The General Theory of Decentralized Applications, DApps

David Johnston, Sam Onat Yilmaz, Jeremy Kandah, Nikos Bentenitis, Farzad Hashemi, Ron Gross, Shawn Wilkinson and Steven Mason

Contents

INTRODUCTION

THE EMERGENCE OF DAPPS

A new model for building successful and massively scalable applications is emerging. Bitcoin led the way with its open-source, peer-to-peer nature, cryptographically-stored records (block chain), and limited number of tokens that power the use of its features. Several applications are adopting the Bitcoin model in order to succeed. BitShares, Mastercoin and Open Garden are just a few of those "decentralized applications" that use a variety of methods to operate. Some use their own block chain (BitShares), some use existing block chains and issue their own tokens (Master Protocol and Mastercoin), and others operate at two layers above an existing block chain and issue their own tokens (OpenGarden).

This paper describes why decentralized applications have the potential to be immensely successful, how the different types of decentralized applications can be classified, and introduces terminology that aims to be accurate and helpful to the community. Finally, this paper postulates that these decentralized applications will some day surpass the world's largest software corporations in utility, user-base, and network valuation due to their superior incentivization structure, flexibility, transparency, resiliency, and distributed nature.

DEFINITION OF A DAPP

For an application to be considered a DApp, it must meet the following criteria:

1. The application must be completely open-source, it must operate autonomously, with no entity controlling the majority of its tokens, and its data and records of operation must be cryptographically stored in a public, decentralized block chain.
2. The application must generate tokens according to a standard algorithm or set of criteria and possibly distribute some or all of its tokens at the beginning of its operation. These tokens must be necessary for the use of the application and any contribution from users should be rewarded by payment in the application's tokens.
3. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by majority consensus of its users.

BITCOIN AS A DAPP

Satoshi Nakamoto, the creator of Bitcoin described his invention as "A Peer-to-Peer Electronic Cash System[2]". Bitcoin has been shown to effectively solve the problems that arise from a trustless and scalable electronic cash system by using a peer-to-peer, distributed ledger, the Bitcoin block chain. In addition to being a peer-to-peer electronic cash system however, Bitcoin is also an application that users can interact with through computer software). But most importantly for the purposes of this paper, based on the criteria outlined above, Bitcoin is a decentralized application. Here is why:

1. All Bitcoin software applications are open-source, no entity (government, company, or organization) controls Bitcoin and all records related to the use of Bitcoin are open and public.
2. Bitcoin generates its tokens, the bitcoins, with a predetermined algorithm that cannot be changed, and those tokens are necessary for Bitcoin to function. Bitcoin miners are rewarded with bitcoins for their contributions in securing the Bitcoin network.
3. All changes to Bitcoin must be approved by a majority consensus of its users through the proof-of-work mechanism.

NOMENCLATURE AND ITS IMPORTANCE

Decentralized applications were initially described as Decentralized Autonomous Corporations, DAC, in an article written by Daniel Larimer, of Invictus Innovations. This papers avoids the term corporation for two reasons.

First, because it carries with it unnecessary preconceptions. For instance, a corporation is established in a jurisdiction, it has shares, a CEO, employees, etc. DApps, like Bitcoin, have none of these characteristics. In addition, the narrative is very important for the way DApps are perceived by various nations and jurisdictions. The same way that governments struggle to learn and regulate Bitcoin because the concept of currency is associated with it, governments might be compelled to regulate an open-source computer program that is a decentralized application.

Second, because traditional corporations may engage in several techniques to raise capital (like selling shares of its stock and pay dividends or borrowing against its stock and pay interest) that a DApp does not need. The concept of a DApp is so powerful and elegant, because it does not include these traditional corporate techniques. The ownership of the DApp's tokens is all that is required for the holder to use the system. It's that simple. The value of the tokens is determined by how much people value the application. All the incentives, all the monetization, all the qys to raise capital are built into this beautifully simple structure. DApps are not required to recreate the functions that used to be necessary in centralized corporations in order to balance the power of shareholders and offer returns for investors and employees.

CLASSIFICATION OF DAPPS

There are several characteristics according to which decentralized applications can be classified. For the purposes of this paper, we will classify DApps based on whether they have their own block chain or they use the block chain of another DApp. Based on this criterion, there are three types of DApps.

Type I decentralized applications have their own block chain. Bitcoin is the most famous example of a type I decentralized application but Litecoin and other "alt-coins" are of the same type.

Type II decentralized applications use the block chain of a type I decentralized application. Type II decentralized applications are protocols and have tokens that are necessary for their function. The Master Protocol is an example of a type II decentralized application.

