Cloudchain

KickOff Document

Project Members

Abdullah Cem Önem - 2031821 | Sinan Erdil - 2098994 | Berk Yaşar - 2036333 | Ekin Dursun - 2098952

Description

Cloudchain is a remote file storage platform that operates in a decentralized network. Nodes in the network communicate in a peer-to-peer manner, and the consensus of the file metadata is formed without a single source of trust.

Cloudchain will provide an open source solution to the problem of utilizing the wasted space in a distributed system formed by personal desktop computers without a central control that violates the privacy of the users.

Groups formed of medium (a small company) to large (a public cloudchain) number of people are the target audience of the product.

Master feature list

MF – 1 : A file may be uploaded to the system, and the uploader may retrieve it without corruption at an arbitrary time.

MF – 2 : Metadata will be stored in the network in a persistent and secure manner, possibly by a blockchain.

MF – 3 : Uploaded files may be read by their corresponding uploaders and other authenticated entities.

MF – 4 : Uploaders may grant authentication to read files to other users and also make the files public to the network. Users without authentication for a particular file may not view it unencrypted.

MF – 5 : The file storage system will not have a single point of failure.

MF – 6 : Users will benefit from the system according to the resources they offer.

MF – 7 : System will provide options to the users in a way that they may store redundant copies of their files, for availability concerns and other reasons.

MF – 8 : The nodes in the network will communicate in a peer-to-peer manner.

MF – 9 : There will be no single source of trust that the nodes rely on for consensus. The network will be completely decentralized.

MF – 10 : Users may query for the files they are authenticated to read.

MF – 11 : The client application will have a Graphical User Interface.

MF – 12 : Users will be able to share files with end-to-end encryption.

Workpackages

The allocated times for the work packages can be seen in Table 1.

Table 1: List of the Work Packages

WP #	Term	WP Title	Estimated number of man-months
1	**491**	Project planning and architecture design	**3**
2	**491/2**	Development of the peer-to-peer file storage system	**6.5**
3	**491/2**	Development of the Consensus Blockchain	**6.5**
4	**491/2**	Integration of the Blockchain and P2P implementations	**3**
5	**492**	Handling of encryption and authentication Issues	**5**
6	**492**	Fair distribution of the system benefits	**4**
7	**492**	GUI development	**2**
B1	**492**	Deployment to mobile platforms	**-**
B2	**492**	Initialization of a digital currency economy within the system	**-**

The following text elaborates the content of the workpackages. Note that WP 2,3,4 will be dealt with concurrently during the year.

Detailed Descriptions of High-Level Workpackages

WP1 - Project planning and architecture design

In this workpackage, the following functionalities / features / work items will be implemented.

1. Develop the list of master features of the project.
2. Produce project development plan in accordance with Master Feature List.
3. Design the overall architecture of the project.
4. Analyze risks and make a management plan.
5. Initial research regarding the methods that will be applied in the project.

WP2 – Development of the peer-to-peer file storage system

This workpackage will be related to the development of a remote file storage system on a P2P network.

1. MF – 1,5,7,8 will be addressed directly.
2. Demands from consensus blockchain by the P2P network will be pinpointed compliant with MF – 2,3,4.
3. MF – 3,4 will be implemented partially, excluding consensus and authentication issues.
4. MF – 10 will be implemented partially, excluding authentication issues.

WP3 – Development of the Consensus Blockchain

The development and tuning of the blockchain in the architecture is the focus of this workpackage.

1. MF – 9 will be addressed directly, possibly by a genuine blockchain architecture.
2. Demands from WP2 about the metadata will be embedded to the blockchain, including but not limited to: hashes of the files, .
3. Possible strategies related to MF – 6 will be experimented on.
4. MF – 4 will be implemented partially, excluding file transfer between nodes, only the consensus on the authentication of the files (note that MF – 4 implies a dynamic state of a file concerning its readability by other users. This may be difficult for a blockchain which ensures that the metadata among nodes never change.).

