Proof of Steak & The Steak Network

Matt Condon

October 10, 2017

Abstract

We present Proof of Steak, an algorithm capable of securing a blockchain where block proofs cannot be computed cryptographically. Proof of Steak is inspired by and modeled after the TrueBit Protocol[1] and Verification Game[2], and uses Delegated Proof of Stake[3] to validate proofs in the event of a challenge.

Further, we present the Steak Network, an implementation of Proof of Steak. In the Steak Network, the proofs are pictures of steak (a "Proof of Steak"). The Steak Network uses Proof of Steak to verify that every proof in the set of finalized proofs (the "Steakchain") is a picture of a steak (and not, for example, a picture of something that is not steak).

Use Cases

Proof of Steak can be used to secure a blockchain in any situation where the proofs are a function of opinion and not mathematics. In the Steak Network, for example, the proofs are pictures of steaks; whether or not a picture is of a steak is not (yet) machine-verifiable and is a function of crowd-opinion.

Additional use cases include - creating a set of verifiably rare memes, - decentrally curating a dataset for machine learning or AI training, - decentralized MTurk[4] - or building a database of every rock on earth.[5]

[1] https://truebit.io/
[2] https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf
[3] https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[4] Mechanical Turk, https://www.mturk.com/mturk/welcome
[5] How Many Rocks Are There, And Where Are They? http://www.howmany.rocks/

Proof of Steak and The TrueBit Protocol

Proof of Steak differs slightly from the TrueBit protocol: firstly, we rename all of the actors in the system for comedic effect. Network participants and Verifiers are Steak Holders. Task Givers and Solvers are Cooks. Challengers (Verifiers that challenge the validity of a solution) are Grill Masters. Secondly, the Task Giver and Solver are the same entity; it can be thought of as providing the Task "submit a Proof" and immediately solving it by including the Proof itself.

Additionally, the TrueBit Verification Game doesn't apply to Proof of Steak; there is no way to computationally and objectively verify that a submitted Proof is valid. Therefore, in lieu of the Verification Game, we propose that Challenges are resolved using the Delegated Proof of Stake protocol ("Grilling the Cook"). All token holders ("Steak Holders") can become a potential DPoS Witness ("Backseat Griller") by joining the Witness Pool ("Backseat Griller Crowd"). They then have a chance to become a Backseat Griller, weighted by staked amount, in the event of a challenge. These Backseat Grillers then follow the DPoS protocol for voting on the validity of a challenged Proof.

Due to the increased number of expensive actions required to become a successful Cook, the Steak Network has an increased the barrier of entry compared to proof submission processes in other stake-based networks. For example, in the TrueBit protocol, solvers simply run virtual machine bytecode and create Merkle proofs of intermediate and final results. In Proof of Steak, participants must locate images of particular cuts of bovine flesh on third-party services such as Google Images, Pinterest, or Real Life. They must then perform additional tasks such as Copy-And-Paste, Save-To-Folder, or Upload-To-Computer. As expected, Cooks must perform many difficult and taxing tasks for low compensation, thereby improving the resistance of the network to attack.

Proof of Steak also:

- limits the number of Challengers ("Grill Masters") to one,
- includes, but slightly alters the mechanics of jackpots and taxes,
- implements forced errors to incentivise Verifiers, and
- alters the economic interactions to account for new actors and protocol implementation.

Proof of Steak and IPFS

The Steak Network Proofs must be made widely available for all network participants. Therefore, they will be stored using the InterPlanetary File System (IPFS): a high-throughput, content-addressed distributed block storage model, with content-addressed hyperlinks. There are low security concerns as no sensitive data are stored and widespread dissemination of network Proofs is encour-

aged. IPFS has been made production-ready through notable projects such as FileCoin.

Proof of Steak Protocol Overview

Any network participant ("Steak Holder") can submit a Proof to the network and stake tokens on its validity. This Proof is considered valid until challenged. If not challenged within the challenge timeout period, it is finalized and the staked tokens are released. If a proof is challenged, the Grilling of the Cook begins, which elects Backseat Grillers to validate or invalidate the Proof. The Cook's stake is burned if the Grilling determines that they have submitted an invalid Proof.

