ContentBox

Empowering a Decentralized Digital Content Ecosystem

CASTBOX.FM

2018-03-31

Contents

Introduction

Problem Statement

For over a decade we have witnessed explosive growth of the digital content industry led by a variety of web and mobile content platforms such as Reddit, Youtube and Spotify. It has become an indispensable part of our modern daily life, with audio and video streaming constituting 70% of Internet data traffic. However, the success and fairness of the industry is impeded by several long standing challenges facing creators, consumers, advertisers, and distributors of digital content.

- **Content creators struggle to profit from their own creations.** It is extremely difficult to monetize one's created content online. On many content platforms such as YouTube and Instagram, users create all the content, from which platforms profit enormously by selling advertisements. However, the vast majority of creators are rarely compensated for their indispensable contributions to these digital platforms. In addition, when creators do get paid for their content, layers of intermediaries siphon off a majority share. Creators are in a weak position and lack bargaining power to negotiate equitable monetization and payout terms. It is not surprising platforms take most of the revenue and creators only collect a small piece of the pie. For instance, when a song is streamed, only about 15% of the sales income goes to its creators, the bulk goes to streaming service providers and record label owners.
- **Content consumers receive no compensation for their contributions.** Consumers engage in a wide variety of value-creating activities vital to content platforms, but are never financially rewarded. *Curation*: users spend valuable time interacting with platform content (e.g., liking, voting, flagging and commenting), filtering low quality from high quality content and receive no payments for their participatory work. They are commercially exploited by powerful platforms (e.g., YouTube) at the expense of users unknowingly providing free services. *Share*: sharing within or outside a content platform (e.g., sharing a YouTube video with followers on YouTube or Facebook) brings more visibility to content and attracts more traffic to the platform. *Attention*: the Internet is flooded with all types of digital content with greatly varying qualities. Therefore, content is no longer scarce, per se, but a user's attention is. A user spending limited attention on content, including advertisements, is valuable.
- **Aggressive competition between content platforms.** Since key user information and content is locked in their proprietary data silos, it's nearly impossible for the content platforms to build mutual trust, which often leads to fierce competition in the digital content industry. It is not uncommon that we see big content platforms bid for copyrights of popular content with insanely high prices, driving up the cost of the bid winner and at the same time, leaving the small and medium-sized platforms no choice but to turn to low quality or pirated content. And usually these surging cost will be transferred to end-users through longer ad times or higher subscription

fees, eventually degrading the user experience.

A Blockchain-based Ecosystem

Our solution to the problems mentioned above is the ContentBox Platform, which aims to build a blockchain-based ecosystem for the digital content industry of tomorrow. Under ContentBox, the whole industry will gain three invaluable features: **a shared content pool, a shared user pool, and a unified payout system**.

Unlike traditional open platforms such as the App Store or WeChat Open Platform[1], the ContentBox Platform is fully **decentralized, autonomous, and driven by the open source community instead of an industry platform giant**. ContentBox will help various web and mobile applications share digital content and user bases in more efficient ways than before, and process payments swiftly without ceding control to a third party.

In principle, ContentBox is designed to benefit all stakeholders in the content industry including but not limited to, creators, consumers, advertisers, distributors, and application developers. ContentBox allows them to collaborate, innovate, build, engage and transact with a new generation of digital content applications that play on fair terms within the ecosystem.

For content creators, ContentBox's payout system will allow them to get rewards every time their content is consumed, motivating them to create more diverse and higher quality content. Top creators of the most popular content still reap big rewards while everyone else now receives compensation in proportion to their content popularity. In addition, ContentBox will connect creators directly with their consumers by streamlining and automating business transactions without intermediaries chipping away at a creator's revenue share.

For consumers, they will be rewarded with tokens according to their contributions. Those contributions can be social sharing, voting or commenting on content, or reporting spam content, as long as they are beneficial and add value to the platform. They can spend their tokens on content consumption, like viewing a movie or streaming a song. If a user has a stake in the success of the platform, they will put more effort and research into curating and advocating for it, as evidenced in the rise of Bitcoin.

Advertisers also will benefit from the new ecosystem. With ContentBox, advertisers can tap into a shared advertisement statistics ledger and pay by actual advertisement viewership automated by smart contracts, instead of relying on opaque statistics reported by distributors. Since the ledger is open, they can audit and verify it and have peace of mind. This can help them to build a unified and coherent marketing strategy, instead of running paralleled campaigns on different platforms. Furthermore, they can lower spending by leveraging a token-based bounty program.

[1] https://open.weixin.qq.com/

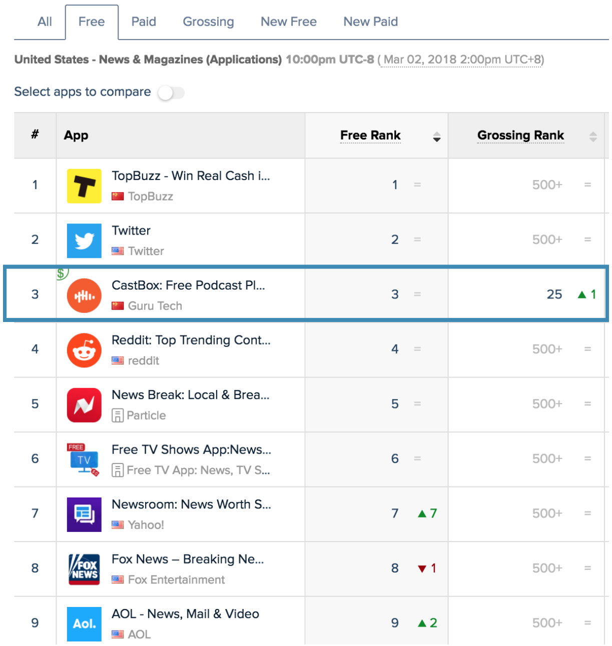
For distribution platforms and social networks, they can together build a shared content and user ledger which benefits everyone by lowering the traffic acquisition cost and IP purchase cost. They can focus on improving user experience instead of competing with each other.

For application developers, they can leverage ContentBox's blockchain-enabled token, the decentralized payment infrastructure and the identity services to build applications with a better user experience and stronger monetization ability.

