# Rockchain

## *Decentralized audited data networks*

## White Paper Release Candidate 2.5

Sébastien Jehan

(sebastien.jehan@rockchain.org)

January 20, 2018

# Abstract

Rockchain provides a decentralized shared discoverable file system, such as bittorrent, where all access rights are managed in the public blockchain.

With no central authority to orchestrate users accesses, the dAppBox network (http://www.dappbox.io) also provides the notarization proofs of file transfers.

In this distributed P2P network, we enable node to node computation respecting data privacy and providing computation integrity. Written in Javascript, our private computation engine generates scripts that run simultaneously on the private data node and on the caller node.

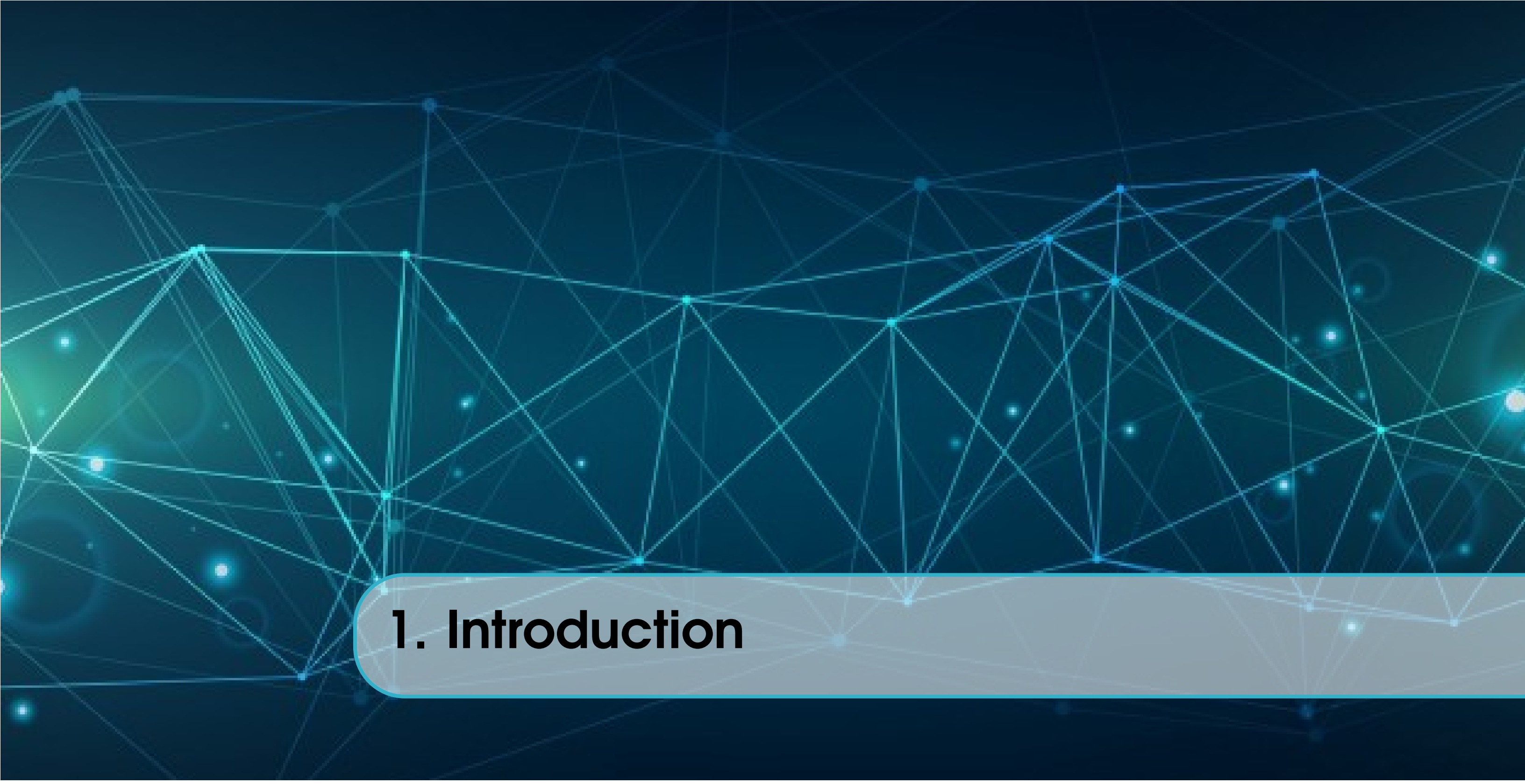
Initially based on the Ethereum blockchain, the Rockchain infrastructure is now opening to several public blockchains. We recommand Cosmos network as the default public blockchain because it enables fast synchronization between dAppBoxes nodes.

The dAppBox P2P network allow file sharing in read or write mode, but also the execution of selected scripts logic, thus allowing peer to peer private computation.

The dAppBox network is a blockchain agnostic peer to peer data transfer network. It is optimized for data updates transfer and distributed public file metadata storage and retrieval.

**Keywords:** *Distributed file system, distributed metadata management, distributed access rights management*

# Contents



# 1. Introduction

## 1.1 What is Rockchain

Rockchain is building a distributed file system with decentralized access rights management and audited events.

## 1.2 Context and scope

New blockchain initiatives (Ethereum [1], Cosmos Network [2], Lisk [4] are enabling distributed consensus for program states, i.e. "smart contracts".

Public blockchain can now be used as an orchestration tool for managing access rights to resources, thus replacing highly centralized systems such as LDAP, Active Directory, etc.

Such distributed infrastructures remove the need of a central authority to allow or deny users accesses: rights are simply delegated to every nodes in the system.

In such a distributed data network, all data remains privately managed, and are open only to selected peers.

Such an infrastructure allow file access in read or write mode, but also the execution of selected scripts that preserve the privacy of the data provider dAppBox node.

# 2. The business context

## 2.1 Truly decentralized collaboration

Companies consortiums are difficult to set up if a global centralized governance system needs to be elected. Having centralized access rights truly give a competitive advantage to one of the consortium player, an often unacceptable status for others.

Besides, not all of the data should be shared among members. Sometimes collaboration only means the ability to define dynamic and fast links for data sharing, relying on a truly autonomous and decentralized platform rather than a human administrative task force.

In such dynamic collaboration contexts, have the ability to remotely perform computation on private data make some sense before requesting access or for auditing / regulatory purposes.

## 2.2 GDPR

New regulation for user data privacy protection in Europe (GDPR – General Data Protection Regulation 2016/679) intend to track any file exchange related to users data. In such a context, audited data transfers between nodes provided by dAppBox network is a required feature.

For big companies, the only way to be cost effective for tracking sensitive data file transfers is to adopt a distributed file system that can natively handle proof notarization. The alternative is to code some proof generation systems for any legacy applications, with duplicated storage costs on many systems.

## 2.3 The dAppBox usages

The dAppBox network can be used for:

- A truly decentralized data exchange framework for companies consortium

- Blockchain solutions that want to orchestrate data exchange using smart contract logic. Example: create a document workflow in a distributed network of independent actors, inside the blockchain.
- Decentralized applications with integrated document notarization and proof needs
- Centralized web applications that need to delegate users data ownership to the user (own your own data)
- Consolidate global metrics from distributed private data sources (producers price)

Centralized social applications (social networks, forums, or slack-like applications) might need to keep their centralized web application hosting while not requiring critical data to be stored on their platforms. They could also choose to decentralize access rights management to the users, in effect improving the ability for the platform user to fine-tune their content access right management.

