DECENT

#liberateyourself

DECENT Whitepaper

Matej Michalko m@decent.ch
Josef Sevcik josef@decent.ch

November 2015
v 0.0.2

Table of Contents

1. Introduction

True innovation is rare, especially in the world of media. More difficult is to determine which aspect of media thrives for development most. Majority of mainstream media do not truly innovate as they are happy with their current business models. Most of the incumbents do not provide as many benefits to the *content consumers* as they could because of lack of incentives.

Moreover, having the obligation to pass through a third party to access digital content is unnecessary. Traditional media companies as Medium, New York Times or Daily Mail choose what they publish and which authors they allow to distribute their content through their fully controlled centralized for-profit platforms. Similarly, many jurisdictions do not provide freedom of speech; people are prosecuted for expressing their thoughts.

This white paper focuses on the challenges and redefinition of the way digital content is shared and freedom of speech is enabled over the Internet. We propose DECENT: Decentralized Open Source Content Distribution Platform enabled by Blockchain and peer-to-peer technology.

2. The Blokchain Era

Bitcoin[1], presented in 2009 by Satoshi Nakamoto was a disruptive change in the way people look at finances. By providing efficiency (worldwide clearing and settlement within 10 minutes) and cost-effectiveness (transaction fees at a few cents per transaction) compared to the traditional banking system, it is getting a massive exposure in media. Unfortunately, in spite of more than 6 years of its existence it did not reach a position it could have attained mainly due to the imperfections in its architecture and design. One of them is the 7-transactions per second (tps) processing capacity[2], which makes Bitcoin hard to be deployed in real world applications as it is unable to fulfil their requirements. For instance, VISA handles about 2000 tps[3] with a peak capacity of 56000 tps[4].

[1] https://bitcoin.org/bitcoin.pdf
[2] https://en.bitcoin.it/wiki/Scalability#Scalability_targets
[3] http://usa.visa.com/merchants/industry-solutions/retail-visa-acceptance.jsp

Similarly, Bitcoin blockchain size of nearly 40 GB (August 2015) with a steep linear growing curve[5] renders it difficult to be distributed in the future. It is inconvenient for most of people to be forced to wait for downloading a few tens of GBs of data in order to send even a tiny amount of money.

Hence, Bitcoin can be understood as a pioneering proof of Blockchain technology concept that has some childhood diseases. Blockchain, as a publicly distributed ledger of transactions, has a great potential to be the next big thing since the advent of World Wide Web. Various financial institutions are investigating this field, some of them even have their own blockchain research departments[6]. Blockchain technologies can help banks to reduce their operating and infrastructure costs in various domains of application. By providing seamless automation, clearing and settlement can run without any human interaction and under control of an indestructible set of business rules. Similarly, Blockchain technologies enable banks' assets to be exchanged without third party validation.

[4] http://usa.visa.com/about-visa/our-business/visa-transaction.jsp
[5] https://blockchain.info/charts/blocks-size?showDataPoints=false&show_header=true&daysAverageString=1&timespan=2year&scale=0&address=
[6] http://cointelegraph.com/news/114889/10-big-banks-that-are-seriously-looking-into-blockchain-technology

Figure 2.1: Blockchain Use Cases[7]

Blockchain has applications in many other domains besides finance, as illustrated on Figure 2.1. Proof of Ownership, Decentralized Storage, Decentralized Peer Review are only a few of them. The world is constantly discovering the immense benefits decentralized applications can bring to it.

3. Manipulation and Freedom of Speech

Nowadays most of the media and content sharing places are private entities that decide by whom and how their platforms can be used. In order to publish content, one has to agree with their terms and conditions and often loses proprietary rights to the content. Third parties can bowdlerize, manipulate or even permanently remove parts or even entire piece of digital content posted by creative

[7] http://n6zgo3se7pe2sazc62u1v9qe.wpengine.netdna-cdn.com/wp-content/uploads/2015/07/1231-1024x699.png

artists. Reddit[8], Twitter[9], Facebook[10], Medium[11] are typical examples of those platforms.

Some of the countries, where freedom of speech is an issue, keep an eye on the traffic to and from the country, in order to prevent inconvenient content or to tag dissident servers or people. Online media need to be licensed and the operations are supervised by the state apparatus.

