buzz around token sales has brought interest to what tokens are and what they mean for the digital products. In this section we will explore the significance of tokens how it influences funding.

What is a Token?

A **token** is a digital asset. It is an object of value itself, or representation of any other asset on a digital ledger. In this case, the Ethereum blockchain acts as a ledger. At ConsenSys, we are building a stand alone DApp that allows people and businesses to issue tokens of all types with specific rights and purposes. We are also currently integrating the system into other DApps and platform ecosystems on Ethereum, which will provide the ability for others to do so in the future.

Historical Context of Tokens

Tokens have been a useful part of society for the purposes of trade: from trinkets and shells, to coins, to the digital era of Bitcoin and Ether. In most of these circumstances, tokens are a way to reduce the social transaction costs. Money thus provides us the ability to work together on grander scales. It has allowed us to incentivize working together towards a common goal efficiently.

All around the world, networks are being built that use tokens to enable the ability to work together and share responsibility in the distributed organizational structures of tomorrow. These include open industry platforms for energy, music, and poker.

Blockchains Enable a Tokenized Future by:

1) Reducing the barrier to entry to create tokens (in terms of security & cost)

2) Allowing global and free trade of tokens

3) (probably the most important) Allowing the tokens to interoperate on a transparent global ledger. Previously, all tokens were contained within their own silos. Being able to automatically exchange on a global scale enables more efficient and far reaching forms of cooperation.

What is a Token on Ethereum?

The Bitcoin token is a successful case study in the ability to send and transfer value on a transparent public ledger. But what else can we do with tokens?

Using the **Ethereum Virtual Machine** (EVM) and an Ethereum programming language (like Solidity, LLL, or Viper), we can add arbitrary computer code to tokenize many different kinds of value. Smart contracts govern rights around their ownership, transfer, expiration, and even decay. Tokens can represent any asset such as:

- an hours worth of rooftop solar energy
- a currency such as dollar, euro, rupee, or gbp
- promise for a product in a crowdfund
- a future download of a song from your favorite artist
- or an insurance policy

Why do We Need Tokens?

Tokens are a mechanism to introduce property into the digital realm. They enable valuable components of a digital economy to become tangible because they can be claimed, and in some cases traded. Additionally, when trades are automated on a permissionless ledger such as Ethereum, it lowers the barrier to entry to create, manage and participate in more efficient networks of value. The conditions also allow more effective price discovery for individuals and groups.

Tokenized assets allows for goods to be traded as close to directly as possible, sometimes without an abstraction of money or an intermediary. Ether, the native token of Ethereum network, acts as the crypto-fuel required for the processing of a transaction. Imagine trading excess solar energy for a ride to work from your neighbor. In this case, the tokens are exchanged on a decentralized platform, like etherex, which can happen automatically and fluidly for the parties involved. Exchange platforms can take a small fee for their services if they are providing value for the swap.

Because Ethereum is an open protocol, the best exchange service for particular use cases will flourish. Services like Etherex will only continue to thrive as they add value in the system, because new ones will have access to the available protocol to outcompete stagnant incumbents. Exchanges could also be managed and governed only by the people that use it: keeping the cost at the market minimum. These models of cooperative governance are also being developed at ConsenSys.

Those token portfolios will become critical parts of our future reputation. They provide the basis for a reputation based economy, facilitating more organic connections between people and projects. For example, imagine Isaac who participated in the crowdfunded albums of 18 of the top R&B artists and 20 public art installation pieces. He wants to find collaborators in a future project that fuses both interests to create a hip hop hall of fame in Union Square NYC Holiday season.

Because individuals maintain their own reputation portfolios using a wallet like uPort.me, these organic connections are only facilitated on the terms of the actual people who control their wallets. Each person decides how they will want to display their tokens, and with whom. The systems are flexible. It's up to us to decide what kind of tokens we want to issue, the rules we decide to have around them, and the kinds of contexts with which they will be useful.

The standards are close to being finalised by the community, so stay tuned for more blog posts on a token-powered future. For an in-depth overview on the tokens core component, check out Simon de La Rouviere's talk at DevCon.

Understanding the Network Effect, Metcalf's Law, and Tokens

A network has value proportional to the number of individuals on the network squared. This is called Metcalf's law. A way to think about Metcalf's Law is in terms of a telephone network - if one person has a phone, then the network has very little value. But if two people have a phone, then there is value in that we can call each other. If our banker, barber, and grocery store all get phones, this, adds more value to the network, at no additional cost to the original adopers.

A method to incentivize early adopters is issuing a token that allows these early users privledges on the network. Issuing a token can be a way to jump start the network effect allows for the platform to more quickly create the network effect.

Tokens as a Protocol as Part of Open Networks

Issuing a token allows for platform interoperability - more people able to get onto and use platforms, and build things on top of them. With Web 2.0, many of the original open networks have become walled gardens that the company who created them maintain. Twitter is able to ban users, and there is little to be done other than turn to the court of public opinion to appeal the decision. An open network would allow the users to potentially vote on whom to ban if their content were deemed offensive, and use an economic incentive to do so.

In this example, a user who find offensive content could report it to the network, and would need to put up a stake in order to challenge the content. This stake would be a token issued by the network, which has some utility within the network, like allowing a user to make a post. The party accused of having the offensive content could take the content down, or contest the ruling, putting up a token as stake as well. Then a group of individuals within the network would convene to rule on whether the content was offensive or not. If the content was found to be offensive, the party who posted the content would lose their token, and it would be distributed to the individual who found the offending content, along with the adjudication board. If the opposite were true, the individual who flagged the content would lose their token to the party who posted the content and the adjudication board.

This gives the power of the network to the users to be a self-determining body to determine the direction of the network. This is important because it puts a check on the monopolization of the network and allows for network governance. We will explore these ideas further in Decentralized Governance and Voting.

Ethereum Request for Comments 20 (ERC20) token standard is the standard which allowed for users of Ethereum to create tokens on top of the existing Ethereum blockchain, making mainnet both an open network and Application Programming Interface (API) that is fueled by Ether. When you hear that a token is an ERC-20 token, it means that the token follows this standard and is a token issued on top of the Ethereum blockchain.

Crowdfunding

If you the reader were tasked with starting a company, the likely methods you would choose in order to initially fund it would likely be putting in your own money, asking those within your network of family, friends, and connections for money, going to an institution that could lend you the money (like a bank or a venture capital investor), or turning to a platform like kickstarter to raise money from the crowd.

Now, imagine that you could tap into all of those funding sources at the same time. It would be a very powerful way to raise funds for the company you are trying to build. Issuing a token on your platform allows you to start your company using investment from individuals or entities that decide to contribute to your venture.

Legal Implications of Tokens

Coinbase, Coin Center, Union Square Ventures and ConsenSys created the following framework as a starting point for developers and companies entering the space and launching a token. It can be used to analyze the likelihood that a particular blockchain token (e.g. any given App Coin) would be subject to US federal securities law. It also establishes a set of best practices for token crowdsales. This is not legal advice, rather a framework for thinking about legal implications of tokens.

A Securities Law Framework for Blockchain Tokens - Coinbase, 2016 [10 min read, minus detailed analysis section]

Self-Sovereign Identity and Reputation

Adapted from The Identity Crisis - By Dr. Christian Lundkvist and Andrew Keys, ConsenSys, 2015

For those of us lucky enough to be in the first world, we have the luxury of claiming our identity because there are centralized organizations or governments that affirm who we say we are through birth certificates, identification numbers, and other means. The blockchain enables a new shift in this space where we can have multiple, decentralized sources attest to our identification while we still maintain control of this data.

In this section we will explore what a self sovereign identity is and the significance of being able to control your identifying information through a blockchain.

Identity

Identity is defined in Merriam's dictionary as "who someone is". As the world and technology evolves one can't help but notice the changes to the notion of who someone is and how this affects their relation to the world. We'll focus on the problems that affect humans in regards to their identities, dividing the conversation into developed and developing economies.

The Problems

Developing Economies

Notwithstanding the millions of humans on Earth that literally have no identity, the members of the developing world are victimized and hindered without official forms of identification. Cost and inefficient infrastructure make simple transactions like opening a bank account, obtaining credit, renting shelter, or purchasing transportation impossible.

Human trafficking is fueled by the lack of identification whereby humans are unable to prove their age or origin, creating oppressive environments.

Developed Economies

We live in a world where our identity is not commonly possessed by the rightful owner. Mark, Sergey, and Larry have earned an exceptional livelihood selling the attributes of digital identities of members of the developed world. In mainstream products like Facebook, you are the *product*. You are being sold to marketing companies as a product based upon your interests, locations, and demographics. Moreover, specific attributes of identity have become vulnerable to attack. Countless stories of cyber-theft occurs where social security and financial data are the eventual goal of hackers worldwide.

