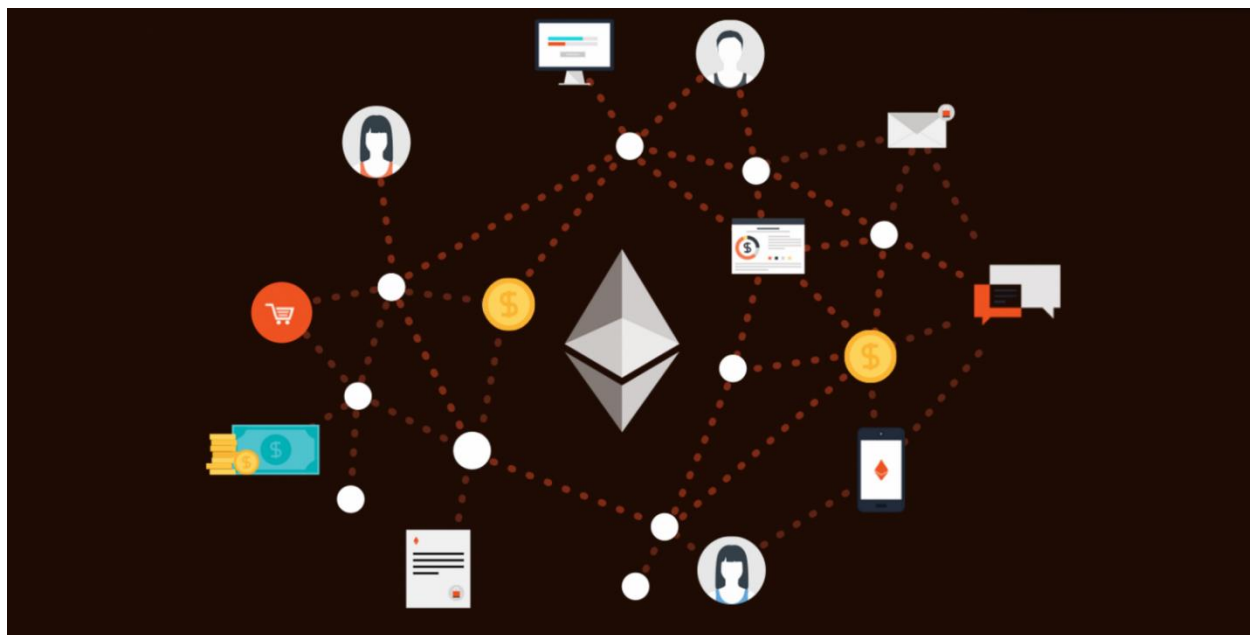


Ethereum and Decentralized Applications



Aaron Liao #14
February 13, 2018

Abstract

With the rise and crash of Bitcoin and Ethereum, cryptocurrencies are taking mainstream media by storm. Regardless of investor sentiment, the underlying technology driving cryptocurrencies, blockchain, will continue to serve a significant role in the future of technology. This paper will describe the building blocks of decentralized applications and their significance. It will also give an overview how Ethereum enables and incentivizes the creation of such applications. Finally, this paper will discuss new project startups utilizing blockchain tokens to raise funds through an Initial Coin Offering (ICO), and the ethical issues behind ICOs.

Keywords: Blockchain, Decentralized Applications, Ethereum, Initial Coin Offering (ICO), Smart Contracts, Tokens



Contents

INTRODUCTION.....	5
THE ETHEREUM PLATFORM.....	5
Smart Contracts and Blockchain Tokens	5
DECENTRALIZED APPLICATIONS	6
Sample Projects.....	7
Fundamental Differences	9
Ethereum Gas	10
Significance	10
ETHICAL ISSUES.....	11
White Papers and Initial Coin Offerings (ICOs)	11
Controversy.....	12
CONCLUSION.....	15
References	16
About the Author	17
Addendum	18
Readability	21

List of Illustrations

Figure 1: Substratum at a Glance [5]	7
Figure 2: Request Network B2B Invoicing [6]	8
Figure 3: Request Network Automated Audits [6]	8
Figure 4: Thin Protocol vs Fat Protocol [7]	9
Figure 5: Funds Raised Through ICOs [11]	11
Figure 6: Cascading Collapse due to BitConnect Shutdown [13]	13
Figure 7: Collapse of Total Cryptocurrency Market Cap in January 2018 [7]	13
Figure 8: Analysis of the Original TRON White Paper [14]	14

INTRODUCTION

In 2009, an anonymous figure known only by the pseudonym “Satoshi Nakamoto” released Bitcoin as the first cryptocurrency. The project’s aim was to take advantage of distributed computing power to create a decentralized currency—one that would work without a centralized entity like the Federal Reserve Bank. To accomplish this goal, Nakamoto introduced the blockchain concept. In short, blockchain is a ledger that is kept consistent across all computers. These computers continuously verify transactions by running cryptographic algorithms. Blockchain technology is decentralized by nature, and has since been adapted beyond its original use case. Now in 2018, blockchain serves as a base for thousands of decentralized applications. Much like how the internet revolutionized the world, decentralization is poised to become the next big step in the future of technology.

This paper will focus on decentralized applications. It will explain how the Ethereum platform allows for easy creation of smart contracts and tokens, which are the building blocks of decentralized applications. It will also introduce the wide variety of use-cases for decentralized applications, how they differ from traditional applications, and why they are important. Afterwards, there will be a discussion on the general methods of how these decentralized application projects launch, and the ethical issues surrounding these projects.

