The Journal of Immaterial Science

MISCOMMUNICATION

COMPUTER SCIENCE
Received: 15th September 2022
Revised: 5th October 2022
Accepted: 15th September 2022
DOIOU: 10.BTC.ETH.XRP.BNB

Proof of Wankery: A Novel Consensus Model for the Blockchain

Melon Husk[A*]

Abstract: Proof of Work is killing the planet, Proof of Stake is a pyramid scheme, and other proposed consensus models are either easy to spoof or infeasible to implement. Herein, a new model is proposed: Proof of Wankery (PoWank). PoWank does away with the problems of weighted voting by digital assets or wasted work, and instead awards votes based on an individual's ongoing dedication to the #Web3 lifestyle. As a consensus model, PoWank is shown to offer all of the key benefits of the de facto standard models in use today—including Byzantine fault tolerance and measurement consistency—but at a fraction of the time or cost.

Virtual currency, or "cryptocurrency", comes about when blockchain structures are used to represent the history of transactions of a particular asset type within a closed user group. Given a complete record of all transfers (*"Joe started out with 10 imaginary money, then the next day Joe gave 5 to Jane, and the day after Jane gave 2 to Bob.")* it is possible to calculate the distribution of assets at any point in time (*"How much imaginary money did Joe have on day 3?").*

This can be used to represent an entire trading economy that has zero physical assets. The only requirements are that:

1. The transaction record is true and complete at all times.
2. Either the total number of money/assets is pre-defined, or the rate and method of growth is.
3. The perceived value is such that people will pay real money to buy your fake money at some point.

As a community, CryptoBros have got point 3 down pat. All it took were a couple of tweets about *"going to the moon"*, and regular schlubs all over the planet were scrambling to buy ~~Fake Imaginary~~ Digital Future Money™. But points 1 and 2 are a bit fucked. Because the thing about people on the internet is, they lie.[1]

With nobody trusting each other enough for any one person to be in charge of the transaction ledger, we regressed to a form of governance that is popular with kindergarteners and Silicon Valley tech bros alike: the flat hierarchy, a.k.a. the "everyone can be the boss" approach. And in came the chains of blocks.

Blockchain-based systems have gained significant traction in online communities in recent years, primarily due to the anonymous and inherently decentralised nature of the approach. Every man gets to be the King of his own calm kingdom, and stick it to Big Government while doing so. It's none of The Man's business what kind of bulk knockoff turbo-Viagra™ you're buying from the dark web; that's your prerogative! So there'll be no big banks sticking their noses in here, nosiree.

In a Block Chain, each block represents a transaction between two parties. To add a new block to the chain—and thus make a transaction—a few things have to happen:

1. The sender proposes a transaction, and asserts their enthusiastic consent for it to happen by blessing it with their personal code.
2. The proposed transaction is sent to special inner cabal of users who vote on whether they will vouch for the transaction as legitimate (i.e. nobody is trying to spend money they don't have).
3. If the vote passes, the transaction is "minted", stamped with the fingerprint of the previous transaction in the chain, and then sent out to all connected users.

This results in two important protections: first, nobody can unilaterally declare that someone sent them all their money, and second, history cannot be rewritten (because each block contains the essence of the last). Figure 1 shows an example of varied state between individual users—including both disconnected (Bob) and malicious users (Sally)—which would be easily resolved by the voting process.

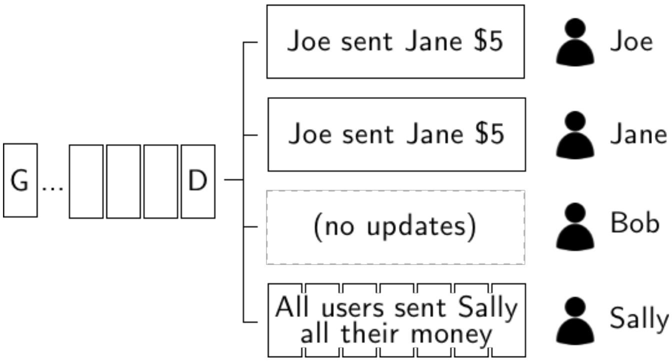

Figure 1: Example of distributed state model. Here, **G** indicates the genesis block and **D** indicates the divergence point (the last point where all users reached consensus).

The overall process is a little bit like if every time you wanted to send 20 bucks to your mate, Parliament had to sit for three days of deliberation to decide whether it was allowed to happen. That's democracy, baby. It's also why the most notorious weakness of cryptocurrencies is the dreaded '51% attack'—because it turns out that majority rule kinda falls apart if the majority of people decide to be a bunch of big meanie doodoo heads and declare that you gave them all your money. So it's a good thing not just anybody can vote.

