BitTorrent (BTT) White Paper

v0.8.7

Feb. 2019

Abstract

The BitTorrent protocol, created by BitTorrent Inc., facilitates the exchange of files between untrusted parties. Its primary limitation is that collaborations between parties using the protocol cannot persist over time, inhibiting the exchange. Blockchain technologies allow for collaborations between untrusted parties to persist over much longer periods of time. BitTorrent has the ecosystem and expertise necessary to integrate blockchain technologies into the BitTorrent protocol. Doing so would both eliminate the protocol's existing flaw as well as open up a new borderless economy in exchanging value for computing resources on a global scale.

To accomplish this, TRON Foundation and BitTorrent Foundation are introducing a new cryptographic token, called BTT, along with an extended version of the BitTorrent protocol. Together, the token and extended protocol will create a token-based economy for networking, bandwidth and storage usage. The initial entry point is to introduce token-based optimizations to the existing BitTorrent protocol, providing a way for the value of shared bandwidth to be captured by network participants. The longer-term vision is to broaden the usage of the BitTorrent protocol far beyond current use cases by providing a distributed infrastructure platform to third-party app developers, creating the foundation for the decentralized web.

The TRON Foundation and BitTorrent Foundation are legal entities incorporated in the Republic of Singapore.

BitTorrent Background

The BitTorrent Protocol

BitTorrent is a pioneering distributed communication protocol invented by Bram Cohen in 2001. As a peer-to-peer protocol, it facilitates the transfer of large, highly demanded files, eliminating the need for a trusted central server.

The BitTorrent protocol enables client software endpoints ("clients") to collaborate with each other to enable reliable simultaneous distribution of large files to multiple clients, reducing reliance on any single weak point (such as a server connection). It does this by attempting to make efficient use of every client's upload and download bandwidth to balance peer-to-peer content delivery across all clients.

To find a peer that has a file or portion thereof, peers either "announce" to a tracker, a server that keeps track of which peers have which files available, or find them via the DHT, a distributed database of peers. Through this process, all peers are naturally segmented into "swarms" of users, with every user in each swarm having a common interest in exchanging pieces of a specific file.

Before an exchange begins, files are cut into pieces. Clients advertise which pieces of a file their user has available, and those pieces are uploaded by users who have them and downloaded by users who need them. Cryptographic hashes, or "info hashes," of the pieces are used to verify that the pieces being shared are the pieces that were requested.

The more pieces a peer receives from another peer in exchange for pieces sent, the more productive a peer-to-peer interaction is considered to be. The most productive piece exchanges are rewarded with further pieces, and the clients with the least productive exchanges are deprecated, disconnected or banned.

Once a user has completed a download, they may allow their client to continue to upload pieces despite no longer needing any download in return; this is called "seeding." The default for most clients is to "seed" to other downloaders. This activity, however, is entirely altruistic. There is no economic penalty for users closing their BitTorrent client once a download has finished.

The BitTorrent Ecosystem

BitTorrent Inc., which maintains the BitTorrent protocol, also created two of the most popular BitTorrent clients[1]: BitTorrent and µTorrent ("uTorrent"). The open protocol has also been used to create dozens of independent clients, and there is healthy competition among the companies and volunteers that maintain those clients.

[1] Wikipedia contributors. "Comparison of BitTorrent clients." *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Comparison_of_BitTorrent_clients&oldid=864318824. Accessed January 17, 2019.

Independent BitTorrent infrastructure providers offer additional services, such as trackers that introduce peers, and torrent sites that index file metadata and provide access to their associated torrents.

The BitTorrent Company

With over 1 billion users, the BitTorrent protocol is the world's largest decentralized protocol. Its number of users far surpasses Bitcoin, the second-largest decentralized application (as of January 11, 2018, Bitcoin had a total of 32.3 million addresses[2]).

In the last 18 years, BitTorrent clients have been downloaded and installed billions of times. The two clients created and maintained by BitTorrent Inc. are in use today by more than 100 million monthly active users around the world, with around one million new software installs every day. Over 160 countries have more than 10,000 BitTorrent protocol users, and 23 countries have more than 1 million protocol users. BitTorrent Inc. clients account for an estimated 40% of BitTorrent protocol activity on the public internet.[3]

In 2018, BitTorrent formed a strategic partnership with TRON. TRON is a blockchain platform that was created to provide the foundation for decentralized applications. The collaboration between BitTorrent and TRON makes the TRON blockchain protocol the world's largest decentralized ecosystem, and the BitTorrent protocol the largest decentralized application in the world.

BitTorrent and Distributed Applications

For more than a decade, BitTorrent Inc. has been exploring distributed applications. We have investigated both adaptations of the BitTorrent protocol as well as the creation of entirely novel protocols with the aim of providing services including distributed messaging, BitTorrent-based CDN, peer-to-peer live video streaming and file synchronization, and distributed website hosting. The recent emergence of blockchain technologies has shifted the paradigm of what is achievable.