THE ETHEREUM PLATFORM



In 2013, 19-year-old Vitalik Buterin released a document describing the Ethereum project. In contrast to Bitcoin’s goal of simply using blockchain for currency, Buterin and a team of developers launched the platform in 2015. Ethereum provides a programming language that allows developers to easily leverage blockchain technology for their own applications. Now, with just “a few lines of code,” creators can quickly create smart contracts using the Ethereum blockchain [1].

Smart Contracts and Blockchain Tokens

Smart contracts are automated agreements with value associated with them [2]. The contract is published on the Ethereum blockchain, and is enacted when transactions are received [3]. A contract may involve the exchange of a certain number of *tokens*, which can

be a representation of any digital asset like transaction fees for a service or rewards for people offering computation power.

To better understand what these terms mean, imagine *tokens* being used to play arcade games. A player may exchange fiat currency like dollars or quarters into tokens using a change machine. The player then uses these tokens on arcade machines which are automated *smart contracts*. These contracts are programmed to accept a certain number of tokens, perform some function, and return entertainment value and tickets to the player. Notice that in this transaction there is no intermediary needed. Similarly in the cryptocurrency space, smart contracts are automatically executed and fulfilled whenever a transaction of tokens is sent to it.



Ethereum’s programming language makes it easy to create and deploy new contracts and tokens on the network. The ERC20 standard, developed by Fabian Vogelsteller, allowed for tokens to be compatible with each other. The cross-compatibility of ERC20 tokens allows for “seamless interaction with other smart contracts” [3]. In other words, the standard facilitates the easy exchange of tokens by using Ethereum as the common base. By defining a set of standard functions that must be implemented in every ERC20 compliant token, any token can be “easily recognized and understood in the Ethereum ecosystem” [4]. The standard was peer reviewed by the Ethereum developer community and published as a memorandum in November 2015. The interaction between smart contracts and tokens is significant in the many use-cases of decentralized applications.

DECENTRALIZED APPLICATIONS

A *decentralized application* is a smart contract with a user interface. End-users interact with decentralized applications in exactly the same way as with any other computer or smartphone applications. The difference is that instead of communicating with servers, decentralized applications communicate with the blockchain. In a centralized configuration, “designated hardware access points” handle data from all users. These high traffic areas become high profile “hacking targets to anyone seeking [users’] personal data” [5]. As a result, data breaches, or attacks, often involve the theft of millions of users’ data. On the other hand, a decentralized configuration removes the intermediary of central servers by distributing content across a large network of computers, eliminating high

traffic access points and thus increasing security [5]. Smart contracts on the blockchain network are cheaper and faster due to their autonomous nature and removal of intermediaries [6].

Sample Projects

One example of a decentralized application is Substratum, which aims to provide peer-to-peer web hosting. This contrasts with traditional web hosting in which central servers store web pages, images, videos, and other content. Figure 1 below shows a simple diagram describing how the Substratum system works.

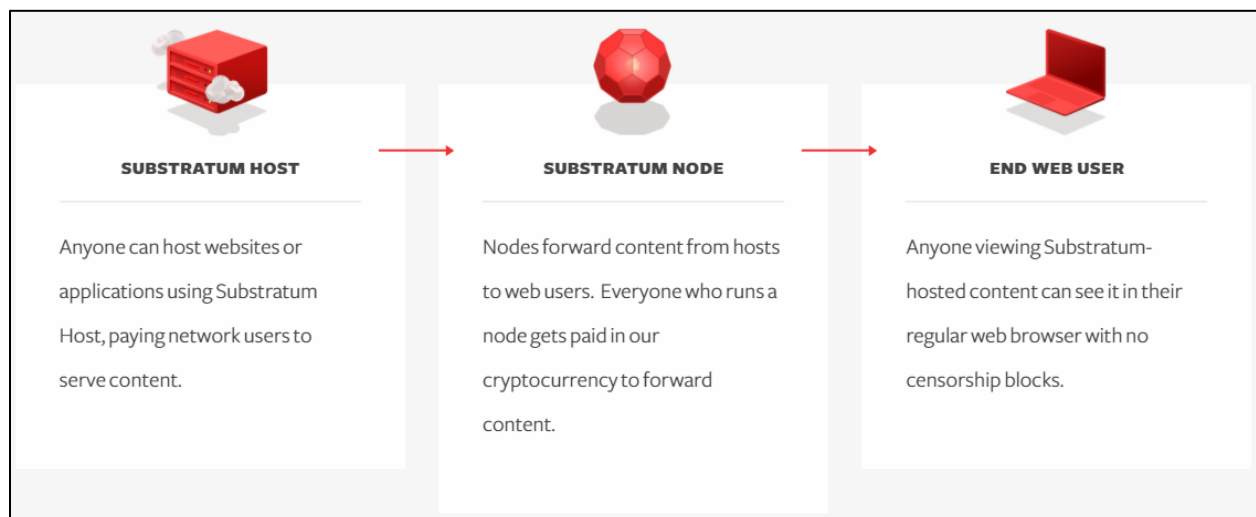


Figure 1: Substratum at a Glance [5]

Consider the following scenario: an Iranian journalist wishes to write articles freely without fear of persecution or censorship. The journalist purchases Substrate tokens and publishes a website onto the Substratum Network. Whenever a reader wishes to access the website, a Substratum Node forwards that content to the reader. Rather than a centralized server or data center providing content, a global network of individual computers act as Substratum Nodes [5]. Tokens are given as rewards to the individuals volunteering their computation power. To combat illegal or unwanted content on the network, each of these individuals have a share in voting on whether a website should be allowed or not. This consensus method restricts content by way of using society's moral compass rather than through censorship by a government or another central entity [5].