The Solutions

Developed Economies

In the developed world the solution to having our identities owned and monetized by third parties is to introduce **self-sovereign identity**. This is a concept where the individual has ultimate control over their identity and is the final arbiter of who can access and use their data and personal information. This is a new concept, in that previous thought around digital identity has always hinged on “identity providers”, which are the entities that own and control our identity. Some discussions on “decentralized identity” have defined “decentralized” as having the option of choosing your identity provider. Self-sovereign identity goes further by having the individual be in control.

Note, with self-sovereign identity the individual still has the option of letting a trusted identity provider manage their identity, so we get the best of both worlds.

What makes self-sovereign identity possible today is the convergence of several technologies: Blockchain technology like Ethereum allows for shared, trusted computation that can fulfill the role played by identity providers today. Distributed data storage systems like Inter Planetary File System (IPFS) have the ability to store data in a more efficient way than a blockchain but still benefit from the security of the blockchain. Finally, modern encryption technologies allow for combining privacy with the public nature of the blockchain.

Developing Economies

In the developing world, digital self-sovereign identity can be a big help to refugees and other disenfranchised people. Digital identities registered and controlled through a blockchain require no central company or organization to maintain, and can survive political and social turmoil so that refugees can retain access to their digital identities even under such difficult conditions.

Furthermore, by using bleeding-edge technologies like Enigma & Hawk, it would even be possible to maintain a biometrics database that can be linked to the identities in privacy-preserving ways. Even without these future technologies policy architectures like those introduced by Vinay Gupta can provide a policy separation between biometrics databases and digital identifiers to implement privacy protection for biometrics.

Implementations

We at ConsenSys have already started building the next generation of digital identity systems, built using the Ethereum blockchain and IPFS. Our uPort digital identity platform is used as a basis for digital identity based on **AML/KYC** (Anti-Money Laundering/Know Your Customer) protocols for our derivatives prototype, the Ethereum Total Return Swap (eTRS), the EtherLoan P2P-lending platform, the Inflekt Events management platform, educational credential issuance through Ethense, and a threaded-discussions platform.

We are currently working on the designs and implementation of our Selective Disclosure features, where the user can encrypt the attributes associated to their identity and selectively choose which other identities they wish to share those attributes with. This is crucial in digital identity systems for governments and banks where the data attributes can be very personal and sensitive.

An Example

Let's explore a use case that many individuals experience. You go to a restaurant and attempt to purchase a beer. The waiter or server asks to see your identification in order to confirm you are the correct age to purchase a beer in the jurisdiction you are in. Currently, this entails providing the server or wait staff with a copy of a state or national identity card, that oftentimes has much more information displayed on it than you would like to share with the wait staff - for example, your home address, height, weight, eye color, and more. You have to trust that the wait staff will not take down this information or use it in any way that could bring harm to you. With self-sovereign identity, you would only have to provide confirmation that you are the appropriate age, not even what age you are. Scanning a QR code on your phone, the wait staff would be given a simple Yes or No to whether they can serve you that beer.

Expanding upon that Example

Centralized repositories of information are similar to our example of trying to purchase that drink, just at a larger scale. Instead of just checking the age, oftentimes an organization will store information about the user, and often more information than was needed to give access to a certain benefit or service. Centralized repositories also carry risk for the users and the organization maintaining the central database - if it is hacked and data gets in the hands of those who would exploit it, the individuals whose data was stored in that database incur a major cost and the business or organization maintaining the central repository is often legally liable and will suffer consequences from users reluctant to trust them. In order to prevent this, the organization often have to invest in preventative measures which raise costs for their users either directly or indirectly. Wouldn't it be better if no one had to take on that level of risk?

Decentralized Governance and Voting

People have been self-organizing since before recorded human history, but until the Bitcoin network was launched, there had been limited successful attempts to build communities agreeing on rules and incentives without relying on central organization. With the blockchain, once theoretical forms of governance that removed central organization or that required a certain amount of frictionless transactions to occur are now in experimentation.

How is Decentralized Governance Possible?

Readers may be familiar with the standard types of governments and governance - a monarch ruling a country, a parliament or congress, a military with it's hierarchy of commanding officers. All of these examples are a different form of governance, and are replicated in religious organizations, companies, athletic clubs, hobby groups, and schools across the globe. Nearly every one of these models require the establishment of a hierarchy, where certain individuals have or are endowed with power in order to make decisions or carry out specific actions on behalf of the whole. That power may come from votes of members of the organization, or come from an individual or group of individuals who have found a means to obtain that power from the group. Without getting into a full history of the philosophy of government, hierarchies tend to bring order and speed to governance, while compromising individual participation in decision-making.

As communication networks have evolved, it has become easier to gauge the opinion of those who choose the decision makers or the policies. This is particularly true for democratic systems of government, and most true for systems where the philosophy of "one person, one vote" is adhered to. When communication networks were slower, under a democratic "one person, one vote" system, the fastest way to get everyone's opinion in a town of 300, would be to call a town meeting and ask for everyone to voice their opinion or vote on a matter - like the budget for the local school. If someone was sick, or away on business, they would either have to have known the information ahead of time and passed on their vote to another citizen of the tow, or abstain from the voting. Over a certain count of individuals, the process of collecting everyone's vote became very difficult and time consuming, preventing more than a certain number of questions to be asked at a time.

Imagine that we keep the model of the town meeting, where everyone comes together to legislate via direct democracy. Getting everyone on Earth in the same room at the same time would be impossible. Above a certain number of individuals we would soon find ourselves unable to make decisions - we wouldn't be able to solicit everyone's opinion, and thus would be limited to giving everyone prepared information that we would ask them to vote on. And we would have to decide who would be given the power to organize and prepare the motions that we were voting on. Fortunately, since communication networks are now much faster, we can use the Internet to secure everyone's vote (provided they have access to the internet), though soliciting opinion would still require some pre-arranged parameters of when individuals can submit proposals, how those proposals would be prioritized, and who would be responsible for the collection of these proposals to vote on. But we can see how a direct form of democracy could be possible on a potentially global scale - that is if we could trust the central authority counting our votes to be fair and honest. Depending on which country you currently reside in, you may have reservations about the ability for a fair election, even on the internet, due to a regime that may have a history of voter manipulation, or malicious actors who would be able to hack the system and change the results, making the outcome look as if it were the will of the people.

This is where the blockchain enters the equation, providing cryptographic protocols, decentralized governance, and economic incentives to answer some of these questions. We will tackle each issue, and introduce what new forms of governance that it allows if that form of governance is something that has been defined.

Problem 1: Trust

In this scenario, our central government becomes a blockchain, which is stood up and a nodes are placed on computers around the world.

Say we are a multi-national charity and we decide that we want every person within our corporation to have an equal vote on how and where we spend our funds. There are many good projects we could spend our funds, so deciding how our pooled resources should be apportioned is going to be necessary to increase our impact while respecting the wishes of the group. Anyone who wants to join our charity would be given access to a smart contract on it, where they could deposit their money. When it comes time to vote on how we spend that money, we each submit a vote.

How can we trust that the votes are what we say they are? If everyone had a public and private key, they could sign their vote with their private key and submit that transaction to the blockchain. All of the votes would be distributed across all nodes, so that the entire public could see the votes. Then the public keys could be used to unlock them, count the votes, and declare a winner. The added benefit is that everyone can verify the votes were counted correctly. What has just been described is a form of **commit-reveal voting**, where votes are committed to a location and then revealed for all to see and verify.

Just because the votes are public does not mean that the identities have to be. As indicated in the previous section, Self Sovereign Identity and Reputation, it is possible to just verify that the individual who voted is allowed to vote in this election, and not identify who they are.

Problem 2: Knowlegeability of the Electorate

If our non-profit was debating whether to use our funds to help with a chemical waste cleanup project or carbon recapture, I might not have any idea of how to vote. The proposals might outline the amount of funds needed and be specific as possible, but I may not be an expert in this area, and instead would look to a knowledgeable source to inform me.

What if one of my friends were an environmental engineer and was very knowledgeable about what is required for both of these projects, and was also extremely interested in taking the time to dig into the details? Well, it would be great if I could delegate my vote to her, so once she digs into the details and makes a decision about the best project, she can vote for me. I want to borrow on her knowledge and expertise in the area, but only for this specific vote.

With the blockchain, I could pass my voting authority over to her for this vote via a token (essentially a tokenized vote), which would allow her to cast a vote for me. I could give her this token for other similar votes, or decide that after this vote, I want to ensure that I vote the next time.

What is described above is often called **Liquid Democracy**, essentially a flux state between direct democracy and representative democracy that is constantly evolving.

Problem 3: Adapting the Rules of Governance

A government or organization that gives power to some set of individuals that comprise it typically writes up its rules for governing - this can be using Robert's Rules of Order to run a recurring meeting, a charter, or a constitution. Similarly, the rules and procedures used for governance on the blockchain can be written, and those written rules could be put into code and enforced through the structure of a smart contract.