Type III decentralized applications use the protocol of a type II decentralized application. Type III decentralized applications are protocols and have tokens that are necessary for their function. A hypothetical Cloud Protocol that uses the Master Protocol to issue 'cloudcoins' that can be used to acquire cloud computing services would be an example of a type III decentralized application.

A useful analogy for a type I DApp is a computer operating system (like Windows, Mac OS X, Linux, Android, iOS) for a type II DApp a general purpose software program (like a word processor, a spreadsheet software, a file synchronization system such as Dropbox) and for type III DApp, a specialized software solution (like a mail-merge tool that uses a word processor, an expense report macro that uses a spreadsheet, or a blogging platform that uses Dropbox.) Using this analogy, it may be expected that due to network effects and the ecosystem surrounding each decentralized application, there will be a few type I DApps, more type II DApps and even more type III DApps.

At this point, it is important to mention that there are currently several excellent open-source projects that leverage type I DApps. Colored coins and CoinJoin, for example, are based on the Bitcoin block chain and provide useful features to their users. These projects however cannot be classified as type II DApps, according to our definition, because they don't issue and manage a token. (The development and operation of these projects depends on donations instead.)

THE OPERATION OF A DAPP

MECHANISMS FOR ESTABLISHING CONSENSUS

There are two common mechanism by which DApps can establish consensus: the **proof-of-work**, POW, mechanism and the **proof of stake**, POS, mechanism.

With the proof-of-work mechanism, decisions about changes in a DApp are made based on the amount of work that each stakeholder contributes to the operation of the DApp. Bitcoin uses that approach for its day-to-day operation. The mechanism for establishing consensus through POW is commonly called mining.

With the proof-of-stake mechanism, decisions about changes in the DApp are made based on the percent ownership that various stakeholders have over the application. For instance, the vote of a stakeholder who controls 10% of the tokens issued by a DApp, carries a 10% weight. The Master Protocol is based on the POS mechanism.

The two mechanisms can be used in parallel, as is the case with Peercoin. Such a combination allows a DApp to operate with less energy consumption than proof-of-work alone, and allows it to be more resistant to 51% attacks.

MECHANISMS FOR DISTRIBUTING TOKENS

There are three common mechanisms by which DApps can distribute their tokens: mining, fund-raising and development.

With the mining mechanism, tokens are distributed to those who contribute most work to the operation of a DApp. Taking Bitcoin as an example, bitcoins are distributed through a predetermined algorithm to the miners that verify transactions and maintain the Bitcoin block chain.

With the fund-raising mechanism, tokens are distributed to those who fund the initial development of the DApp. Taking the Master Protocol as an example, Mastercoins were initially distributed to those who sent bitcoins to a given address at the rate of 100 Mastercoins per bitcoin sent. The bitcoins collected were then used to fund the development of applications that promoted the development of the Master Protocol.

With the development mechanism, tokens are generated using a predefined mechanism and are only available for the development of the DA. For example, in addition to its fund-raising mechanism, the Master Protocol used the collaboration mechanism to fund its future development. An additional 10% of the Mastercoins generated through fund-raising was set aside for development of the Master Protocol. Those Mastercoins become available through a pre-determined schedule and are distributed via a community-driven bounty system where decisions are made based on the proof-of-stake mechanism.

To summarize: Tokens of a DApp that establishes consensus through proof-of-work are distributed by mining, by people buying directly from miners and by trading for goods and services; that is the case with Bitcoin. Tokens of a DApp that establishes consensus through proof-of-stake are distributed based on the contribution of stakeholders during a fundraiser, by people collaborating on the development of the DApp and by trading for goods and services; that is the case with the Master Protocol.

FORMATION AND DEVELOPMENT OF A DAPP

Development of decentralized applications takes place in three steps.

Step 1: A whitepaper is published describing the DApp and its features

As in the case of Bitcoin, the most common way by which a DApp takes form is by the public release of a whitepaper that describes the protocol, its features, and its implementation. After the public release, feedback from the community is necessary for the further development of the DA.

Step 2: Initial tokens are distributed

If the DApp is using the mining mechanism to distribute its tokens, a reference software program is released so that it can be used for mining. In the case of Bitcoin, a reference software program was released and the initial transaction block was created.

If the DApp is using the fund-raising mechanism, a wallet software becomes available to the stakeholders of the DApp, so that they can exchange the tokens of the DA. In the case of Mastercoin, an Exodus fund-raising address and a wallet script were publicly released.

If the DApp is using the development mechanism, a bounty system is put in place that allows the suggestion of tasks to be performed, the tracking of the people who are working on those tasks and the criteria by which bounties can be awarded.