This hybrid hosting mode, which is neither a DAPP (decentralized APP) nor a centralized web application that controls all of the user data files and content, is a path yet to be explored, on which Rockchain is well positioned. (You can check our first implementation trial on https://www.dappbox.io/apps.html).

## 2.4 The competition

We have seen Enigma Catalyst platform [7] successfully raised $45,000,000 through their ICO (https://sangus.org/ico/540). Since they raised 150% their ICO max cap 5 days before the end of the ICO (https://steemit.com/enigma/@yonatangov/enigma-catalyst-raises-their-max-cap-in-150-5-days-before-the-ico), we have a negative hedge towards their governance. This should not even have been possible in their smart contract. Beside, they focus on the Enigma Catalyst trading platform, a project revamping the open source Zipline trading platform (https://github.com/quantopian/zipline) and adapting it to crypto assets (https://enigmampc.github.io/catalyst/). This confirm for us the governance issue and the lack of focus on privacy matters.

Another project is keep.network (http://keep.network). Their technology is ambitious and is based on secret sharing techniques. Rockchain privacy engine rely on 2 part multiparty computation and has taken the less ambitious path of one private node requiring to perform computation on private data on another. Our "privacy-engine" is already coded for the "honest but curious case" (the case where the external node does not cheat on the algorithm but still try to get the private data by any mean). We are now looking at resolving the case where some node will look at altering the protocol, with well identified papers on the subject.

Factom [8] wants to become the TCP/IP of proofs and his basing the proof notarization on bitcoin, which is more expensive as a proof storage system than Ethereum.

## 2.5 Initial ICO attempt

Rockchain launched an initial ICO on 1st november 2017 on the premises of distributed machine learning on private datasets. This was requiring consequent invesments to optimize such a network, which premises lie on seminal research papers on deep learning techniques on private datasets, where we believe our chosen privacy preserving computation framework (based on Yao's Garbled Circuit protocol) makes sense [3].

Since our ICO received very few attention from the community (we were solely based on the Ethereum blockchain at that time), we stripped out all the long term ambitions to focus on what we already had in house, i.e. a working protocol for 2 nodes computation preserving data privacy, and an the peer to peer file exchange client, optimized for updates transfers, with its modules for managing access rights on public blockchain. Adapting only those two frameworks to current blockchain opportunities led to the current Release Candidate 2.5 white paper version.

## 2.6 The pricing

The dAppBox infrastructure is currently available using monthly subscription fees. Whereas the dAppBox client is free, the subscribed services provided by the public infrastructure nodes are:

- Storing metadata on public network nodes
- Cheap notarization services, for data transfer proofs and document notarization proofs.

# 3. The technology

## 3.1 Overview

The dAppBox network is a peer to peer network implementing https://www.cloudwards.net/block-level-file-copying/ block level file copying. It is perfect for collaboration on large files, as only the difference is synchronized between nodes.

With this block level copying technology, the dAppBox network is able to broadcast live data streams on the network, for example for datalakes.

The access rights between dAppBoxes are managed using the public blockchain network. At this stage, the most relevant blockchain for our use case was the Cosmos Network with its ABCI interface and it protobuf data transfers. However, the dAppBox have modules for other blockchain, and we also have an Ethereum module which is fast to update but quite slow to synchronize the state of distributed access rights because of a https://github.com/ethereum/go-ethereum/issues/15091known issue in the framework, which has not been yet closed but merged in a https://github.com/ethereum/go-ethereum/pull/14631 master issue. We are looking forward for Ethereum team to resolve this major architectural issue for extra-layers wanting to do something with their consensus engine. However, the Ethereum module is ready for the dAppBox.

Whereas private dAppBox nodes root their data content without any need for public infrastructure nodes services, they can also publish metadata about their content and notarize both their content and the proof of transfers. Due to the high cost of storage of public blockchain, a network of public dAppBox nodes maintain a distributed public storage system to host metadata for a cheap price, and keep notarization proofs that they also aggregate and store on the blockchain to maintain a secondary proof of transfers. With that mechanism, nodes can proof their content and data transfers on several public blockchains at a fraction of the cost.

Private dAppBox nodes can perform privacy preserving computation in a peer to peer way, and notarize the computation script and computation results without breaching privacy on the public dAppBox nodes network.

The public dAppBox nodes provide cheap and persistant storage for both public metadata and notarization proofs.

## 3.2 The dAppBox access rights system

The dAppBox maintain document level access rights, as well as folder level access rights. The following rights are maintained:

Read access right: the remote dAppBox receives a fresh copy each time the data owner modified the content.

Write access right: the remote dAppBox can modify the content of the file. The authoring dAppBox emit an authoring proof of the file as a separate document, including the timestamp, the signature of the modified document by the author.

The dAppBox maintains group level permissions on folders, with 2 types of groups:

The N-N group: all members share the same view of a specific folder. In the N-N read group, all dAppBox can only edit its own file and all others have a read view on the files. In a N-N write group, everyone can edit any file.

The 1-N group: one node has all views on other dAppBox. In the 1-N read group, a unique node can view in read mode all other nodes contributions. In the 1-N write mode, a unique node has the ability to update all other nodes documents.

## 3.3 About notarization and public distributed file storage

IPFS [5] is a decentralized file system that uses DHT (Distributed Hashtable) and Merkle DAG (Directly Acyclic Graph) data structures. It uses a protocol similar to bittorrent to decide how to move data around the network. Although calling itself a decentralized file system, it doesn't adhere to the number one required property for a file system: the guarantee for a file to be here unless deleted.

While nodes in IPFS only store files they need, FileCoin incentivize nodes with an internal cryptocurrency to store files. This increase the probability for files not to disappear from the network, without yet any proven guarantee however.

NameCoin [6] a decentralized key-value database using the blockchain datastructure and proof-of-work consensus database.

We believe the blockchain infrastructure is not the optimal distributed datastructure to store readonly content. Indeed, there isn't any "double spend" attack on such a distributed system, making the chain of block inadequate and expensive as a data structure. Besides, a requirement in this system is the absolute certitude to permanently store the data, and that's the only property of the blockchain infrastructures to be kept. Thus IPFS is not relevant for such persistence scheme.

In Rockchain, we design a distributed public datanodes network for permanent readonly storage (inserted one time and not updatable, such as in a blockchain) optimized for cheap storage costs, thus allowing "big data" applications to connect to the system. The use cases for such a storage system is to allow cheap notarization proofs (which is the number two use case of blockchain applications after payment) and reliant public medata storage for dAppBox nodes.

For that, we use an optimized routing protocol (Spanning Tree [9]) optimized to take into account bandwidth between public datanodes. The computation of the optimal tree is done using the blockchain consensus engine, which differs a lot from usual routing protocols computing the optimal routing network in a distributed way, and removing a lot of the complexity. The nodes routing configuration is stored on the blockchain.

Going back to the fundamentals of the internet (routing protocols, defined by Radia Pertnam in 1985). Ironically, Radia Perlman, inventor of the routing protocol making the internet possible, is sceptical about the `https://blog.apnic.net/2017/12/14/dont-get-caught-blockchain-hype/`"black box magic" approach of many blockchain projects, and think the blockchain infrastructure can't answer all distributed use cases.

We do not use the minimum Spanning Tree algorithm, but an algorithm allowing an acceptable level of fault tolerance among public nodes. On the first version of the public network, all nodes will store the same data. Nodes are incentivized using their bandwidth capability measured by at least 2 concurrent nodes and a proof of storage where their signature and the hash of the global stored content is involved.