While many new decentralized protocol proposals suggest ambitious technical paths forward, almost all are silent on how to confront the enormous challenge of building critical mass, which is the technical crux of distributed systems. Some projects are addressing this challenge by introducing a cryptographic token to existing user bases. However, these projects lack the experience BitTorrent has in designing a protocol which balances diverse economic interests effectively and at scale.

The BitTorrent ecosystem has the critical mass and BitTorrent Inc. has the protocol engineering expertise necessary to take advantage of the possibilities introduced by the blockchain. By integrating blockchain technologies into the BitTorrent ecosystem, we can enable developers to

[2] "Blockchain Wallet Users." Blockchain.com. Accessed January 17, 2019. https://www.blockchain.com/charts/my-wallet-n-users.

[3] BitTorrent Inc. internal market share research.

create new, decentralized applications on top of our existing ecosystem. Therefore, we believe that BitTorrent is the best-equipped entity to create the infrastructure of the imminent decentralized web.

BitTorrent Expansion

As we examined how BitTorrent's expertise and ecosystem could be used to realize the potential of blockchain technologies, we identified three key insights::

1. Internet users are reluctant to pay for digital goods and services online with fiat currency. Instead, they pay with their attention.
2. The BitTorrent protocol suffers from structural inefficiencies that limit the lifespan of swarms and thus limit its overall efficacy as a protocol.
3. There is a large untapped market for the application of BitTorrent technology to new use cases

Project Overview

To execute on the synthesization of these insights, we will create a platform for building elements of the decentralized web, enabling app developers to directly reward consumers who provide its underlying resources and enabling consumers to use this "found value" to transact with publishers and app developers without fiat currency.

In order to implement a distributed infrastructure services economy, we will extend the BitTorrent protocol and introduce a new token, BTT. Within the BTT economy, end users may offer infrastructure services in small increments in return for tokens. A blockchain solution will provide a store of value and medium of exchange that will scale to meet expected demand.

We will accelerate introduction of the platform by eliminating current BitTorrent protocol inefficiencies with the launch of BitTorrent Speed. This will provide a strong attraction for the foundational technology as well as broad familiarity of the existence, user experience and economics of the token. The introduction of Speed will also prove the effectiveness of using blockchain-based rewards for the provision of infrastructure services in small increments across a large installed base.

In parallel, we will work with third-party developers to create and promote APIs and a marketplace for distributed infrastructure services based broadly on networking and storage primitives, which are underpinnings of the existing BitTorrent technology. We will also work with third-party publishers and app developers beyond the existing BitTorrent ecosystem on services which consumers may spend their tokens on.

Ultimately, hundreds of millions of end users will be equipped with a robust means of deriving small amounts of value from their technical resources, and will be able to spend that value on goods and services.

Below, we outline BTT, around which we plan to build a new economy, and present the

blockchain technology on top of which transaction processing will operate. Then, we outline the proposed approach to optimize the existing BitTorrent protocol with BitTorrent Speed. Next, we describe how BitTorrent Speed will be operationalized with BTT. Finally, we discuss the generalization of BTT services and describe the first three decentralized applications being built on the new platform.

BitTorrent Tokens (BTT) and the Blockchain

BitTorrent Inc. is introducing a TRON TRC-10 cryptographic token called BitTorrent Token (BTT). BTT will act as a general purpose mechanism for transacting in computing resources shared between BitTorrent clients and a liquid market of service requesters and service providers. BTT will be the unit which denominates transactions for the provision of services in the BTT-enabled BitTorrent ecosystem. It will be made available as a divisible token, allowing for granular pricing.

Due to expected volume, direct use of the public TRON blockchain for all transactions is unfeasible. Therefore, BitTorrent Inc. will deploy an “on-chain/off-chain exchange.” The exchange will enable the transfer of tokens between a high-performance private ledger and the public TRON blockchain.

Introduction to BitTorrent Speed™

BitTorrent swarms suffer from structural inefficiencies which frequently lead to the premature deterioration or death of swarms. Due to upload/download speed asymmetry, files frequently complete downloading long before a peer has been able to upload an equivalent number of bytes. Once the downloading peer has the entire file, there is no economic incentive to continue to make the file available to other downloaders through seeding. That means users leave swarms without uploading as much data as they have downloaded, which results in BitTorrent swarms not lasting as long as they need to.

