BlockFame: Proof-of-Celebrity Consensus with Fame at Stake

August 2018

Abstract

With the rapid expansion of interest in cryptocurrency, many challenges become apparent when blockchain inefficiencies arise. The traditional Proof-of-Work consensus engines used in popular cryptocurrencies such as Bitcoin and Ethereum become power hungry protocols that prevent scalability while also prohibiting developers from easily building complex decentralized applications on-chain. In order to secure a Proof-of-Work network, miners are incentivized with rewards to solve arbitrary puzzles, and in many cases, these cryptographic hashing algorithms are running while providing little to no reward at all for the miners. The cost of securing a network with such protocols only serve the interests of individual financial gain while leaving the supporting community vulnerable to mining fees and block reward induced price volatility.

We propose a solution to mitigate an inefficient community structure by incentivizing a new philanthropic model within the community. A model where miners are only given access to mine on the network if they place their fame at stake, in combination with a charitable cause to which their mining rewards will be donated, through a transparent, smart contract powered distribution mechanism.

1 Introduction

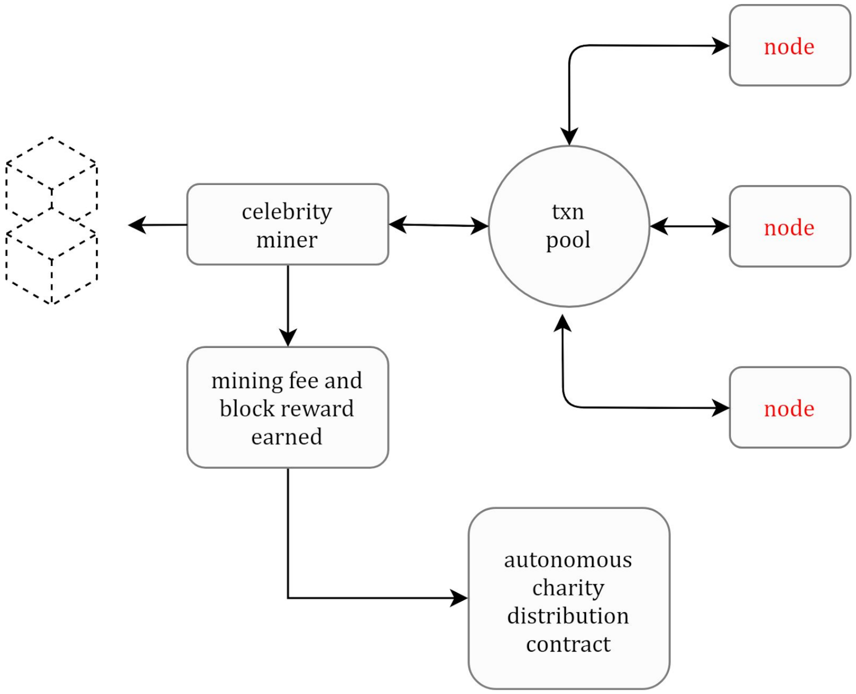
Accepting cryptocurrency donations has been ubiquitous amongst many charitable organizations since mainstream media recognized a new growing digital asset on the rise. Bitcoin became a worldwide sensation that many did not fully understand but still found value in. With mass adoption gaining traction, charities also found value in accepting bitcoin to help solve problems we as a society face together. There will always be a need for giving, a true virtuous purpose where the cryptocurrency community has always exemplified dedication. Whether its cryptocurrency centric companies eliminating fees for non-profit organizations or cryptocurrency platforms set up to optimize and improve the giving process, the community has always understood the potential surrounding the technology.

Blockchain technology has become the latest standard to solve trust issues, a decentralized immutable ledger designed for public transparency. A transparency that can perfectly support the motivations of a charity and the relationship between themselves and their donors. A declining public trust in charities is evident worldwide, it is not only scams that the public fear, but also misuse of funds. Solving trust issues between donors and charities while also utilizing network transaction fees to further benefit charities is a path worthy of discernment.

Donating to charities is one of the most selfless things celebrities can do to support a cause while improving their public image at the same time. Celebrities have the power to change lives and influence others, it is with their help that we aim to change the world by using celebrity fame as a means to a just cause. With fame comes money, and the incentivization for financial reward or malicious activity becomes minimized to smallest of risk factors.