The timestamping of proofs is guaranteed by the storing the whole database content hash on the public blockchain periodically, along with the update of local routing tables by nodes to maintain a coherent global routing tree. As the data is read only and insert only for updates, it is easy to reconstruct any local file proof using a node content and the blockchain database hash at a specific given time.

Whenever the database size doubles (the initial size is 50 GB, current Ethereum size), it is split in two and dispatched on two identical groups of nodes randomly selected. The rewards at this stage is also split in two. This splitting strategy ensures the network size scalability and an incentive for new comers to join. To overcome disk usage planing costs it is still possible to run several identical public dappBox nodes on the same server, however at a penalty cost since it can easily be detected by the network. This splitting strategy prevent any concentration of storage and thus risk of public network monopoly. Since in our model, the reward is proportional to the bandwidth availability, storing two public dappBox on the same computer would in effect divide the reward by two, and also adds a small penalty fee.

## 3.4 Computation on private data

### 3.4.1 Case 1: node to node (2 parties) computation on private data

The true challenge of performing computation on private data is providing computation integrity by the private datanode, i.e. ensuring the computation has been done honestly.

We achieve it using a compiler that takes Javascript as an input script and compile an output circuit. The execution is done on 2 nodes, the private and the public node, and requires the deployment of a

"RockEngine agent" on the private node (the node containing the private data).

We released a first `https://www.rockchain.org/RockEngine_Benchmark_V3.pdf` encouraging benchmark about RockEngine performance compared to other open source framework implementing Yao's Garbled protocol on 26th october 2017 and improved the compilation time and execution time since.

The major benefit and chosing RockEngine is it's abstracting the complexity of the Yao's Garbled Circuit protocol, allowing developers to focus on writing algorithms that are natively running on two nodes simultaneously rather than a single node as we user to have in traditional virtual machines. The two nodes (the private data node and the public node looking for computation results) communicate in a completely secured, encrypted and obfuscated manner, while the algorithm is making progress in the computation. The private node cannot alter the running algorithm to fake the computation results, the only way to cheat is to provide fake data for algorithm (which is controlled by dAppBox content notarization services in case any litigation occured).

### 3.4.2 Case 2: Knowing if an item is in a list without breaching privacy

We use a specific encrypted version of bloom filters for this purpose.

### 3.4.3 Case 3: Aggregating a distributed set of private data items

Using dynamic routing between the dAppBox nodes computed by the consensus engine, we are able to perform a near real time aggregate public aggreagation (average, standard deviation, variance and weighted average) over a list of distributed private items.

# 4. The market

## 4.1 The need of truly decentralized networks permissioned and audited networks

Like the internet, file exchanges system between companies (using dropbox as an intermediary) needs openness in their access rights management, allowing new rules to be encoded and chosen by the community. That's how the public blockchain can help model new governance models inside data sharing networks.

## 4.2 The need for cheap document proof notarization

Although the documentation is very parse on this broad use case, storing an hash on the Ethereum blockchain (in the format of a solidity byte32 variable, not a string, it would cost at least twice more) is about 29,000 gas. The median Gas price today (18 January 2018, it's always evolving) is 34 GWEI. It went up 850% from 6 months ago in GWEI price, without much press about it.

We can add to this that the Ethereum price itself went up 440% from 6 months ago, it makes a combined hash storage price increase of 3700%. At today's price, the cost of an hash notarization in the Ethereum blockchain is 29,000*34 GWEI = $1 roughly.

This is highly impractical for one of the most common usage, proof storage on the blockchain. It cannot apply to high volume transactional applications needing regular proofs. To solve such an issue, we implement an infrastructure that can slash proof costs by a minimum factor of 10,000. Whereas the Solidity EVM is a very generic engine, our public storage will only have two purposes: to store proofs of documents and file transfers, and to store metadata associated to dappBox nodes content for later search. We address the market of proofs with a unique price proposal.

## 4.3 The need for hybrid dapps: centralized hosting with decentralized content and access rights management

The "DappRevolution" is probably difficult to achieve (facebook disruption etc) if we consider the difficulty of installing a dApp on a PC (this installing a light blockchain node locally) let alone one a mobile. Without decentralizing the whole webserver infrastructure, some Dapps with centralized web servers relying on public distributed content architecture might be a reasonable intermediary step.

## 4.4 The need of privacy computation in the public cloud

Cloud infrastructure services is the fastest growing market (42.8% in 2016) inside the already fast growing cloud services market (17.2% growth rate on average). The cloud services market is now estimated a $200 billion a year industry.

Serverless infrastructure has been popularized by AWS Lambda and implies running logic on the cloud on demand. It also implies putting all private data on the cloud. With Yao's Garbled Circuit protocol, it can be improved by allowing private data to be used on the public cloud and to release only computation results to serverless infrastructure (think of sensitive information such as genomics database, tax evasion database, HR internal salary database, private community conversation history, etc).

This emerging part of an emerging market (the serverless infrastructure market) in the booming cloud industry represents already several millions USD.

# 5. Team

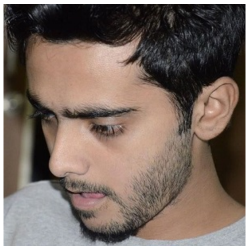
## 5.1 Core team

The core team is or will be fully dedicated to the project.

### Sébastien Jehan – CEO, Rockchain Inventor

Sébastien is a veteran software architect with .NET, Java, GoLang and R experience. He studied Telecommunications, cryptography, internet networks as an engineer, econometrics and finance regulation as a Finance MSc, which naturally led him to be interested in blockchain in 2015 where he started his first venture on the subject. 2 years later, Sébastien built Rockchain to answer major unanswered challenges about data privacy and data storages costs in the blockchain.

### Aayush Anand - Technical project coordinator and cloud architect



Aayush has worked with different startups and companies, helping them realize their IT and cloud automation potential. He is a graduate in information technology. He is currently working in maintaining and creating cloud infrastructure for Rockchain and helping assessing technical tasks dependencies as a coordinator.

### Régis Gourdel - GO & Cryptop developer

Régis has a strong theoretical background in cryptography and is a GO developer. Régis is a graduate from Telecom ParisTech (applied mathematics on cryptography and quantum computing), and is doing an MsC in applicable mathematics in London School of Economics (game theory, advanced algorithms and financial maths).

### Miguel Velasco - GO developer

Miguel is a programmer and a telecommunication engineer. He is a graduate from the University of Carabobo. Experienced developer in Ruby, Python, Javascript, Golang. He is currently developing Golang software and frontend for Rockchain.

## 5.2 Advisors

### Sébastien Collignon - Rockchain Enterprise Alliance roadmap

Sébastien is a business leader with a strong ability to build partnerships between technology providers. He managed several worldwide partnerships for Cisco in the IoT field.

Sébastien is an active contributor and advisor on the Rockchain project.

### Pierre Bittner - Banking Business Model Decentralization Roadmap

Now working as strategist and advisor to banks looking to take their Data Culture to the next level. Pierre is an executive manager with strong focus on leadership, building and guiding elite teams, business and technology transformation, change management and innovation through the latest technologies.

### Laurent Grangeau - Rockchain Cloud Appliances

Laurent Grangeau is a cloud solution architect. He is helping on the automation of dAppBox networks deployment in public clouds.