Overall, by opening the black box our digital content industry is today, the whole industry, including all stakeholders, can flourish with cooperation and transparency by collaboratively building a new content economy. To foster the collaboration of all stakeholders, ContentBox will introduce a new token, named **BOX**, which will play a key role in the ecosystem's economy.

About CastBox

CastBox is one of the most popular mobile audio platforms across the globe, ranked #3 in News & Magazines on Google Play (Figure 1) along with TopBuzz and Twitter. It pioneered in-audio search to deliver contextual recommendations for listeners of podcasts, on-demand radio, and audiobooks. Today, CastBox has about 50 employees with offices in Beijing, San Francisco, New York, and Hong Kong.



United States - News & Magazines (Applications) 10:00pm UTC-8 (Mar 02, 2018 2:00pm UTC+8)

Select apps to compare

#	App	Free Rank		Grossing Rank	
1	TopBuzz - Win Real Cash i... TopBuzz	1	=	500+	=
2	Twitter Twitter	2	=	500+	=
3	CastBox: Free Podcast Pl... Guru Tech	3	=	25	▲ 1
4	Reddit: Top Trending Cont... reddit	4	=	500+	=
5	News Break: Local & Brea... Particle	5	=	500+	=
6	Free TV Shows App:News... Free TV App: News, TV S...	6	=	500+	=
7	Newsroom: News Worth S... Yahoo!	7	▲ 7	500+	=
8	Fox News – Breaking Ne... Fox Entertainment	8	▼ 1	500+	=
9	AOL - News, Mail & Video AOL	9	▲ 2	500+	=

Figure 1: Rank in News & Magazines, Google Play, USA (Source: App Annie)

Founded in early 2016 by an ex-Googler, the application currently has over 50 million+ volumes of audio content available, with over 15 million installed users. It is also the winner of Google Global Android Excellence Program 2017, the Most Entertaining of Best Apps by Google Play in 2016 and a number of other awards. CastBox is listed as Editors' choice in 135 of Google Play's countries.

The Foundation

A non-profit organization, Contentbox Foundation Limited ("the Foundation"), has been established to oversee productive and positive growth of the new ecosystem on the ContentBox Platform. The Foundation will administer use of the proceeds and ensure healthy circulation of the BOX token. As the ultimate goal of the ContentBox Platform is to build a fully decentralized and autonomous ecosystem for the digital content industry, governance and operation of the Foundation will be kept as transparent as possible. In the long run, **the Foundation will be transformed into a totally software defined organization**.

As the founding member of the Foundation, CastBox will pioneer the transition from a centralized app to a decentralized blockchain-based app and introduce BOX to its tens of millions of users to help improve their experience and enjoyment with creating, consuming, and distributing digital content. In the near future, CastBox will also open source the vast majority of its currently proprietary codebase after BOX is successfully integrated into the app, encouraging the open source community to drive the evolution of the ContentBox Platform.

Technical Architecture

Why A New Blockchain?

The digital content industry has unique requirements which warrant developing a dedicated blockchain.

- **High frequency.** The digital content industry is quite different from the payment or e-commerce world in terms of action frequency. Typically a person transfers his money or buy/sells goods no more than several times a day. But on a digital content platform, it is not uncommon for a user to stream a song, watch a movie clip, and tip an article author within a few minutes. Clearly we expect much larger transaction volumes in the digital content world serving millions of users. This requires the underlying blockchain to support high transaction throughput, potentially hundreds or even thousands of transactions per second.
- **High bar for privacy protection.** The appeal of a public blockchain such as Ethereum partially lies in its transparency: all smart contracts are stored publicly on every node and are independently auditable. However, users on digital content platforms often prefer to have confidential

transactions. A podcast creator would not want his income information streamed to parties outside the transaction. Privacy for competitive and regulatory reasons is even more critical for enterprise user transactions. Furthermore, the visibility of increasingly complex smart contracts brings severe security risks as demonstrated by The DAO[2] and Parity[3].

- **Prevalence of micropayments.** It is expected the majority of content transactions will transfer small denominations. For example, a user supports content creators with small donations, or they pay for access to premium content like watching an episode of a popular TV show. The industry needs a frictionless micropayment solution to foster a vibrant and healthy community. This translates to a blockchain with minimal or even zero transaction fees.

Evidently, current mainstream blockchains, such as Bitcoin and Ethereum, are not a natural fit for the digital content industry. Consequently, it leaves us no choice but to find novel solutions and build a light-weight yet scalable blockchain. Admittedly, many nascent projects are claiming they can solve the problems above, but none of them has proven mature in production or onboarded enough users and developers to form a scalable, self-growing ecosystem.

To address the aforementioned challenges, we propose an architecture consisting of three main components:

- **BOX Payout**. A fast and secure blockchain to carry out multiparty contingent payments.
- **BOX Passport**. A blockchain-based identity and attribution service across multiple applications.
- **BOX Unpack**. A turn-key solution for small and medium-sized partners to setup a content platform easily and quickly.

We elaborate on the components above in the following sections.

Design Goals and Principles

Before delving into the details of the core components, we would like to introduce the goals and principles considered in the design of the ContentBox Platform.

To be concise, the major design goals of the ContentBox architecture are:

- Scale when content and users grow rapidly.
- Support most common smart contracts for the content industry.
- Protect transaction privacy.
- Support micropayments.
- Easily integrate with existing applications.