To incentivise Verifiers, the network also introduces forced errors, which invert the game theory and slightly alter the economic incentives. When a Cook submits a Proof, they are told whether a forced error is in effect or not. In the case of a forced error, the Cook submits an intentionally incorrect Proof. Then, upon a successful challenge and Grilling, Grill Masters are awarded a jackpot payout.

If a Cook, Grill Master, or Backseat Griller is determined to have acted maliciously, their stake is forfeited to the jackpot at tax rate T and otherwise burned ("burned to the Jackpot").

Proof of Steak Protocol Detail

The following section provides a detailed look into the operation of Proof of Steak.

1. A Steak Holder becomes Cook by submitting a Proof to the network. This involves:
   - Generating a random secret number r, the hash of which is published to the blockchain,
   - Preparing one valid Proof A,
   - Preparing one invalid Proof B, and
   - Staking token amount S on their rational behavior.
2. The next block is mined.
   - The hash of the block header is determined.
   - The Cook knows both the secret number r and the block header hash and can determine whether or not a forced error is in effect.
     - If a forced error is NOT in effect, commit the valid Proof A
     - If a forced error IS in effect, commit the invalid Proof B
3. Between this point and timeout, any Steak Holder may become Grill Master and Challenge the committed Proof.

- If no Steak Holders become Grill Master:
  - The Proof is considered valid and finalized.
  - The Cook's stake is released.
- If a Steak Holder becomes Grill Master, the Grilling of the Cook begins.

The Grilling of the Cook

1. Grill Master stakes token amount Sm on the invalidity of the committed Proof.
2. Cook reveals secret number r, allowing the other actors to determine if a forced error is in effect.
3. If a forced error is NOT in effect:
   1. Elect Backseat Grillers from the Backseat Griller Crowd, weighted by staked token amount.
   2. Backseat Grillers vouch for the validity or invalidity of the revealed Proof by witnessTimeout.
      - If the Proof is determined to be valid:
        - Cook's stake is released,
        - Grill Master's stake is burned to the Jackpot,
        - Incorrect Backseat Grillers' stake is partially burned to the Jackpot,
        - Proof is finalized.
      - If the Proof is determined to be invalid:
        - Cook's stake is burned to the Jackpot at tax rate T and otherwise awarded to the Grill Master,
        - Grill Master's stake is released,
        - Incorrect Backseat Grillers' stake is partially burned,
        - Proof is discarded.
4. If a forced error IS in effect:
   1. Cook reveals valid Proof A, discarding invalid Proof B
   2. Between now and 2 * timeout, Cooks can become Second Grill Master and Challenge the validity of Proof A
      - If no Cooks become Second Grill Master:
        - The Cook's stake is released.
        - The Grill Master's stake is released.
        - The Grill Master is awarded Jackpot J.
        - The Proof A is considered valid and finalized.
      - If a Cook becomes Second Grill Master, the Grilling of the Cook begins.
        1. Second Grill Master stakes token amount Sm on the invalidity of Proof A.
        2. Elect Backseat Grillers from the Backseat Griller Crowd, weighted by staked token amount.
        3. Backseat Grillers vouch for the validity or invalidity of the

Proof A by witnessTimeout.
- If the Proof A is determined to be valid:
  * The Cook's stake is released.
  * Grill Master's stake is released.
  * The Cook is rewarded with Jackpot J
  * Correct Backseat Grillers are awarded with fractional Jackpot Jf
  * The Proof A is finalized.
- If the Proof A is determined to be invalid:
  * Cook's stake is burned to the Jackpot.
  * Grill Master is awarded fractional Jackpot Jf
  * Incorrect Backseat Griller' stake is partially burned to the Jackpot,
  * Proof is discarded.