### Elie Cezard - Asset management industry

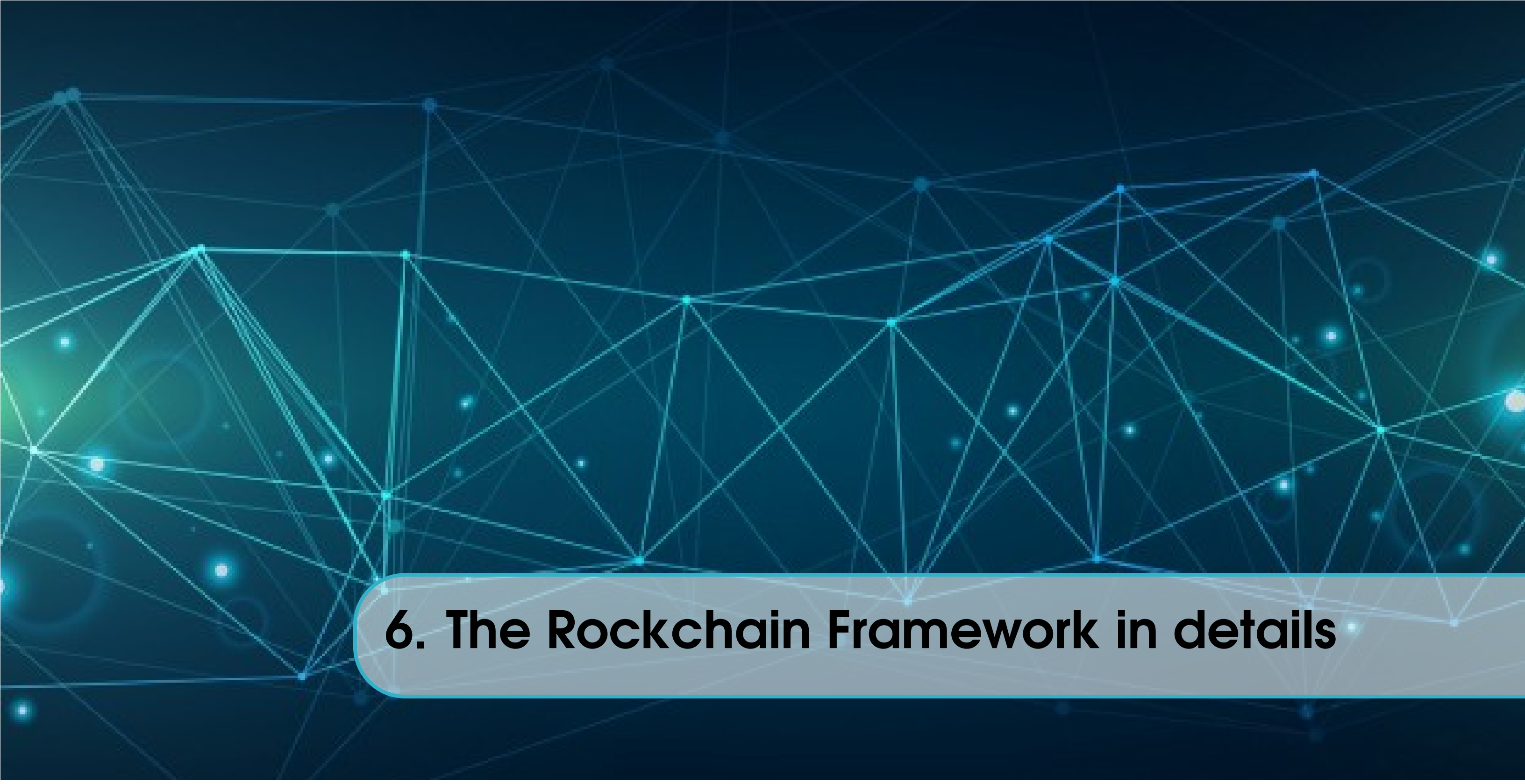
Elie is a business leader in the asset management industry and organizer of the Paris Blockchain Meetup. He is advising on the business opportunities to disrupt traditional approaches in the financial markets.

### Jeff Guilbault- Digital content strategic advisor

Jeff is an expert in digital assets trading platforms. He was driving the European operations of Corbis (Bill gates digital content distribution company), was a senior manager at Getty Images, and is now a director of Taboola, the leading platform for content discovery and recommendation. Jeff is helping us implementing a strategy on digital assets rights.

### Christophe Ozcan - Blockchain Ecosystem Advisor

Christophe is an experienced advisor and entrepreneur on Blockchain Ecosystem. He is an active participant of Blockchain community by promoting the technology through his interventions. CEO of Crypto4All a Blockchain consulting company and also an expert member of ISO/TC-307 committee for standardization of Blockchain and distributed ledger technologies. His interest in Blockchain technology began back in 2013 when he discovered Bitcoin and started to become a miner of cryptocurrencies with his own mining rig. Christophe is helping on the ICO project.



# 6. The Rockchain Framework in details

## 6.1 The distributed access rights system

The Rockchain maintains a specific distributed access rights sytem for defining the sharing strategy of each datafolder of each dAppBox (FactMapNode). This access rights system is similar to the UNIX file system permissions. [10].

We have three groups of users in the Rockchain access rights system:

- The local nodes group: only local nodes in the corporate network (discovery of those nodes and synchronization with those nodes use the UDP protocol, without support for internet communications).
- The peers nodes group: the peers node are connected through the internet and can belong to distinct corporate networks. However, they have been accredited by the current dAppBox to connect, through the global access rights management ethereum smart contract.
- The others group: this group contains all dAppBox connected on the Rockchain infrastructure.

The possible rights attributed to folders in groups are:

- READ: Other dAppBox can download the files you share on your folders, but they cannot update them.
- WRITE: Other dAppBox can download the files you share on your folders, and also update them. Updates on the files will be merged with all other dAppBox updates, including yours, using the modular merge pipeline.
- EXECUTE: Allow datascripts to be executed on the files included in the folder.

## 6.2 The public dappbox node incentivisation scheme

The dAppBox public nodes will be incentivized by 3 factors:

- The size of the database: It's agreed on using a node consensus. The nodes consensus is periodically defining the size of the whole database.
- The download rate history (cross validated by the reciprocal node upload rate)
- The upload rate history (cross validated by the reciprocal node upload rate)
- The bandwidth history

- The number of concurrent nodes on the same server: A penalty is applied if several nodes run on the same server, allowing optimal decentralization.