[2] https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

[3] https://cointelegraph.com/news/lessons-from-parity-attack

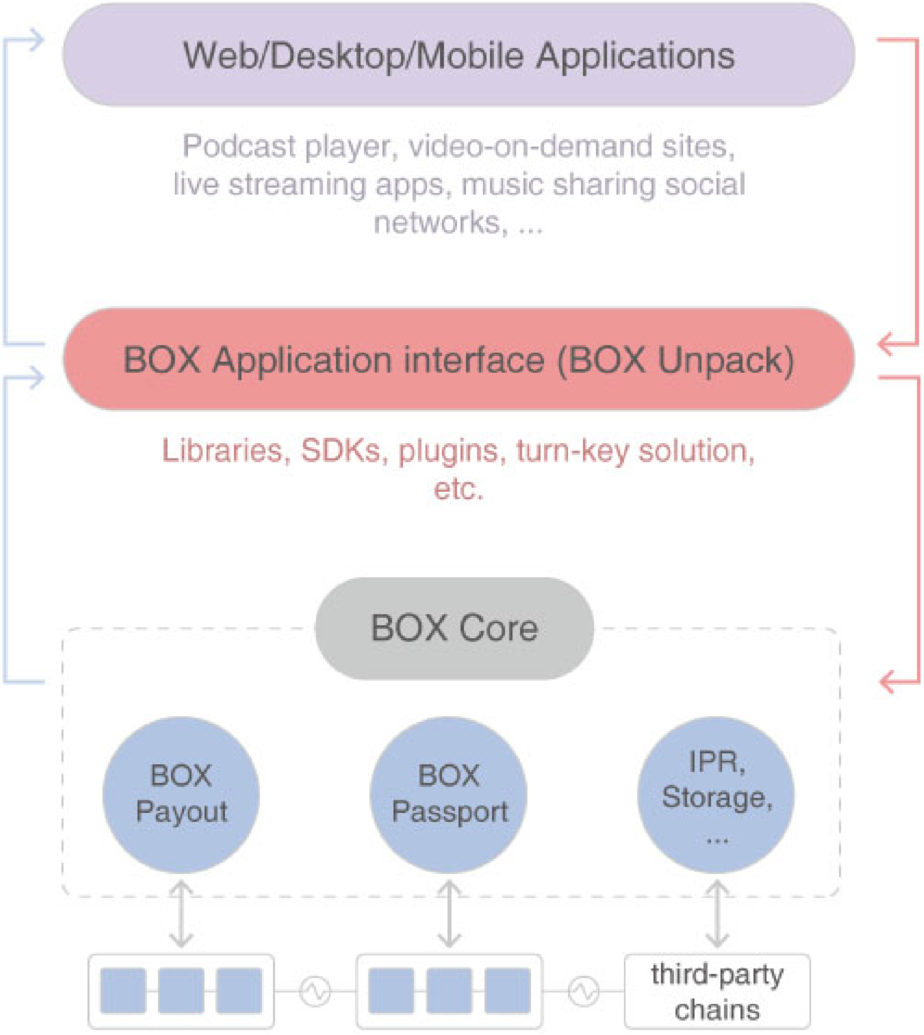

Web/Desktop/Mobile Applications
Podcast player, video-on-demand sites, live streaming apps, music sharing social networks, ...
BOX Application interface (BOX Unpack)
Libraries, SDKs, plugins, turn-key solution, etc.
BOX Core
BOX Payout
BOX Passport
IPR, Storage, ...
third-party chains

Figure 2: Overview of ContentBOX Architecture

Conceptually, all of the above goals can be achieved by designing a more powerful, fully-functional, EVM(Ethereum Virtual Machine)-compliant blockchain. However, ContentBox plans to take the approach of not building a monolithic blockchain. The design of ContentBox follows the **UNIX philosophy**: building a large system on top of a series of simple, modular, and reliable small parts, which can be easily debugged and upgraded.

In addition, ContentBox attempts to make the whole system **friendly to developers** throughout its design. An ecosystem cannot be successful just because of its technological superiority; more importantly, it needs to win the hearts and minds of users and developers. Therefore, another principle applied throughout ContentBox is to avoid reinventing the wheel whenever possible and to reuse proven, widely-used, state-of-the-art technology stacks.

Another important principle is to keep concepts **orthogonal**. Our goal is not to build a multipurpose blockchain that's difficult to build and hard to implement. Additionally, we do not want two components sharing common functionalities, which could confuse application developers. Orthogonality makes it easier to reason about what happens when things combine.

BOX Payout

A Chain Without a Virtual Machine

BOX Payout is NOT a blockchain that supports a general purpose Turing-complete virtual machine. The main purpose of the BOX Payout blockchain is to support fast and secure conditional transactions which are of great importance in a digital content world. Undoubtedly, a Turing-complete virtual machine similar to an Ethereum Virtual Machine ("EVM") can carry out arbitrary conditional transactions and ensure its execution and results, but it may not always be the optimal solution.

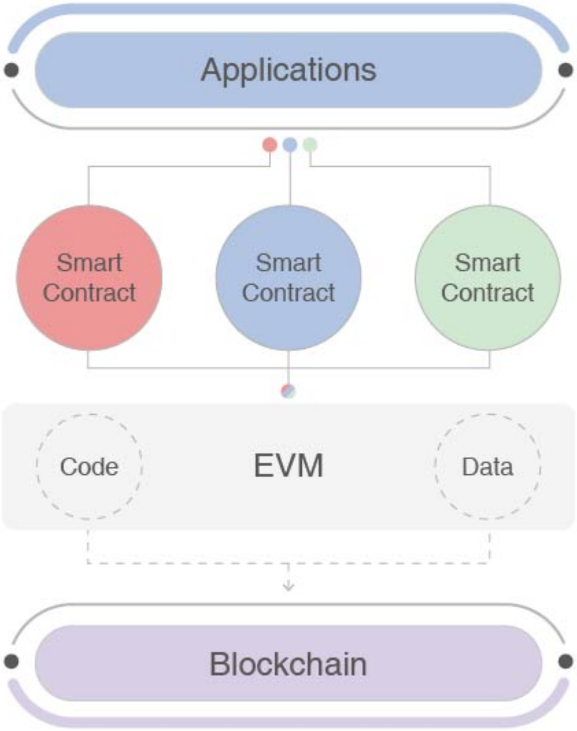


Figure 3: Traditional On-chain Smart Contract. Applications Interact with Blockchain through EVM

A simple example of conditional transactions in the digital content area is shown previously involving a user, a piece of content, and a platform. To enforce such a multiparty payout, one can write a smart contract to govern the token transfer to each party, let the EVM execute it and validate the result.

Obviously, this is a very resource-intensive approach. With the diversity of content comes the diversity of smart contracts, thus bringing a heavy burden to the blockchain. This is because **every contract will be executed for every message on every node**. But luckily, the advancements made in cryptographic research and work spearheaded by Andrew Poelstra, a scientist at Blockstream, point to an alternative way to achieve the same goal without a virtual machine, which we call *Crypto Contracts*:

Crypto Contracts

Essentially, Crypto Contracts are a kind of smart contracts that can be translated into a series of crypto primitives. Developers can also think of them as off-chain smart contracts.

