Proof-by-Location as a Socially Responsible Financial Infrastructure

Donald J. Patterson
Department of Computer Science
Westmont College
Santa Barbara, CA, USA
dpatterson@westmont.edu

Bill Tomlinson
Department of Informatics
University of California, Irvine
Irvine, CA, USA
wmt@uci.edu

***Abstract*—The Proof-of-Work algorithm that underlies Bitcoin and many other cryptocurrencies is well known for its energy-intensive requirements. The Proof-of-Stake algorithm that underlies Ethereum2 and various other cryptocurrencies is less impactful environmentally, but it has a second, looming issue: the problem of wealth inequality. We have developed an alternative to Proof-of-Work and Proof-of-Stake, called Proof-by-Location, that has the potential to address both of these issues. This paper describes Proof-by-Location and a financial platform called Xylem that is based on it. This platform seeks to distribute transaction fees to billions of cryptocurrency "Notaries" around the world (essentially, anyone with a smartphone), who work together to establish a distributed consensus about financial transactions. Using Xylem as a global financial infrastructure could lead to significantly better social and environmental outcomes than existing financial platforms.**

***Index Terms*—cryptocurrency, sustainability, wealth inequality, energy use**

I. Introduction

State-of-the-art cryptocurrencies, and blockchains generally, consume large amounts of energy when they employ Proof-of-Work consensus algorithms. Critics have noted this issue in academic venues [1] and in news articles [2].

In platforms based on the main alternative to Proof-of-Work—Proof-of-Stake—transaction fees reward "wealthy" individuals in exchange for leveraging their currency holdings. As such, Proof-of-Stake-based platforms may be seen as rich-get-richer schemes where wealthy participants are more likely to receive rewards and influence the ecosystem.

This paper proposes an alternative strategy, called Proof-by-Location, that confirms blocks by communicating among agents at particular geographic locations. The core hypothesis explored by this paper is that the speed of light, rather than mathematics, can function as an incontrovertible mechanism for a distributed consensus to emerge in a cryptocurrency platform. The paper also describes the implementation of a platform, called Xylem, that uses Proof-by-Location to create a global payment system.

In response to key concerns about cryptocurrencies, this paper contributes a novel, location-based mechanism for blockchain block validation. Whereas other cryptocurrencies are founded on cryptographic hashes and/or the threat of currency loss, Xylem leverages the inviolability of the speed of light to secure blocks of transactions. This platform could form the basis for a global-scale, environmentally-friendly, economically-redistributive financial platform.

II. Related Work

This section describes existing platforms that Xylem and Proof-by-Location seek to complement or replace, and also details previous research that relates to the technological underpinnings of the proposed platform.

A. Proof-of-Work

The core functionality of the blockchain underlying Bitcoin [3] relies on computers conducting an enormous number of calculations, called "hashes". Bitcoin "miners" pick unconfirmed transactions that have high transaction fees to pack into a space constrained block. The miner adds random nonces to the block until its hash matches a cryptographic signature in exchange for a reward. This mining process is a computationally-expensive and energy-intensive task.

Among the costs to the miners are electricity, hardware, real estate, and network bandwidth. Competition among miners incentivizes faster mining, mining in parallel, and mining with less energy per hash. The algorithm responds to more efficiency by increasing the difficulty of the cryptographic signature. Electricity now dominates the mining cost, entailing the consumption of very large amounts of energy and the emission of large amounts of CO_2 [4].

B. Proof-of-Stake

Ethereum2's Proof-of-Stake [5] reduces energy consumption compared to Bitcoin by allowing only entities with existing wealth to determine which transactions are valid (and thereby earn transaction fees). This platform greatly reduces the number of hashes that need to be calculated, and thus the energy footprint of the platform. The Ethereum Foundation's blog claims that the transition from Proof-of-Work (Ethereum) to Proof-of-Stake (Ethereum2) will result in a 99.95% reduction in energy usage [6]. As such, it goes a very long way toward addressing the problematic energy consumption often discussed as a key shortcoming of cryptocurrencies.

However, Proof-of-Stake has a different problem. The only way to earn transaction fees on a Proof-of-Stake platform is to have existing wealth that one "stakes". Stakers are incentivized

to maintain the integrity of the system because falsifying a block can cause a stake to be forfeited and also reduce general confidence in the currency which the staker has invested in. However, it also means that Proof-of-Stake-based platforms tend to increase wealth inequality. Wealth inequality leads to negative outcomes, such as threatening food security [7] and population health [8].