Request Network is another example of a decentralized application. Request Network seeks to automate and reduce the cost of a wide variety of financial applications [6]. To put it simply, by integrating traditional finance tools on an automated smart contract, there will be fewer possibilities of errors and less overhead associated with

business-to-business invoices [6]. Because of blockchain, all transactions are immutable and transparent. This means that auditing becomes a simple check on the system [6]. The simplification of these processes is shown in the following figures 2 and 3.

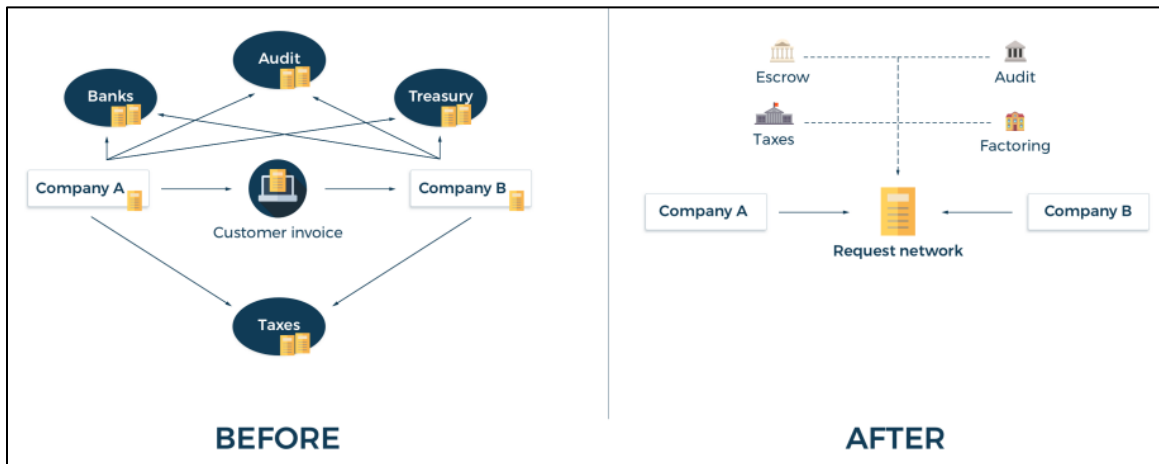


Figure 2: Request Network B2B Invoicing [6]



Figure 3: Request Network Automated Auditing [6]

In addition to business-to-business operations, Request Network can also handle business-to-consumer transactions. In this regard, Request Network also seeks to be an online payment method to replace PayPal. By combining the benefits of PayPal and a decentralized network, merchant cost can be decreased as transaction fees are reduced, and security can be increased as no sensitive credit card or banking information can be intercepted [6]. These are just a few of the benefits that a decentralized payment platform like Request Network can provide.

These brief descriptions of Substratum and Request Network demonstrate just a couple of the many different use-cases for decentralized applications. At the time of

writing, there are about 500 decentralized applications that are utilizing ERC20 tokens, 360 of which have market caps over \$1 million [7].

Fundamental Differences

Though decentralized applications can be for a variety of purposes, many projects are working towards developing protocols and infrastructure for blockchain. This higher concentration in the protocol level is known as “fat protocols.” This is in stark contrast to traditional Internet companies like Google and Facebook which started with building primarily on the application level [8]. The traditional internet startups that built applications saw higher returns on investment and thus more value was captured in developing applications rather than protocols [8]. In contrast, Bitcoin and Ethereum both hold market caps of over \$80 billion, compared to almost all applications built on top of them having market caps of less than \$1 billion. Thus, we can see that the value captured in cryptocurrencies is reversed compared to the traditional Internet [8]. Figure 4 below shows a visual representation of the blockchain’s fat protocol layer versus the internet’s fat application layer.

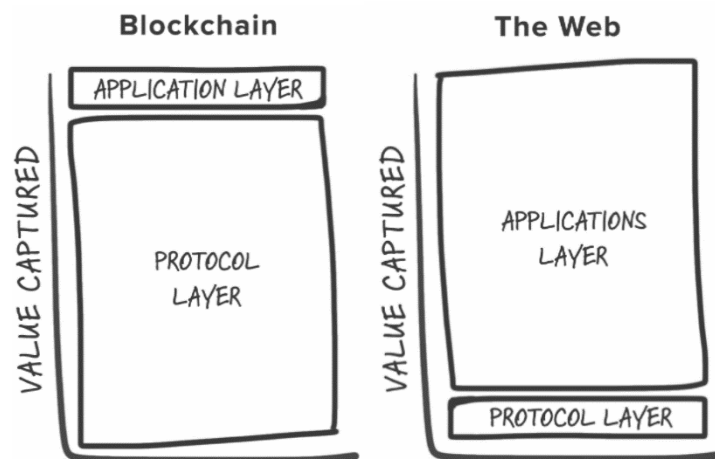


Figure 4: Thin Protocol vs Fat Protocol [8]

The reason there is more value found in the protocol layer in the cryptocurrency space is due to the *shared data layer* and the growth potential with decentralized applications [8].