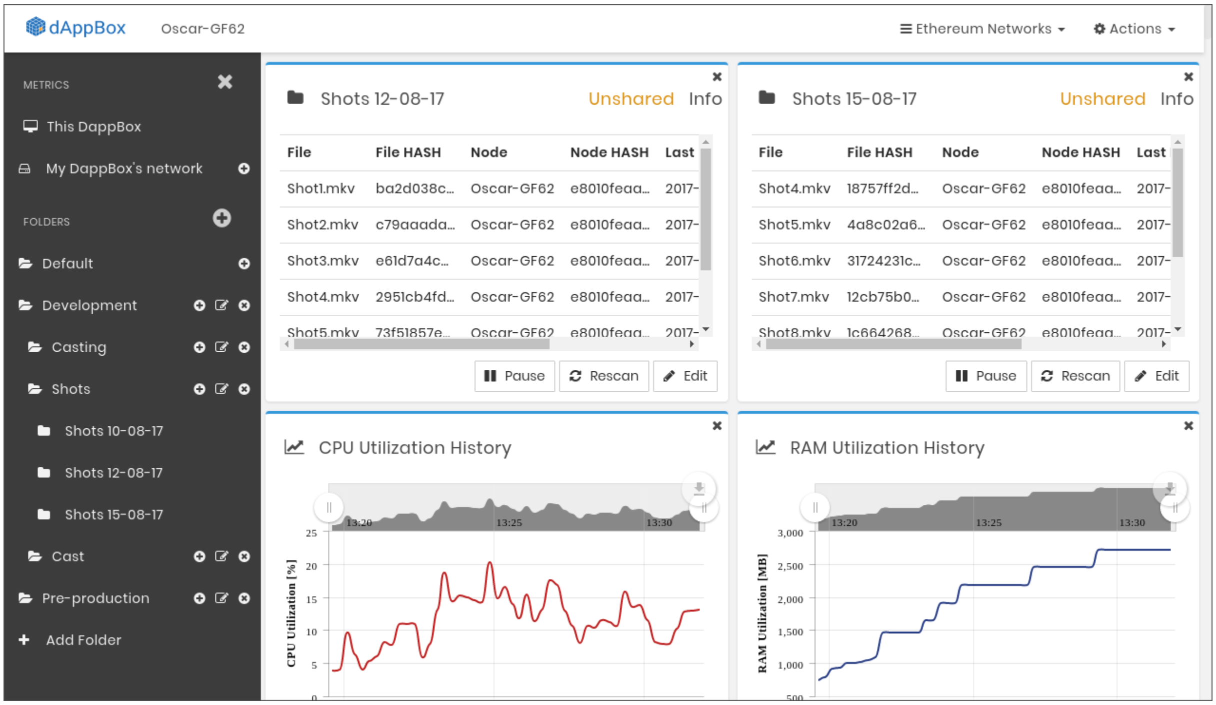
## 6.3 The dAppBox

The dAppBox is the core client of Rockchain infrastructure, both for public infrastructure usage and private node usage.

The dAppBox is optimized for updates, allowing the sharing of big time-based databases between nodes for live stream (producer / consumer pattern).

Any method of the dAppBox is APIfied, allowing DAPP or any local application to easily integrate with this file sharing client.

The dAppBox features descriptions are available at `http://www.dappbox.io`, while there is an old version demo video `https://www.youtube.com/watch?v=8LKE_y6GGsw`( october 2017 ).



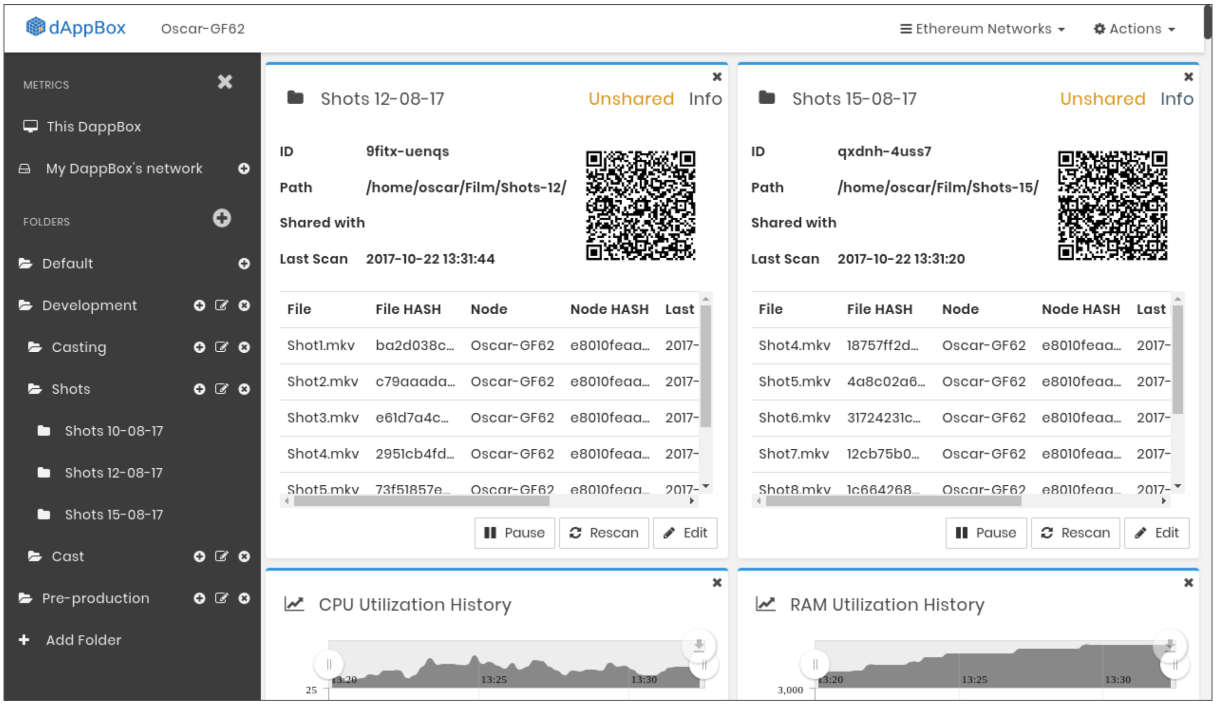
Shots 12-08-17

| File | File HASH | Node | Node HASH | Last |
|---|---|---|---|---|
| Shot1.mkv | ba2d038c... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot2.mkv | c79aaada... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot3.mkv | e61d7a4c... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot4.mkv | 2951cb4fd... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot5.mkv | 73f51857e... | Oscar-GF62 | e8010feaa... | 2017- |

Shots 15-08-17

| File | File HASH | Node | Node HASH | Last |
|---|---|---|---|---|
| Shot4.mkv | 18757ff2d... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot5.mkv | 4a8c02a6... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot6.mkv | 31724231c... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot7.mkv | 12cb75b0... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot8.mkv | 1c664268... | Oscar-GF62 | e8010feaa... | 2017- |

Figure 6.1: Shared folders overview in a dAppBox



Shots 12-08-17

ID 9fitx-uenqs
Path /home/oscar/Film/Shots-12/
Shared with
Last Scan 2017-10-22 13:31:44

| File | File HASH | Node | Node HASH | Last |
|---|---|---|---|---|
| Shot1.mkv | ba2d038c... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot2.mkv | c79aaada... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot3.mkv | e61d7a4c... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot4.mkv | 2951cb4fd... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot5.mkv | 73f51857e... | Oscar-GF62 | e8010feaa... | 2017- |

Shots 15-08-17

ID qxdnh-4uss7
Path /home/oscar/Film/Shots-15/
Shared with
Last Scan 2017-10-22 13:31:20

| File | File HASH | Node | Node HASH | Last |
|---|---|---|---|---|
| Shot4.mkv | 18757ff2d... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot5.mkv | 4a8c02a6... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot6.mkv | 31724231c... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot7.mkv | 12cb75b0... | Oscar-GF62 | e8010feaa... | 2017- |
| Shot8.mkv | 1c664268... | Oscar-GF62 | e8010feaa... | 2017- |

Figure 6.2: Every shared file or folder in a dAppBox network has a unique identity that can be shared (by email for example)