Now let's say that that our non-profit has a group of individuals that decide they would prefer to only use their money for projects that help clean up oil spills. It would be painful to untangle all of the finances and voting procedures, right? Well, we could institute a **hard fork**, where starting at a certain block number, the group of investors who want to only donate their money to cleaning up oil spills would be able to do so, and keep the prior history of the transactions up to this point. And the original group would continue on, but without those individuals who decided to break off. In a hard fork, the miners would only accept transactions from certain addresses, thus forking the blockchain. This would allow both new groups to keep the historical records of the group and the current voting mechanisms, but change the membership.

The Big Idea

It is assumed that most models of governance and voting can be moved to the blockchain, though we have not specifically confirmed this claim. One of these models - Futarchy - we will cover in more detail in the next section (Prediction Markets). However, the general idea is that prediction markets can be used as part of a governance structure. The blockchain is not part of the model, but as a platform, it allows for a Futarchy to be build on top of it. Similar ideas are in place for liquid democracy and other forms of governance, which did not seem possible to do on a large, distributed scale until blockchain technology had grown in its adoption. New governance structures and voting paradigms are emerging, both from historical works on governance that were theoretical in nature, as well as new forms that have evolved out of prior experiments. This is just a cursory overview of these governance models and voting mechanism that can occur on the blockchain. A key takeaway is that decentralized governance via the blockchain is at the intersection of philosophy and technology, where the potential for individuals to have a greater voice in governance is possible.

Cryptoeconomics

Cryptoeconomics - sounds like something to do with how cryptocurrencies are spent and the economies that exist around cryptocurrency, but it isn't quite that.

Cryptoeconomics is the combination of cryptography and economic theory to create sustainable operating protocols for trust-less and decentralized platforms. Cryptoeconomics is how to get all the participants on the blockchain - the miners and the entities transacting - to act in ways to reduce the likelihood of unfavorable behaviors that could happen on the blockchain that would impact other actors.

Cryptography allows for the passing of messages in a secure way. By obscuring a third party from seeing messages passed between two parties (Alice and Bob are the names of the two parties passing messages in the tradition of literature written on cryptography, with the eavesdropper being named Eve), peer to peer interactions of all types become secure. Layering economic incentives on top of the secure protocols compels users of a platform to act in certain ways on the platform because of rewards or penalties tied to their behavior.

An Example

Let's look at the Bitcoin blockchain. To remind you, Bitcoin is a network for peer to peer financial transactions.Two individuals, *Alice* and *Bob*, want to transact with each other. Alice decides to send some money to Bob in order to pay for a bicycle we sold to her. In order to send Bob the money, Alice signs her transaction with her private key. Bob can use her public key to verify that the transaction is from Alice. Thus, cryptography is used in the transaction in order to prove that Alice owned the coin she is transferring to Bob. In order to prevent Alice from spending that same coin again, an economic incentive is created within the network for others to check for a double spend, without needing a central authority (a bank or government, for example) to do this checking.

On the Bitcoin blockchain, individuals running a node will compete to combine the transactions that are sent out to all nodes into a set block, and if they are successful in solving a hashing problem (once again, using cryptography) that is accepted by the other individuals running nodes, then they are given a reward - in this case a set amount of Bitcoin for their troubles of using their computing power to create the next block in the blockchain. (citation of the Bitcoin white paper) If they were to allowed a double spend, and this is caught by others who are verifying the transaction, and it would not be accepted as a block in the chain. Thus, every miner is incentivized to ensure that there is not a double spend of Bitcoin.

You can see how cryptography, as used in peer-to-peer transactions and the creations of the blocks, is combined with an economic incentive to compel actors on the network to behave in a way that ensures spending of tokes, work required to sync the ledger, and verification of transactions is done in such a way that it meets the expectations of those using the blockchain. Specifically, as illustrated in our example above, some of the problems that cryptoeconomics allows us to solve in blockchains deal with malicious actors. Others deal with how we can create value on the network, or incentivize entities or individuals to use their computing power in order to sync the ledger, store data, provide other entities with data, or do a host of other activities.

Decentralized Storage

Adapted from Decentralized Storage: The Backbone of the Third Web - ConsenSys Media, 2016 and An Introduction to IPFS - ConsenSys Media, 2016

In the last decade much of the internet has moved onto "cloud storage" which has powered the new web. Most of the applications we use on a daily basis have our data stored in server farms owned by Amazon, Google, or Microsoft. In this new era of decentralized applications, developers are turning to decentralized storage as a way to avoid censorship, server outages, and hacks. This section will explore some of the solutions for storage in web 3:

Since the World Wide Web hit the mainstream in 1994, we've seen the network expand to encompass almost every aspect of human life. The underlying infrastructure of the Internet and the services built on top of it are interdependent, one informing the other as new use cases and technologies arise. There have been two clear generations in the services and structure of the web thus far, but today we are moving into a third. This section will look at what characterized Web 1.0 and 2.0 and what may characterize Web 3.0. We will then look at the storage technologies that are likely to form its backbone: the decentralized storage network IPFS and it's incentive platform Filecoin and Swarm, an emerging Ethereum oriented storage platform that uses IPFS.

Web 1.0 & 2.0

Web 1.0 was the birth of a new idea. If we can connect all of the computers in the world through a global network, the Internet, then we should be able to make the collective content pool universally accessible. For this mass of data to be usable it needed to be indexed and browsable. This necessity was behind the innovation that led to the first generation of the World Wide Web.

Web 2.0 took this new global resource, a universally accessible pool of content, and began plugging things into it. Programs could connect and use the Web as a way to store information and communicate with each other. Central intermediaries, today's Googles and Facebooks, assumed the roles of data silos and switchboards, offering scalable resources and routing traffic. While these new corporations have changed the way we live and provide amazing services, they also leverage their centralized position for profit and power.

In their orange paper, "Swap, Swear and Swindle: Incentive System for Swarm", Viktor Trón, Aron Fischer, Dániel a. Nagy, Zsolt Felföldi, Nick Johnson writes that:

Context-sensitive targeted advertising offered a Faustian bargain to content producers. As in 'We give you scalable hosting that would cope with any traffic your audience throws at it, but you give us substantial control over your content; we are going to track each member of your audience and learn—and own—as much of their personal data as we can, we are going to pick who can and who cannot see it, we are going to proactively censor it and we may even report on you, for the same reason.' Thus, millions of small content producers created immense value for very few corporations, getting only peanuts (typically, free hosting) in exchange.

As the Web grew, we reached scaling limits. Central nodes required ever more bandwidth to cope with even increasing data flows. Over time, as things were shuffled around, links broke and content was lost, vanishing due to unsearchably into the mass of information.

To compound these problems, security never achieved a level appropriate for the new communication and commerce services provided through the Web. The client-server model relies on a system of digital certificates, which are issued by third parties to secure connections. The problem is that if the third party is compromised, so, potentially, are all the connections made using its certificates.

According to Juniper Research, "the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015." Thus, the scene is set for a paradigm shift and a cluster of new technologies are emerging. They promise to solve the problems plaguing the existing system and create a new way of using the web.

Web 3.0

Following the trend set by earlier iterations, the idea of Web 3.0 posits a change in the way content and programs interact. If central intermediaries like Facebook and Google are cut out of the picture, many of the problems we have today will go with them. Instead, *content addressing* and related techniques will allow content and programs to link to one another directly and in a more robust fashion. Blockchain technologies like the digital currency Bitcoin and the smart contract platform Ethereum use unbreakable *public key cryptography* to secure the connection between programs and protect data.

This is an alternative to the centrally issued SSL (Secure Sockets Layer) Certificates used today. Because there is no central intermediary routing traffic, connections can dynamically find the most efficient pathway through the internet and route around congestion or damage.

These systems were designed for financial transactions though. They are not suited to storing and relaying the volume of information required to replace a central server. BitTorrent is a popular solution that has excellent storage and scaling characteristics. However, navigating the *Distributed Hash Table* used to index content on the network can take seconds. This kind of latency (wait time) is fine for large file transfers but no good for datacenter use cases.

InterPlanetary File System (IPFS)

Described by Viktor Tron as “the lego kit for the third web,” IPFS is a new system for storing data on a large number of computers. It is transport layer agnostic, meaning that it can communicate through transport layers like transmission control protocol (TCP), uTP, UDT, QUIC, TOR, and even Bluetooth)

Instead of a central server, a *peer to peer network* is used to establish connections. Public key cryptography is built into the node addressing system and *content addressing* is used to index content. Both node and content addresses are stored in a decentralized naming system called InterPlanetary Naming System (IPNS).