WP4 - Integration of the Blockchain and P2P implementations

This workpackage refers to the issues with the integration of WP2 and WP3.

1. MF – 2,3 will be completely implemented.
2. The blockchain will be integrated to the P2P file storage system or will have its own network which interacts with the file storage system at node level.
3. Demands from the WP1 on MF – 2,3,4 will be completely met after integration.

WP5 - Handling of encryption and authentication Issues

This workpage is in connection with the encryption of the files and the authentication per node.

1. MF – 4,12 will be completely implemented.
2. The vulnerabilities of the strategies on MF – 4 and the potential of the blockchain will be decided on, dealt with if applicable.
3. MF – 10 will be completely implemented.

WP6 - Fair distribution of the system benefits

A blockchain system requires processing power from its nodes to ensure consensus. However a node may also rely on the nodes that sacrifice itself (miners in bitcoin) for the safety of the network. There has to be an incentive for the users to offer resources to the system. MF – 6 and WP6 is mainly related with these problems.

1. Strategies about MF – 6 will be elaborated. Potential setbacks of each strategy will be discussed (such as 51% attack vulnerabilities).
2. MF – 6 will be implemented with respect to the best applicable strategy.
3. The role distribution between nodes (miner etc.) will freeze.

WP7 - GUI development

A GUI desktop computer client will be implemented throughout this package.

1. MF – 11 will be addressed.

WPB1 - Deployment to mobile platforms

A mobile implementation of the platform with GUI will be implemented in this bonus package.

1. A node role that can comply with mobile hardware capabilities will be ported to a mobile OS, with GUI functionalities.

WPB2 - Initialization of a digital currency economy within the system

A currency will be embedded to the blockchain within the system in this bonus package.

1. An blockchain token will be introduced to the system, enabling money transactions among nodes.
2. File/money trade may be implemented.

Overall Systems Architecture

The conceived initial implementation of the platform will consist of a network of nodes, each one called a CloudChain Node. There may be two kind of networks among the nodes, one for blockchain transactions and one for file transfer and agreement about file storage contracts between clients and storage hosts. A diagram for the tentative overall architechure is given below in Figure 1 (next page).