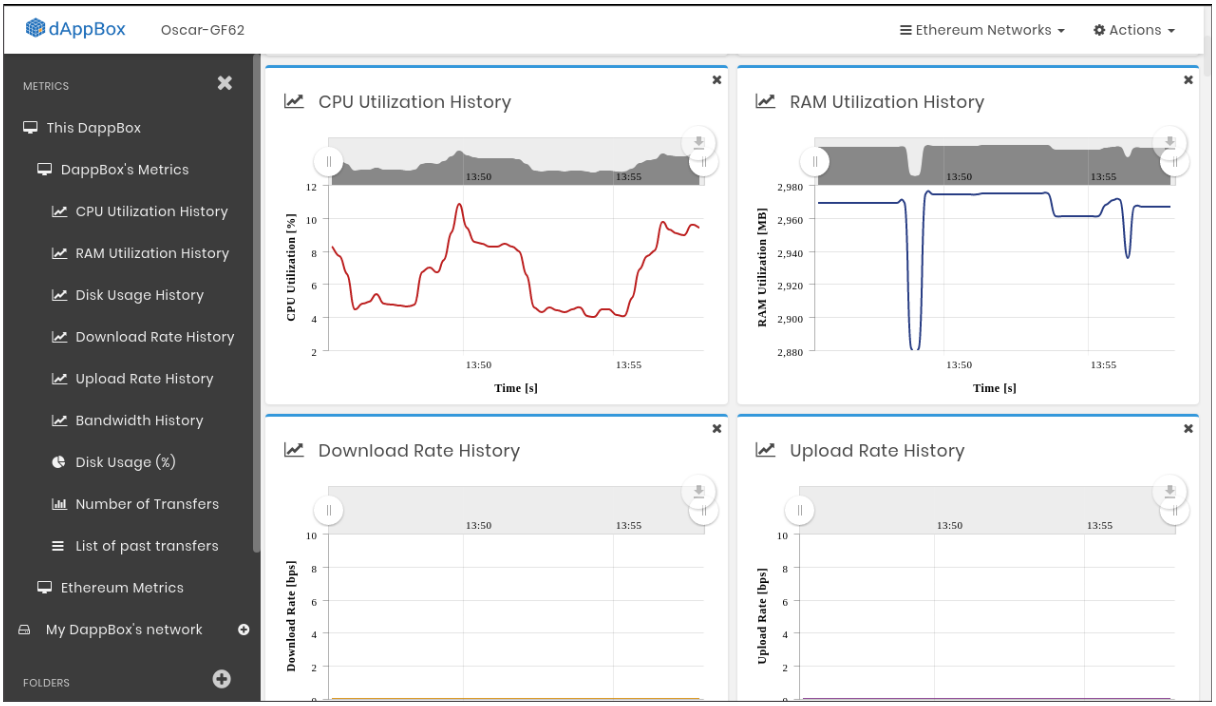


Figure 6.3: The dAppBox performance indicators. Some of the indicators (Bandwidth, download rate and upload rate) are used in the dAppBox incentivisation scheme

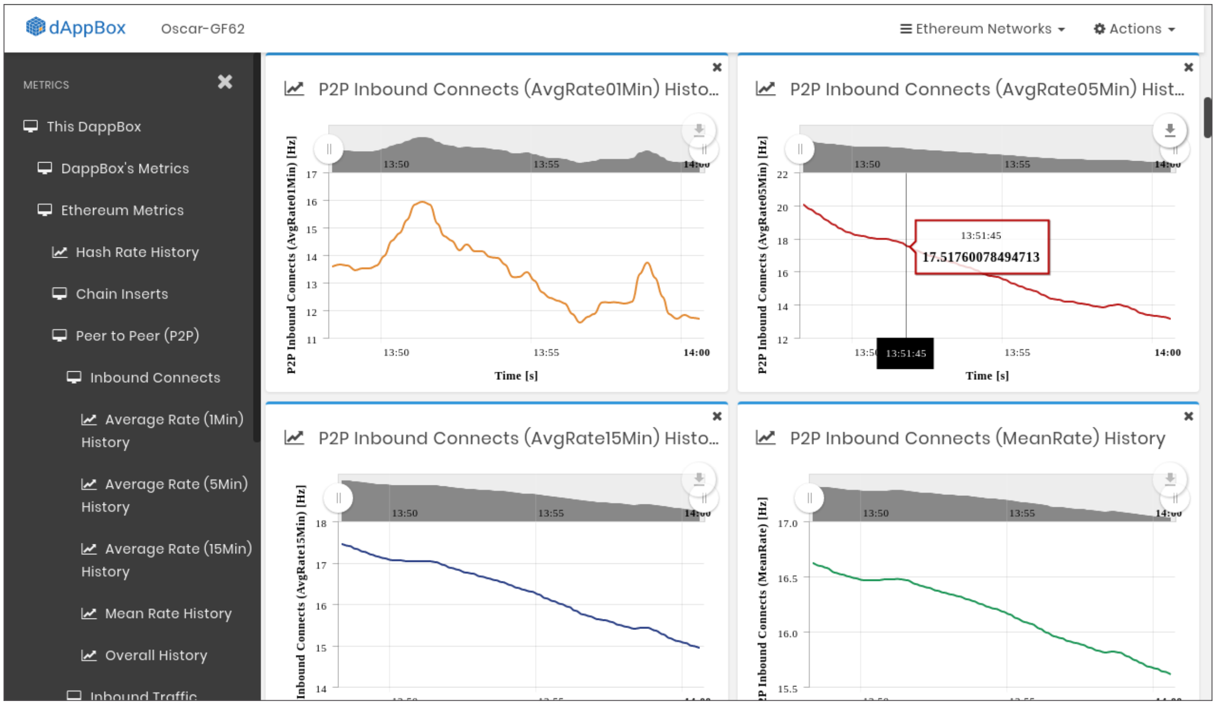
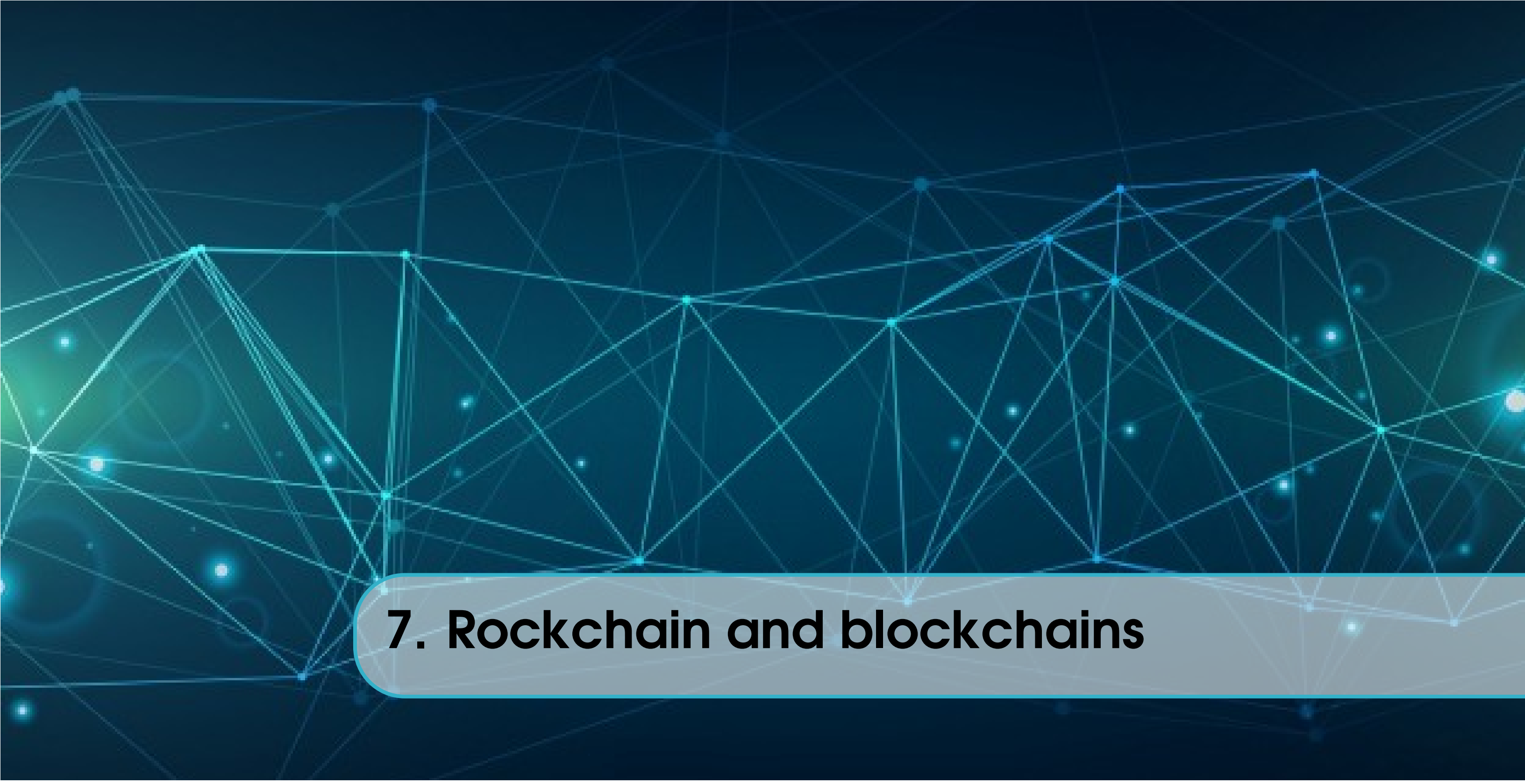