Node addressing and connection security

- Nodes in the peer to peer network each hold private keys and release public keys, just like in Bitcoin or Ethereum.
- Node addresses are derived through *hashing* their public keys. Allowing connection verification through message signing.
- Their public keys can be used to encrypt data before it is transferred, preventing interception and theft.

Solutions to the security issues of today’s web are built into this addressing system. There is no need for a trusted central certificate issuer to provide connection verification tools and all connections can easily be encrypted by default. No more SSL.

A High Level Approach to IPFS

At its core, IPFS is a versioned file system that can take files and manage them and also store them somewhere and then tracks versions over time. IPFS also accounts for how those files move across the network so it is also a distributed file system.

IPFS has rules as to how data and content move around on the network that are similar in nature to bittorrent. This file system layer offers very interesting properties such as:

- websites that are completely distributed
- websites that have no origin server
- websites that can run entirely on client side browsers
- websites that do not have any servers to talk to

HTTP vs. IPFS to find and retrieve a file

HTTP has a nice property where in the identifier is the location so it is easy to find the computers hosting the file and talk to them. This is useful and generally works very well but not in the offline case or in large distributed scenarios where you want to minimize load across the network.

In IPFS you separate the steps into two parts;

1. Identify the file with content addressing
2. Go and find it—when you have the hash then you ask the network you're connected to 'who has this content? (hash)' and you connect to the corresponding nodes and download it.

The result is a peer to peer overlay that gives you very fast routing.

To learn more, watch the Alpha Video.

Content Addressing

A content address is derived by hashing a piece of content.

- That content address is then hashed again to derive a *key name.*

- The key name is associated with a human readable name in IPNS (IPFS' address registry).

Instead of referring to objects (pictures, articles, videos) by which server they are stored on, IPFS refers to everything by the hash on the file. The idea is that if in your browser you want to access a particular page then IPFS will ask the entire network "does anyone have this file that corresponds to this hash?" and a node on IPFS that does can return the file allowing you to access it.

IPFS uses content addressing at the HTTP layer. This is the practice of saying instead of creating an identifier that addresses things by location, we're going to address it by some representation of the content itself. This means that the content is going to determine the address. The mechanism is to take a file, hash it cryptographically so you end up with a very small and secure representation of the file which ensures that someone can not just come up with another file that has the same hash and use that as the address. The address of a file in IPFS usually starts with a hash that identifies some root object and then a path walking down. Instead of a server, you are talking to a specific object and then you are looking at a path within that object.

In today’s web, if a file is moved, all links to that file need to be updated if they are to resolve. Because IPFS addresses are derived from the content they refer to, if the content still exists anywhere on the network, links will always resolve. This removes any need for duplication of content, except for the purposes of greater persistence security or for scaling up serving capabilities.

However, for a decentralized storage system to grow to replace the current model, it needs a way to incentivize the storage and serving of content.

Filecoin is one solution being developed by Protocol Labs, Swarm is another being developed by the Ethereum foundation. Both projects make use of IPFS technology but have different philosophies on how to incentivize participation.

Filecoin

Filecoin is a protocol launched by Protocol Labs, the same entity that developed IPFS. If you want to dive in in much greater detail, we will refer you to the Filecoin White Paper.

Filecoin uses an established consensus process already in use securing a financial network. By requiring nodes to solve puzzles based on randomly selected data chunks, a Proof of Work algorithm can be built, which will reward the nodes that store more data chunks and have better connectivity. Tools for adding redundancy and the ability to select nodes based on reputation, whether that be tracked within the protocol or outside it, will address the problem of persistent storage.

Swarm

Swarm was conceived of as a storage protocol tailored for interoperation with the Ethereum smart contract ecosystem. Like Filecoin, it will piggyback on Ethereum’s consensus process in order to provide a decentralized alternative to our existing client/server infrastructure. Incentivising persistent storage is a challenge, however. The downside of a node deleting data and losing some income is potentially much less significant than a user losing his or her valuable data.

Swarm takes the approach of rewarding nodes for serving content. Because more often requested content is more profitable to store than rarely requested content, rewarding nodes only for recall would incentivise the trashing of rarely accessed data. Failure to store every last piece of a large data set can result in the entire set being rendered useless, so in these cases a solution must exist to balance this downside asymmetry.

Using content recall as the base reward mechanism and distributing content randomly among nodes, weighted for location, puts Swarm in a good place to start solving the persistence problem:

- Nodes offering “promissory” storage, or storage with a promise of persistence, must first post a security deposit covering the time for which they are offering storage.
- If data is lost during this period, the bond is forfeited.

The smart contract infrastructure of Ethereum automates this whole process, making the “upload and forget” experience seamless.

Prediction Markets

Adapted from Why & How Decentralized Prediction Markets Will Change Just About Everything - ConsenSys, 2015 and Markets for the Future - ConsenSys, 2016

What are Prediction Markets?

Prediction markets (or the original coined term by Robin Hanson: “idea futures”) aren’t new. What are they?

Prediction markets (also known as **predictive markets**, **information markets**, **decision markets**, **idea futures**, **event derivatives**, or **virtual markets**) are exchange-traded markets created for the purpose of trading the outcome of events.

You essentially bet against each other (the market) how an outcome will turn out. For example one could bet that Bernie Sanders will be the Democratic candidate vs Hillary Clinton in the next election.

You buy shares of each outcome that basically correlate to a percentage chance that the event will occur. Once the event has occurred, the prediction market will allow your shares to be redeemed for $1, while the other shares become worthless. For example, if you buy a Bernie Sanders outcome at $0.6 and Hillary Clinton outcome at $0.4, and Bernie becomes the candidate, you believed with a 60% chance that it will happen. Your Bernie token becomes worth $1. And your Hillary Clinton token becomes worth $0. Getting tokens is as simple as paying $1, upon which you get both. You can then precede to buy or sell them with others at various prices. If you don’t trade either of the outcomes that you bought, you will just get your money back (since one will go to zero and the other to 1).

Prediction markets have existed prior to the invention of the blockchain and still do exist. Intrade was popular but had to exclude US traders. It’s not an easy space to be in, since in some jurisdictions it is seen gambling, while in others it is seen options trading. The other worry is that it could create controversial incentives such as predicting the death of a global leader.

A global prediction market has thus not flourished as well as it could have. Even if it worked properly, building on top of it as a platform (with APIs and such) is also not an easy job, and there’s little guarantee that there won’t be another clamp down.

Enter Decentralization

Decentralized systems where innovation can happen without permission have allowed new (& old ideas) to flourish in wondrous new ways. We wouldn't have Facebook, Wikipedia, or Twitter if the web wasn't open. Free permission to innovate with information has led to where we are today. An open prediction market platform will come. It will most likely come to live on a blockchain. It not only helps with maintaining an open infrastructure for it, but it also allows separation of concerns (who is doing what in this market).

Currently there are 3 known decentralized prediction market efforts underway: Truthcoin/Hivemind (Bitcoin-based sidechain), Augur (recently raised $5.3m from a crowdsale, built on Ethereum) and Gnosis (working prediction market platform on Ethereum). We will focus on what this will look like on Ethereum.

Ultimately, a prediction market will exist that will allow anyone to create markets, bet on outcomes and resolve/report the outcomes. The difference comes in when you add the following to this:

An Arbitration Market for Reporting

At the end of the limit, the outcome of an event must be reported. In the past, this was usually reported by the people who ran the prediction market itself (and you had to trust them to report correctly). With a decentralized system you can swap this out for various systems. A market for an event can have one person decide.

If this person is trusted, then liquidity will come. If they are not, then multiple persons can report an outcome (where 2 of 3 need to agree, for example). Market participants can vote for who they want to report as well. Systems such as Augur have a token system where those who hold the token and vote on outcomes as a crowd. All these styles are swappable. In some circumstances you wouldn't even need a report to be submitted. If the information is already on Ethereum, the resolution will happen without requiring a trusted source to report. For example, if someone is selling their song on Ethereum, and that is publicly accessible by other contracts, you can use that as is.

Finally, and perhaps the most interesting, is that all you need is a threat of an outcome for the market converge to the right outcome. The closer to the time an event comes, the more it starts to converge to the actual outcome as clarity increases. Thus, in a way, the tokens become worth zero on the one side and 1 on the other, automatically resolving itself. In a scenario where this actually ended up wrong, users can put up a deposit to dispute it: which results in arbitrator that has to come in and decide.

Automatic Betting

This is arguably the most important. If it is an open layer any program can start predicting. Prediction markets only played by slow humans who have do the thinking won't ever have enough liquidity to be useful. Programs can absorb much more and make much better predictions about the future.

Automatically gathering knowledge about the world & combining it correctly will result in financial gain. Thus, companies like Google & Facebook will be at a considerable advantage, betting on these prediction markets. Dumb sensors in every avenue could either predict themselves or sell the information (more on this later). And finally, you can build bots that predict based on some model: it could be based off a person, a group, or any combination (also more on this later).