Many protocols for blockchain are being developed as ERC20 compliant tokens because of the common interface it provides and the ease in which Ethereum allows smart contracts and tokens to be created. Since these tokens are attributed to the same Ethereum blockchain, the same set of resources and data is freely available to all Ethereum-based decentralized applications [9]. This is the concept of the *shared data layer*. Having the same protocols and blockchain allows for easy creation of decentralized applications. This

creates a low barrier to entry, resulting in a “vibrant and competitive ecosystem of products and services” [8]. The shared data layer on blockchain results in interoperability between services, meaning that an end user can easily switch between competing applications. Competition drives innovation and forces developers to build better products that users will want to use.

In addition to having the shared data layer, there is incentive in developing protocols from a market value perspective. Decentralized applications can easily leverage these protocols simply by using the token’s smart contract. In the future, as more and more projects are developed on the application layer of blockchain, protocols will be used to serve as the baseline for those new projects. Since “the success of the application layer drives further speculation at the protocol layer,” there is further incentive in developing protocols that future successful decentralized applications will use [8].

Ethereum Gas

All sorts of developers can write smart contracts, meaning that inexperienced programmers could publish inefficient or wasteful code on the blockchain. To address this issue, the designers of Ethereum created a mechanism called *gas*. All operations, including storage, memory, and processing, have a gas cost associated with them [3]. To inhibit contracts from performing heavy computation or storing copious amounts of data on the blockchain, Ethereum sets gas limits and charges contract owners a small transaction fee. Since operations are limited and not free, users are deterred from storing large amounts of data or performing large computations [3]. The concept of using gas for operations adds an element of competition to the development process. Gas cost incentivizes competing applications to optimize their algorithms so they can pass the savings onto end users in terms of lower transaction fees.



Significance

With the vast potential of use-cases for decentralized applications, there is a great amount of competition in developing well-designed, fuel efficient protocols for them to use. There is no doubt that there is enormous economic gain to be had in developing protocols, as “the market cap of the protocol always grows faster than the combined value of the applications built on top” [8]. In the future, however, we may very well see the fat protocols start to thin out, as decentralized applications start to supplant traditional centralized applications.

“The market cap of the protocol always grows faster than the combined value of the applications built on top”

ETHICAL ISSUES

With an understanding of decentralized applications and blockchain projects, we can now discuss the methods in which potential startups propose and start projects, and the ethical issues associated with them.

White Papers and Initial Coin Offerings (ICOs)

Every project begins with an idea. White papers are the most popular approach in describing an overview of a team’s goals and ambitions to the world. A white paper typically points out the shortcomings of current technologies, and then proposes a solution with a high-level explanation of the approach and implementation. For projects that use tokens, the white papers may also include the purpose and usage of those tokens and the means of distribution.

Cryptocurrency startups often finance their projects through token sales, or “initial coin offerings.” Substratum and Request Network both generated funding through an ICO, raising \$14 million in one month, and \$33.6 million in three days respectively [10]. Three months later, at the time of writing, their market caps have both increased five-fold to \$88 million and \$183 million respectively at the time of writing [10]. These figures are just a fraction of the billions of dollars that ICOs have raised. Figure 5 below shows the explosive increase in the amount of funds raised in initial coin offerings.

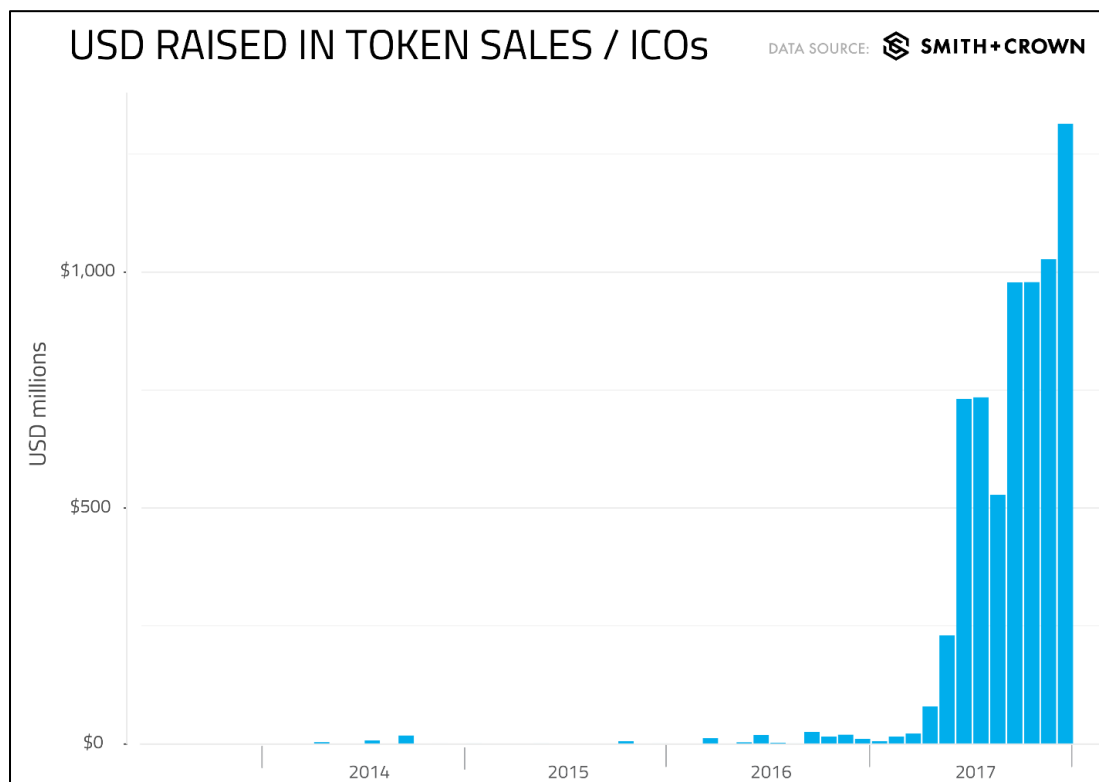


Figure 5: Funds Raised Through ICOs [11]