Even in Western democracies where people are generally free to express their opinions, the manipulation takes place at the level of unnecessary middlemen running the media. There is a lack of direct relationship between authors and content consumers (readers, listeners, viewers, ...).

Moreover, authors do not have enough opportunities to monetize their work or the existing content distribution platforms are too complicated to be dealt with. For instance, bloggers can either use the service of a third party provider such as Medium or start their own websites. In the former case, the bloggers are unlikely to get financially compensated for their work, unless they are between the most rated ones on the server. In the latter, they would need to get users to their websites, which is usually a hard task and requires skills from multiple domains, such as SEO or inbound marketing. Later, they would also need to find their own business models, such as installing Google Ad Sense[12] and of course agree with their terms and conditions of use. Those are the things authors usually do not want to deal with. Their main job is to write (producing music, video, software) and not to be bothered with ads.

Online e-books' resellers, such as Amazon, charge tremendous fees for online book publishing and distribution. Amazon's 35% or 70% royalty rates[13] keep the poor writers with 65% or 30% of the revenue paid by readers, respectively.
One can now see the non-freedom of speech, manipulation of media and unnecessary middlemen making profit on author-reader relationship is a real issue.

[8] https://www.reddit.com/
[9] https://twitter.com/
[10] https://www.facebook.com
[11] https://medium.com/
[12] https://www.google.com/adsense/start/
[13] https://kdp.amazon.com/help?topicId=A29FL26OKE7R7B

4. Historical Approach

The problem of manipulation and censorship stems from historical reasons. In the age of print media, only few people and companies had access to publishing and distribution of content. That led to imbalance between opinions, colossal manipulation and misuse of the information distribution monopoly.

In 1517, Pope Leo X started to sell indulgences. The campaign was successful for some time. A radical change came when an ordinary German priest Martin Luther put a document called "The Ninety-five Theses" on the door of Wittenberg cathedral.
Thanks to the word of mouth and availability of printing press it got quickly spread within whole Germany in a few weeks. Eventually, Martin Luther's ideas against indulgences got a serious traction all over Europe[14]. This would not be possible a few decades ago without the Guttenberg's 15th century invention of effective printing press. That was one of the first major events that showed the benefits of fast distribution of information on the freedom of speech. Similarly, some 300 years later, Ronalds, Cooke & Wheatstone and Morse's electrical telegraph[15] was a harbinger of mass personal communication era. With the unique system of coding it allowed transmission of any kind of text information. At the end of the 19th century, telegraph lines already covered all inhabited continents[16]. Another disruptive invention was the Bell's telephone[17] that boosted telegraph system to the domain of voice communication.

In parallel, Marconi and others' works on wireless telegraphy[18] enabled the transmission over air. This undermined the importance of physical cables as the only transmission media. Any hard links were no longer needed. Thanks to their invention, people were able to listen to either government owned or commercial radio stations.

[14] http://www.bbc.co.uk/history/historic_figures/luther_martin.shtml
[15] https://en.wikipedia.org/wiki/Electrical_telegraph
[16] https://en.wikipedia.org/wiki/Electrical_telegraph#/media/File:1891_Telegraph_Lines.jpg
[17] https://en.wikipedia.org/wiki/Telephone
[18] https://en.wikipedia.org/wiki/Wireless_telegraphy

Although printing press, telegraph, telephone and radio were major advances in the easiness of access for everyone, they do not provide any security layer, as wax sealed letters or polyalphabetic ciphers used hundreds of years beforehand. Besides of military purposes, massive proliferation of encrypted communication has not yet come. Most people are not aware of the consequences that non-encrypted online communication has. Government agencies are buying data from software platforms, in order to pursue their goals. Edward Snowden's case in 2011[19] only pointed out to this issue. PGP encrypted emails provide only a partial solution to this problem[20] due to the lack of scalability and user convenience. Generally, a holistic approach to decentralized, non-manipulable, secure, trusted, efficient and cost-effective digital content distribution is needed.