The difference here vs. a traditional market maker is subtle. The purpose is not facilitate trading, but to automate predictions.

The Result?

Once you add these parts, you get wonderful potential emergent behavior. Here are some examples:

Information Markets

You sell your information to be used in markets. If the information is in the same ecosystem as the prediction markets (say, Ethereum), then you can sell this information to be used in a trust-less manner inside the market itself. This is a holy grail for several reasons. The oft talked about “Internet of Things” will be extremely useful here. A sensor can produce information, & put it on the blockchain (public). If it's used for reporting, it can charge for that information. It could also result in markets where the information is not made public, but encrypted, upon which it can then be sold to others to gain knowledge to predict more effectively. So, information markets can develop around selling information to help predict & report. This won't just exist for sensor data. It would eventually become the norm to report any kind of data into the blockchain, especially for reporting purposes. It not only means that you can have audited & transparent information in there, but it also means you immediately provide a trust source for information to be bet on, at very little cost to the producer.

New Kinds of Organizations

With the rise of social media, people have been seeing its ability to move people together in new ways: driven by a common goal, bereft of normal bureaucratic process. The Arab Spring is a good example, where these movements remain relatively head-less. Recently, in

South Africa a movement to reduce tertiary tuition fees rallied around a hashtag (#feesmustfall) that formed the locus of the liquid organization.

These organizations are unlike what we’ve seen before because social media allows near instant communication and allows important news & events to immediately filter up (based on retweets) and then subsequently affect and inform the rest of the organization. Affiliation is as easy as using the hashtag. It’s the network’s version of an organization. There is no permission to be a part of it.

How does one build ways to incentivize these new organizations and how do you help it make decisions? You use prediction markets. Just as these hashtag organizations move like crowds do, so should its decision making. As the organization goes about its goals, various outcomes are constantly generated, upon which the people in the organization and those outside of it, bet on the outcomes, leading it automatically towards outcomes which serve the goals of the organization.

Since these network organizations move at the speed of social media, you might need some help from our bot friends to bet on your behalf. And this leads to the next part...

Wealth Sharing

If prediction markets will be so useful in creating wealth for those are in the know, then you might want to developed automated personalized prediction bots. These bots automatically bet on events based on who you are & what you do. If you join a hashtag organization (the tweet appears in your feed), then the bot automatically detects this and assumes this as indicator that marginally this movement might succeed and thus bets on those outcomes (resulting in automatic financial gain). Another example is where if you frequent a coffee shop, your bot will automatically start betting on the revenue that will be posted by this shop. You are directly influencing its success by being a patron and thus you can partake in the financial gain of it.

This presents a potentially whole new way of looking at organizations. Perhaps into the future we won’t even need things like shares/equity. Money simply flows towards some locus, upon which it is used to improve a metric that can be predicted upon. It paints a new model of “investment”. If you donate $10,000 to an organization or group, you know that its metric of success will improve and thus you can benefit from that financial gain. There are countless metric which could be influenced in this manner- just by “being alive”, you affect them. These opportunity will become available to all, at any scale.

Protecting Natural Systems

Is it possible to use prediction markets to protect our climate & environment? Karl Schroeder describes such a potential system in this forum post.

In essence, you have AI automatically interacting with a natural system, in order to protect it. At the base of this could be prediction markets. A metric could be something like: growth of new trees in an area.

If you are interested in seeing the ecosystem flourish, you can get financial gain from it, by simply protecting & fostering it (you first predict, then enact the change). You make sure that a certain amount of trees are planted. Sensors can provide much more nuanced feedback and reporting vs more concrete outcomes (such as trees planted). For example, measuring pollution. This information will be sold to interested parties. To bring these sensors into existence they can be crowdfunded by a group of environmentalists, who will earn these fees, which subsequently can result in further creating a sustainable ecosystem.

Futarchies

Policy decisions are at the core of all governance models. Organizations must make decisions on which policies to implement in order to maximize future welfare. For a government, this could mean deciding budget allocation. Should a portion of the budget be allocated for infrastructure projects or for education? Which will result in greater GDP?

Within a corporation, disputes could arise over whether or not to acquire a company. Metrics on share price or future revenue may be the deciding factors. In most cases of governance, such decisions are made using a range of Democratic or Autocratic processes. The former involves a voting process in which members of an organization or government cast votes (allocated through an egalitarian or proportional representation) where a plurality, majority, or supermajority is required to implement a decision. The latter involves a hierarchical model in which designated individuals make absolute decisions over their areas of control. Both of these models suffer from information inefficiencies, often resulting in the implementation of policies that poorly optimize future welfare.

Futarchy - An Alternative Market-Based Approach to Governance.

In Futarchy, markets are used to decide on and implement policies. These markets follow a general form of “What will a future welfare metric be if a policy is implemented?”

For example, a corporation could ask, “What will our Q4 revenue be if we fire our CEO?” and conversely, “What will our Q4 revenue be if we don’t fire our CEO?” Following this, speculators who believe they hold unique insights into the outcome of firing or keeping the CEO are incentivized to participate in these markets. If they think that revenue will be maximized by firing the CEO, then they will buy long shares in the expected revenue if the CEO is fired and short shares in the expected revenue if the CEO is not fired. Upon market closure, a decision is made corresponding to the greater expected outcome. In our CEO example, if the market value for expected Q4 revenue if the CEO is fired is greater than the revenue if CEO is not fired market, then the organization fires the CEO. Market participants are then rewarded depending on their accuracy in predicting future revenue.

In this model, governance is both marketized and automated. Policies are determined by values found on an open market and implemented through bound delegates or an automated process. Prediction markets have shown to be the most efficient information aggregation tool leading to the prediction that Futarchy can more accurately identify policies that will optimize outcomes while also lowering bureaucratic overhead.

Futarchy Applications in a Variety of Institutions

Nearly all existing organizations can improve their model of governance by using an implementation of Futarchy. State governments can allow citizens to democratically vote on which metrics to optimize for and create markets to let the wisdom of the crowd inform how to reach those goals. Corporations can overhaul stockholder decision making using Futarchy while also reducing the need for high level management. Perhaps most interesting to the Ethereum and Blockchain ecosystem is the ability for Futarchy to provide a governance model for Decentralized Autonomous Organizations which is both effective and less reliant on centralized trust and decision-making processes.

Robin Hanson, the inventor of Futarchy and father of modern prediction markets, argues that

> Futarchy seems promising if we accept the following three assumptions:
>
> 1. Democracies fail largely by not aggregating available information.
> 2. It is not that hard to tell rich happy nations from poor miserable ones.
> 3. Betting markets are our best known institution for aggregating information.

The first of these conditions has become evident through political gridlock between parties, as well as yellow and captured journalism leading to a poorly informed populace. The second condition is provided by widely available metrics such as income per capita, GDP and the World Happiness Index, and the last is a conclusion of the efficient market hypothesis. Primary barriers to Futarchy adoption are lack of real world case studies, lack of general purpose Futarchy solutions, and entrenched institutions that are resistant to new models.

Conclusion

A prediction market is a powerful idea. A decentralized prediction market is an even more powerful idea. Once we combine the capability to automate predictions with AI, Machine Learning, and the Internet of Things, it becomes something that could change just about everything. It will result in being able to model externalities in a much better fashion.

Decentralized Exchanges and Peer-to-peer Trading

Interest in investing and trading cryptocurrencies has caused large amounts of wealth to be centralized on exchanges. While this allows for trades to happen quickly on the markets, with multiple buyers and sellers available, and easier price discovery, there is still risk related to volatility and security of these exchanges. If the exchange does not take care to use proper security, centralization leaves users of the exchange exposed to risk. The blockchain community has discussed and started working on peer-to-peer trading platforms or through exchanges entirely on the blockchain. Two ConsenSys projects have started to tackle this problem and their solutions are linked below, in case you are interested.

Introducing AirSwap - AirSwap Blog, 2017 [2 min read]

You can start by reading this quick overview (along with a link to the the AirSwap whitepaper), detailing a decentralized, peer-to-peer trading platform:

> The two forces behind our design are decentralization and peer-to-peer. Decentralization allows users to exchange value in a “trustless” way rather than depending on the security, ethics, and diligence of a central entity. Peer-to-peer allows users to quickly and privately trade with known counterparties, rather than posting orders to a public order book.

Introducing Omega One - ConsenSys Media, 2017 [4 min read]

This blog post introduces the Omega One platform as an decentralized broker between two traders. Member who want to trade will lock some of token A in a smart contract and send an order to trade to token B. Omega One will then take on a token B position in the market using our own exchange accounts and funds, then trade directly with the member as a simultaneous swap of tokens in the smart contract.