In some cases, it is possible for a swarm to enable the completion of a download even in the absence of a seed. This possibility is computed and displayed in some implementations as an “availability” metric,[4] typically expressed as the number of distributed copies available. If there is at least one active non-seed peer holding each of the pieces, then the file is said to be “available.” Additionally, the BitTorrent protocol uses a design decision known as “rarest first,” which dictates that a client should prioritize requesting to download the pieces that are held by the fewest peers in the swarm to which it has connected. This mechanism is intended to flatten the distribution of pieces to decrease the likelihood of a swarm losing a key peer or peers who are the sole providers of a required piece. While these two considerations mean that seeds are not strictly necessary to complete a download, research has shown that in approximately 86%

[4] Vuze wiki contributors. "Availability." Vuze wiki, https://wiki.vuze.com/w/Availability. Accessed January 17, 2019.

of seedless cases, this sort of collective reconstruction is not feasible.[5]

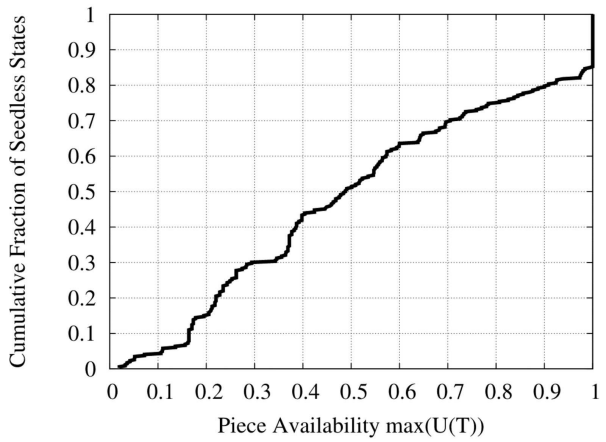

Figure 1. Only 14% of torrents that had no seed in the swarm could reconstruct the whole file.

To eliminate this problem, we are developing a new BitTorrent feature called BitTorrent Speed. This feature is will enable peers to offer each other cryptographic token incentives to continue to seed files after the full download has completed.

To be clear, BitTorrent currently functions well. Nothing proposed in this optimization will alter the protocol's functionality, and users of the protocol will not experience an interruption in their usage. The addition is simply an overlay on top of the current protocol which will allow existing BitTorrent swarm participants to exchange tokens in return for ensuring the continued availability of a file for download.

BitTorrent Speed will be integrated into future participating BitTorrent and uTorrent clients. It will add a new set of extensions to the BitTorrent protocol, enabling users to advertise their bids within a swarm and to trade BTT in exchange for continued prioritized access to seeds. The intended result is that peers will choose to seed for longer, leading to increased swarm longevity and faster download times for all swarm participants.

BitTorrent Speed and BTT Operations

Peers will be able to act as both "service requesters" and "service providers." A peer offering BTT in exchange for other users' local resources will be a service requester, and a peer offering local resources in exchange for BTT will be a service provider.

[5] Kaune, S., R. C. Rumin, G. Tyson, A. Mauthe, C. Guerrero, and R. Steinmetz. "Unraveling BitTorrents File Unavailability: Measurements and Analysis." *2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P)*, 2010. doi:10.1109/p2p.2010.5569991.

Service Discovery

The BitTorrent Speed life cycle will begin when peers discover each other via existing BitTorrent protocol mechanisms.[6]

Initial Balance

BTT will be airdropped to existing uTorrent/BitTorrent users so they can bootstrap with a small initial balance. In the future, BTT will also be purchasable via crowdsale and exchanges.

Bidding Rounds

Bids will be sent via a new BitTorrent protocol extension message to each peer that has at least one piece wanted by the service requester. The message will contain the number of BTT the service requester is willing to pay per piece.

After winning a bidding round, a service requester must establish an escrowed BTT balance with the service provider. They do this by placing some BTT into a payment channel between the service requester and service provider.

Bidding User Interface

By default, bidding will be automated. Users' clients will bid to and from their token balance on their behalf. We may enable user interface controls to allow users to toggle the feature, toggle it for certain torrents, adjust the spending rate, set a reserve price, or exercise granular control over the bidding process.

Automatic Bidding

For the initial release, clients will use a simplified auto-bidding mechanism. In this version, the client simply bids a fraction of the remaining BTT balance in the service requester's wallet. This is how the bid is calculated:

$$bid = (spending\ rate \times remaining\ balance\ in\ BTT)/(remaining\ download\ in\ kilobytes)$$

This formula implies that as a download progresses, the bid will change. For the initial release, the client will not rebid until the bid changes by more than 10% from the previous bid.

The spending rate (a parameter that can vary from 0.0 to 1.0 depending on how aggressive the client should be bidding) will be defined to be 1.0. If the number of kilobytes remaining is equal to zero, then the bid automatically stops in order to prevent division by zero.

In the future, this algorithm will be refined. For example, based on existing bid message traffic and current transfers, the client will be able to estimate a market rate for bandwidth. The client

[6] For detailed description of BitTorrent protocol operations, see https://en.wikipedia.org/wiki/BitTorrent.

also has a picture of piece rarity it can use to inform bid amounts.