5. DECENT: Characteristics & Advantages

As there is no comprehensive solution to the problems mentioned above, we came up with the idea of an open platform solving all of them. DECENT is a Blockchain based decentralized autonomous organization[21] that will run with no third party intervention. It is a Decentralized Open Source Content Distribution Platform for creative people, authors, bloggers, publicists and the fans and followers allowing borderless publishing of any text, picture, video or music content. DECENT is acting as a resourceful and independent unit. It allows information sharing without any boundaries and restrictions. The platform is dedicated to the freedom of speech. It is served by the P2P network and secured by cryptographic and Blockchain technology. Sharing information is easy and protected. No third parties can control or influence the content. Main characteristics of DECENT are:

Independent

DECENT is owned directly by its users and will never be affiliated with any economic, media or political party.
It is a piece of software that you can run. However, once people

[19] https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html
[20] http://recode.net/2015/05/13/encrypting-your-email-what-is-pgp-why-is-it-important-and-how-do-i-use-it/
[21] https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

download and start running it, its creators no longer hold any control over it. Similar to how Bitcoin is developed, DECENT foundation updates and improves the code which is open source so anyone can see the changes made to it. Anyone can fork it, alter it for his/her uses or simply not update it. The whole power lies with its users.

Borderless

Our aim is to eliminate all political and geographical barriers in the publishing segment, so people around the world will have the same opportunity to express themselves freely. Thanks to its P2P nature firewalls are ineffective, since the content isn't served only from one but many computers at the same time. Therefore it is practically impossible for any organization or government to block it.

Stable

DECENT is fully decentralized and not dependent on any single server thanks to utilizing the blockchain. With no single point of failure the access to the information is boundless.

Fair

On DECENT platform every author starts at the same level. They work to build high reputation through the quality and engagement of the content published. Readers take into account author's reputation when deciding if the content is worth purchasing. The bottom line is – the better content, the higher chance for authors to gain exposure and high profits.

Profitable

Readers can buy content directly from their favourite authors. There are no cuts taken by DECENT and never will be. Developers are free to build their own apps and monetize them by their will. All without paying any hidden fees to middlemen or any third parties like media houses.

Spam free

Our spam-free mechanism makes the extensive publishing very expensive for spammers, while keeping the resources available for legitimate authors.

Secure & Anonymous

Authors can publish the content anonymously. If the authors do not want, no one can reveal their identity. Similarly, all the content shared via DECENT is fully encrypted and available to the people of authors' choice: either paying ones or non-paying ones.

Recommendations-enabled

Thanks to DECENT recommendation authors and their pieces of work get feedback from verified content purchasers. This feedback is embedded in the blockchain all the time and good authors can get decent reputation over time.

6. DECENT: Who can use it & why

Book, blog, podcast and video Authors

No third parties, no censorship, no publishing fees.
There is no third party who authors have to deal with when they want to publish. The phrase "get published" has no meaning in DECENT ecosystem. DECENT gives the power back to the Authors where it belongs. It is completely up to you as an author to decide what the price of your book is. You can give it for free, or put a price tag on it. DECENT takes no cuts from your profits, while providing the infrastructure for people to find and get your books.

Free speech activists and supporters, whistle-blowers

Anonymous, ineffective national firewalls, no censorship, content is impossible to take down.
On DECENT you can be completely anonymous along with your supporters. Thanks to its P2P nature it cannot be blocked by a

firewall, because your content isn't served only from one but many IP addresses at the same time. Thereby, it is practically impossible for any government to block. If anyone who seeds your content is shut down, there are many others who have the same content and share it too. Moreover, even seeders themselves do not know what content they are seeding, so it cannot be pinpointed to any specific person or server, therefore impossible to shut down. Thanks to utilizing the Blockchain it is practically impossible for anyone even the author to delete or alter the content in any way.

Cryptocurrency miners, data centers

Make money, use your hardware more effectively, support free of speech.
If you are already running a data center or a mining operation, you can start "mining" DCTs. As many people realized with Bitcoin, if you get on board at the beginning you are in for big bucks. You will also take part in creating a whole new way of how data is distributed across the Internet.