What is exciting about decentralized exchanges and peer-to-peer trading (and why we have devoted a short section to them in this e-book) is that it once again returns power to the individual to interact with any other individual. Engineering ways to do this safely allows for more individuals to participate in markets worldwide.

Price Stabilization

Adapted from StabL Bringing Stable Tokens and Derivative Products to the Ethereum Blockchain - VariabL Blog, 2017

One of the big problems holding back users from spending and vendors from accepting cryptocurrencies is the price volatility. Risk averse users avoid adopting crypto and risky investors hold and trade crypto rather than spend it. This has led to price fluctuations that have occurred over the last quarter of 2017 and the start of 2018.

In this section we explore a specific ConsenSys project looking to solve this problem by attempting to peg the value of crypto to more traditional assets like the United States Dollars (USD) or gold.

Stable Tokens

Stable tokens have been a leading topic of discussion since the birth of Ethereum. Using the decentralized platform that is the public Ethereum blockchain makes it necessary to hold ether, not only to use it as gas or fuel, but also to gain access to the shared public resource of the mainnet. This also makes it a standing store of value. The problem with using ether as a currency is that it is a currency with a variable price. If this obstacle of volatile price were overcome with the introduction of a cryptographic asset that tracks, for example, USD, it would pave the way for massive acceleration of Ethereum adoption.

What is at Stake?

A Stable token is a crypto-token that keeps a stable value against a specific index like the price of one US Dollar.

A crypto-token is a transferable asset stored on a blockchain. Every token stored on the Ethereum blockchain benefits from the properties of ether itself: distributed verification of transactions, pseudo-anonymity, almost instantaneous and low-fee transfers, censorship-resistance, access to smart contracts etc. A USD Stable token means mainly two things:

1. **Crypto-properties are added to dollars.** (You have an asset that has the same value as one USD bill but with better properties: you can do much more with it)
2. It is now possible to **store USD-stable values** within the blockchain with these tokens.

The Spectrum of Stable Assets

A stable asset is something you can own that keeps a stable value against an index. For instance a gold-stable asset that is worth 500g of gold today will be worth 500g of gold for its entire lifetime. There are plenty of different assets that fit this definition. Here is a list of them and an analysis of how they differ from one another:

Assets that directly represent gold:

- 500g of gold buried in a desert.
- 500g of gold ingots.
- 500 g of gold coins in a purse.
- Bank deposit box that contains 500 g of gold
- 500 DGX tokens (Ethereum tokens, cheer guys :))

Assets that are valued at a stable gold weight but do not directly represent gold:

- A contract with a friend that states they owe you 500g of gold, with a set due date that is 6 months from now.
- Gold ETF shares. (SPDR Gold Shares ETF for instance). Shares of a fund with variations that follow gold price variations.
- Position in a Contract For Difference (CFD) USD vs Gold (i.e: In 6 months from now, I will buy 500 g of gold at a specific price determined today)
- Gold StabL Tokens bought on StabL platform (Ethereum tokens that represent a position in an on-chain cash settled future contract. We will not focus on Gold StabL tokens in our early stages, but this is a good example to explain our approach)

Every previously listed asset has different properties. Let’s try to compare our listed assets with the most important properties.

Value Storage Property: Ownership of your Asset and its Underlying Value

What guarantees you that the underlying value of your asset will remain?

How secure is your ownership?

When you store gold yourself (coins, lingots, buried gold), you trust yourself. When you use a bank deposit box, you trust your bank not to be robbed (or to have good insurances). When you use an Ethereum token (StabL, DGX), you trust the Ethereum technology and yourself with the way that you store your private key.

It is difficult to rate these assets against this property since it depends a lot on ourselves? (How do I bury gold? How do I keep my private key? What Bank do I chose? How do I store the written contract I signed with my friend?).

Long term, we are convinced that owning a token that lives on a blockchain like Ethereum is the most secure way to own an asset. The Ethereum community is still in the early stage, but mature tools to store and back up private keys along with privacy will make owning tokens seamless yet secure.

Given that your ownership is secure what makes its value guaranteed?

Of course when owning physical gold, there is no risk of your asset losing value. When owning physical gold through a proxy (bank deposit box, DGX), you trust this proxy.

When owning a financial asset like Gold ETFs or Gold futures, it is a bit more complicated. The value is guaranteed by the robustness of the theoretical financial mechanism that includes an ecosystem of traders, arbitragers, hedgers, index providers, laws enforcers, etc. You also usually trust the exchange that gives you access to these assets.

Transferability: Ability to Transfer the Asset.

Gold coins are more transferable than lingots or raw gold but still need to be exchanged in the physical world. Buried gold or gold stored in a deposit box have poor transferability properties.

Ethereum tokens that represent a stable value of gold (DGX or Gold StabL Tokens) are definitely the assets that have the best transferability properties (20 sec on-chain transfers, instant using state channels, low fees, secure).

Liquidity: Ability to Trade the Asset.

For an asset to be liquid (meaning you can sell/buy a large amount of it quickly), you need it to be available on exchanges that have large volumes. Volume is one of the key factors that relate to velocity. The most liquid assets are positions in CFD/Futures and ETFs. Indeed, since they don't represent physical gold but positions in a financial system, it is easy to buy/sell them. You don't need to move any physical good.

New CFD/Future contracts can be created (on the so called primary markets) as soon as two parties agree on a Future contract. Then these two parties can sell their position in the Future contract (on secondary markets).

In today's financial world it harder for small investors to trade on the primary market. With Ethereum and easy digital contracts creations, this market becomes way more accessible: the difference between primary markets and secondary markets are blurred, making for an overall more efficient market.

StabL Tokens have the same mechanical properties: if our on-chain financial products (Futures-like products) attract a large number of traders (lot of Future contracts created), our tokens (that represent a position in one of these contracts) will be much more liquid than any gold-backed token. If there does not exist enough Future positions that are stable against USD (represented by a USD StabL token), you just create some by being matched with a trader around a Future contract as easily.

Non-Financial Properties: What can you do with these Assets?

Gold can be used to store value, to transfer value, to wear value, even to lend value as vehicles in contracts. Futures and ETFs have better trading properties since they are well suited for the internet world, yet they rely on centralized parties whereas gold, as a chemical element, relies on, well, physical trust-less laws.

On-chain stable tokens open a whole new world to gold. Both DGX and StabL Tokens can be used in smart contracts. For instance, they can be used as a currency in a trust-less crowdfunding platform like WeiFund. What is even more powerful with StabL tokens is that since their value is guaranteed by a decentralized game theoretical mechanism (based on Futures market), the only potential point of failure lies in the design or the implementation of the mechanism. Even if we think we have found a design that works in the on-chain world, we are very well aware that offering such a mechanism at all once is near impossible (especially in the current youth of the Ethereum ecosystem) and we differentiate ourselves by taking a lean approach.

Conclusion

We have just scratched the surface of the many topics in the ever evolving ecosystem of decentralized technologies. Congratulations!

If you want to expand your learning, go deeper into a particular topic, or are looking for information on something that is not covered here, please visit the ConsenSys Academy website for more information on educational offerings. We can also direct you to more resources and case studies, where you can deepen your knowledge and really dig into concepts in more granularity and mathematical detail. Please review the bibliography for sources and links for further reading. If there are any suggestions for additional content we can add to this book, please let us know. Welcome to this exciting space, we are happy to have you along for the journey!

Bibliography

What's The Big Deal?

Citations

Addy Yeow. (2018). Bitnodes. Retrieved from https://bitnodes.earn.com

About the Ethereum Foundation. (2018). Retrieved from https://www.ethereum.org/foundation

Enterprise Ethereum Alliance. (2018). Retrieved from https://entethalliance.org/

Further Reading

Institute for the Future (IFTF). (2016, April 18). Understand Blockchain in Two Minutes. Retrieved from https://www.youtube.com/watch?v=r43LhSUUGTQ

The Economist. (2015, October 31). The Trust Machine. Retrieved from https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Brian Armstrong. (2016, August 31). How Digital Currency Will Change the World. Retrieved from https://blog.coinbase.com/how-digital-currency-will-change-the-world-310663fe4332

Fred Wilson. (2016, July 31). The Golden Age of Open Protocols. Retrieved from http://avc.com/2016/07/the-golden-age-of-open-protocols/

Joseph Lubin. (2015, August 19). Darkest Before Ethereal Dawn. Retrieved from https://media.consensys.net/darkest-before-the-ethereal-dawn-63b351d0491c

Reid Hoffman. (2015, May 15). Why the Blockchain Matters. Retrieved from https://www.wired.co.uk/article/bitcoin-reid-hoffman

Deep Patel. (2017, June 4). Business in the Age of Ethereum. Retrieved from https://techcrunch.com/2017/06/04/business-in-the-age-of-ethereum/

