White Paper

The FaceCoin Network

FaceCoin (FC) - Cryptocurrency for the decentralized social network.

Introduction

Decentralized peer-to-peer technologies have evolved to replace conventional services such as filesharing and currency, with the latest blockchain based virtual machines able to create feature rich applications for web services such as exchanges, blogs, and social networking. We believe users want to eliminate the problems associated with centralized services, and we want to give back the community to the very people who create it.

Centralized social networks have the problem of constant privacy violations and data mining. Most people know the phrase, "if it's free, then you are the product being sold". Advertisers spend billions of dollars annually to collect your information and usage patterns on social networks in order to profit off of you. Big internet companies are also paying huge amounts of money to learn more about the activities of users. Most people have accepted the fact that their browsing history and web traffic patterns are being stored in a central server somewhere.

How does FaceCoin solve the problems of centralized social networking services?

We are bringing the decentralized web to everyday users without the need of additional software beyond a web browser. However, a small minority of technically savvy users will be able to service requests and earn FaceCoin microtransactions for the use of their internet bandwidth and storage. The nodes will have zero knowledge about the users of the platform, and they will not be able to read messages and content. We will run thousands of nodes at the coins launch to keep transaction costs at an acceptable level.

Anonymity

Steps will be taken to ensure users are anonymous on the FaceCoin network. The absence of registration with the use of public and private key encryption, and strict spam bot prevention ensures a clutter free environment for users.

What is a smart-contract?

A smart-contract is code deployed on the blockchain. It is used to define and enforce the relationship between actors on the blockchain. And since the blockchain is immutable the code of the smart contract cannot be altered. On a blockchain, a smart-contract is like any other actor. It has an address, a balance and can do actions (sending money etc...) but it also has a brain: it can perform actions and store information.

What is IPFS?

IPFS stands for InterPlanetary File System, a protocol designed for peer-to-peer addressable file systems. This technology enables storage of pictures, text, messages, and other connections that can be easily accessed through a smart contract.

How will we use these technologies?

Our engineering team has studied the possibilities of Ethereum to build smart-contracts on the Ethereum blockchain that define the relationship between users of a social network. Further, we will use an extended IPFS to store data without a central data point, and have developed a robust message routing

system with minimal data usage overhead.

Incentive for running a node

Users running the FaceCoin node software will earn FaceCoin tokens based on the amount of users and requests they service. FaceCoin tokens can be used by other users or businesses to create FaceCoin pages and other apps. We have many more plans on how the tokens can be used more in the future.

Who We Are

The team behind FaceCoin is based in the US with over 15 years of experience developing software solutions for Fortune 500 companies. We specialize in cloud solutions and server architecture.

Bridge

Bridge provides an object store, whose primary function is to expose an API to application developers. Developers do not require a knowledge of the network, auditing, or even cryptocurrencies to use the Bridge API. The developmental use has been made into a streamlined process as an abstraction layer.

In the current implementation, the responsibility for contract negotiation and verification is handled by Bridge while the client is responsible for encryption and file key management. In addition, because nodes can be relied on to have a high uptime, integration is possible into unreliable UX applications making use of a RESTful API.

Photon

FaceCoin implements a peer to peer store/subscribe system called Photon. To operate Photon, FaceCoin extends Kademlia with several new message types. These help to facilitate the propagation of filters, with each node maintaining information about topics in which it subscribes. Nodes may respond to requests to update their filter lists and push changes to their nearest neighbors in the subscription chain.

Nodes will not relay messages with a hop exceeding the TTL, or a TTL that would exceed any of a new message. To prevent replaying of messages, nodes add their

ID when they are forwarded, indicating that they have already seen the message. This prevents redundancy in the form of communication overhead.

BitSwap

IPFS uses a concept called BitSwap ledgers, which are simply a local accounting of previous interactions with other nodes. As the BitSwap protocol is primarily concerned with the distribution of objects in a Kademlia style DHT, BitSwap ledgers count bytes sent and bytes read. Instead of attempting to reach global consensus about the reputation state of the entire system, these ledgers only deal with one-to-one relationships, and do not account for latency, throughput, discoverability, or other QoS factors. Almost all of the behavior of the node is left to the implementer, with some discussion given to potential exchange strategies. This means that BitSwap ledgers can scale well and are extremely versatile.