2 Proof-of-Celebrity

Consensus algorithms ensure network participants work together to achieve an agreement on a data point. The Proof-of-Celebrity consensus maintains an efficient standard by invoking a virtuous relationship for celebrities that are willing to leverage their social capital, while easily supporting a cause of their choice through a transparent manner supported by blockchain technology.


node
celebrity miner
txn pool
node
mining fee and block reward earned
node
autonomous charity distribution contract

2.1 Blockchain Technology

The Proof-of-Celebrity network will be built upon Parity Technologies Proof-of-Authority[1] consensus infrastructure which was originally built to supplement Ethereum as a fast and stable testnet (Kovan). This technology when properly applied only allows non-consecutive block approval from any one validator, meaning that the risk of serious damage is minimized and overall network performance is improved. Utilizing this technology in partnership with celebrities who have a public reputation at stake will create an efficient and reliable public network.

Decentralized autonomous distribution wallets will support the platform by managing and logging all transactions to a public ledger that verifies the amount of funds the miner has accumulated and to which charity it will be distributed. After a designated period, funds will be distributed in accordance with a previously defined Miner Initialization Contract which sets forth the allocation parameters agreed upon between the miner, charity, and network consortium. All the parameters defined within the Miner Initialization contract will be made available for public audit and accountability through the BlockFame Blockchain Explorer.

2.2 Miner Selection

The Proof-of-Celebrity protocol makes certain that all available miners have an equal opportunity to be selected to produce blocks. However, from a security point of view, we prefer to minimize risk further by not composing the order for miners to generate blocks to be in any type of predictable pattern. The Aura (Authority Round) consensus does not utilize a pseudo random number generator (PRNG) and therefore, in order to prevent deterministic behavior, we introduce an anti-deterministic pseudo random mechanism (PRM) while integrating the concept of a basic scoring system of miners to assist with the decision whether a particular miner is eligible for generating a block with a certain height and timestamp.

Our PRNG proposal is the linear congruential generator[2]:

A sequence of integer numbers x_i is generated by

$$x_i = (ax_{i-1} + b)\ mod\ M,\ i = 1, 2, \ldots$$

The parameters in the method $a, b, x_0, M,$ are non-negative integers such that $a, b, x_0 < M$ and $a \neq 0$. The sequence is initialized by the seed x_0 and has the following properties:

1. $0 \leq x_i \leq M - 1$
2. the period is at most M

The first property follows from the definition of mod. In a sequence of $M + 1$ numbers x_i at least two of them must be equal.

In Rust:

```
use std::rand::{Rng, SeedableRng};

struct LinearCongruentialPRNG {
    seed: u32
    rand_state: u32
}

fn main() {
    let mut rng: LinearCongruentialPRNG =
SeedableRng::from_seed(5);
    for f in 0..=21 {
        println!("{}", rng.next_u32() % 100);
}
```

2.3 Celebrity Selection

Celebrity selection will be limited to a certain number of miners spanning several geographic locations. Powered by celebrities all over the globe, this helps ensure no dominant interest can be established within a closed geographic area, maintaining the FAME coin's intention as a worldwide currency that can be used by anyone. The amount of miners assigned to each country will be determined by the size of the geographical area, ensuring that the network will be evenly distributed throughout the globe.

Sample:

Country/Continent	# of Celebrities
Canada	3
United States	3
Australia	1
Asia	4
Africa	2
Europe	3
South America	2
Russia	3

2.4 End User Benefits

In addition to a drastic improvement in network performance and reduction in transaction fees for all users, charities that have working relationships with celebrities will have a prioritized opportunity to become a network verified charity. Charity verification will be based upon industry standard rating systems that take into account financial health, accountability, and transparency.

Following the launch of the BlockFame network, additional transparency workflows will be established in cooperation with our verified charities to establish goal based objectives to which charities must adhere to in order to receive further donations. Processes will be designed with ease of use in mind while incorporating mandatory reporting methodologies.