Actors and Incentives

What follows is a summary of the actors in the network, their definitions, and their incentives for participating in the network.

Steak Holders (Network Participants & Verifiers)

Steak Holders are holders of the network token. They have the ability to become Cook by submitting Proofs to the network, as well as the ability to become Grill Master and challenge another Cooks' Proof.

Cook (Task Giver & Solver)

Any Steak Holder may become Cook by submitting a Proof and staking tokens on its validity. If a Cook behaves correctly, their Proof is finalized and included in the set of valid proofs. If a Cook's Proof is challenged and the Cook is the loser of the Verification Game, their stake is burned to the jackpot.

Grill Master (Challenger)

Any Steak Holder may become Grill Master by challenging a Cook's Proof of Steak and staking on its invalidity. If the Grill Master is the winner of the Verification Game under normal conditions, they receive a small payout, deducted from the Cook's stake. If the Grill Master is the winner of the Verification Game under forced-error conditions, they receive a jackpot payout, deducted from the shared jackpot pool. If the Grill Master loses the Grilling of the Cook, their stake is burned.

Backseat Griller (DPoS Witness)

By staking large amounts of the network token, Steak Holders can join the Backseat Griller Crowd (DPos Witness Pool). When a Proof of Steak is challenged and the Grilling of the Cook begins, Backseat Grillers are randomly selected by the network via the Delegated Proof of Stake protocol. Backseat Grillers have the ability to vouch for the validity or invalidity of a Proof of Steak. Backseat Grillers that side with the minority have their stake burned. Under forced-error conditions, Backseat Grillers that side with the majority receive a share of the jackpot payout.

Steak Network

The $TEAK Token

Usage

The $TEAK token fulfills a few purposes[6]:

1. It makes the "$TEAK Holder", "$TEAK Stake", and "burning $TEAK" jokes possible,
2. It aligns the financial incentives of network participants by providing:
   - negative incentive for malicious activity, and
   - postitive incentive for altruistic and rational activity, and
3. It is necessary for the operation of Delegated Proof of Stake[7] as the medium being staked.

Total Supply

To arrive at the total supply of $TEAK tokens, we follow the following formula[8]:

$$G(\varrho) = \text{literally just googling the phrase } \varrho$$

$$\zeta = G(\text{"how many cows are in the world"}) \approx 1,500,000,000\text{cows}$$

$$\varsigma = G(\text{"how many steaks does a cow make"}) \approx 430\text{lbs} \approx 195044\text{grams}$$

$$\omega = \text{average steak size} = G(\text{"ikinari steak menu"}) \implies 300\text{grams}$$

$$\tau = \text{total supply} = \frac{\zeta * \varsigma}{\omega} = 975,220,000,000 \text{ \$TEAK}$$

[6] (besides being justification to run an ICO)

[7] An argument could be made for simply using Ether as the medium being staked, but then we wouldn't be able to satisfy *point 1*.

[8] No, the greek letters don't mean anything, I chose the most obscure ones I could find. Please be impressed at my

$$L^{a}Te^{\chi}F\theta\tau^{\alpha^{T^{T^{\iota^{\eta^{G}}}}}}$$

Initial Cutting of Steak (ICS)

The Steak Network would benefit heavily from using the Interactive Coin Offerings[9] algorithm to conduct its ICS, but we aren't yet in a perfect utopia where the IICO protocol is implemented. Until the Interactive Coin Offering protocol is production ready, we'll have to make do with the following ICO strategy:

1. Literally just sending $TEAK to anyone that gives us ETH, at an arbitrary valuation until it's all gone.
2. Donating 100% the proceeds to the Ethereum Foundation and second-layer infrastructure projects.
    - This follows Vitalik Buterin's pledge[10] to donate advisor shares to charity and second-layer infrastrcuture.
    - Steak Network will also follow similar criteria for selecting second-layer projects.