dAppBox
Oscar-GF62
Ethereum Networks
Actions
METRICS
This DappBox
DappBox's Metrics
Ethereum Metrics
Hash Rate History
Chain Inserts
Peer to Peer (P2P)
Inbound Connects
Average Rate (1Min) History
Average Rate (5Min) History
Average Rate (15Min) History
Mean Rate History
Overall History
Inbound Traffic
P2P Inbound Connects (AvgRate01Min) Histo...
P2P Inbound Connects (AvgRate01Min) [Hz]
17
16
15
14
13
12
11
13:50
13:55
14:00
Time [s]
P2P Inbound Connects (AvgRate05Min) Hist...
P2P Inbound Connects (AvgRate05Min) [Hz]
22
20
18
16
14
12
13:51:45
17.51760078494713
13:50
13:55
14:00
Time [s]
P2P Inbound Connects (AvgRate15Min) Histo...
Inbound Connects (AvgRate15Min) [Hz]
18
17
16
15
14
13:50
13:55
14:00
P2P Inbound Connects (MeanRate) History
P Inbound Connects (MeanRate) [Hz]
17.0
16.5
16.0
15.5
13:50
13:55
14:00

Figure 6.4: Measuring the activity of the dAppBox. Most of the activity is providing distributed search facilities



# 7. Rockchain and blockchains

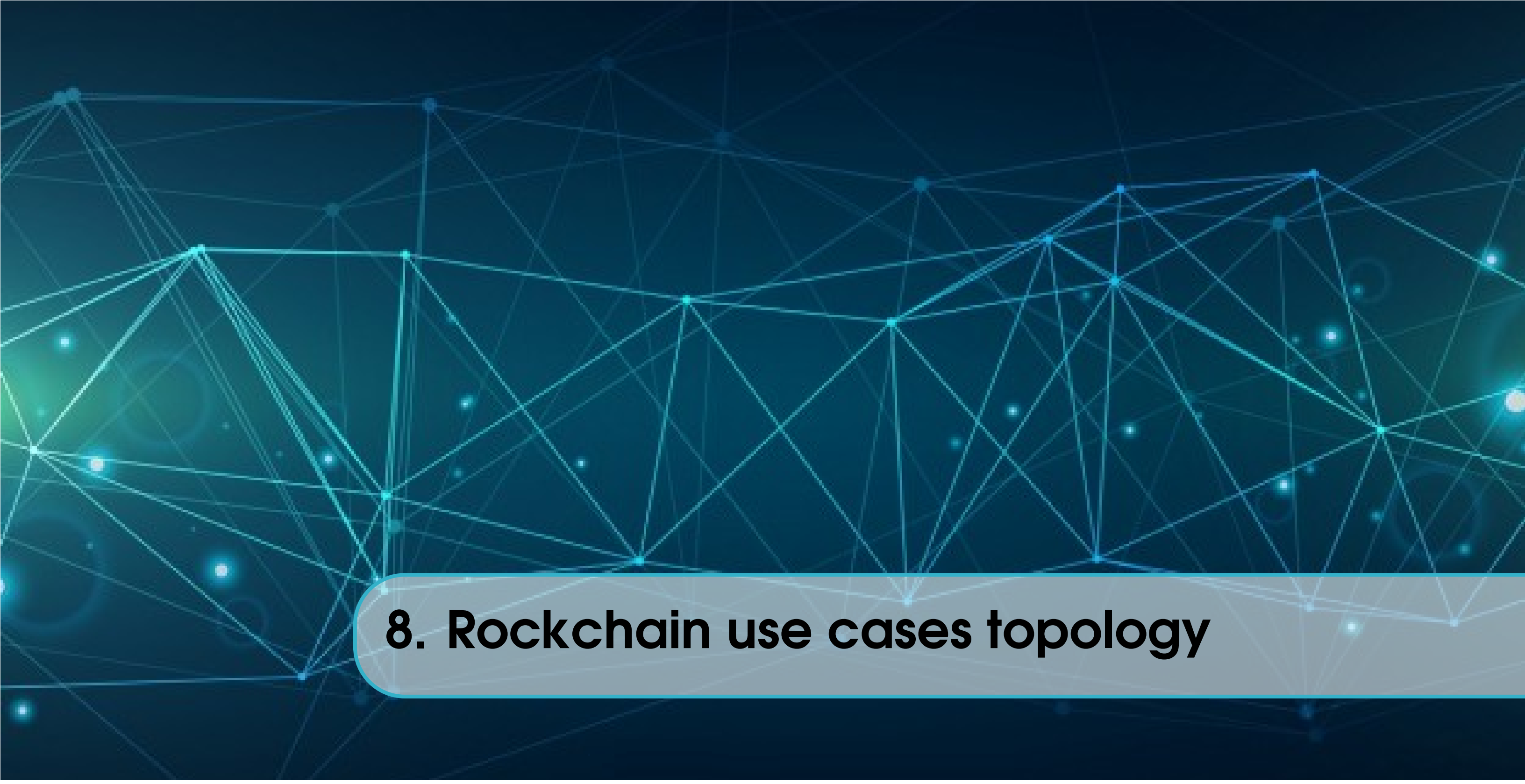
## 7.1 Blockchain connectivity modules

We provide open source public Blockchain connectivity modules, that offer transparency in the way document proofs are computed, and also how the blockchain consensus engine is called.

For now our preference go to Cosmos Network blockchain where we are investing our development efforts to finalize a version using the ABCI interface. It allows a fast scynrhonization between nodes for both the access rights distributed table, but also in the long term for the routing tables between the public dappBox nodes in rockchain public infrastructure.

We will always required a public blockchain to get a consensus engine about the states of distributed access rights and the states of the optimal routing tables for the distributed public permanent file system. We plan to

RelayDappBoxes are dappboxes that can advertise private networks content for other internal networks nodes to the dAppBox network. They serve as a proxy between private networks and public networks, such as internet proxy servers.