2.5 Mainstream Features

Users who hold more than 10 FAME Coins in their BlockFame wallet will have the option to associate their address to a username. Users who opt for this feature will be able to receive funds through an easily identifiable unique username instead of the standard 42 character 0x address. Sending funds to a BlockFame username will only be possible from compatible wallets which integrate the BlockFame Explorer API.

2.6 Community Benefits

Throughout history, money has always been donated to the needy knowing that it will make a difference in the world. Charity, non-profit, non-governmental, and social organizations that spearhead initiatives for community or group benefit will have extended opportunities to execute on their goals through a surplus of funds made available to them through the generosity of the celebrities that represent them. Positive impacts will be recognized worldwide through a transparent process that the public can easily track.

2.7 Miner Benefits

It is often said that the good causes of the famous only benefit themselves more than the charities they represent.[3] This common misconception can be eradicated effortlessly through our processes justified by blockchain technology. A large majority of the public have difficulty identifying charities to which a celebrity advocates. On the BlockFame network, blockchain records will indicate which celebrity validated each transaction, placing the celebrity miner’s name at the forefront of each block that is generated for the blockchain, along with total transaction fees identified for automatic disbursement to the charity or charities defined in the Miner Initialization Contract.

All miners on the network will have full control over their mining availability. Should any conflict of interest arise between the charities and the miner that represents them, the miner will have the option to forego their mining key and any allocation parameters set within the associated Miner Initialization Contract. In order to regain access to mining on the network, the miner will have to revalidate their celebrity status on the platform, get consortium approval, and define new allocation parameters for the charities of their choice.

3 Network Sustainability

Placing the security of a network in the trusted hands of the few who represent a piece of the altruism in today's society will help ensure the network isn't compromised by greed and financial motivations. Network mining will be secured by authenticated mining keys granted after completion of the Miner Initialization Contract.

3.1 Network Efficiency

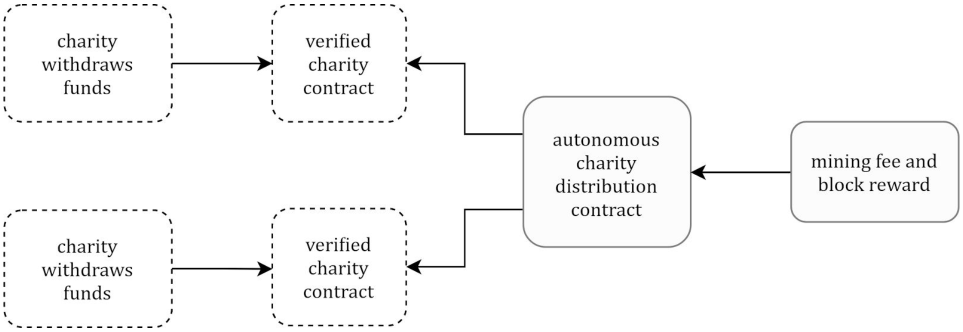
The Proof-of-Celebrity consensus algorithm is a substantially more efficient and lightweight algorithm than Proof-of-Work. The network delivers rapid transaction speeds when compared to Bitcoin and Ethereum while being more cost effective at the same time. Both transactions and smart contract deployments will benefit from the BlockFame Network. As an Ethereum sidechain, the BlockFame Network will support any future state channel solutions, such as Plasma or Raiden, to further improve network performance.

Network	TPS
Bitcoin	7
Ethereum	20
BlockFame	1000
VISA	2000+

3.2 Governance

Consortium governance will be managed through a transparent, public viewable web application. Voting keys will be distributed to each miner a minimum of 90 days after completion of the Miner Initialization Contract. This time period will serve as a collusion prevention measure to help ensure no hostile acts of cooperation between miners can compromise the network. Counter measures that can be taken to remove malicious miners from the network will be simplified within the smart contract based voting process available to those with a voting key.