Matchmaking

The BitTorrent protocol uses a sharing algorithm called “tit-for-tat”, which is implemented using a mechanism called “choking.” BitTorrent clients classify peers as either choked or unchoked. An example choking algorithm might sort peers based on how much data the client has received from each one since the choking algorithm was last executed. The first *n* peers (where *n* is the number of unchoke slots, a fixed value chosen by each client) are classified as unchoked and the rest as choked.

Only unchoked peers are eligible to receive data. The choke state of all peers is recalculated periodically (typically every 15 seconds). Seeds do not receive any data from peers, so they use the amount of data sent to each peer to determine which peers are eligible to be unchoked in the next round. This means seeds optimize for maximum throughput, with no regard for any other factor.

There is also a separate choking algorithm called “optimistic unchoking” which uses a number of reserved unchoke slots (typically one). Optimistic unchoking selects a peer to unchoke in a random or round-robin fashion. This allows new peers an opportunity to receive some data so that they can start reciprocating with other peers.

Choking is the primary means of allocating resources within a BitTorrent swarm. BitTorrent Speed will extend this mechanism so that a service provider will include both BTT bid data and peer upload rate in its decisions about which peer to unchoke.

How this inclusion takes places will vary depending on how the client’s choking algorithm is implemented. When it comes time for the client to run its choking algorithm, it first compiles a list of eligible bids. The example algorithm described above could be modified to sort peers by a combination of highest eligible bid and most data received.

When an eligible bidder is unchoked, the service provider will send a new BitTorrent protocol extension bid response message to the bidder containing the rate in BTT/byte the bidder is expected to pay. This message will be followed by a normal unchoke message.

Clients may implement any auction format, but a variant of the Vickrey-Clarke-Groves auction is expected to produce optimum results. See Figure 2 for an outline of the auction mechanics, which ends up being a multi-unit uniform price auction.

Each service requester bids on only one unchoke slot per service provider. Clients would charge each unchoked bidder the rate of the highest losing bid.

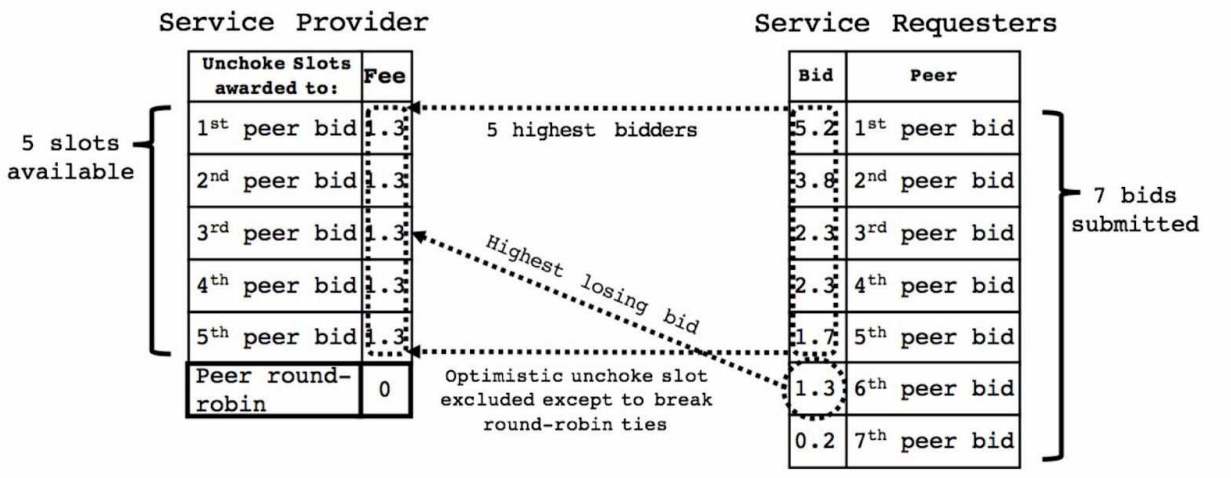

Figure 2. Auction mechanics of a multi-unit uniform price auction.

Caution must be exercised when dealing with optimistic unchoking due to its importance in allowing new peers to bootstrap into the swarm. The optimistic unchoke slot(s) should not be subject to the same auction format as the regular unchoke slots. If the client is using a round-robin algorithm for optimistic unchoking, it should only apply an auction to break ties between peers which have gone the same amount of time since being choked. This means auctioning of the optimistic unchoke slot will typically only happen between bidders that have never been unchoked.

In swarms with both BTT-enabled BitTorrent clients and legacy BitTorrent clients, service requesters will be able to offer BTT to service providers. However, upload speeds from legacy BitTorrent clients will be maximized without regard for any BTT bids.

Transaction Processing

Once a service requester receives both the bid response and unchoke messages, it opens a payment channel on the private ledger whose output is addressed to the service provider. The service provider expects payment to be delivered via a new or existing channel for each complete piece received by the service requester.

Below, the service requester is the party sending BTT, and the service provider is the party receiving it.