Since the birth of Ethereum, smart contracts have been an indispensable part for many blockchain projects. However, most contracts need only one thing from the blockchain: an immutable ordering of commitments to prevent double-spending. Therefore, instead of using complex and resource intensive smart contracts to align the interests of stakeholders and automate payment related transactions, we can aggregate simple signatures to achieve the same goal, but with much higher performance.

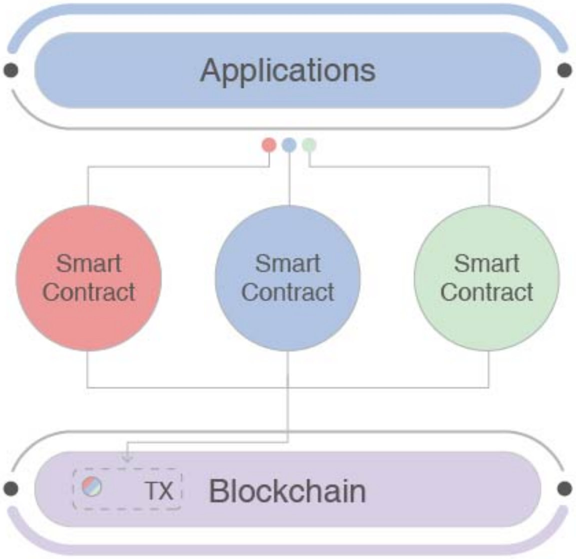


Figure 4: Off-chain Smart Contract. Applications Interact with Blockchain Directly

Basically, a set of parties can decide on some sort of contract or protocol that they want to execute, and as a result of faithful execution they will produce a valid signature and the blockchain and its verifiers can validate that the signature is valid. The blockchain does not need to know any of the details of the original transaction. By using a signature itself as a witness, the bulk of transactions can be moved off-chain and **leave the blockchain to do what it is really good at: check a multi-signature**. In other words, a smart contract can be compiled into a series of cryptographic primitives; when someone signs and validate an ordinary transaction with these primitives, it holds that a smart contract that is not hosted on the blockchain still executes faithfully.

A crucial piece of this approach is Schnorr Signature[4]. Unlike ECDSA signatures, Schnorr signature has **linearity** in its math, which makes it ideal for creating "adaptor signature" that can be used in settling off-chain transactions automatically. By replacing the signatures embedded in each input with an aggregated single signature, a blockchain can save large amount of disk spaces and become very lightweight, yet more powerful than before.

Consider a simple case: Alice wants to stream an online movie owned by Bob, and she would like to pay Bob 1 BOX in exchange for a one-time access key to the movie. Now suppose Bob embeds the access key in a secret *t*, and the process that Alice gets *t* can be described as follows:

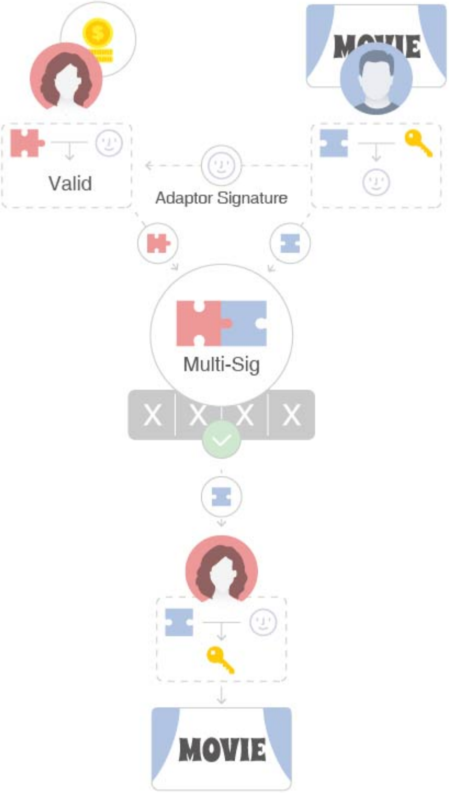


Figure 5: Alice pays Bob to gain a movie access key with an adaptor signature

1. Alice and Bob construct joint key $J(A, B) = P'_A + P'_B$, where $P'_A = H(H(P_A||P_B)||P_A) * P_A$, $P'_B = H(H(P_A||P_B)||P_B) * P_B$ (P_A, P_B are public keys)
2. Alice and Bob share P_A, P_B, R_A, R_B (random nonce points); Bob calculates $T = t * G$, and gives

[4] Technology roadmap - Schnorr signatures and signature aggregation https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/

T to Alice

3. Alice and Bob therefore agree on random challenge $e = H(J(A,B)||R_A + R_B + T||m)$ (H denotes hash algorithm, and these two steps not shown on the figure)
4. Bob provides adaptor signature $s' = r_B + e * x'_B$ (shown on the upper-right corner of the figure, x'_B is the private key for P'_B)
5. Alice verifies: $s' * G = R_B + e * P'_B$
6. If OK, Alice sends Bob her signature: $s_A = r_A + e * x'_A$ (x'_A is the private key for P'_A)
7. Bob completes, atomically releasing t: first, construct $s_B = r_B + t + e * x'_B$, then combine: $s_a = s_A + s_B$, sign the transaction and broadcast it on blockchain, then Alice sees s_a
8. Alice subtracts: $s_a - s_A - s' = (r_B + t + e * x'_B) - (r_B + e * x'_B) = t$

Consensus Mechanism

To further improve the scalability of the BOX Payout blockchain and make it mobile-friendly, a derivation of Proof of Stake ("PoS"), named Proof of Network Effect ("PoNE") will be adopted as the major consensus mechanism.

PoS is a category of consensus mechanism for public blockchains which depends on a validator's proportion of the total number of tokens in the network. In Proof of Work ("PoW") based public blockchains, the algorithm rewards participants who solve cryptographic puzzles in order to validate transactions and create new blocks. In PoS-based public blockchains, a set of validators take turns proposing and voting on the next block, and the weight of each validator's vote depends on the size of its stake.