NAT Traversal

Not all devices are publicly available through the network. To enabled systems behind NAT or other network devices to participate, FaceCoin implements a robust reverse connection system. A unique message ordinal allows a node to determine whether it is publicly available from other nodes. Nodes joining the network should immediately respond to the request and based on the response, will either operate successfully or continue the process of finding a tunnel node.

The providers must create a tunnel for a node if they are capable. The node will open a keepalived connection to the provider, to ensure a simple and flexible interface to receive updates. Tunnels are operated over TCP with a simple protocol which provides a flexible interface for additional tunneling.

Identity and Permissions

FaceCoin uses public key cryptography to verify clients and access. Users register public keys with nodes, and API requests are signed. Buckets can be permissioned individually by registering a set of public keys as given access. This provides a logical separation between users and permissions. For instance, the publisher

of a file can divide each user into a separate bucket accessible only by those keypairs.

Objects in Encrypted Shards

Sharding has a number of advantages to security, privacy, and availability. Files should be encrypted client side before being sharded into smaller encrypted pieces. The reference implementation uses AES256 in cipher feedback mode, but other encryption schemes can be substituted easily. The content of the data is protected from the storage provider, host node, and unauthorized users. Distributing shards across multiple nodes reduces the impact of retrieval on any given node. In addition, parallel transfer can be done by the end user as a performance enhancement.

Routing By Shard Hash

Shard buckets have a fixed maximum size in bytes, S. This maximum of a K store of $S * B$ bytes collectively form a B-Table of up to 4 TiB. Nodes will use their 160 bit Node ID as a reference identifier, which can be arbitrary. The following sorting algorithm implies $O(\log n)$ lookup.

1. Let $g = [log_2(B)]$.
2. Let h be the first g bits of R.
3. Let i be the first g bits of the shard hash.
4. Let $n = h + i$.
5. Store the shard in Ln.

Mirrored Erasure Coding

Erasure coding algorithms work by breaking a file into m shards, with k parity shards. Availability makes use of the fact that $P = 1 - \prod_{0}^{m} a_m$ with at least $m + 1$ available nodes. To prevent loss of the file, shard loss tolerance levels can be set by data owners. Because node uptimes are known through the bootstrapping process, tolerance levels can be automatically optimized based on the characteristics of the nodes involved. This also decreases the on-disk overhead needed to achieve a given level of availability for any given object.

Probability Distance

As the network grows and additional shards are created, it becomes progressively more difficult, without prior knowledge of the locations of its shards, to locate a given object. The probabilities of locating a targeted object can be calculated from k shards by n random draws in a network containing N shards modeled as a geometric distribution with $K = k$.

$$Pr_{Success}(N, k, n) = \frac{\binom{N-k}{n-k}}{\binom{N}{n}}$$

N	k	n	$Pr_{Success}(N, k, n)$
100	10	10	5.777e-14
100	10	50	5.934e-04
100	10	90	3.305e-01
100	50	50	9.912e-30
500	50	200	5.493e-04
500	50	400	1.961e-22
900	10	200	7.361e-06
900	10	400	2.457e-07
900	10	800	2.823e-04
900	50	200	3.060e-01
900	50	400	1.072e-35
900	50	800	4.023e-19

Challenges

Current social networks are confronted with many challenges. Primary information, composed of private messages and direct content lookup, is ubiquitous and does not pose any problem for any network. However, it is not feasible to digest this primary information into secondary information to be shared. There are several strategies to bring this information together reliably.

Quality Content

In the same way that web search algorithms gives weight to material that is linked from other sources, creating a trust score, a person's past reputation is a good proxy to determine the quality of their future work. However, human beings are prone to produce inconsistent results, coupled with the difficulty in translating to online content. Additionally, the psychological phenomenon of social popularity and mind share influencing perceived branding can manifest itself. Many social networks have replicated this by representing cumulative likes or upvotes.