1. The service requester creates a public key (K1) and requests a public key from the service provider (K2).
2. When the service requester wishes to pay the service provider, it opens a channel on the private ledger with K2 as the destination account. When the channel is created, the service requester transfers some of its BTT into the channel. This BTT is deducted from the account associated with K1.

3. The service requester generates a transaction on the channel which disburses the initial payment amount to K2 and the remainder of the channel's BTT to K1.
4. The service requester signs the transaction, then sends the transaction and the signature to the service provider.
5. If the service provider has not seen the channel before, it requests the channel information from the private ledger. The service provider only accepts the payment if the channel information retrieved from the ledger matches the information received from the service requester.
6. When the service requester wishes to send another payment to the service provider, it adjusts the transaction to allocate more value to K2. It then re-signs the new transaction and sends the transaction and the signature to the service provider.
7. If the service requester wishes to send more payment, but the existing channel's BTT is entirely allocated to the service provider, the service requester opens a new channel on the ledger and uses it to send payment as described in steps 2-4.

This process continues until the service requester confirms that the transfer is complete. The service provider then signs the last transaction it saw and sends it to the private ledger, allocating the final amount to itself. This closes the channel; it cannot be used for further payments.

In case the service provider stops at any point, leaving the allocated value in limbo, the private ledger implements a timeout for each channel. The timeout period is indicated in the channel's information when the service provider retrieves it from the ledger. If the service provider does not close the channel before the timeout expires, the ledger automatically closes the channel and disperses all of the channel's BTT to the service requester.

If the BTT transfer does not complete after a timeout, the service requester is choked and receives no further data. Repeated failures to transfer BTT by a service requester can result in the service provider banning the service requester. Banned service requesters are disconnected from service providers, and any attempt to reconnect is rejected for a specified period of time. Similarly, failure to verify data from the service provider can result in the service provider being banned.

Each party progressively contributes pieces or BTT, with a signed transaction produced for each step in the process. The maximum breach exposure of the service provider at any given time is therefore one piece worth of bandwidth; since service requesters pay only on verified delivery, they have zero breach exposure.

Bidding Revisions and Frequency

As the client may receive data for less than its maximum bid (and very frequently for free, as is currently the case in BitTorrent), the bid computed by dividing the remaining total spend by the remaining data will trend upward over time. The client can implement any heuristic it likes to

determine when to send bid messages with a new bid value; it should not, however, send new bids more than once a minute. If the user changes the amount of BTT bid, then the client should send the new bid immediately.

Generalized BTT Services

Optimizing the existing BitTorrent protocol sets a precedent of allowing users to store value from sharing small amounts of infrastructure in order to spend that value later. It is an obvious first step in the introduction of a cryptographic token, but it is a small fraction of what is becoming possible. We are preparing to dramatically extend both the earning opportunities and the spending opportunities for users of BTT-enabled BitTorrent clients.

We are developing a range of generalized BTT services, as well as preparing to open up the platform to third-party developers to allow use of the wallet and BTT in their applications. After extensive discussions with partners interested in our platform, we have concluded that the following three basic BTT services should be offered by BitTorrent:

(1) A decentralized content delivery service to enable service requesters to advertise bids and pay BTT for bandwidth to receive a particular piece of content. This service will be well-suited for mass distribution of content, especially in the presence of censors or other attackers. Service providers will be incentivized to serve content to as many people as possible, thus ensuring robust performance even with high numbers of service requesters.

(2) A decentralized storage service to enable service requesters to pay for storage over time, and to download the stored data from service providers for a prearranged fee. Service providers will agree to store data and provide on-demand proofs-of-storage to the service requester. Service providers will naturally seek out content which offers the highest payment rate over time. This service will be useful for remote backup and sharing of private data among small groups.

(3) A decentralized proxy service to enable service requesters to pay a service provider for retrieval of content by URL. This will be useful to highly mobile applications or those that seek to evade IP-level network controls. The service will be designed to allow content to be requested in chunks. This will, for example, allow clients with intermittent connectivity, such as mobile users relying on Wi-Fi, to reliably retrieve web resources without needing to maintain an open connection long enough to receive the complete contents.

As shown in Figure 3, the various enhancements to the BitTorrent protocol will serve as building blocks for distributed applications.

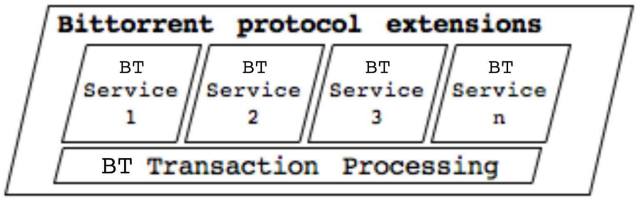

Figure 3. BitTorrent protocol extensions.

More BTT services can be implemented and introduced into the service provider network as demand emerges from new BTT applications. BitTorrent Inc. will provide a forum for discussion and standardization of new BTT services similar to that provided for the BitTorrent protocol.