Because of the specific domain the ContentBox Platform is serving, PoNE has also been added on top of a plain PoS. The probability of being selected as a validator will depend on the amount of the validator's deposit, the content creation and consumption of that particular node. Together with PoS, the score of a node being selected as a validator will be as follow:

$$\mu_i = \frac{s_i}{\sum s} + \frac{c_i * \omega_i}{\sum (c * \omega)}$$

μ_i denotes the score of a node

s_i is the stake of a node

c_i is the contribution score of a node, affected by the quantity and frequency of content contribution related this node

ω_i is the weight value largely like the impact factor used in academia

In order to perform mining on the blockchain of BOX Payout, nodes will be bonded by the protocol and make a security deposit. Every round of the block creation, a list of 5 ordered validators will be selected randomly with the score stated in the formula above. If the first selected validator is offline and can not perform the validation, the second will substitute and take its place.

Significant advantages of this consensus mechanism include security, reduced risk of centralization, and energy efficiency. Transaction throughput will also be improved and it will greatly affect the user experience when consuming the content. For example, when a piece of audio is played, the time should be recorded, and the relevant payment, either from advertising or subscription, should be instantaneously be distributed back to their right holders. This is the whole premise for building BOX Payout.

Since the ContentBox Platform is targeting the digital content consumption market which usually happens on mobile nowadays, it is essentially targeting a large distributed validator population with minimal resource consumption. The potential nodes will be established on mobile devices, given the consumption pattern set forth above. The computation power may not be as strong, while the quantity of nodes could number in the hundreds of millions. This builds the foundation for using PoS without the concern of the initial distribution of token.

BOX Passport

With the growth of the ecosystem on the ContentBox Platform, a plethora of content applications are expected to be built on top of it. A single user shall have a consistent identity across all of applications, instead of having to create an independent identity for each of them. Therefore, ContentBox will introduce a powerful **decentralized interoperable identity service** called “BOX Passport”. It allows a user to transact frictionlessly **across multiple apps or websites** with a single digital identity and will enhance the user’s privacy, security and control as well.

BOX Passport establishes this identity by extending the wallet concept to store personal information such as reputation alongside token account. This identify service is not stored in any application’s centralized databases and is inherently decentralized, thus less vulnerable to hacks. Users have full control over their identity and decide who can access which part of it for how long. Furthermore, BOX Passport will bind a creator to his artworks transparently and permanently, which helps him build an ongoing reputation in the digital content world.

Based on BOX Passport, we will introduce a new feature for the ecosystem, named BOX Login, and will open it to every developer in the community. Similar to Facebook Login in concept, Box Login is a secure and convenient way for people to sign into any website, desktop app or mobile application in the ContentBox ecosystem. However, BOX Login is implemented on the blockchain and will not be controlled by any single company or organization, which will set it apart from any of today’s third-party authentication system.

Third party identity services such as Keybase[5] and uPort[6] will be possibly integrated into the identity service for broader interoperability.

BOX Unpack

Application Interface

BOX Unpack is the application interface of ContentBox, including a series of libraries, SDKs, command line and web-based tools aiming to assist potential partners and general developers to build next-generation digital content applications. Unlike Ethereum, BOX Unpack does not require the developers to learn a new programming language to write smart contracts, instead, it allows the developers to integrate blockchain related services easily and intuitively with familiar languages: Java, Go, Python, etc.

The major functionalities of BOX Unpack include: sign up and log in with BOX Passport, build and commit transactions on BOX Payout, upload and register digital contents, account migration and aggregation, and a set of tools to manage content on the blockchain. In particular, BOX Unpack also encapsulates a few AI-based algorithms developed in-house at CastBox into reusable modules which can help developers implement some advanced features on a decentralized application:

- **In-audio Search.** This is a novel search technology recently introduced by CastBox that allows users to find content he/she wants to hear in a more efficient way. Traditionally, audio search is implemented by crawling tags and title descriptions which are often manipulated by some savvy podcasters (we can see similar things occurred in App Store SEO). But CastBox implements it in a new way: it uses its Natural Language Processing (NLP) algorithm to transcribe spoken audio content, combined with machine learning to surface personalized results tailored to each user's search and listening habits. By using this technology, ContentBox application developers can develop a fast and intelligent search engine which can help users discover interesting contents across multiple digital content platforms.
- **Deep learning based recommendation engine.** The recommendation engine in CastBox is built on the basis of a wide & deep model used in Google Play[7] along with a denoising autoencoder developed in house. Compared with traditional recommendation models, deep learning techniques provide a better understanding of user's demands and high-quality recommendations. Leveraging this technology, combined with the blockchain libraries provided by BOX Unpack, developers can build an unprecedented recommendation engine for every user on the ContentBox platform.

[5] https://keybase.io/
[6] https://www.uport.me/
[7] https://arxiv.org/abs/1606.07792

Turnkey Solution

In addition to the developer tools mentioned above, BOX Unpack also provides a turnkey solution for small startups who want to provide digital content services to users but lack funding or technology to set up a full-fledged online platform. Imagine a small team wanting to create a better video app with an outstanding player they just built. Their first challenge is overcoming high copyrights purchasing costs. With this turnkey solution, the team can overcome said copyright hurdle by setting up a revenue-sharing scheme easily without programming any smart contract. We believe this turnkey solution will dramatically lower the barrier to entry for potential partners to join and grow ContentBox.

Related Work

There are a plethora of projects currently working to solve scalability and privacy issues of current blockchains. Unfortunately, none of them can be directly applied to solve the unique challenges ContentBox aims to overcome. Nevertheless, there are many potential techniques to be leveraged, and we are actively monitoring their progress.

Sharding

Similar to database sharding in traditional database software systems, such as MySQL, sharding on blockchain is an approach to improve system scalability. The key idea to split the overall state of the chain into different shards, and each shard only processes a small part of the state and does so in parallel[8].

Many blockchain developers see sharding as a promising approach to solve blockchain's scalability problem, and many blockchain projects have based their solution on this technology. However, we are a little bit more conservative regarding its full-fledged implementation on the main net in the near future. Basically, in sharding, the blockchain wants to create a network where every node only processes a small portion of all transactions, while still maintaining high security. A fast and secure solution for this problem is not easy to find because a transaction executed on the blockchain can depend on any part of the previous state in the blockchain, which makes it difficult to do things in parallel. And inter-shard messaging compounds the complexity.

Overall, we believe sharding still has a long way to go before becoming a widely accepted solution to scale the blockchain. We will pay close attention to the progress in this area but will not use it as a core technology in our solution for now.