Olaf Carlson-Wee. (2017, January 8). The Futuere is a Decentralized Internet. Retrieved from https://techcrunch.com/2017/01/08/the-future-is-a-decentralized-internet/

Principles of Decentralization

Citations

Vitalik Buterin. (2017, February 6). *The Meaning of Decentralization*. Retrieved from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Jesse Grushack. (2015, November 5). *Welcome to 3.0*. Retrieved from https://medium.com/@ConsenSys/welcome-to-3-0-f4552fb02302

Further Reading

Klint Finley. (2017, April 4). Tim Berners-Lee, Inventor of the Web, Plots a Radical Overhaul of His Creation. Retrieved from https://www.wired.com/2017/04/tim-berners-lee-inventor-web-plots-radical-overhaul-creation/

Don Tapscott. (2016, September 16). How the blockchain is changing money and business. Retrieved from https://www.youtube.com/watch?v=Pl8OlkkwRpc

Bettina Warburg. (2016, December 8). How the blockchain will radically transform the economy. Retrieved from https://www.youtube.com/watch?v=RplnSVTzvnU

A Brief History of Blockchain

Citations

Satoshi Nakamoto. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Further Reading

Nick Szabo. (2015, November 13). History of Blockchain. Retrieved from https://www.youtube.com/watch?v=7Y3fWXA6d5k

Andrew Keys. (2015, August 26). Here's the Epoch of Blockchain. Retrieved from https://media.consensys.net/it-was-the-best-of-times-it-was-the-worst-of-times-3fc8c0865c6c

Cameron McLain. (2017, July 8). A Brief History of Blockchain: An Investor's Perspective. Retrieved from https://medium.com/hummingbird-ventures/a-brief-history-of-blockchain-an-investors-perspective-387c440ad11c

Blockchain Basics

Citations

Ethash. (2017, August 3). Retrieved from https://github.com/ethereum/wiki/wiki/Ethash

Block #5000171. (2018, January 30). Retrieved from https://etherscan.io/block/5000171

Yunyun Chen. (2016, June 1). Guide: An Introduction to Encryption. https://media.consensys.net/guide-an-introduction-to-encryption-9afd17f5da6d

Yunyun Chen. (2016, June 3). Guide: Hashing. https://media.consensys.net/guide-hashing-33dc0467c126

Further Reading

Collin Thompson. (2016, October 2). How does the Blockchain Work?. Retrieved from https://medium.com/blockchain-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093

Sean Au. (2016, November 29). If you understand Hash Functions, you'll understand Blockchains. Retrieved from https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d

Tess Rinearson. (2017, July 21). Making Money Trustworthy. Retrieved from https://medium.com/@tessr/making-money-trustworthy-6c552a1cfc25

Aleksandr Bulkin. (2016, May 3). Explaining blockchain - how proof of work enables trustless consensus. Retrieved from https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

Public vs Private Blockchains

Citations

Vitalik Buterin. (2017, August 7). On Public and Private Blockchains. Retrieved from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

R. Tyler Smith. (2017, February 28). Public and Private Blockchains: Enemies or Allies? Why the Enterprise Ethereum Alliance will prove the latter. Retrieved from https://medium.com/@rtylersmith/public-and-private-blockchains-enemies-or-allies-45f050c38fc0

Further Reading

Collin Thompson. (2016, October 4). Private Blockchain or Database? . Retrieved from https://medium.com/the-intrepid-review/private-blockchain-or-database-whats-the-difference-523e7d42edc

Matt Chwierut. (2016, July 21). Asking Permission: What’s the difference between a public and private blockchain?. Retrieved from https://www.smithandcrown.com/permission-blockchains/

Connecting Blockchains Together

Citations

Paul Kohlhaas. (2017, February 7). An Introduction to Polkadot and Parachains. Retrieved from https://keepingstock.net/a-dummies-guide-to-polkadot-and-parachains-93708bd90775

Further Reading

Joseph Chow, Simon de La Rouviere. (2015, December 9). Taking Stock: Bitcoin and Ethereum. Retrieved from https://medium.com/@ConsenSys/taking-stock-bitcoin-and-ethereum-4382f0a2f17

Jae Kwon, Ethan Buchman. (1899, December 30). Cosmos: A Network of Distrubted Ledgers. Retrieved from https://cosmos.network/dev/whitepaper

The Ethereum Blockchain

Citations

Daniel Finley. (2017, February 16). Dan's Intro to How Ethereum Works. Retrieved from https://www.youtube.com/watch?v=-SMliFtoPn8

Further Reading

Daniel Oberhaus, Jordan Pearson. (2017, June 16). Okay, WTF is Ethereum?. Retrieved from https://motherboard.vice.com/en_us/article/newkqz/okay-wtf-is-ethereum

What is Ethereum?. Retrieved from http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

Karl Floersch. (2016, December 8). Introduction to Ethereum: The Internet's Government. Retrieved from https://karl.tech/intro-to-ethereum/

Fred Ehrsam. (2016, May 24). Ethereum is the Forefront of Digital Currency. Retrieved from https://blog.coinbase.com/ethereum-is-the-forefront-of-digital-currency-5300298f6c75

William Mougayar. (2015, May 24). The Business Imperative Behind the Ethereum Vision. Retrieved from https://blog.ethereum.org/2015/05/24/the-business-imperative-behind-the-ethereum-vision/

Ethereum Limitations and Scaling Solutions

Citations

Vitalik Buterin. (2017, July 6). IMO the most valid criticisms of Ethereum as it currently stands are. Retrieved from https://www.reddit.com/r/ethtrader/comments/6lgf0l/vitalik_drops_the_mic_on_rbtc/dju1y8q/

Vitalik Buterin. (2018, January 2). Ethereum scalability research and development subsidy programs. Retrieved from https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/

The Beam. (2017, December 7). The energy consumption of the crypto world. Retrieved from https://medium.com/thebeammagazine/the-energy-consumption-of-the-crypto-world-b20e3628e0d2

Giulio Prisco. (2017, November 29). The Ethereum Killer Is Ethereum 2.0: Vitalik Buterin’s Roadmap. Retrieved from https://bitcoinmagazine.com/articles/ethereum-killer-ethereum-20-vitalik-buterins-roadmap/

Further Reading

Vitalik Buterin. (2016, January 15). Privacy on the Blockchain. Retrieved from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

OkayOKay. (2017, May 29). I accidently lost the key to my wallet. Retrieved from https://ethereum.stackexchange.com/questions/16785/i-acccidently-lost-the-key-to-my-wallet

Alex Hern. (2017, November 8). $300m in cryptocurrency' accidentally lost forever due to bug. Retrieved from https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether

Fred Ehrsam. (2017, June 27). Scaling Ethereum to Billions of Users. Retrieved from https://medium.com/@FEhrsam/scaling-ethereum-to-billions-of-users-f37d9f487db1

A Further Discussion of Smart Contracts

Further Reading

Anthony Lewis. (2017, March 7). Three common misconceptions about smart contracts. Retrieved from https://bitsonblocks.net/2017/03/07/three-common-misconceptions-about-smart-contracts/

William Mougayar. (2016, March 23). 9 Myths Surrounding Blockchain Smart Contracts. Retrieved from https://www.coindesk.com/smart-contract-myths-blockchain/

Alyssa Jarrett. (2016, September 9). Busting Myths around Blockchains . Retrieved from https://ripple.com/insights/busting-myths-around-blockchains/

Tokens and Crowdfunding

Citations

Simon de La Rouviere, Ashley Taylor. (2015, December 2). A Token-Powered Future on Ethereum. Retrieved from https://medium.com/@ConsenSys/tokens-on-ethereum-e9e61dac9b4e

John Lilic. (2015, November 16). Ethereum Enabled Community Energy Market Sharing Economy Phase 2; Here's How ConsenSys is Building The TransActive Grid. Retrieved from https://www.linkedin.com/pulse/ethereum-enabled-community-energy-market-sharing-economy-john-lilic-6071756565017305088?trk=pulse_spock-articles

Simon de La Rouviere. (2015, December 1). DEVCON1: Tokens - Simon de la Rouviere. Retrieved from https://www.youtube.com/watch?v=kE5oGw8oKsY

Fabian Vogelsteller & Vitalik Buterin. (2015, November 19). ERC-20 Token Standard. Retrieved from https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

A Securities Law Framework for Blockchain Tokens. (2016, December 7). Retrieved from https://www.coinbase.com/legal/securities-law-framework.pdf

Further Reading

Nick Tomaino. (2017, March 14). The Token Economy. Retrieved from https://thecontrol.co/the-token-economy-81becd26b9de

Chris Dixon. (2017, June 1). Crypto Tokens: A Breakthrough in Open Network Design. Retrieved from https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef

Balaji Srinivasan. (2017, May 27). Thoughts on Tokens. Retrieved from https://news.21.co/thoughts-on-tokens-436109aabcbe