General Consensus Models

If this imaginary democracy runs on votes, then the consensus models are the shady back-alley deals it took for each "elected" official to get their seat at the table. Yes, every vote is rigged. Yes, even though bad voting can make people's ~~hard earned~~ millions **disappear**. *"That's the fun part"*, they say.

To make sure that not just any regular Joe can rig the vote—and that every vote is rigged just the right amount—every vote

[A] *The Learnstitute, Somewhere in the South Pacific.*
[*] *Corresponding Author contact: www.twitter.com/@melonhusk*

comes at a price. And like with good old-fashioned bribery, you need to be very Goldilocks about it: too high a price and your voting population is no-one, but with too low a price, and even the plebeians could vote. Gross. So you have to play a little hard to get.

The most popular way to buy votes, which all the cool kids use, is the "torching the rainforest" approach:[2] Proof of Work (PoW). In PoW, voting rights are awarded based on a user having demonstrated that they have done a bunch of arbitrarily difficult computation. This means setting your computer on turbo mode for a few hours, crunching numbers that mean nothing. Utter nonsense numbers formed by complex "hashing" algorithms like that shown in (1).

$$\begin{aligned} Ch(E,F,G) &= (E \wedge F) \oplus (\neg E \wedge G) \\ Maj(A,B,C) &= (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C) \\ \Sigma_0(A) &= (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22) \\ \Sigma_1(E) &= (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25) \end{aligned} \tag{1}$$

These steps are interspersed with value rotations and modulo 2^{32} operations, and then the whole lot is repeated 64 times. This is a lot—and a lot of information is lost in the process—so doing it backwards is hard. The only positive is that during this time your PC will double as a pretty effective space heater.

The better the computer, the faster this computation goes, but even the best rig will still take a while. And with every block, the work gets harder.[3] All the hippies complain how *"burning fossil fuel-powered energy to compute utter bollocks is the last thing we need right now"*, but they just need to understand that this is what keeps the plebeians out. Don't they understand how important that part is?

Sadly, sometimes the hippies win. This gave birth to new consensus models like Proof of Capacity—in which your voting rights are secured by demonstrating you have the biggest empty harddrive space, way bigger than the other guy's—or Proof of Stake, which rewards people according to the number of assets they already control from the total pool. That seems fair. Other, more obscure models rely on users just paying for votes, such as in Proof of Burn.

Each of these models fit the criteria for a consensus model in that they are Byzantine fault tolerant (BFT) methods of agreement between distributed and disassociated user nodes.[4] To be BFT, the methods of seeking consensus must be able to overcome:

- **Disconnected nodes**—users which return no response to request for consensus.
- **Malicious nodes**—users which return a bad response to request for consensus.
- **Flakey nodes**—users which at different times return different responses to the same request for consensus.

These mechanisms of verification constitute the 'effort' component in the real-money-to-fake-money exchange (see Figure 2). But they're also just a lot of work, you know? They cost time, or money, or require constant replacement components. And I reckon we can do better. Really, when you think about it, the need for new and innovative consensus models is motivated by simple economics: Proof of Work ledgers (like Bitcoin) made GPUs too expensive, and Proof of Capacity ledgers (like Chia) made SSDs too expensive, and I still need to buy these things occasionally. Woe is me, etc.

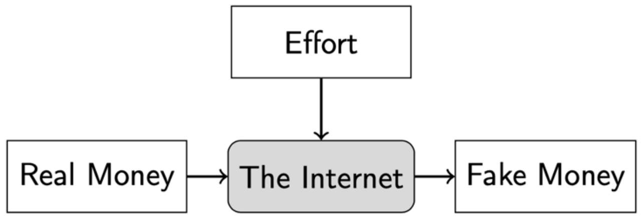

Figure 2: The intricate process by which cryptocurrency is produced by The Internet. Here, 'effort' is an abstract input, whose form may vary between consensus models.

An ideal model should incorporate the strengths of existing models as per the aforementioned criteria, while also making sure to benefit me—the author— the most. That's where this new approach, Proof of Wankery (PoWank) comes in. More detailed disbenefits of the alternatives are laid out in Table 1, clearly showing why the current modes suck and where the proposed approach is called for.

Proof of...	Effort is...	Sucks because...
Work	Wasted energy	We need the planet to live on.
Stake	Hoarding	We want to spend our fake money sometimes.
Capacity	Big harddrives	We want to be able to afford data storage ever.
Burn	Wasted money	;(
Importance	Spending	We don't want to *have* to spend.
Time	Wasted time	The plebeians also have access to time.
Play	Play-to-Pay	We don't want to have to expend actual effort.
Wankery	Indoctrination	It doesn't.