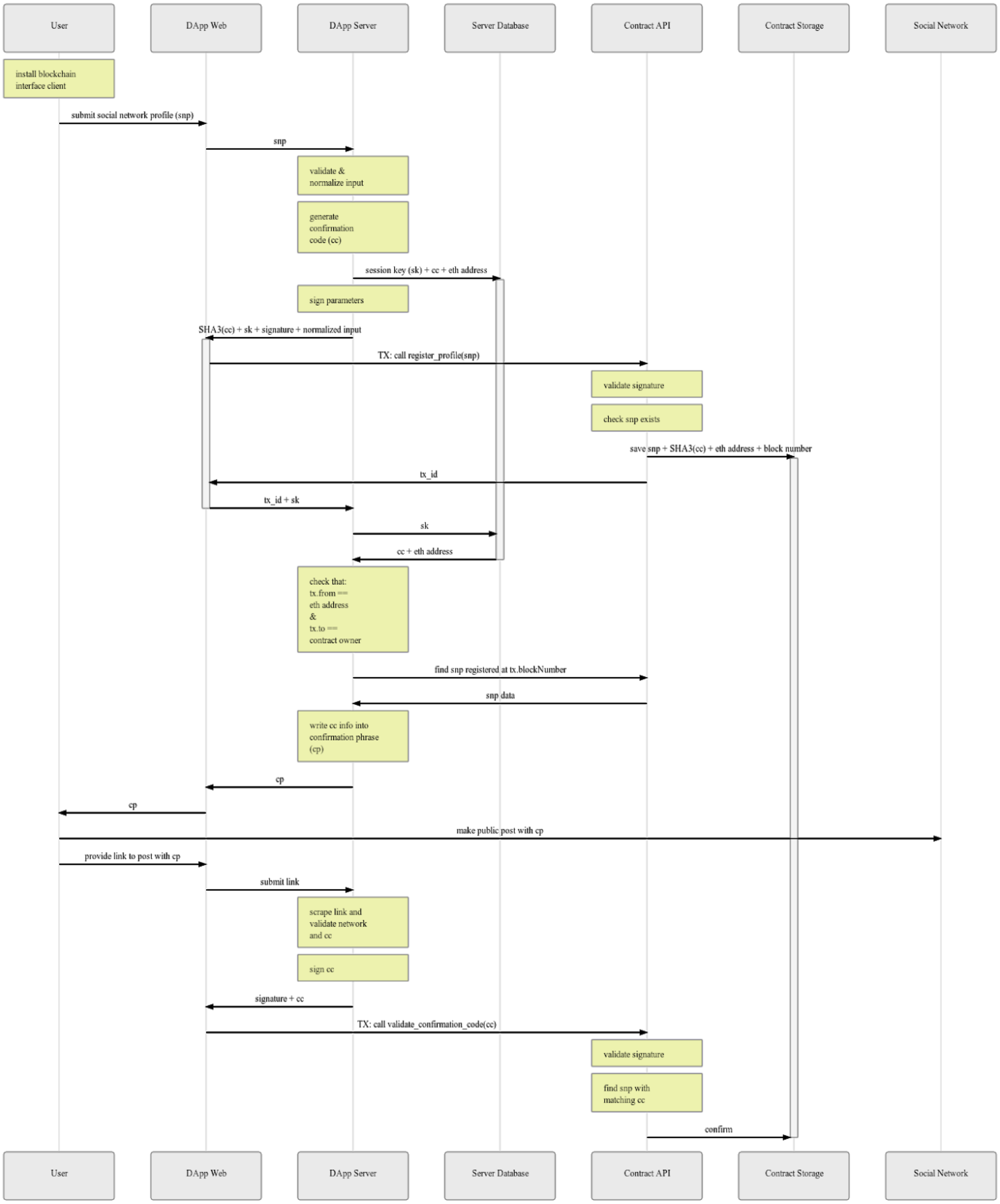
Consortium members with a voting key can exercise their right to launch a public ballot that seeks the termination of a verified charity or miner. Voting will take place for 21 days, where each member will have an opportunity to cast their vote. When the ballot expires, the outcome will be executed according to the option with the highest number of votes. In the event of a tie, the outcome will result in non-termination of the charity or miner.


charity withdraws funds
verified charity contract
autonomous charity distribution contract
mining fee and block reward
charity withdraws funds
verified charity contract

Charity proceeds will be managed through the BlockFame Explorer. Charities can only withdraw funds in accordance with an amount set for a goal based objective that the charity has made record of.