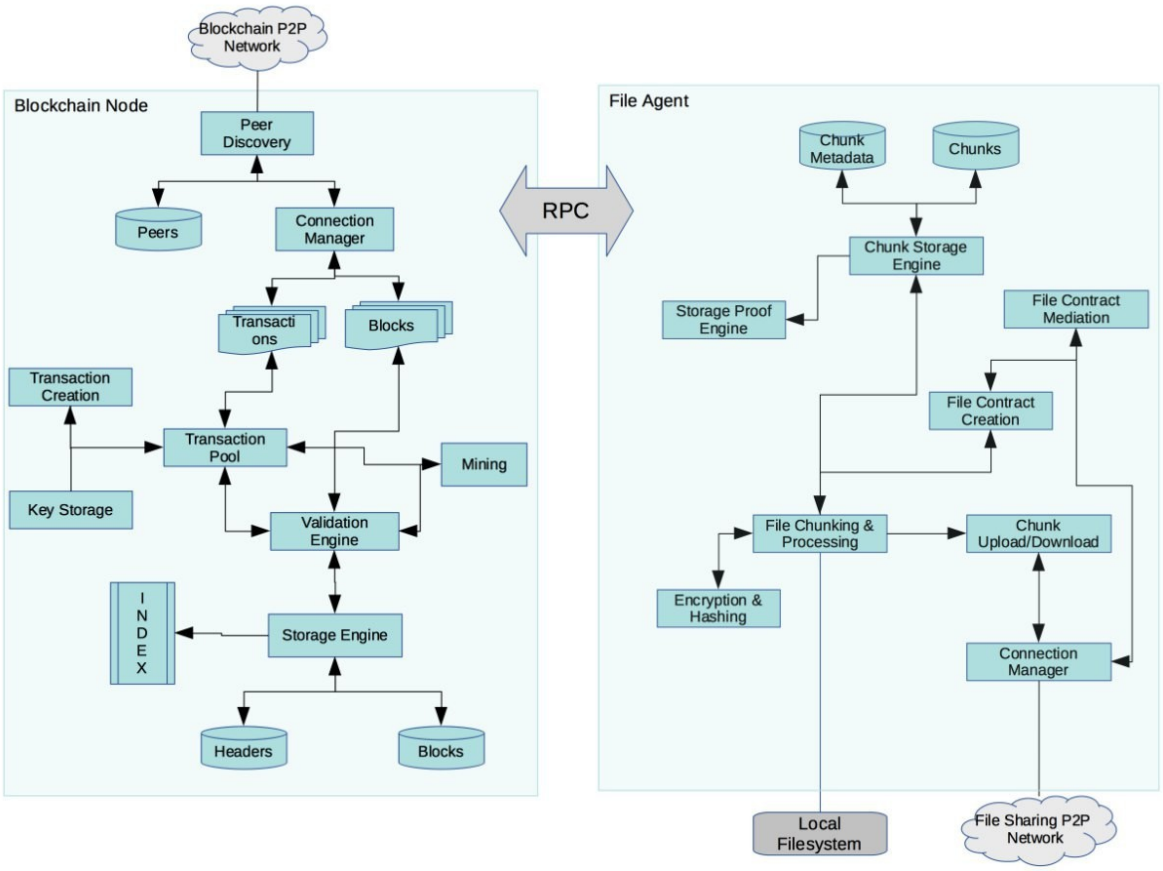

Figure 1: A Schematic of the Overall System Architecture

TimeLine

The gantt chart is located in the appendix. The important dates are on Table 2.

Table 2: Important Dates of Progress

Task name	Start date	End date
Total estimate	*18.10.2017*	*09.05.2018*
Cloudchain	**18.10.2017**	**09.05.2018**
WP1	18.10.2017	08.11.2017
WP2-Fall	08.11.2017	17.01.2018
WP3-Fall	08.11.2017	17.01.2018
WP4-1	22.11.2017	29.11.2017
MF-1 Complete, First working version	29.11.2017	29.11.2017
WP4-2	03.01.2018	17.01.2018
MF 1,2,3,5,7,8 Near Completion, Alpha Ready for Demo	17.01.2018	17.01.2018
WP2-Spring	07.02.2018	28.02.2018
WP3-Spring	07.02.2018	28.02.2018
WP4-3	19.02.2018	28.02.2018
WP5	03.03.2018	04.04.2018
MF 1,2,3,5,7,8,9 implemented, 10 partially complete excluding user authentication, first phase of the project finished	26.02.2018	26.02.2018
MF 4,10,12 implemented, Authentication features available	04.04.2018	04.04.2018
WP6-2	04.04.2018	25.04.2018
All features except GUI implemented, Beta Ready	25.04.2018	25.04.2018
WP7	25.04.2018	09.05.2018
WP6-1	06.12.2017	13.12.2017
GUI implemented, Final Product	09.05.2018	09.05.2018

Risk Assessment

Possible risks in the project can be viewed in Table 3.

Table 3: Possible Risks

Risk #	Description	Possible Solution(s)
1	Blockchain cannot support the issues in WP3: The staticity of the blockchain makes it impossible to implement one of MF – 2,3,4.	Lighter solutions that are similar to a blockchain technology that ensure less strict forms of consensus could replace the blockchain.
2	Some of the features cannot be tested due to the lack of genuine distributed nodes at hand.	Ineks could be used to test the system after the consent of the moderators.
3	The frameworks/libraries used for the development cannot be customized regarding a certain feature, especially with the blockchain implementation.	If the framework is not tightly embedded to the current project, build a new one from ground up (undesired), else discard the feature or approach the problem differently.

APPENDIX

The Gantt Chart