App builders

Lot of traffic for your web or Android/OS app, Blockchain based system, open source platform.
Application programmers can implement DECENT protocol and make apps for traditional use cases to create their own Amazon, Medium or any other content oriented website or application. As a programmer you can also find completely new use cases for it. Thanks to DECENT's transaction layer the content can be both free and premium. It provides you with stability and transparency thanks to the Blockchain and takes care of the whole backbone - data keeping, metadata, recommendations, bandwidth, etc., it is only up to you how you want the front end to look. The whole code is open source, so you can change it or fork it if it suits your needs.

Publishing houses, media oriented webs

Low costs, No need for data management, infrastructure, transparent, low bandwidth requirements.
As an online publishing company you can use DECENT as your PaaS (Platform as a Service) infrastructure solution. Your content

storage, distribution and payments are taken care of by our platform. Thanks to utilizing public ledger, it is all completely transparent. All you need to do is to program your own app or web interface.

Data center providers

Low costs, high transparency, PaaI.
DECENT used as PaaI (Platform as a Infrastructure) can completely replace the data center you need to run for yourself or your customers. This solution is transparent, decentralized, all files are encrypted, stored at more locations and can be made available freely or for a fee.

7. DECENT: Technical description

DECENT is an autonomous Type I Decentralized Application (Dapp)[22] enabling digital content publishing. It has its own independent blockchain[23], which is a public distributed ledger of all the transactions that will occur since the genesis block[24] (beginning of the use of DECENT protocol).

DECENT has 3 functional roles:

- *Authors*: content makers, writers, music producers, etc
- *Content Consumers*: readers, listeners, viewers
- *Publishers*: miners

[22] https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md#classification-of-dapps
[23] https://en.wikipedia.org/wiki/Block_chain_%28database%29
[24] https://en.bitcoin.it/wiki/Genesis_block

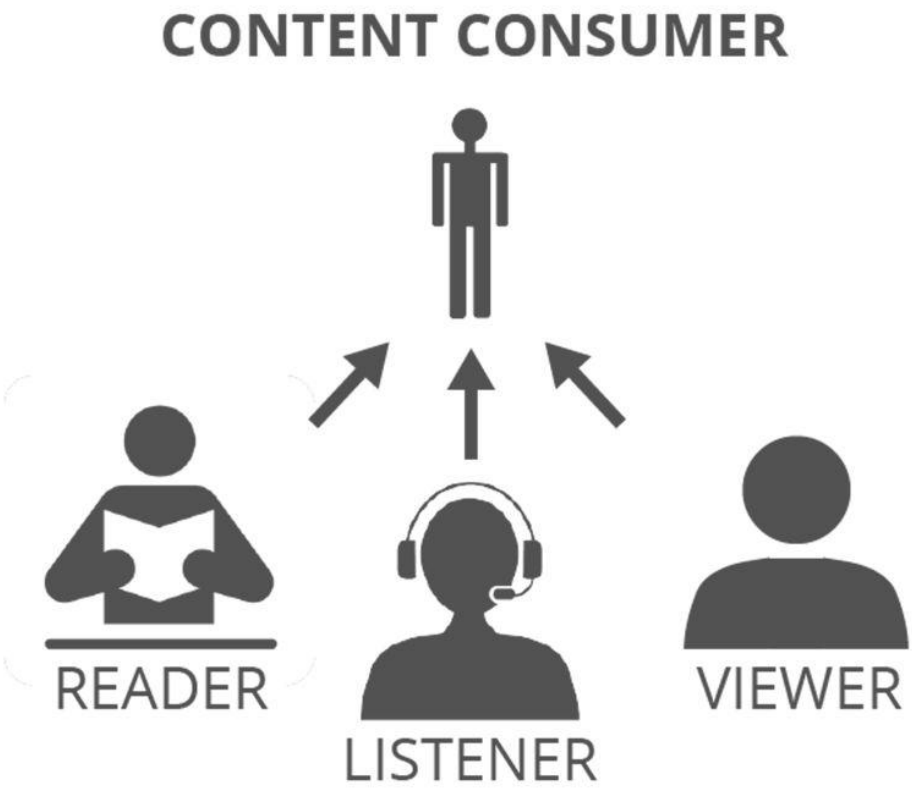

Figure 7.1: Content Consumer Types

One can see illustrated on Figure 7.1 the type of *Content Consumer*. *Content Consumers* are a generalization of Readers, Listeners and Viewers.