3.3 Mining Key Issuance

The BlockFame Network will launch initially with 21 celebrity miners with variation divided amongst several countries. As the market capitalization increases when the network grows, each incremental milestone gain of $100 Million will unlock the network consortium to authorize 2 additional celebrity miners to the network. So as the network scales, the number of miners to secure the network grows in proportion. The complete list of celebrity miners will be announced at the launch of the BlockFame mainnet.


User
DApp Web
DApp Server
Server Database
Contract API
Contract Storage
Social Network
install blockchain interface client
submit social network profile (snp)
snp
validate & normalize input
generate confirmation code (cc)
session key (sk) + cc + eth address
sign parameters
SHA3(cc) + sk + signature + normalized input
TX: call register_profile(snp)
validate signature
check snp exists
save snp + SHA3(cc) + eth address + block number
tx_id
tx_id + sk
sk
cc + eth address
check that: tx.from == eth address & tx.to == contract owner
find snp registered at tx.blockNumber
snp data
write cc info into confirmation phrase (cp)
cp
cp
make public post with cp
provide link to post with cp
submit link
scrape link and validate network and cc
sign cc
signature + cc
TX: call validate_confirmation_code(cc)
validate signature
find snp with matching cc
confirm
User
DApp Web
DApp Server
Server Database
Contract API
Contract Storage
Social Network

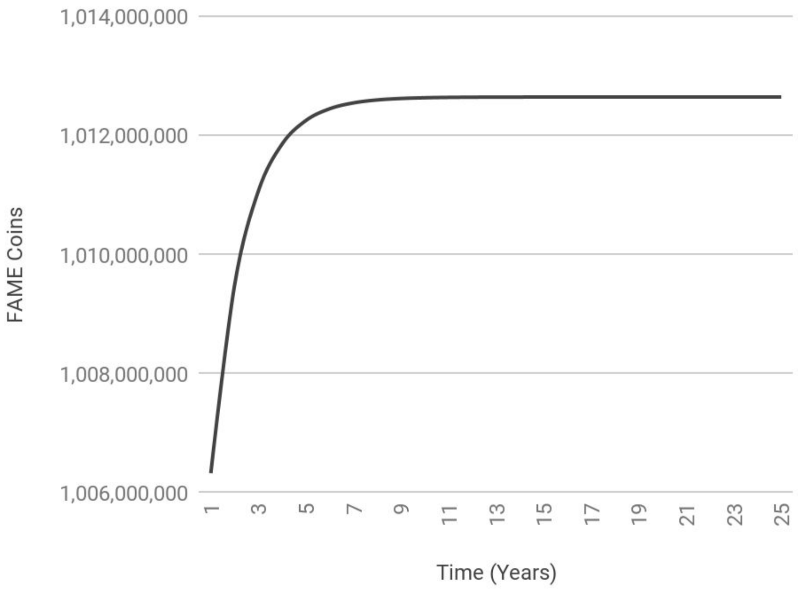
3.4 Charity Key Issuance

A Charity Key will be issued to all verified charities. This key will allow the withdrawal of funds to the charity's private wallet in order to execute on their proposed funding objective. Charities are responsible for providing enough detail on the fund usage collected through the BlockFame Explorer.