# 8. Rockchain use cases topology

The topology of links and access rights inside dAppBox networks helps categorizing the different business models addressed by the implementation of the dAppBox network.

## 8.1 Publish Subscribe business models: 1-N Read networks

One dAppBox is the certified proof of content delivery and broadcasts his files to subscribers networks.

## 8.2 Collaborative (anarchic) models: N-N Write Networks

Anyone collaborate on any file.

## 8.3 Survey models: 1-N Write Networks

Anyone can write a file but only one node sees the contribution. Can be used for survey participants to fill similar documents.

In all those scenarios, every file data transfer proofs is notarized in the dAppBox public network, and the author of the document also notarizes the first time he advertises it on the network (thus prooving he is the original author or publisher of the file).

# 9. The delivery roadmap

The first version of the dAppBox private network will be commercially deployed in Q1 2018. We're still waiting for Cosmos Network API to stabilize in order to deliver.

The public dAppBox data storage infrastructure is to be conceived during 2018, although it depends on our auto-financing capabilities.

# 10. The DAPB Tokens usage

## 10.1 The types of proofs

We first possible proof stored in the public dappbox network id a proof of document storage. It contains the following items:

- The dappBox protocol version - 1 byte
- The dappBox public blockchain key (notarizing the document) - 64 bytes
- The hash of the document (Keccak256 hash) - 32 bytes
- The timestamp (uint256) is 1 byte
- The reference merkle tree root hash that is keeping a proof on the blockchain - 32 bytes

The total proof size for a single document, file or document extract is 130bytes.

We second possible proof stored in the public dappbox network id a proof of document transfer between two dappboxes. It contains the following items:

- The dappBox protocol version - 1 byte
- The sending dappBox public blockchain key (sending the document) - 64 bytes
- The hash of the document (Keccak256 hash) 32 bytes
- The receiving dappBox public blockchain key (receiving the document) - 64 bytes
- The timestamp (uint256) is 1 byte
- The reference merkle tree root hash that is keeping a proof on the blockchain - 32 bytes

The total size of the proof for a document transfer is 162bytes.

## 10.2 The DAPP token and its usage

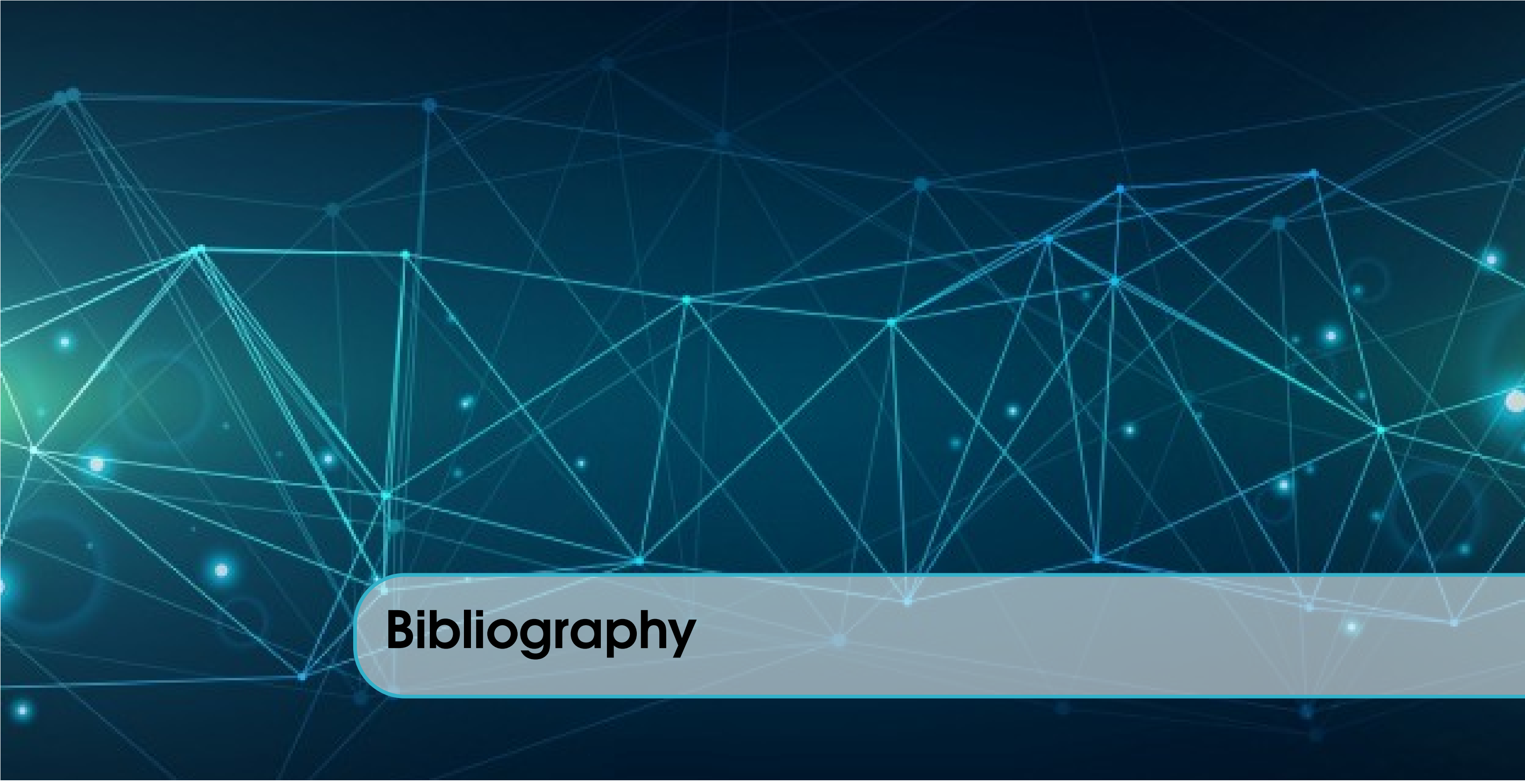
At the launch of the network, 1 DAPP token will give the ability to forever store 10,530 bytes (10.28KB) on the public dAppBox network. This is the equivalent of storing:

- 81 documents documents proof of existence
- 65 proofs of documents transfers between dappBoxes
- 10,53 KB of public metadata storage

The first global database split will occur at 5.1416015625 GB, i.e. 42,467,328 documents notarization proofs, or 66,530 transfers proofs. Once this database will have reached this stage, the reward will be split in two, so the public dappBoxes will be rewarded 1 DAPP for 162 proofs of storage hosting.

The next split will occur at 324 transfers proofs, and so on.

The fact that the DAPP can be traded on exchanges will help public dappBox nodes to smooth their rewards in time, thanks to market anticipation of the future split (it is sufficient to look at the public dappbox database growth rate to know when the split will approximatively occur and to arbitrage on that knowledge if the price is disconnected to storage costs expectations).



# Bibliography

[1] Ethereum White Paper https://github.com/ethereum/wiki/wiki/White-Paper

[2] Cosmos Network https://cosmos.network/about/whitepaper

[3] DeepSecure https://arxiv.org/abs/1705.08963

[4] Lisk https://docs.lisk.io/v1.4/docs/the-lisk-protocol

[5] IPFS https://ipfs.io/

[6] NameCoin https://namecoin.org/

[7] Enigma Catalyst https://www.enigma.co/

[8] Factom https://www.factom.com/

[9] Spanning Tree https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

[10] File system permissions in Unix https://en.wikipedia.org/wiki/File_system_permissions