The BitTorrent protocol extensions will be submitted for comment to the BitTorrent community BEP process – an informal but open standards-setting process[7] – and facilitated by BitTorrent Foundation, which has guided protocol enhancements for more than a decade. Following community feedback, we will develop and test our implementation of these extensions via engineering and release management practices which are well established at BitTorrent.

Furthermore, as is our practice with highly important updates, we will subsequently release these extensions as an open source library and establish support and incentives for integration into third-party BitTorrent protocol implementations.

BTT Incentives

The continued evolution of the BitTorrent ecosystem will require both coordination of activities and provision of incentives to a broad range of existing and future participants. BitTorrent client implementers, third-party app developers, and online publishers will all be eligible for a system of BTT incentive awards.

The BitTorrent ecosystem has proven that millions of people will enthusiastically share their resources if they can cooperate safely and securely, bound by the rules of a protocol they trust. By introducing a mechanism for value storage and exchange, we aim to greatly broaden the universe of possible participants – either as service requesters, service providers, or both.

To maximize the chances of success, it is vital that we ensure that BitTorrent Inc. is not a central monopolist in the BTT-enabled BitTorrent ecosystem, just as it is far from a monopolist in today's BitTorrent ecosystem. The BTT project depicted in Figure 4 is one in which the success of ecosystem partners will lead to increasing returns for all ecosystem participants.

[7] Harrison, David. "Index of BitTorrent Enhancement Proposals." BitTorrent.org. January 10, 2008. Accessed January 17, 2019. http://www.bittorrent.org/beps/bep_0000.html.

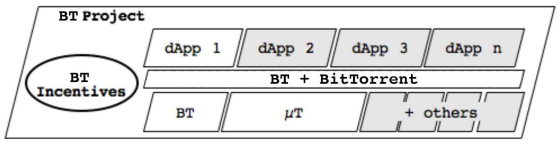

Figure 4. Ecosystem success benefits all participants.

The purpose of the BTT incentives will be to:

- Promote the BTT project to current and prospective participants, whether they are service providers, service requesters or both. This means finding and introducing new application developers who are interested in participating in service requests or service provision.
- Govern membership and participation rules for the BTT ecosystem, with the overarching objective of establishing a level playing field on which all can participate fairly.
- Govern the equitable and transparent distribution of rewards and incentives such that promising ideas have a fair chance and productive outcomes are fairly rewarded.
- Partner with BitTorrent.org volunteers to facilitate discussion around future BitTorrent protocol extensions.

Once the BTT project is running sustainably, we may consider transitioning the rules and procedures it has established for administering BTT incentives into an instrument with lower overhead, such as a decentralized autonomous organization (DAO).

Implementation Considerations

Blockchain

BTT applications will be supported by the tens of millions of BitTorrent daily active users. To minimize opportunities for fraud, BTT applications will provide service in small increments, waiting for payment to be confirmed before additional service is provided. This will require transactions to be handled at a granular level and confirmed in a matter of seconds, ideally in less than a second. Even the most conservative estimates of capacity requirements anticipate dozens of transactions per second. With these needs in mind, it is clear that existing public blockchains will not be able to support on-chain processing and settlement in the near future.

User Controls

We plan to introduce features such as BitTorrent Speed and BTT transactional support into BitTorrent and µTorrent clients in phases to allow us to iterate towards the clearest possible user education journey and thus to optimize end-user participation. Participation in BTT transactions is required to be both fully disclosed and completely optional for end users.

Initial Disbursement

The first available use-case for BTT will be BitTorrent Speed, which will be unproven at the outset. Since new services take time to become prevalent, we may pursue a strategy of pre-seeding the market with promotional quantities of BTT.

BitTorrent Wallets

As part of the rollout of new BTT-capable BitTorrent and µTorrent software, we will be distributing integrated cryptographic token wallets to all users. As we will be distributing these wallets on a large scale to mass market end users, and not necessarily to cryptocurrency enthusiasts, we will need to pay close attention to simplicity and usability.

Use Case Diversification

The introduction of BTT wallets on the scale anticipated by this project may create opportunities for new uses for the token that are unrelated to BitTorrent technology. We expect that many millions of users will accumulate small quantities of BTT from providing services. These small quantities may not have material value unless they are aggregated by service providers. Such users may look for ways to spend their BTT that go beyond their need to incentivize seeding.

In due course, we expect to publicize this new ability for users to earn and spend tokens, and we expect to explore partnerships to accelerate merchant acceptance of this new type of micropayment mechanism. This will be particularly advantageous to merchants who want to aggregate and use tokens to pay for distributed infrastructure services to support their ongoing services.