Authors produce content and upload it to the network. *Publishers* are the key element in keeping DECENT network up and running. The incentive for their time and resources are DCT digital tokens, similar to BTC sent to Bitcoin miners.

DECENT uses a modified Proof of Stake (POS)[25] mechanism in order to achieve consensus of various nodes in the network. This is based on the stake of space/time ratio provided by publishers ("miners") and their CPU time spent by distributing keys.

[25] https://en.bitcoin.it/wiki/Proof_of_Stake

Use cases

Think about the way media works nowadays. *Authors* have to go through publicists, recording studios or governments who determine whether the content can be, should be or is good enough to be released. As an app builder one can see there are too many restrictions.

DECENT offers to app developers a safe and secure way for their apps' users to share the content freely. Not only will it provide direct reader - author payment system through blockchain and data distribution. It also includes the recommendations that secure the quality and popularity of the content.

The typical use case of DECENT can be publishing of articles and stories, similar to Medium[26]. The *author* uses the application to write and organize articles or add media files. When the *author* is happy with the result, he or she presses the "Publish" button. Later the *author* can specify the price for the content, select a part of the article that will be free to read and add metadata. The application will encrypt the content, find the *publishers* (independent computers connected to DECENT network running publishing software to keep the network running and receive a reward for doing so), calculate the publishing fee and after confirmation, it will instruct *publishers*' computers to download the content and broadcast relevant metadata over blockchain.

Once *content consumers* find the content of their interest, they may be notified that their favourite *author* has published a new article, they will get recommendation based on their preferences or they will simply browse newly published content. They can choose to download and read the "free to read" part. And then they can decide to buy the rest of the article by paying a small fee specified by the *author*. DECENT protocol processes the payment that will be attributed to the *author* and the *content consumer*'s application will get the decryption keys for the rest of the article.

Over time, the *publishers* will be rewarded for storing the content and will get their fair share of publishing fee the *author* has paid.

[26] https://medium.com/

Everyone is welcome to build applications or clients on the top of DECENT protocol with their independent business models. This will enable the *authors* to share their content. It can be any kind of digital content: video or audio files, texts (books, articles, news) or pictures. And it actually offers all sorts of possibilities and opportunities, for example:

- Medium[27] like blogging and publishing
- Soundcloud[28] like music publishing
- Amazon[29] like e-book publishing
- Software publishing
- Shutterstock[30] like photo sharing
- Electronic newspaper publishing
- Costless academic paper publishing

[27] https://medium.com/
[28] https://soundcloud.com/
[29] http://www.amazon.com/
[30] http://www.shutterstock.com

Detailed procedures

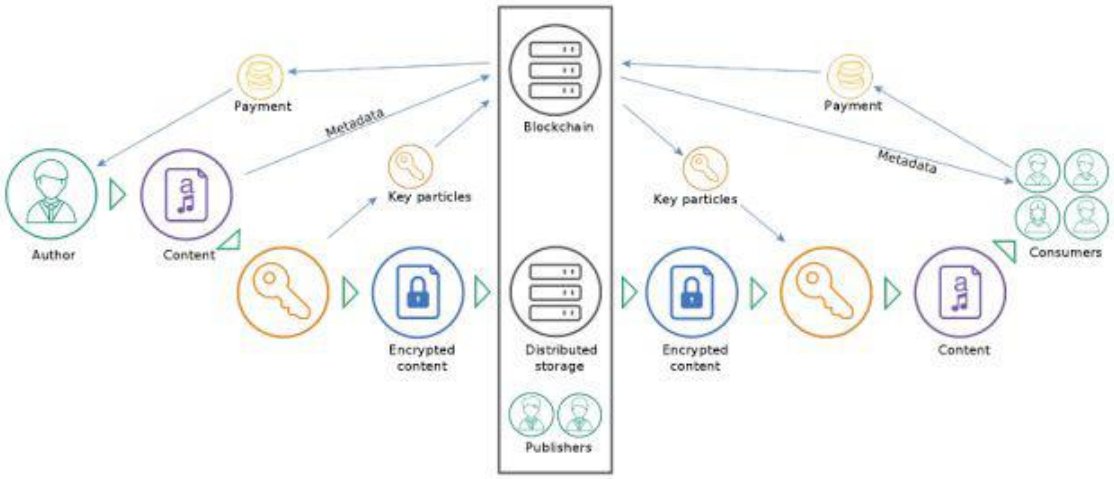

Figure 7.1: DECENT Flow Diagram

Most of the actions in DECENT are performed by adding a transaction to the blockchain. While logical chain of events continues to grow, every network node verifies it and contributes in the voting mechanism.