Step 3: The ownership stake of the DApp is spread

As tokens from mining, fund-raising and collaboration are distributed to a greater number of participants, the ownership of the DApp becomes less and less centralized and participants that held a majority stake at earlier have less and less control. As the DApp matures, participants with more diverse skills are incentivized to make valuable contributions, and the ownership of the DApp is distributed further. Through market forces the tokens of a DApp are transferred to those who value it the most. Those individuals then can contribute to the development of the DApp in the areas that they have an expertise.

The case of Bitcoin illustrates the point. By some estimates, Satoshi Nakamoto mined many of the first 1,000,000 bitcoins. As developers contributed code to Bitcoin and miners contributed computational power to the Bitcoin network, the market began to value bitcoins more highly. As the system matured even more, people with diverse skills started valuing Bitcoin and contributing to its development. Now that more than 12 million bitcoins are in circulation and Satoshi Nakamoto's high original ownership stake has been diluted.

LEGAL MODEL FOR THE OPERATION OF DAPPS

Operating under open-source licenses allows DApps to be open for innovation without restrictions of copyright or patent. In addition, by being completely open-source, decentralized applications can operate under the legal model of open-source software. Bitcoin, for example, uses the MIT open-source software license. The Master Protocol similarly, requires all code that is based on it to be open-source and available to the community.

ISSUANCE AND HOLDING OF TOKENS

From a technical perspective, those issuing tokens as part of a crowd-sale are selling access to software for the users of that software. The private keys associated with the tokens that the users purchase are literally the passwords that the users need to access a DApp's software. From a tax perspective, those holding tokens are holding digital property. If the tokens have no market value outside of their use in the DApp, it is hard to determine their actual value.

Because very few jurisdictions have publicly given guidance on how tokens issued by DApps will be treated from a regulatory and tax perspective, legal expert in the particular jurisdictions should be consulted.

NON-PROFIT ORGANIZATION

There are no legal entities required for a DApp to operate because it is not a company. Owners of tokens do not need to be represented by a corporation and contributor do not need any specific legal entity either. However, sometimes tokens are issued by a non-profit organization that will never receive financial benefits from the DApp. Such an organization will have the following responsibilities:

1. Issuance of initial tokens
2. Holding of developer tokens
3. Management of bounty payments
4. Determining the DApp direction

Ideally, the non-profit organization will make decisions in a decentralized manner, using a "proof of stake" voting mechanism for any decision.

BEST PRACTICES FOR CREATING A DAPP AND FREQUENTLY ASKED QUESTIONS

WHAT QUALIFIES A SOFTWARE APPLICATION AS A DAPP?

1. The application must be completely open-source, it must operate autonomously, with no entity controlling the majority of its tokens, and its data and records of operation must be cryptographically stored in a public, decentralized block chain.

2. The application must generate tokens according to a standard algorithm or set of criteria and possibly distribute some or all of its tokens at the beginning of its operation. These tokens must be necessary for the use of the application and any contribution from users should be rewarded by payment in the application's tokens.

3. The application may adapt its protocol in response to proposed improvements and market feedback but all changes must be decided by majority consensus of its users.

WHAT IS A TOKEN?

The purpose of a token is to allow access to a computer application. For example, an individual must own a number of bitcoins in order to be able to perform any transaction on the Bitcoin network. Tokens in DApps do not represent any underlying asset, they do not give rights to a dividend, and no equity is represented through them. Although the value of a DApp token may increase or decrease over time, tokens are not equity securities.

HOW DO TOKENS GET DISTRIBUTED?

There are several ways by which the tokens of a DApp may be distributed:

1. Crowd-sale tokens: An initial one-time sale of tokens is a common way to initially fund a DApp. The funds raised from such a crowd-sale should be controlled by an entity that is independent of the founders, commonly a Foundation.
2. Developer tokens: A portion of the tokens can be set aside for developers working on the project. As the market sets a valuation for the project, the developer tokens will gain value, attracting additional contributors to the project.
3. Premined tokens: It is best if no tokens are premined because most communities and investors are negatively predisposed to it. A premine may be successful only if a meaningful reason is provided by the founders.
4. Minable tokens: Distribution of tokens by mining incentivizes the community to contribute resources to the DApp. In Bitcoin for example, there is a block reward every ten minutes, that incentivizes miners to provide hashing power to Bitcoin. Similarly, DApps need to determine how to incentivize the network to contribute the required resource as this is the most important decision about the token distribution.

HOW DO I START DEVELOPING A DAPP?