We expect to be able to establish an economic cycle, as depicted in Figure 5, in which BTT are introduced primarily by distributed app developers, are then traded between service requesters and service providers both within and beyond the BitTorrent ecosystem, and may ultimately aggregate in materially significant pools at some service providers, who may or may not be part of the BitTorrent ecosystem.

At this point in the cycle, the service providers will exchange the BTT for distributed infrastructure services provided by BitTorrent users, returning the BTT to the open market. For example, long-term seeders who have earned a significant amount of BTT would be able to exchange the tokens for distributed file storage or other services.

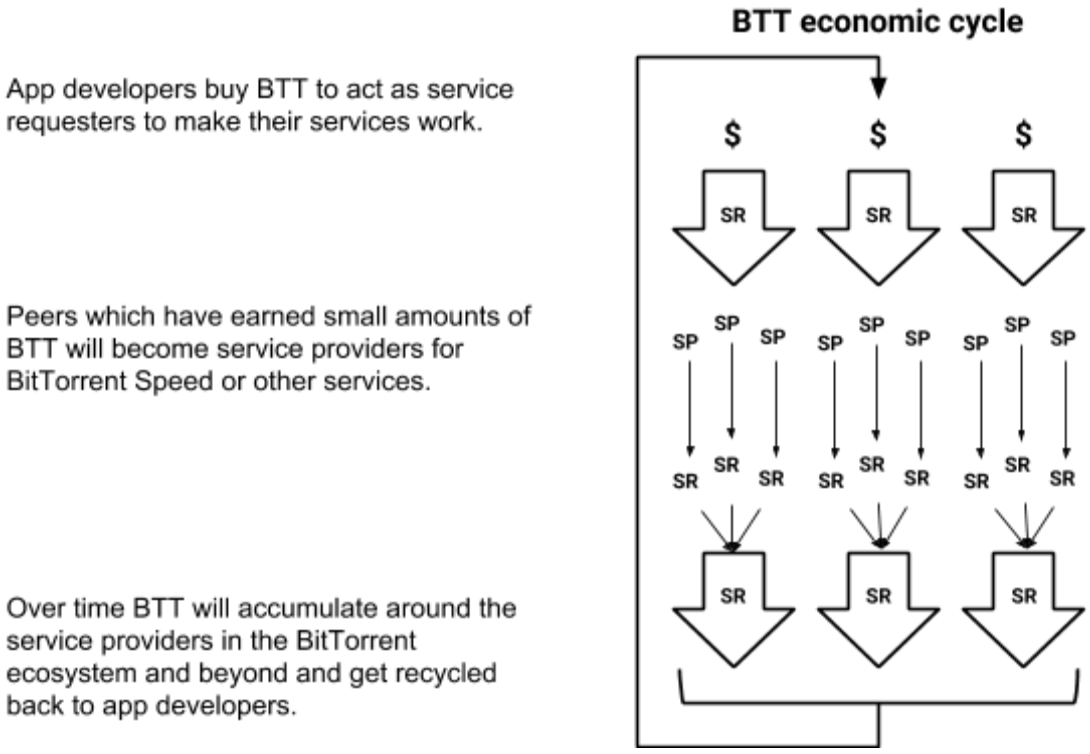

Figure 5. The full BTT economic cycle.

Identity

BitTorrent as a protocol has never provided any type of identity service beyond identifying a client on a particular IP + port number. Essentially, BitTorrent identifies instances of software running on machines – not people. This is analogous to the identity framework behind cryptocurrencies. If a user has access to the cryptographic token wallet software that stores a token, then it is generally assumed that it is that user's token. With the implementation of BTT, we expect to follow a very similar approach to identity, tying BTT tightly to a participating piece of client software. Beyond possibly placing a password on that wallet, we do not currently anticipate that the BTT project will directly give rise to the need for an additional layer of identity management in BitTorrent.

BTT Token Issuance

We will create a total supply of 990,000,000,000 BTT. Issued tokens will be distributed in the following proportion:

- Public sale tokens constitute 6% of total token supply
- Private sale tokens constitute 2% of total token supply
- Seed sale tokens constitute 9% of the total token supply

- Tron airdrop tokens constitute 10.1% of total token supply, to be spread out over the next six years
- BitTorrent protocol airdrop tokens constitute 10% of total token supply
- BitTorrent Team and the BitTorrent Foundation were allocated 19% of total token supply
- TRON Foundation received 20% of the total token supply
- BitTorrent ecosystem is allocated 19.9% of the total token supply
- Partnership tokens constitute 4% of the total token supply

More information can be found at Binance Research.

Users of BitTorrent Inc.'s torrent clients,and possibly other torrent clients which choose to implement the required set of protocol extensions, will be able to submit a CAPTCHA or proof of work that will allow them to access an initial balance of BTT.

Conclusion

We have presented our motivation, qualifications and plans for extending BitTorrent via the BTT project, starting with a new core feature designed to improve the BitTorrent ecosystem, a new cryptographic token, and a practical implementation of cryptographic token transaction processing at scale.