Fred Ehrsam. (2017, August 1). Blockchain Tokens and the dawn of the Decentralized Business Model. Retrieved from https://blog.coinbase.com/app-coins-and-the-dawn-of-the-decentralized-business-model-8b8c951e734f

Fred Ehrsam. (2016, November 2). How to Raise Money on a Blockchain with a Token. Retrieved from https://blog.gdax.com/how-to-raise-money-on-a-blockchain-with-a-token-510562c9cdfa

Vitalik Buterin. (2017, June 9). Analyzing Token Sale Models. Retrieved from http://vitalik.ca/general/2017/06/09/sales.html

Steven McKie. (2017, June 14). Understanding the Ethereum ICO Token Hype. Retrieved from https://medium.com/blockchannel/understanding-the-ethereum-ico-token-hype-429481278f45

Will Warren. (2017, February 2). The Difference between App Coins and Protocol Tokens. Retrieved from https://medium.com/0x-project/the-difference-between-app-coins-and-protocol-tokens-7281a428348c

Token Summit I - State of Tokens with Erik Voorhees, ShapeShift CEO. (2017, June 3). Retrieved from https://www.youtube.com/watch?v=0dl6ahjoBm8

Self-Sovereign Identity and Reputation

Citations

Dr. Christian Lundkvist, Andrew Keys. (2015, November 25). The Identity Crisis. Retrieved from https://medium.com/@ConsenSys/identity-is-defined-in-merriam-s-dictionary-as-who-someone-is-a3d6a69f5fa4

Further Reading

Michael Mainelli. (2017, March 16). Blockchain Will Help Us Prove Our Identities in a Digital World. Retrieved from https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world

Albert Wenger. (2014, March 10). Decentralizing Identity. Retrieved from http://continuations.com/post/79187457919/decentralizing-identity

Anthony Lewis. (2017, May 17). A Gentle Introduction to Self Sovereign Identity. Retrieved from https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

Noah Thorp, Harlan Wood. (2017, May 16). How Decentralized Reputation Can Help People Thrive. Retrieved from https://media.comakery.com/accessing-opportunity-with-portable-reputation-ae7112e64e97

Decentralized Governance and Voting

Citations

Nick Tomaino. (2017, February 28). The Governance of Blockchains. Retrieved from https://thecontrol.co/the-governance-of-blockchains-5ba17a4f5da6

Token Summit I - Blockchain Governance (featuring Z Wilcox, D Zakrisson, L Xie, J Zawistowiski). (2017, June 3). Retrieved from https://www.youtube.com/watch?v=JNSYYJj03Q8

Further Reading

Patrick Murck. (2017, April 19). Who Controls the Blockchain?. Retrieved from https://hbr.org/2017/04/who-controls-the-blockchain

Vlad Zamfir. (2017, June 1). Some Thoughts on Blockchain Governance. Retrieved from https://medium.com/@Vlad_Zamfir/some-thoughts-on-blockchain-governance-4b88e63d4e64

Ralph C. Merkle. (2016, May 31). DAOs, Democracy and Governance. Retrieved from http://merkle.com/papers/DAOdemocracyDraft.pdf

Dominik Schiener. (2015, October 28). PublicVotes: Ethereum-based Voting Application. Retrieved from https://medium.com/@DomSchiener/publicvotes-ethereum-based-voting-application-3b691488b926

Cryptoeconomics

Further Reading

Nick Tomaino. (2013, June 4). Cryptoeconomics 101. Retrieved from https://thecontrol.co/cryptoeconomics-101-e5c883e9a8ff

Kyle Wang. (2017, July 21). Cryptoeconomics: Paving the Future of Blockchain Technology. Retrieved from https://hackernoon.com/cryptoeconomics-paving-the-future-of-blockchain-technology-13b04dab971

Vitalik Buterin. Introduction to Cryptoeconomics. Retrieved from https://edcon.io/ppt/one/Vitalik Buterin_Introduction to Cryptoeconomics_EDCON.pdf

Decentralized Storage

Citations

ConsenSys. (2016, June 30). Decentralized Storage: The Backbone of the Third Web. Retrieved from https://media.consensys.net/decentralized-storage-the-backbone-of-the-third-web-d4bc54e79700

Dr. Christian Lundkvist, John Lilic. (2016, February 17). An Introduction to IPFS. Retrieved from https://medium.com/@ConsenSys/an-introduction-to-ipfs-9bba4860abd0

Viktor Trón, Aron Fischer, Dániel A. Nagy, Zsolt Felföldi, Nick Johnson. (2016, May). swap, swear and swindle:incentive system for swarm. http://swarm-gateways.net/bzz:/theswarm.eth/ethersphere/orange-papers/1/sw%5E3.pdf

Juniper Research. (2016, May 12). Cybercrime Will Cost Businesses Over $2 Trillion by 2019. http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Yunyun Chen. (2016, June 1). Guide: An Introduction to Encryption. https://media.consensys.net/guide-an-introduction-to-encryption-9afd17f5da6d

Yunyun Chen. (2016, June 3). Guide: Hashing. https://media.consensys.net/guide-hashing-33dc0467c126

Juan Benet. (2015, February 20). IPFS Alpha Demo. https://www.youtube.com/watch?v=8CMxDNuuAiQ

Protocol Labs. (2014, August 14). Filecoin: A Decentralized Storage Network. https://filecoin.io/filecoin.pdf

Further Reading

What is Storj?. (2016, September 28). Retrieved from https://medium.com/@storjproject/what-is-storj-part-1-of-3-the-storj-network-90fb1300112f

Max Kaplan. (2017, June 25). Sia: Blockchain’s Brightest Star. Retrieved from https://hackernoon.com/sia-blockchains-brightest-star-ab584992391

Prediction Markets

Citations

Simon de La Rouviere. (2015, December 16). Why & How Decentralized Prediction Markets Will Change Just About Everything. Retrieved from https://medium.com/@ConsenSys/why-how-decentralized-prediction-markets-will-change-just-about-everything-15ff02c98f7c
Matt Liston. (2016, May 4). Markets for the Future. Retrieved from https://medium.com/@ConsenSys/markets-for-the-future-c73fa73fe35d

Further Reading

Unclouded Vision.(2015, September 26). The Economist. Retrieved from https://www.economist.com/news/books-and-arts/21666098-forecasting-talent-luckily-it-can-be-learned-unclouded-vision

Cade Metz. (2017, March 22). Forget Bitcoin. The Blockchain Could Reveal What's True Today and Tomorrow. Retrieved from https://www.wired.com/2017/03/forget-bitcoin-blockchain-reveal-whats-true-today-tomorrow/

Vitalik Buterin. (2014, August 21). Introduction to Futarchy. Retrieved from https://blog.ethereum.org/2014/08/21/introduction-futarchy/

Decentralized Exchanges and Peer-to-Peer Trading

Citations

Introducing AirSwap. (2017, May 10). Retrieved from https://media.consensys.net/introducing-swap-a-protocol-for-decentralized-peer-to-peer-trading-on-the-ethereum-blockchain-d4058f3179cf

Introducing Omega One. (2017, June 8). Retrieved from https://media.consensys.net/introducing-omega-one-a-cheaper-and-safer-way-to-trade-cryptocurrencies-and-tokens-b59b9ccf29c4

Further Reading

Linda Xie. (2017, July 3). A beginner’s guide to 0x. Retrieved from https://blog.0xproject.com/a-beginners-guide-to-0x-81d30298a5e0

Price Stabilization

Citations

Hadrien Charlanes. (2017, February 16). StabL Bringing Stable Tokens and Derivative Products to the Ethereum Blockchain. Retrieved from https://blog.variabl.io/stabl-bringing-stable-tokens-and-derivative-products-to-the-ethereum-blockchain-df4d5eba89d9

Further Reading

Nick Tomaino. (2017, April 3). Stablecoins: A Holy Grail in Digital Currency. Retrieved from https://thecontrol.co/stablecoins-a-holy-grail-in-digital-currency-b64f3371e111

Vitalik Buterin. (2014, November 11). The Search for a Stable Cryptocurrency. Retrieved from https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/

Robert Sams. (2015, April 28). A Note on Cryptocurrency Stabilisation: Seigniorage Shares. Retrieved from https://github.com/rmsams/stablecoins/blob/master/paper.pdf

Rune Christensen, Nikolai Mushegian, Daniel Brockman, Kenny Rowe, Andy Milenius, Ryan Zurrer. (2017, October 17). The Dai Stablecoin System. Retrieved from https://github.com/makerdao/docs/blob/master/Dai.md

Rune4444. (2015, December 8). A list of stablecoin systems. Retrieved from https://www.reddit.com/r/Stablit/comments/3vzt82/list_of_stablecoin_systems/