The recent explosive increase in token sale popularity is reminiscent of the dotcom bubble. With most projects easily increasing their market caps many times over in the course of just a few months or weeks, many investors are “jumping on the bandwagon” so to speak. This immense exuberance from “speculative investors look to cash in on initial coin offerings” is a clear indication of a bubble [12].

Controversy

1. SEC Shutdowns of ICOs

Since token sales are simply done online using other cryptocurrencies, these initial coin offerings can be performed extremely quickly, as we saw with Request Network’s raising of tens of millions in just a few days. The United States Securities and Exchange Commission (SEC) has shut down several illegal unregistered initial coin offerings in the past, with the most recent one in January of 2018 by a project called AriseBank [12]. This prospective decentralized bank “allegedly used celebrity endorsers — including boxer Evander Holyfield — and social media to swindle retail investors out of \$600 million of the firm’s \$1 billion goal” [12]. AriseBank’s controversy extends well beyond simple social media advertising tactics, with the project publishing a press release fabricating its acquisition of a Federal Deposit Insurance Corporation (FDIC) insured bank holding company [12].

2. Ponzi Schemes and Scams

The loosely regulated cryptocurrency environment has also recently caused the collapse of the infamous Ponzi scheme called BitConnect. With a peak market cap of over \$2 billion, the company announced its shutdown citing bad press and several cease-and-desist letters from multiple U.S. states [13]. The shutdown also halted users’ abilities to withdraw currency, essentially causing the disappearance of billions of dollars from the cryptocurrency market over the course of a day. Not only did the shutdown cause the loss of all investors’ assets, but it also cascaded into the collapse of the cryptocurrency bubble [13]. As seen in figure 6 on the next page, Bitcoin and Ethereum lost over 20% of their value in the crash of January 2018. This caused public sentiment to plummet, increasing the fear, uncertainty, and doubt in cryptocurrency’s viability [13]. This caused the total cryptocurrency market cap to fall from a peak of \$830 billion to a low of \$283 billion within the span of a month, as seen in figure 7 below [7].



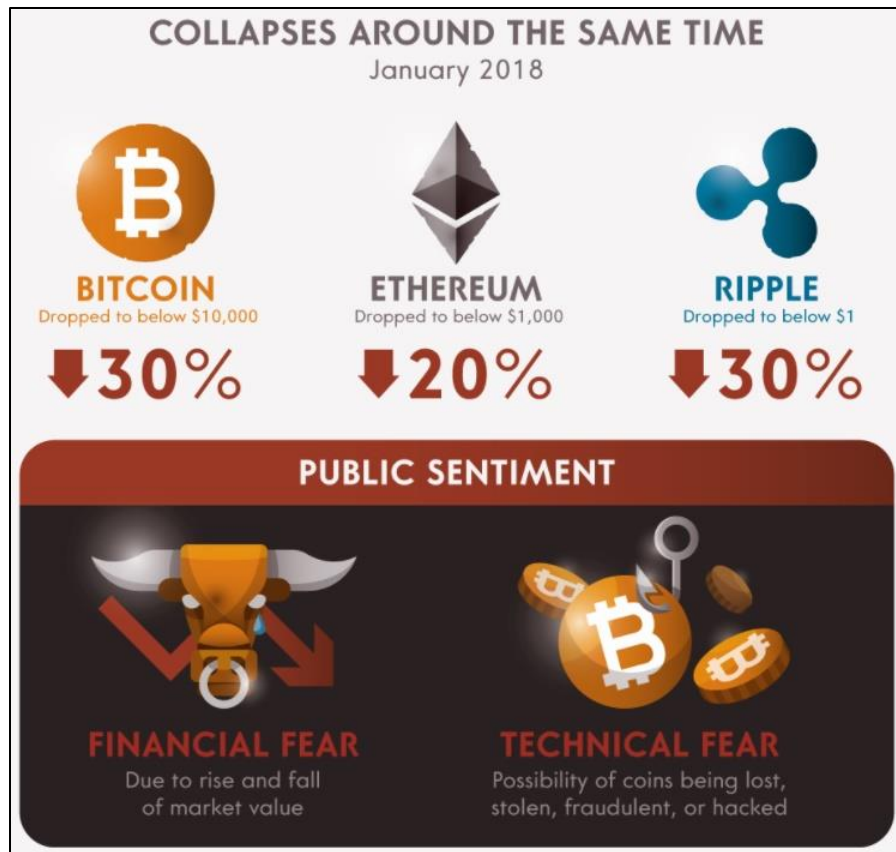


Figure 6: Cascading Collapse due to BitConnect Shutdown [13]