We have outlined how we are generalizing this approach to enable other distributed app developers to use a distributed infrastructure platform composed of more than 100 million consumer BitTorrent clients for the provision of networking and storage resources in return for BTT.

We have described the mission and operation of the BTT incentives program, which will be dedicated to driving the number and success of the BTT distributed apps. It will manage the progressive release and distribution of BTT to the ecosystem participants that are successful in driving useful platform adoption.

We have discussed implementation considerations and challenges and how we expect to address them.

And we have presented a plan for how tokens will be issued and shared in the pursuit of a stable, thriving economy built around the sharing of computing resources by millions of ecosystem participants.

The potential of this project is compelling due to the disruptive decentralized applications that it will enable; its open ecosystem approach, which will welcome and reward participants at every level; and the enormous head start the BitTorrent ecosystem enjoys in the building and deployment of a decentralized computing economy.

FAQ

Why not rewrite the BitTorrent protocol?
We considered a fundamental rewrite of the BitTorrent protocol to allow collaboration to be persisted over time and to ensure the “right seeding behavior” was rewarded so that valuable content with only occasional demand would be available for longer. We imagined a protocol which would both download (like BitTorrent) and hand out longer-term incentives (like bitcoin mining rewards). After lengthy consideration, we discounted this approach for several reasons:

1. Difficulty of the problem. Implementing an incentive system at the protocol level requires precise thinking about objectives. We found it impossible to articulate clearly what the long-tail seeding objectives should be and how to avoid gaming them; there are plenty of BitTorrent swarms that die because no one cares (e.g., a better version of a file becomes available). The only tractable answer seemed to be to implement a voting system to let consumers judge, but that seemed to call into question the desire to wrap everything into the protocol. In short, trying to systematically discern what should and should not be preserved seemed like a problem we were poorly equipped to solve.
2. The strict need to be better than the existing BitTorrent protocol (a.k.a. “soft-fork not hard-fork”). The BitTorrent ecosystem is now so big that a hard fork would have an extremely low chance of success. Any protocol rewrite would have to be compatible with the existing BitTorrent ecosystem; that immediately rules out features such as penalties for not seeding, as users would just choose clients which implemented the “old” BitTorrent protocol, which did not penalize them.
3. Conviction that we were over-complicating the solution. The likely need for human agency in the system (people voting) convinced us we should focus on simpler extensions to the current BitTorrent protocol, and design a voting system that was based around a cryptographic token. This has the advantage of allowing the market to determine what should be seeded while leaving BitTorrent enhanced, but not changed at its core.

Why did BitTorrent not include incentives when it was invented?
Projects that were forerunners to BitTorrent did try to imagine how a system of persistent incentives might be managed. They foundered largely due to the difficulty of finding an effective solution to “keep the score” while operating at scale. Blockchain and distributed ledger solutions using cryptographic tokens present a powerful way to keep the score such that transactions can be processed and a ledger may be managed at scale even without perfect trust between all parties.

How can this solution help me circumvent net neutrality adversaries?
Proxying from IP to IP will enable users to find content that is blocked by an ISP in their geographic area by connecting to it via an intermediary to which both site and requester can connect.

How will you protect end users' computers from malicious attacks?
The usage of end-users' technical resources will be strictly limited to the provision of technical services such as networking or storage within carefully bounded limits. Network connections will be protected by uTP, a self-adjusting bandwidth mechanism which ensures applications throttle back if there is any indication of other apps (even on other devices) using the network connection. Storage will be encrypted and limited to a user-configurable maximum. Users will be able to configure which applications they accept and which they do not. The provision of BTT services is limited to simple infrastructure operations and will in no way permit untrusted third parties to execute code on a user's device.

Can users opt out if they do not want to provide their resources or earn tokens?
Yes. Users will always be able to configure the parameters of their sharing or turn it off entirely if they choose. There will be nothing mandatory about BitTorrent extensions, and users will retain the right to opt out at any time and for any reason.

References

"Blockchain Wallet Users." Blockchain.com. Accessed January 17, 2019. https://www.blockchain.com/charts/my-wallet-n-users.

Harrison, David. "Index of BitTorrent Enhancement Proposals." BitTorrent.org. January 10, 2008. Accessed January 17, 2019. http://www.bittorrent.org/beps/bep_0000.html.

Kaune, S., R. C. Rumin, G. Tyson, A. Mauthe, C. Guerrero, and R. Steinmetz. "Unraveling BitTorrents File Unavailability: Measurements and Analysis." 2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P), 2010. doi:10.1109/p2p.2010.5569991.

Vuze wiki contributors. "Availability." Vuze wiki, https://wiki.vuze.com/w/Availability. Accessed January 17, 2019.

Wikipedia contributors. "Comparison of BitTorrent clients." Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Comparison_of_BitTorrent_clients&oldid=864318824. Accessed January 17, 2019.