Factual Content

The measure of the reliability of content is also affected by social psychology. Journalism ordinarily needs to be sourced from a trusted institution or source with a pre-existing level of reputation. Sources of weak reputation may receive invalid mind share from cognitive bias. The network effects of social sharing can potentiate information.

Censorship

Moderation is often required in any environment that many people use to remove illegal material or to prevent scams, spam, and other unwanted material. However, a decentralized system enables unfettered freedom of expression and universal access.

Sybil Attacks

The power to upvote can be abused by bots, sock puppet accounts, and sybil attacks. Quality content is often determined by voting to attain an accurate measure. The premise solution is representation through proof of work or other proof, identities. Requiring a proof to perform content voting or to assume an identity creates a high cost for malicious actors.

Separation of Social Network and Blockchain Layer

The blockchain layer runs on top of the Ethereum protocol, enabling social proof to be distributed and created. The social layer is completely decoupled from this and is used for content distribution and interaction. This separation is ideal to allow each layer to implement features independently of each other. Additionally, specialized social networks can be created separate from one another, or with exposing only a small subset of properties with one another.

Architecture

There are a series of functional layers making up the service.

- Innermost domain layer, applications environment is made up of a domain language with underlying libraries, networking implementations, and function interfaces.

- Second processing layer, objects are translated into interfaces with lower-level semantics.
- Peripheral layer, semantical encodings are exposed to the domain model as services.

FaceCoin Node

There is no cost to run a FaceCoin node beyond bandwidth and hardware. The only other requirement is a valid FaceCoin wallet address on Ethereum where earnings can be sent to. Nodes will be easy to set up with no technical knowledge needed to configure. An easy installer will allow fast setup on Mac, Windows, and Linux computers. Setup of the node software exposes options to schedule bandwidth limits on a time basis, as well as memory and cpu limits.

FaceCoin DNS

In order to allow users without the node to access the network, the existing DNS system is used to forward requests to a series of servers running node using fast fluxing techniques as load balancing. When initially contacting a node, a bootstrap process is performed to determine the geographical distance and latency to the node, and to optionally forward to a different server for optimal speed. All of this happens transparently and incurs a modest wait comparable to TLS negotiation. Nodes will periodically optimize their connection list for the highest speed optimization at all times.

Future Developments

Currently FaceCoin is in private beta, with many features already working. There are several ideas that will be implemented in future versions. Numerous possibilities that have great potential to become their own popular products in their own right are in planning.

FaceCoin Messenger

Not only do users of social networking desire the ability to create posts and upload photos, but users want a way to send messages to one another instantly, and in a secure manner. We are currently in early stages of developing a messenger that is also usable through standards compliant web browsers. We

believe security is the number one priority for the future, and will implement provable end-to-end encryption from day one, on top of the already secure network. Only the sender and receiver will be able to read their messages, and our testing shows that this is possible utilizing standard web browser technologies of today. An updated messenger is planned afterwards to allow group conversations and possibly voice.

FaceCoin Pay

Already there are multitudes of cryptocurrency options used to pay for services and as exchange of goods. We believe implementing a payment method directly into FaceCoin is a natural step in the progress towards decentralizing everything we do online. Methods of arbitration using multisig and security implications are being analyzed by the team for future implementations.

FaceCoin Marketplace

A popular activity inside of social networks is to buy and sell goods and services. Much like other services that exist on the regular internet as central websites, we wish to develop a marketplace that users of the network can use in a similar fashion.

[1] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. 2015.

[2] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for c: Verifying program executions succinctly and in zero knowledge. In Advances in Cryptology–CRYPTO 2013, pages 90–108. Springer, 2013.

[3] Protocol Labs. Technical Report: Proof-of-Replication. 2017.

[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[5] V. Buterin et al. A next-generation smart contract and decentralized application platform, (2014).

[6] D. DeFigueiredo, E. Barr. Trustdavis: A non-exploitable online reputation system, (2005).

[7] G. Hall. Storj core tutorial: Transferring file shards, (2016).

[8] P. Maymounkov, D. Mazieres. Kademlia: A peer-to-peer information system. based on the xor metric, (2002).

[9] B. Bloom. Space/time trade-offs in hash coding with allowable errors, (1970).