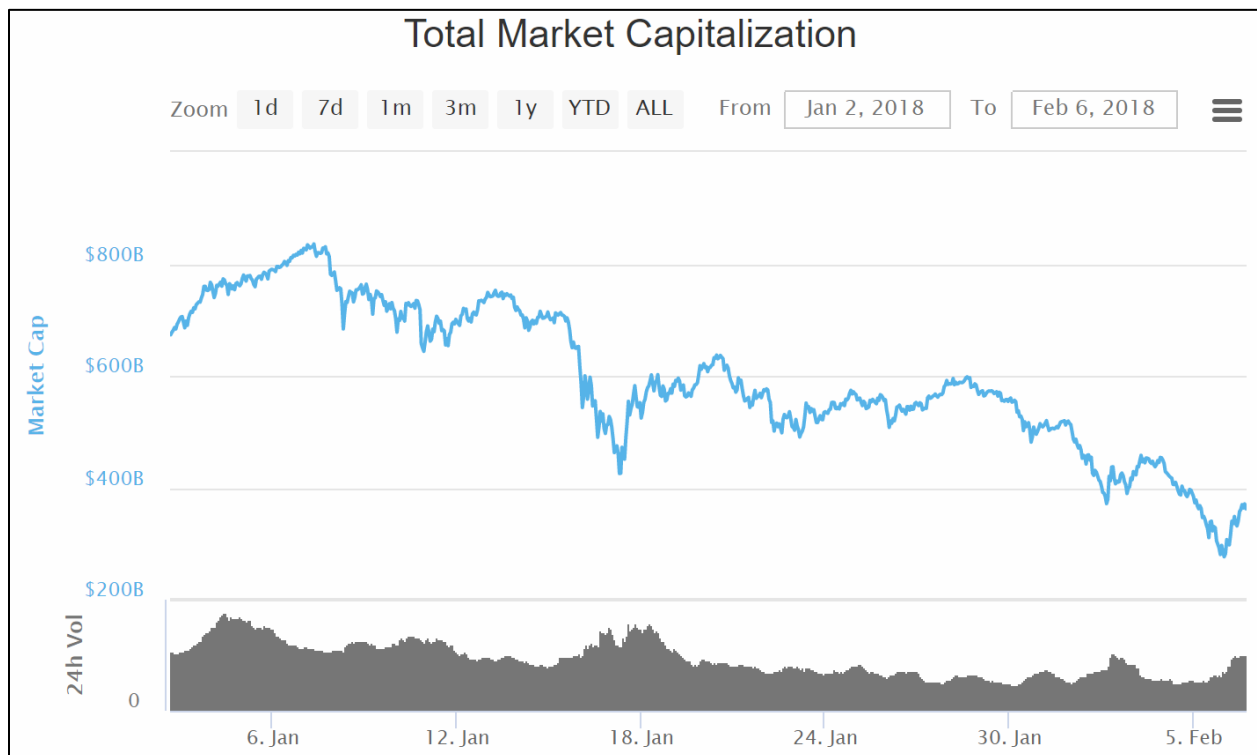


Figure 7: Collapse of Total Cryptocurrency Market Cap in January 2018 [7]

3. Plagiarized White Papers

Controversy among cryptocurrency projects also extends to the white papers that define the project's ambitions and goals. TRON, a decentralized application that seeks to build a free decentralized web for entertainment, generated over \$70 million in 3 days in its ICO [10]. Four months later, the market cap for TRON peaked at almost \$20 billion before the great BitConnect collapse [7]. However, an individual performed an analysis on TRON's published white paper and discovered that it lacked any references, and had large portions copied straight from other white papers [14]. Figure 8 below shows a breakdown of the plagiarized portions of the original TRON white paper.