[8] https://github.com/ethereum/wiki/wiki/Sharding-FAQ

Lighting Network and Raiden Network

Basically, both the Lightning[9] and Raiden[10] networks rely on off-chain state channels. The core idea here is that participants put some bitcoin or ether into a multi-signature address, open a payment channel and then sign transactions without submitting to the blockchain. Payment channels can be organized into a network and thus a payment between two parties can be conducted through multiple hops. The payment channel can be closed by either party at any time, and the last-signed transaction with the most up-to-date balances for both parties is the one that will be committed to the blockchain.

Both of these two approaches can increase transaction throughput and lower fees effectively in their respective environment (one for Bitcoin and the other for Ethereum) if properly implemented. However, there are still some limitations in practice. For instance, all participants of a transaction need to lock up some tokens on-chain until the channel is closed, thus discouraging usage of the payment network.

Plasma

Plasma[11] is one of the most promising proposals for scaling smart contract computations on the blockchain. With Plasma, the blockchains are composed into a tree hierarchy, and each branch treated as a blockchain with its own history and computations that are map-reducible. Therefore, the root chain only needs to handle a small amount of merkleized commitments from child chains, which results in high scalability.

Both authors of Plasma are masterminds in the blockchain field, and they proposed a novel solution to the long standing problem of current mainstream networks. Ideally, it will be appropriate for the digital content industry and could serve as the basis of ContentBox. However, this project is still in its infancy, and some critical challenges need to be addressed, such as how to handle an attack occurring on a child chain. The Plasma paper's solution of moving participants to another chain is far from perfect as moving funds smoothly cannot be easily implemented and guaranteed. And their entire system of smart contracts is still prone to potential security breaches.

Therefore, we view Plasma as an upgraded and improved Ethereum which still requires time to demonstrate production level capability, so we will refrain from using it to lay the groundwork for ContentBox.

MimbleWimble

MimbleWimble[12] is a new blockchain design proposed about a year and a half ago which can theoretically increase privacy, scalability and fungibility compared current main stream blockchains. The core

[9] https://lightning.network/
[10] https://raiden.network/
[11] http://plasma.io/
[12] https://github.com/mimblewimble/grin

idea is that people can verify the state of the system without downloading all of the transaction data. Instead, the chain can compact the transaction history efficiently and rely on cryptographic primitives to achieve full public verifiability (which is very similar to our solution). The project has made great progress recently by launching a testnet[13] and integrating Bulletproofs[14].

However, a full node of MimbleWimble still needs a lot space on disk which makes it unfriendly to mobile devices. And arguably, the design of stripping out the Bitcoin's scripting system will make it hard to do soft-forking and debilitate its power on enforcing contingent payments which is of great importance in the digital content industry. Nevertheless, MimbleWimble is a promising solution towards scaling blockchain and we can borrow a lot from its design and implementation. For example, the structure of transactions, the cut-through used for packing block and its ASIC-resistant mining algorithm (Cuckoo Cycle) that encourages mining decentralization.

Steem

Steem is a blockchain for producing Smart Media Tokens which facilitate a decentralized blogging and social network: Steemit[15]. By design, Steem leverages the Delegated Proof-of-Stake (DPoS) consensus protocol to achieve a high throughput of transactions. In addition, it introduced several innovative built-in features, such as Reward Pool, ChainBase, and a stake-based voting and incentivization mechanism to support the operation of Steemit.

Generally, Steem is a well-designed blockchain for a social media platform with great performance and rich built-in features. However, as an infrastructure, Steem is too application-specific. While supporting the operation of Steemit well, the reward and voting system also limit the use of Steem in applications other than social blogging. For example, a mobile video app might not need a voting action to determine a user's interest on a video clip; they can learn by simply observing the user's behaviors like browsing, viewing, pausing, fast forwarding, etc. Actually, many startups are using users' behavioral data and advanced AI algorithms to curate and dispatch personalized contents.

The basic design of Steem appears impressive but it's not suitable for the Box core system. Instead, we prefer to use the blockchain as a microkernel of the whole system and restrict the rewarding or voting components to the application level to improve flexibility. Our architecture is a better way to develop an open-source ecosystem that lays the foundation for ContentBox adoption by the digital content industry.

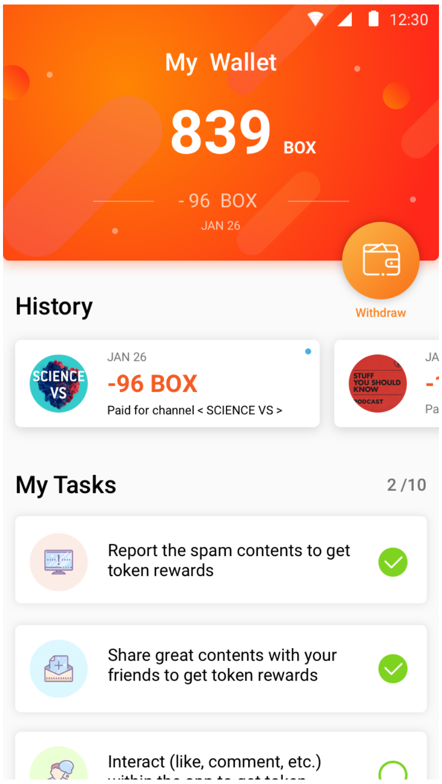
[13] https://www.coindesk.com/magical-realism-mimblewimble-just-launched-first-testnet/
[14] http://web.stanford.edu/~buenz/pubs/bulletproofs.pdf
[15] https://steemit.com/

Integration with CastBox App

Mobile Wallet

A light wallet will be integrated into CastBox application. With the built-in wallet, a user can instantly see his balances and transaction history while using the app, including token rewards for their contribution to the CastBox community. In the future, the wallet will show balances across apps.

As a popular mobile app, CastBox is a logical host for a mobile wallet of BOX tokens. By onboarding millions of CastBox users and building an immediate online ecosystem, ContentBox will avoid the cold start that plagues most startups. Additionally, since CastBox is a frequently used app, users will naturally interact with ContentBox multiple times a day and become familiar with crypto token related concepts. In the long run, as users become comfortable with BOX tokens and experience the benefits of a new blockchain-based system, they will accelerate other applications working with ContentBox, growing and expanding the ecosystem of players.