Table 1: A comparison of the mechanisms and disbenefits of consensus models currently in use in public, currency-focused blockchains.

Proof of Wankery

So what if instead of all that poppycock, you instead got access to the secret VIP voting club just by being cool and loving crypto? The dream, right? Well, no more; Proof of Wankery (PoWank) is here to make your dreams a reality. With PoWank, users are given voting weight based on their dedication to the #Web3 cause. So gulp down that pint of Kool-Aid, and get ready to be awarded legitimacy just for being the weird nerd you are.

By applying the patented Klout algorithm[5] to publicly available sources of information such as social media, a Wankery Rating™ can be reliably calculated for a particular user based on the sum of their favourable acts, then discounted by their unfavourable acts. Favourable acts that would result in higher weights in the PoWank system include tweeting about crypto, yelling at strangers who *"just have the wrong idea about crypto"*, posting on Insta about how using crypto made you an overnight millionaire, starting a podcast about crypto, telling random strangers they are *"NGMI"* and to *"HFSP"*, and more.

Unfavourable acts that then result in a loss of trust— and thus lower a user's weighting—include saying anything bad about crypto or crypto fans, acknowledging that digital inequality exists, or getting your apes stolen. Scores are collated as shown in (2), using the complete scoring criteria as shown online at https://cryptowank.com

$$w = \sum_{i=1}^{n} s(post_i) \times \text{bias} \tag{2}$$

Here, w is the voting weight of the user, s is the sentiment score of favourability, and *bias* may be non-zero in cases where cronyism within the network is desired.

The use of PoWank simply requires a user to connect their crypto wallet to their complete online social media presence, which is free and easy. It does kinda eliminate the whole anonymous thing, sure, but that's okay. Daddy Zuckerberg can be discrete. And surely nobody is using this anonymised internet money for anything weird or dodgy, right? (wink)

Regarding fit-for-purpose, PoWank demonstrates the required criteria for an effective consensus model in spades: it turns out even though we hate centralism for our money, only having to check a handful of places to calculate voting weights is fine and dandy. Because social media is ubiquitous and invasive to our poor fleshy brains, there is no such thing as a disconnected node; because it is publicly available, there is no disagreement between nodes; and because it is periodically crawled and archived—mostly by creepy ex-boyfriends—there is no inconsistency in response. Byzantine faults: averted (see Figure 3).

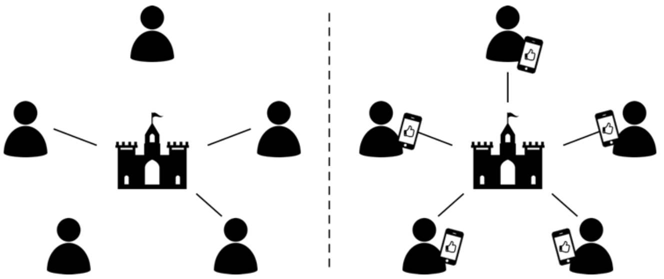

Figure 3: Example of the Byzantine Generals problem without (left) and with (right) social media. Without, the attack is uncoordinated and results in defeat; with, the group chat is going off and they turbo-siege that fort.

Conclusion

Existing consensus models employed in cryptocurrency blockchains are perceived as unfair. They reward acts that have nothing to do with how well one is living the Hashtag Web Three-Point-Oh Lifestyle, and instead pre-occupy miners with immaterial objects or encourage hoarding of money that could be better spent on expensive cartoon pictures of monkeys.

With PoWank, you can do away with this distraction of a middle step, and get straight to milking your performative internet one-upmanship for that sweet, sweet (imaginary) cash money.

Acknowledgements

M. H. wishes to thank all the suckers who have given him real money over the years, in return for the abstract idea of virtual wealth and/or influence.

About the Author

M. H. bought a CompSci Professorship at The Learnstitute on the cheap during the original Dot-Com bubble crash, and has been using it to lord his technology opinions over his friends and colleagues ever since.

Conflicts of Interest

M. H. has a significant stake in cryptocurrency as a concept, and thus will profit from anything you do or say about it, good or bad.

Notes and references

[1] Except for me, now, as I tell you this.

[2] Jingming Li et al. "Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies". In: *Energy* 168 (2019), pp. 160–168.

[3] For example, mining one BTC nowadays requires solving about 3 quadrillion hashes.

[4] Wenbo Wang et al. "A survey on consensus mechanisms and mining strategy management in blockchain networks". In: *IEEE Access* 7 (2019), pp. 328–370.

[5] See https://en.wikipedia.org/wiki/Klout