Percent	Project or Charity	Reason
10%	The Ethereum Foundation	Doing Ethereum Stuff
50%	TrueBit Establishment	Protocol Inspiration (aka doing most of the work)
40%	Other Projects	TBD

Note: while this paper is in draft mode, please mention @shrugs to propose a project.

The ISC begins whenever we start it and will end whenever all of the $TEAK is fully distributed, or we have reached the inevitable heat-death of the universe, whichever comes first.

Steak Network Implementation

The Steak network will be implemented as a mobile app, supporting the latest iOS and Android operating systems. It will also function as an ERC20-compatible wallet for interacting with the $TEAK token contract.

$TEAK Wallet

The Steak Network App (the "App") will allow you to become a $TEAK Holder by providing a locally generated secret key and Ethereum address to which you can send $TEAK. Once you are a $TEAK Holder, you can fully interact with the Steak Network.

[9] https://people.cs.uchicago.edu/~teutsch/papers/ico.pdf
[10] https://twitter.com/vitalikbuterin/status/911217245094686720

The Steakchain Feed

The primary screen of the app is the Steakchain feed, where $TEAK Holders act as verifiers. It is an instagram-style, infinitely scrolling set of Cook-submitted Proofs of Steak. You can:

1. "Heart" Proofs of Steak[11] to save them to your personal table,
2. Rate Proofs of Steak[12], and
3. Become Grill Master by challenging a Cook's Proof of Steak.

The Proof Submission Page

$TEAK Holders can also become Cook and submit Proofs to the network for validation. This involves committing two Proofs to the network, one valid and one invalid. In the case of the Steak Network, this means we commit one picture is *is* of a steak, and one picture of anything that is *not steak*. Let it be known that hotdogs are not steak.

The Backseat Griller Crowd Page

$TEAK Holders can join the Backseat Griller Crowd by staking appropriate amounts of $TEAK.

When they have been elected as a Backseat Griller during the Grilling of the Cook, they receive a push notification, informing them of the privilege. They then have until the Backseat Griller timeout to vouch for the validity or the invalidity of the challenged Proof.

The Steak Network presents this as a Tinder-style card stack where Backseat Grillers swipe right to vouch for the validity of a Proof and swipe left to vouch for its invalidity.

~~Backseat Grillers can purchase Steak Network Gold™ to see which steaks have liked them already.~~

Your Steak Table

The Proofs of Steak that you "heart" show up here, where you can add notes and give them nicknames for later reference.

Strategic Partnerships

The Steak Network will also be integrated into Internet-of-Things Grills.

[11] This is to justify our rediculous valuation when we IPO.
[12] Ratings range from "rare" (the best) to "well done" (the worst).

Future Obstacles

Note that due to the Steak Network's use of Proof of Steak, forks are not only possible, but highly encouraged. The Steak Network must also implement cutlery-based slashing conditions for disincentivizing Delegated Proof of Stake protocol violations.

Advisors and Investors

The Steak Network Foundation is proud to be advised by:

- Jackson Palmer, creator of Dogecoin

The Steak Network is supported by:

- Ryan Zurrer, Polychain Capital.

We never actually asked if we could use his name, but there it is:

- Vitalik Buterin, creator of Ethereum

NOTE: Literally anyone remotely interested in being listed here, join #steak-network and mention @shrugs and I'll add you. But you need to come up with your funny bio for the website first. The more absurdist the better.

Conclusion

In summary, we have illustrated Proof of Steak, a protocol capable of computing non-cryptographically-modeled proofs, backed by Delegated Proof of Stake.

We further presented the Steak Network, the canonical implementation of Proof of Steak, powered by the $TEAK token. We detailed the ICS process for ensuring optimal $TEAK distribution, ensuring that the Steak Network is inherently secure from the start.

Acknowledgments

Jason Teutsch for his work on the TrueBit Protocol, as well as the Interactive Coin Offerings protocol.

Wayne Chang for valuable additions, clarifications, and "fork" jokes.

Robbie Bent, Harley Swick, Sina Habibian for valuable feedback.

Dhruv Lutha for joining the Slack channel.