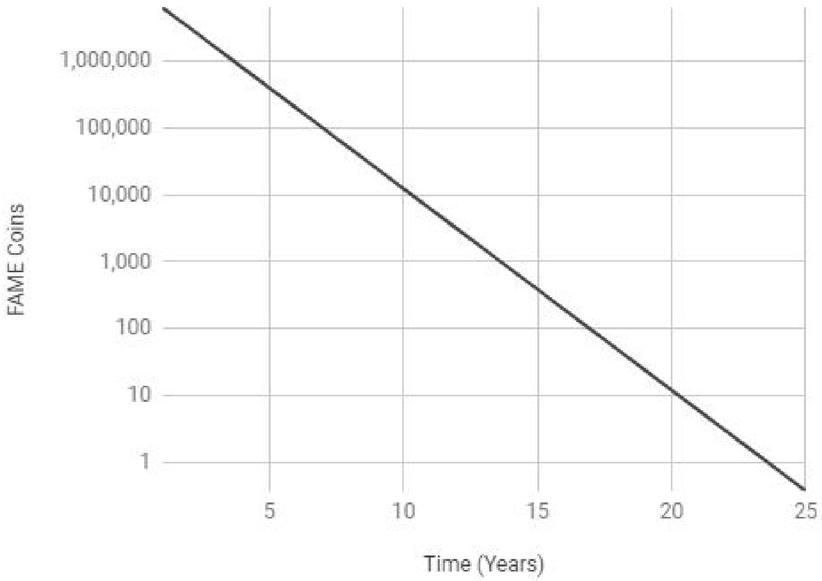
4 Economy

For each block that is generated, 1 FAME Coin will be rewarded to the block miner. This will occur every 5 seconds after the genesis block. After each period of 1 year, or each 6,624,480 blocks, the block reward will be halved. The BlockFame genesis block will allocate 1 billion coins to support network liquidity between the Ethereum and BlockFame bridge. As such, the FAME total supply will increase at a maximum rate of 6.32% the first year, with a 50% reduced increase each year thereafter for a total finite network supply of 1,012,648,960 coins and tokens spread between the Ethereum and BlockFame network.

Total supply over time



Yearly issuance over time



4.1 Bridge to Mainnet

ERC20 FAME Tokens can be utilized on our cross-chain bridge to the BlockFame Network. The cross-chain bridge is a DApp that will provide a method for transferring ERC20 FAME tokens to native FAME Coins. Token distribution will take place prior to the official mainnet launch in order to create the initial liquidity for the FAME Coin.

4.2 BlockFAME Token Specifications

- Smart Contract Platform: Ethereum
- Contract Type: ERC-20
- Token: FAME
- Token Name: BlockFame Network Token
- Total Issuance: 1,000,000,000
- FAME Token Supply: 1,000,000,000

4.3 Even Distribution Model

Unlike other projects, BlockFame has decided not to conduct an ICO, fair market value will be driven by the community using an even distribution model, such that tokens will not be sold in tiered pricing in order to reduce volatility and promote coin stability.

5 Blockchain Design Philosophy

We propose a simple and effective solution, a blockchain design that will maximize the Proof-of-Celebrity protocol efficiency by utilizing and optimising already developed technologies. These optimizations can be seen as a secondary layer scaling solution, combining ideas from existing larger scale communication protocols.

The following points describe the philosophical design of our blockchain motivation and architecture:

Speed The number one inefficiency in modern day blockchains is the delivery of data. This should be done with low latency, enabling developers to deploy applications in a limitless environment.

Trust Transmission of data among the blockchain should be seamless and safe, to ensure data arrives intact and unaltered with proper network incentives and disincentives.

Ethical Distribution The volatile nature of cryptocurrencies come from inadequate distribution models, greed, and bad market economists.

6 Summary

Performance, scalability, and trust are only one part of a successful equation for a new PoA blockchain. The primary motivation to establish users in the network will come from the compassion and good will found within many of us. Through an altruistic expression of connectedness to one another, it is with our deepest moral obligation that 100% of all block rewards and transaction fees always go towards charity. We have a firm belief that it is possible to grow while giving, and with the BlockFame Network, our commitment to growing a better future begins here.

References

[1] Proof-of-Authority, Parity Technologies [html]

[2] Overview of Random Generation Algorithms [html]

[3] Celebrities good causes benefit themselves more than the charities, Independent.co.uk [html]

Glossary

Block A block holds batches of validated transactions that are hashed and encoded into a Merkle tree. 1-4, 8, 10

DApp Abbreviation for Decentralized App, a software application where the backend code is running on a decentralized peer-to-peer network. 9

Genesis Block Also known as block 0, the first block in a blockchain that contains hard-coded information to which the rest of the blockchain must follow. 8

ICO Abbreviation for Initial Coin Offering, an unregulated means by which cryptocurrency funds are raised for a new related venture. 9

PoA Proof-of-Authority, a consensus engine used with Ethereum Virtual Machine based chains. Blocks must be validated by an authority node to become permanent record. 10

Smart Contract A pre-defined self executing contract, or piece of code, that resides on, and interacts with a blockchain, when deployed on a network. 1, 5, 9

State Channel A component or methodology where trusted transactional records can be created off-line, with only intermittent communication to a blockchain. 5