Publishing

Publishing is a process when the new content is stored in the network and information about it is spread among the community. The detailed process is as follows:

1. An *author* creates content in the form of computer files and selects two integers n and m such that $n>m>2$.

2. The *author*'s application generates unique AES[31] key and encrypts a part of the content that is not "free to read".
3. The *author*'s application selects distribution protocol - currently bittorrent[32] with distributed tracker[33] is the only supported protocol - but more are on a roadmap - and creates a distribution package containing a free to read and encrypted content.
4. The *author*'s application splits the encryption key into *n* shares so that *m* shares are required to retrieve the key[34].
5. The *author*'s application finds *n* suitable *publishers*. One of the possibilities is to utilize DHT Kademlia[35] network and crawl the network for nodes that are ready to store content of a given size while minimizing the distance between the torrent info hash[36] and node IDs.
6. The *author*'s application encrypts the *n* encryption key parts created in step 4 with public keys of the *n publishers* assigning one share to a single *publisher*.
7. The *author*'s application instructs *publishers*' nodes to download the content at the same time.
8. The *author*'s application generates the content submit transaction. The transaction will contain all content's metadata, such as title, synopsis or tags, and network relevant data such as validity, price, list of *publishers*, and list of shares encrypted for each selected *publisher*.
9. The publishing fee is deducted from the *author*'s account. It depends on the size and time the file should be available. This fee is used to pay *publishers* for providing storage and bandwidth. It also acts as anti-spam prevention. Publishing large amount of content will soon become expensive.
10. *Publishers* will download the content and issue the proof-of-retrievability[37] transaction to confirm the content has been successfully published.

Example

[31] FIPS Publication 197: "Announcing the Advanced Encryption Standard". Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[32] http://www.bittorrent.org/
[33] http://www.bittorrent.org/beps/bep_0005.html
[34] Shamir, A.: "How to share a secret". Communications of the ACM, November 1979, Volume 22, Number 11
[35] Maymounkov, P. and Mazières, D.: "Kademlia: A Peer-to-peer information system based on the XOR Metric"
[36] http://www.bittorrent.org/beps/bep_0003.html
[37] Shacham, H. and Waters, B.: "Compact Proofs of Retrievability". Retrieved from https://cseweb.ucsd.edu/~hovav/dist/verstore.pdf

Buying is the process when a *content consumer* decides to buy some published content. It has form of a contract, starting

Buying

Buying is the process when a *content consumer* decides to buy some published content. It has form of a contract, starting with promise-to-pay and finishing with payment from the *content consumer* to the *author* when the *publisher* was provably delivered the content. The detailed procedure is as follows:

1. The *content consumer* selects content they wish to buy and their application downloads the distribution package using the chosen protocol, i.e. forming the magnet link using the info hash and downloading by means of bittorrent with a distributed tracker.
2. The *content consumer*'s application generates request-to-buy transaction. This transaction will effectively block the required amount of tokens from their account.
3. The *publishers*' nodes see the request-to-buy in the blockchain. They will decrypt the respective share (from the content_submit transaction) with their private key and encrypt it again with *content consumer*'s public key.
4. The *publishers*' nodes will generate delivery keys transaction containing the share encrypted with *consumer*'s key and proof-of-delivery.
5. When there are enough shares delivered through the Blockchain:
    a. The *publisher* will pay to the author from the reserved amount and assign a part of the newly generated tokens to the *publishers* for providing the keys; and
    b. The *content consumer* will decrypt the shares with their private key, reconstruct the decryption key and decrypt the content.
6. Finally, the *content consumer* can rate the content by submitting rating transaction into the Blockchain. These transactions can be collected by different rating and classification engines and used to generate various recommendations for the *content consumers*.