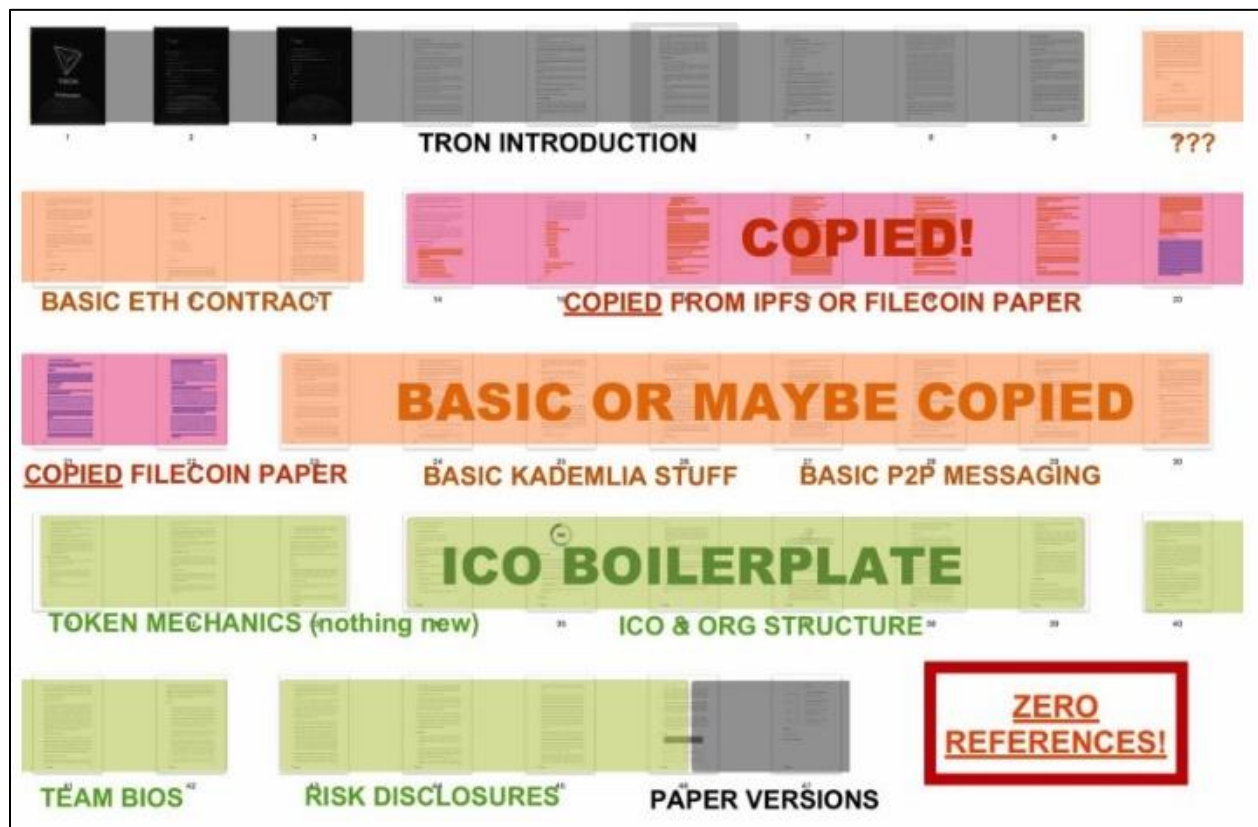


Figure 8: Analysis of the Original TRON White Paper [14]

TRON CEO Justin Sun claimed that this was simply a loss in translation from the original Chinese version of the white paper, even though there were no significant differences between the English and Chinese versions of the white paper [14]. The original white papers have since been removed from the TRON website, and at the time of writing have not been republished.

CONCLUSION

The underlying trend with bubbles is no different in the cryptocurrency space. With investor sentiment at an all-time high, there will undoubtedly be some companies that seek to raise funds through ICOs and profit solely on the bandwagon effect, often with white papers lacking substance or even copied straight out. However, history has shown repeatedly that technology does not simply disappear or fade from existence due to the bubble popping. After the dotcom bubble popped in 2000, what remained was a strong, but under-utilized internet infrastructure that was easily accessible to consumers [12]. What came afterwards was a surge of applications like Google, Facebook, and Amazon to build upon the infrastructure created by the surge of development that came beforehand [12].

Similarly, the Ethereum platform and other blockchain networks will serve as the infrastructure for decentralized applications and protocols of the future. With competition running rampant to develop the most efficient and scalable protocols for applications to build on top of, investor sentiment after the BitConnect collapse is only a minor correction to the potential value of blockchain technology. By looking past market value and more in depth into projects with substantial white papers and detailed plans for responsible governance, we can witness the ushering in of a new age of technology.

References

- [1] V. Buterin, "Ethereum White Paper", GitHub, 2013. [Online]. Available: <https://github.com/ethereum/wiki/wiki/White-Paper>.
- [2] C. Cusce, "What Are Smart Contracts and What Can They Do?", Medium, 2017. [Online]. Available: <https://medium.com/animal-media/what-are-smart-contracts-and-what-can-they-do-748899120d26>.
- [3] V. Dhillon, D. Metcalf and M. Hooper, "Blockchain Enabled Applications". Berkeley, CA: Apress, 2017.
- [4] Y. Chen, "Blockchain Tokens and the Potential Democratization of Entrepreneurship and Innovation", Assistant Professor, Stevens Institute of Technology, 2017.
- [5] J. Tabb, et al, "Substratum White Paper", Substratum, 2017. [Online]. Available: <https://substratum.net/wp-content/uploads/2017/12/Substratum-Whitepaper-English.pdf>.
- [6] E. Tatur, et al, "Request Network White Paper", Request Network, 2017. [Online]. Available: https://request.network/assets/pdf/request_whitepaper.pdf.
- [7] "Cryptocurrency Market Capitalizations", CoinMarketCap, 2018. [Online]. Available: <https://coinmarketcap.com/tokens/views/all/>. [Accessed: 12- Feb- 2018].
- [8] J. Monegro, "Fat Protocols", Union Square Ventures, 2016. [Online]. Available: <http://www.usv.com/blog/fat-protocols>.
- [9] J. Monegro, "The Shared Data Layer of The Blockchain Application Stack", joel.mn, 2014. [Online]. Available: <http://joel.mn/post/104755282493/the-shared-data-layer-of-the-blockchain>.
- [10] "ICO Drops", ICO Drops, 2018. [Online]. Available: <https://icodrops.com/>.
- [11] B. Downes, "2017 Token Sales in Review (Part I)", Smith + Crown, 2018. [Online]. Available: <https://www.smithandcrown.com/2017-year-review-part/>.
- [12] B. Carmody, "Understanding the Blockchain Bubble", Inc.com, 2017. [Online]. Available: <https://www.inc.com/bill-carmody/understanding-blockchain-bubble.html>.
- [13] "The Rise and Fall of Bitconnect", ValueWalk, 2018. [Online]. Available: <http://www.valuewalk.com/2018/02/bitconnect-alleged-fraud/>
- [14] "Tron's Whitepaper is Copied, Plagiarized", Hacker Noon, 2018. [Online]. Available: <https://hackernoon.com/trons-whitepaper-is-copied-plagiarized-cefce74335ce>.