Paid for channel < SCIENCE VS >

Report the spam contents to get token rewards ✓

Share great contents with your friends to get token rewards ✓

Interact (like, comment, etc.) ○

Figure 6: In-app light wallet

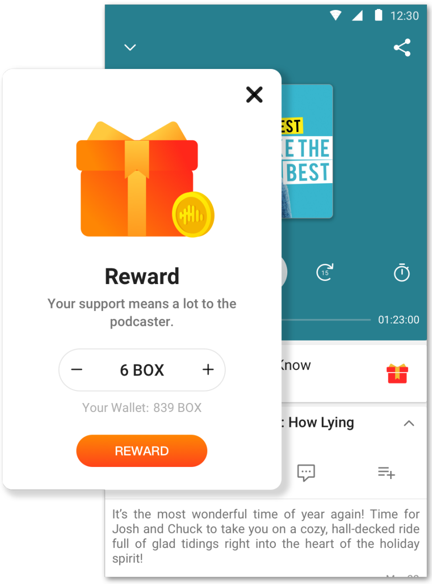
BOX Login

CastBox will migrate the opt-in accounts onto the blockchain and grant users a secure universal BOX ID once the BOX Passport system is in production. After the migration, CastBox's backend servers will no longer store user account and credential information. Instead, the app client will access the blockchain to retrieve and verify a user's identity during the sign-in process.

Using BOX Passport will bring benefits to CastBox's operator as well as its end-users. Given that user authentication and authorization is moved from the app's servers to a public blockchain, the operator is no longer burdened with manually guarding against hacker attacks on user information. On the other hand, the app users also gain back control of their own data, mitigating the risk of personal data breaches.

In-app Token-based Reward System

Along with the light wallet, a token-based reward system will be built into CastBox as well. The reward system serves mainly two goals: to incentivize authors to create more valuable content and to motivate users to curate and spread good content. For example, if a listener finds an interesting podcast in CastBox, submits a comment, and then shares it with his friends on social networks (such as Facebook or Twitter), he will receive BOX tokens as rewards.



Your support means a lot to the podcaster.

It's the most wonderful time of year again! Time for Josh and Chuck to take you on a cozy, hall-decked ride full of glad tidings right into the heart of the holiday spirit!

Figure 7: Earn BOX by flagging spam

Users can also gain tokens for helping filter spams. Spamming is a challenge for every online community and results in reduced user experience if not efficiently controlled. Usually digital content platform owners solve this problem by hiring more moderators or invest in the researching and deploying of AI-based algorithms for automatically filtering spam. However, both of these approaches are costly and inefficient in practice. Through the built-in incentive system, CastBox users receive rewards for proactively flagging low-quality content.

Example Applications Beyond CastBox

When developers use BOX Unpack and BOX Passport, many new applications are created and deployed on the ContentBox platform. The digital content open source software community we're fostering brings potentially unlimited use case possibilities. Here are a few high-level examples:

Content Marketplace without Middleman

Control of content distribution is concentrated in a few centralized marketplaces such as iTunes and Google Play. These marketplaces unilaterally determine how creators are paid. As a result, the vast majority of creators globally are greatly underpaid, if paid at all.

ContentBox allows for an open, fair, and creator-centric decentralized marketplace that enjoys many advantages over a centralized one.

- Lower fees. Since there is no hyper-scale digital platform company between creators and consumers, taking a big cut, more revenue will flow to creators.
- More liquidity. In the music industry, for example, it could take six to eighteen months after a song is released before the artist receives the first royalty check. In our new digital marketplace, an artist can be paid automatically in tradable built-in tokens while her song streams anywhere in the world.
- More Transparency. Since all critical information is logged in a public blockchain, an artist knows exactly how many times and when her song is streamed and how much revenue it was generating.

Native Mini Crowdfunding Launchpad

Traditionally, content creators have very few ways to fund their creative projects and rely on powerful intermediaries such as music labels and film studios, which take a significant cut of the whole pie. With ContentBox, creators can raise funding truly independently. A filmmaker can pre-sell tokens to fans to fund an independent film, which grant them access to the film once it is made. The crowdfunding smart contract can also include advanced features. For instance, fans can share in a portion of the film revenue per their tokens. Or fans can specify funds to be gradually released, contingent upon reaching production milestones. The same applies to other forms of creative endeavors such as music and TV shows.

Crowdfunding within the ContentBox ecosystem can leverage the network effect of a large captive user base, which is more likely to support digital content projects than users on other crowdfunding platforms. Also, these native tokens can be utilized frictionlessly on the ContentBox blockchain without the additional cash out hurdles of running an external crowdfunding campaign.

Decentralized “AdSense” for Content Platforms

AdSense is a program run by Google that allows publishers in the Google Network of content sites to serve automatic text or multimedia advertisements, that are targeted to site content and audience. On the ContentBox Platform, we can run a similar program to AdSense which will facilitate transactions between advertisers and content publishers. But unlike Google AdSense, this program is based on public blockchains instead of a central giant platform like Google. Advertising inventory can be organized on a decentralized file system like IPFS, and the dispatch engine can be developed by leveraging the modules provided by BOX Unpack. And the monetization and payments can be made via BOX Payout.

Compared with Google AdSense, this decentralized program can provide a more transparent and reliable service. Without a central authority, all parties enjoy more flexibility; advertisers pay less in fees, and publishers receive higher remuneration.

Cross-service On-demand Video Player

Usually a media player is just a desktop or mobile software that can decode many multimedia file formats. However, a new type of player can be developed on the ContentBox Platform. Besides the function to play a video clip on user's device, this new player can allow its users to search on a wide range of digital movies registered on ContentBox platform, although they will be potentially hosted on different server farms owned by various partners of ContentBox. While streaming, the player can also collect BOX tokens in real-time and automatically distribute them among the copyright owners, streaming platform and storage providers according to a pre-defined smart contract.

The core functionality of this new player is to interact with our BOX Payout and BOX Passport. Aided by these core components of ContentBox, the player can tap into the vast shared pool of genuine contents and enhance the user experience in video-on-demand greatly. Without the infrastructure provided by ContentBox, this innovative software idea would be inconceivable.