To develop a DApp it is advised to follow these steps:

1. Create a whitepaper that has at least the following sections:
    - Intentions and goals of the DApp
    - Plans for token distribution
    - Mechanism for establishing consensus
    - Structure of the non-profit that oversees the DApp
    - Management of developer bounties
    - Technical description of the DApp
2. Gain community engagement by releasing the plan and by revising it based on feedback.
3. Set a date when the community can contribute to the crowd-sale.
4. Sell the initial tokens based on your whitepaper and establish a non-profit to oversee the development of the DApp.
5. Begin executing your idea while the non-profit plans future development.

WHY IS A DAPP A PROFITABLE MODEL FOR DEVELOPERS, USERS AND CONTRIBUTORS?

The model allows contributors to get involved with the project as purchasers of tokens, as project contributors or as providers of resources to the network. All of these contributors benefit from the exchange of the tokens and from the possible appreciation of their value.

WHAT IS A USER-BEHAVIOR REWARD?

A user-behavior reward is given to contributors that provide utility to the network. The whitepaper should outline what constitutes utility for the DApp. (For example, hashing power is utility on the Bitcoin network and it is rewarded.) Utility should be measurable, like in the case of a data storage DApp, amount of storage is measurable.

THE CURRENT STATE OF TYPE II AND III DAPPS

One mechanism by which type II DApps can leverage the block chain of type I DApps is by embedding additional data to the transactions taking place in the type I DA. The Master Protocol, for example, embeds additional data on the transactions of the Bitcoin network. Although currently (February 2014) Mastercoin embeds its additional data in an ad-hoc way into the Bitcoin block chain, the release of the 0.9 version of the Bitcoin reference client will provide a standard method for that embedding. By using the methodology of "provably prune-able outputs," type II decentralized applications that are based on Bitcoin will be able to embed data in a systematic way and Bitcoin miners will have the option to prune those data.

Given this development, several type III DApps are in various stages of development. They include:

- MaidSafe provides a "proof of resource" mechanism and decentralized data structure for storing files privately or publicly in the cloud.
- StorJ provides a front-end, Dropbox-like cloud storage of files utilizing MaidSafe and other systems in the back-end.
- Ethereum provides consensus-based scripting and computing resources.
- OpenGarden provides mesh network-based Internet services.
- Scalion provides an incentivized version of the Tor Network with nodes serving as Tor relays and exits.
- Shared Miles provides a proof of transportation mechanism that allows for an open source transportation standard.
- BlockAuth provides a multi signature OAuth-style system for sharing private data with third parties.
- API Protocol provides an open source standard for hosting, normalizing, and sharing API data.

CONCLUSION

DApps have the potential to become self-sustaining because they empower their stakeholders to invest in the development of the DApp. Because of that, it is conceivable that DApps for payments, data storage, bandwidth and cloud computing may one day surpass the valuation of multinational corporations like Visa, Dropbox, Comcast, and Amazon that are are currently active in the space.

APPENDIX

RESOURCES FOR AN ECONOMIC MODEL OF DAPPS

- A comparison between Metcalfe's, Zipf's and Bitcoin's law.

"In fact there is a strong correlation (R2 = 0.82) between number of users and price. All these things are not understood by too many people, unfortunately. Also the price doesn't grow linearly with the number of users but instead with the power of 1.45 of the number of users. That is nice because for the price to increase 1000 times you need only 140 times the number of users of today. We have about 2 million BTC users." https://i.imgur.com/CiOxeBY.jpg. Credit for images and quote gsantostasi.

- Correlation between the value of a DApp and Metcalfe's Law. Credit for image Peter R.

A PROPOSED METAPHOR FOR DAPPS

It would be beneficial to have a well-grounded and easily accessible metaphor for DApps. Such a metaphor would ideally have the virtue of simplexity, so that it could be used for human-computer interfaces.

Such a metaphor could be a zygote. A zygote is the point where one biological cell generation ends and the next one begins. A zygote acclimates, and it responds to the outside world without changing its genes, it cannot be regulated, it is stuck with its own genes and its recursive. The zygote is autonomous because it is stuck with its own genes, it is an application because it is a cell, it is distributed, and it is authorized to act as a single entity from other other cells; it shares, in other words many of the characteristics of a decentralized application.

Terms that could created out of the term zygote include *zyprotocol*, the zygotic protocol, *zapp*, the zygotic application, *zen*, the zygotic entity, and *zybit*, the zygotic bit.

JOHNSTON'S LAW

"Everything that can be decentralized, will be decentralized". David A. Johnston

Based on the economic and efficiency advantages of decentralized applications its clear that existing centralized services will be displaced over time by decentralized alternatives. This shift is likely to come most quickly for services in which the network effect advantages of Metcalfe's Law are most critical to the success of the service provider.