Mining

When a *publisher* generates the block using PoS, he or she will:

1. Verify all transactions, including proof-of-retrievability and proof-of-delivery.
2. Distribute payments to the author (see buying process).
3. Distribute payments from the publishing fee to the *publishers* based on the stored content (proof-of-retrievablity).
4. Distribute payments from the newly generated tokens to the *publishers* based on the delivered keys (see buying process).
5. Keep a part of the distributed tokens for themselves.

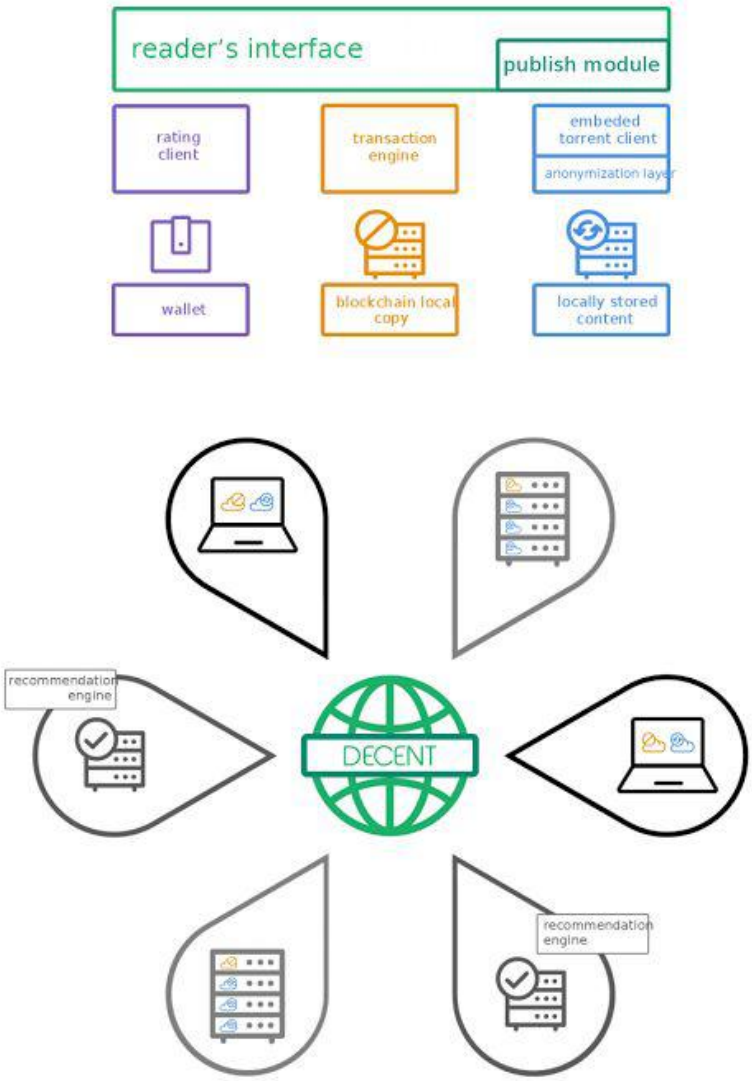

Figure 7.3: DECENT App Diagram

Figure 7.3 illustrates holistic view of DECENT network. *Content consumers* have access to rating client, transaction engine, embedded torrent client with an anonymization layer, own wallet, local copy of Blockchain and locally stored content.

8. Next Steps

DECENT is a non-profit project supported by DECENT Foundation, which will never have financial benefits from DECENT platform. Its main roles will be the issuance of digital tokens, holding of developer tokens, management of bounty payments and determining the DECENT direction. Future development of DECENT Protocol will be covered via the pre-sale in Q3 2016. More details about the pre-sale and updates of this white paper will be published soon.

For more information, please visit http://decent.ch or http://sale.decent.ch.

9. Conclusion

One can see that the market of Digital Content Distribution is dominated by oligopolies worldwide. Centralized Digital Content Distribution Platform take unnecessary fees from authors and/or content consumers and have the ultimate right to manipulate (or refuse to publish) the created by authors, according to their Terms of Use.
DECENT offers a Blockchain based open source decentralized solution to this problem, free to use for everyone.