Roadmap

The CastBox and the ContentBox Platform technical roadmaps include the following milestones:

- 2016.01 CastBox team founded
- 2016.02 CastBox for Android launched
- 2017.01 CastBox for iOS launched
- 2017.10 Deep in-audio search feature launched
- 2018.03 Token sale
- 2018.09 Token integrated into CastBox app
- 2018.12 Launch of BOX Passport (alpha version)
- 2019.03 Testnet of BOX Payout online
- 2019 Q4 Launch of BOX Payout Mainnet

Token Distribution

The native digital cryptographically-secured utility token of the Contentbox Platform (BOX) is a major component of the ecosystem on the Contentbox Platform, and is designed to be used solely on the platform. Before the official launch of the native blockchain on the ContentBox Platform, BOX will initially be issued as ERC-20 standard compatible digital tokens on the Ethereum blockchain. Once the main net of BOX Payout is online and stable, the ERC20 token gets converted to the chain token on a 1-for-1 basis.

Allocations

Percentage	Usage	Detail
25%	Pre-sale	Target selected institutional investors, with locking period up to 6 months.
15%	Team	Rewards for in-house R&D team and open-source contributors with a 4-year vesting period.
30%	Ecosystem Incentives	Incentivize all participants in the ecosystem, such as the creators, the audiences, the individual investors, the platform, etc.
20%	Foundation	Protect the BOX token from speculative trading and fund the operations of the Foundation.
10%	Partnership	Fund the bounty program and build partnership with other audio/video websites or mobile apps.

Use of Proceeds

Percentage	Item
50%	R&D
25%	Marketing & Promotion
15%	Legal, Auditing, and Compliance
10%	General & Administrative

Team

- **Renee Wang** - Founder and CEO of CastBox. Renee founded CastBox in 2016, and has spearheaded the meteoric rise of the company over the past two years. Throughout this period, she has not only built a global team of 50 talents but has closed more than $30 million dollars worth of investments. Renee was a part of the global mobile advertisement team for Google Beijing, Google Dublin and Google Japan. She was the 7th employee and Android engineer at Umeng, a China-based startup acquired by Alibaba, and was one of the earliest Android developers in 2008. Renee holds a Bachelor's degree in Psychology from Peking University.

- **Hu Gang** - Chief Crypto Officer and ContentBox CTO. Gang is a serial entrepreneur, system architect and full-stack engineer with more than a decade of experience in building web and mobile applications. He earned his Master's degree in Computer Science from Peking University in 2002. He also earned his MBA from Duke University. He was previously a partner and CTO at 5miles, a leading mobile e-commerce app in US with millions of daily active users.
- **Alex He** - Co-Founder of CastBox and CTO. From 2003 to 2015, Mr. He has worked at Motorola, Borqs, and Xiaomi, with a focus on the Linux/Java/Android mobile software research and development. Since 2007, he has been engaged in the research and development of Android mobile technology and was one of the earliest Android developers in China. Mr. He joined the Founder Institute of Peking University after graduation, working in software research and development in the field of multimedia. Mr. He has managed R&D teams numbering in the hundreds. Also, he is an active open source developer on GitHub. Peking University Class of 1999.
- **Dr. Xiaohui Liu** - Blockchain Scientist. Former Research Scientist at Facebook, designing and implementing distributed protocol for next generation wireless mesh networks. Dr. Liu has 10 years of research and development experience in distributed networking protocols. He also owns 1 patent and 9 papers in international premier conferences and manages 2 Facebook open source projects. He earned his Ph.D. in distributed networking from Wayne State University, USA and holds a bachelor degree from Wuhan University, China.
- **Fangqin Dai** - Tech Lead. Previously Senior Software Engineer at Google. Developed mining pool software and mined ETH with over 1000+ GPUs, and is fluent in smart contracts development. Fangqin has 7 years of industry experience from working at top companies such as Baidu, Intel, Taobao, and KingSoft. He has amassed 2200+ followers on GitHub and has contributed to many popular projects such as Apache Spark. Fangqin received his Master's degree from Tsinghua University in Beijing, China and his Bachelor's degree from Wuhan University in Wuhan, China.
- **Yiqiang Wang** - Founder and former CTO of Kaitong Finance, a fintech company founded in 2015. Until January 2018, the company had served hundreds of large and medium-sized Internet platforms and financial institutions, and the total trading volume had reached more than 100 million yuan. Before joining Kaitong, Yiqiang was a founding member and core developer at Umeng, which provided services such as data analytics for domestic mobile application developers in China. Yiqiang holds both a Master's and Bachelor's degree in Computer Science from Fudan University.

Risks

You acknowledge and agree that there are numerous risks associated with purchasing BOX, holding BOX, and using BOX for participation in the ContentBox Platform.

Uncertain Regulations and Enforcement Actions

The regulatory status of BOX and distributed ledger technology is unclear or unsettled in many jurisdictions. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including BOX and/or the ContentBox Platform. Regulatory actions could negatively impact BOX and/or the ContentBox Platform in various ways. The Foundation (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, the Foundation will apply a cautious approach towards the sale of BOX. Therefore, for the crowdsale, the Foundation may constantly adjust the sale strategy in order to avoid relevant legal risks as much as possible. For the crowdsale, the Foundation is working with Tzedek Law LLC, a boutique corporate law firm in Singapore with a good reputation in the blockchain space.

Competitors

It is possible that alternative networks could be established that utilize the same or similar code and protocol underlying BOX and/or the ContentBox Platform and attempt to re-create similar facilities. The ContentBox Platform may be required to compete with these alternative networks, which could negatively impact BOX and/or the ContentBox Platform.

Loss of Talent

The development of the ContentBox Platform depends on the continued co-operation of the existing technical team and expert consultants, who are highly knowledgeable and experienced in their respective sectors. The loss of any member may adversely affect the ContentBox Platform or its future development.

Failure to Develop

There is the risk that the development of the ContentBox Platform will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or BOX, unforeseen technical difficulties, and shortage of development funds for activities.

Security Weaknesses

Hackers or other malicious groups or organizations may attempt to interfere with BOX and/or the ContentBox Platform in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Foundation or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of BOX and/or the ContentBox Platform, which could negatively affect BOX and/or the ContentBox Platform.

Other Risks

In addition to the aforementioned risks, there are other risks (as more particularly set out in the Token Purchase Agreement) associated with your purchase, holding and use of BOX, including those that the Foundation cannot anticipate. Such risks may further materialise as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Foundation (and its affiliates), the ContentBox team, understand the overall framework and vision for the ContentBox Platform prior to purchasing BOX.