About the Author



Aaron Liao is an undergraduate Computer Engineering major at the University of California, Irvine. His foray into technology and DIY was heavily influenced by being immersed in technology all throughout his academic career. Aaron's professional experience includes two internships at Boeing, with an upcoming full-time career at Western Digital. In his spare time, Aaron loves to travel the world and follow exciting new advancements in technology.

Aaron's most recent following in technology is cryptocurrencies, which is why he chose decentralized applications as the topic of this paper. To further his interest and understanding in this new field of technology, Aaron took this opportunity to research blockchain technology and decentralized applications for personal interest and development.

The most important takeaway that Aaron took from this research is that despite investor sentiment and volatility in the market, the blockchain concept will remain as a building block for the future of technology.

This work will affect Aaron's future professional life by offering a general understanding of how decentralization works, and how the future of the global industry may be look like with decentralization replacing the many centralized solutions of today.

Addendum

Decentralized Applications

Aaron Liao #14
February 8, 2018



Overview

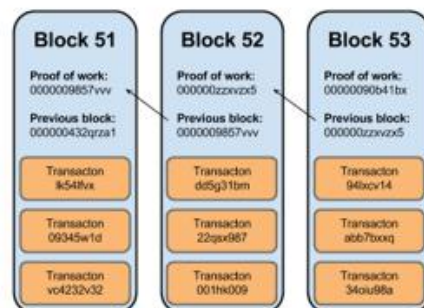


BLOCKCHAIN

- Significance of Blockchain
- Decentralized Applications
- Project Startups
- Ethical Issues

Introduction

- Current Technology
- Blockchain in a nutshell



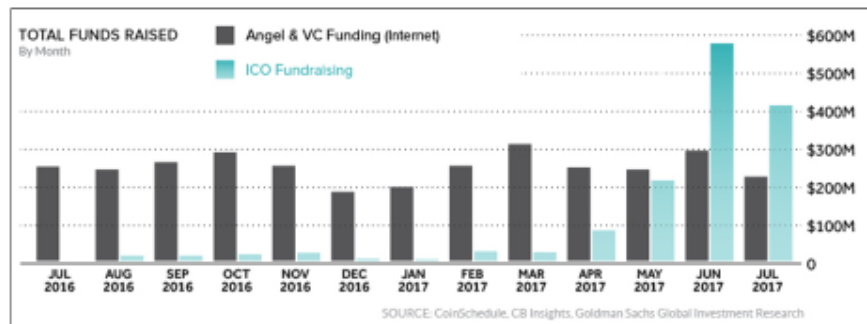
Decentralized Applications

- Tokens & Smart Contracts
- Analogy: Arcade machines
- Examples:
 - Stellar: Banking solution
 - Substratum: Web hosting
 - Request Network: Payment solution



Startups

- White papers
- Initial Coin Offerings (ICOs)



Ethical Issues

- ICOs as cash grabs
- Plagiarized white papers

SEC halts \$600 million alleged cryptocurrency scam that aimed to revolutionize banking

AriseBank claimed it was building the world's first "decentralized bank"

January 30, 2018 Ben Lane 0 Comments

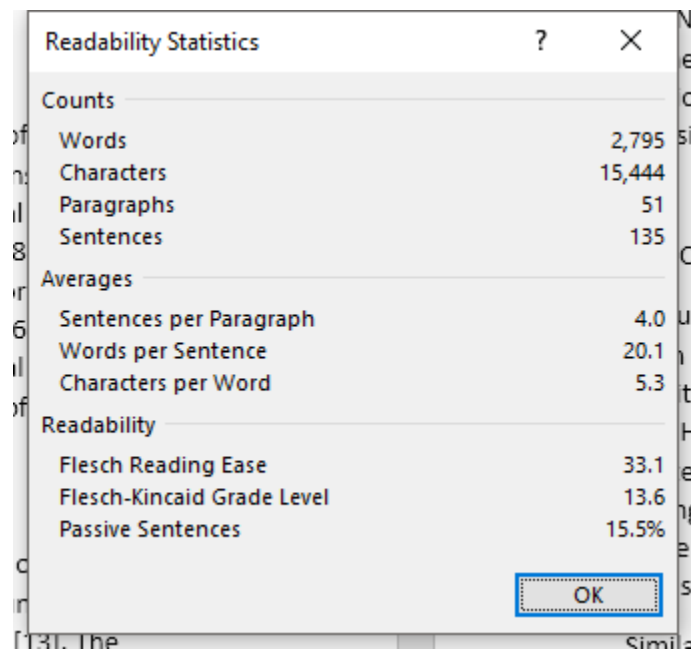


Conclusion

- Bandwagon → Bubble
- Dapps on Blockchain have disruptive potential



Readability



A screenshot of a 'Readability Statistics' dialog box. The dialog box has a title bar with a question mark and a close button. It contains three sections: 'Counts', 'Averages', and 'Readability'. Each section lists a metric and its corresponding value. An 'OK' button is located at the bottom right of the dialog box.

Readability Statistics	
Counts	
Words	2,795
Characters	15,444
Paragraphs	51
Sentences	135
Averages	
Sentences per Paragraph	4.0
Words per Sentence	20.1
Characters per Word	5.3
Readability	
Flesch Reading Ease	33.1
Flesch-Kincaid Grade Level	13.6
Passive Sentences	15.5%
OK	