C. Other Block Validation Mechanisms

Numerous alternatives to Proof-of-Work and Proof-of-Stake have been proposed, including FOAM's similarly-named-but-conceptually-different Proof of Location [9], Proof of Authority [10], Proof of Weight, [10], Delegated Proof of Stake [10], and Proof of Burn [11]. Xylem's Proof-by-Location draws on various aspects of several of these systems, in particular geolocation (similar to FOAM), the selection of a subcommittee (similar to the Pool in Delegated Proof of Stake), and the requirement to have registered as a Notary on the blockchain (similar to an aspect of Proof of Authority). To distinguish our work from FOAM's Proof of Location, we note that FOAM's "Zone Anchors" (radio beacons) require triangulation via custom hardware to enact geolocation, thus creating a significant barrier to wide-scale adoption. In addition, FOAM's primary goal is to verify location, rather than to use location to validate blocks of financial transactions. Proof by Location was discussed by Oppliger [12], but our identification of speed of light as a mechanism by which to enact location verification, and our connection to the cryptocurrency domain were not included in Oppliger's discussion. There here have been other efforts to provide computational location verification, e.g., [13], [14]; we build on elements of several of these systems in the Proof-by-Location mechanism described below.

III. Methods

In the research process described here, we engaged in iterative design and implementation of a software system. Through this process, we converged on the design of a platform, with Proof-by-Location at its center, that enables the speed of light to serve as the core mechanism through which a distributed consensus may emerge. This iterative design and implementation unfolded across the course of 16 months from April 2021 through August 2022.

IV. Results

This section describes the core operation of Xylem and Proof-by-Location. See Figure 1 for a summary of the process.

In Xylem, there are three main "roles" for computational entities that coordinate the movement of funds. The base role is the "Notary", a low-computing-requirement entity meant to be operated on potentially billions of smartphones and other devices, managed by (and producing income for) billions of individuals. A subset of Notaries are "Keepers" (an abbreviation of "BookKeepers"); this role serves a similar function to Miners in Proof-of-Work or Proof-of-Stake, but with different responsibilities. There are two types of Keepers: TransactionMakers (who coordinate the connection between sender and recipient) and BlockCheckers (who assemble transactions into blocks and work with Notaries to validate the blocks).

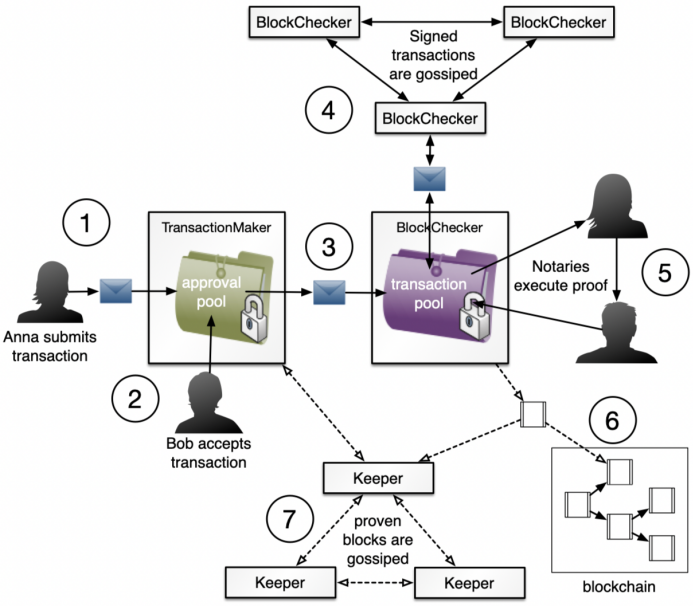

Fig. 1. In the Xylem transaction process, a sender, Anna, initiates a transaction (1) by contacting a TransactionMaker (TM), who confirms that the recipient, Bob, wants to receive it (2). (see Figure 2 for detail.) TM sends it to a BlockChecker (BC) (3) who gossips it out to other BCs (4). A BC works with Notaries (5, see Figure 3) to create a location-based proof for a block of transactions. This proven block becomes part of that BC's representation of the blockchain (6), and is gossiped out to the rest of the Keepers (TransactionMakers and BlockCheckers) (7).

A. Making a transaction

When a person, Anna, (see Figures 1 and 2) wishes to send Xyla (a Xylem coin) to another person, Bob, she first sends information about the recipient and amount to a TransactionMaker, TM, who will coordinate the transaction. Anna creates a transaction, T, by verifying that she has cryptographic rights to previous transactions (UTXOs) by using her private key. Additionally she signs T to validate that it originates from her and sends the transaction to TM who confirms the transaction's integrity.

Xylem uses a two-part transaction-signing process, in which transactions are signed by both senders and recipients. This process reduces accidental loss of currency (compare to Bitcoin, for which there are thousands of Google hits for "Bitcoin sent to wrong address"), and also requires that recipients accept responsibility for currency sent to them (which supports "Know Your Customer" (KYC) laws [15] and reduces implicating recipients without consent).

Xylem will have a transaction size of 1KB. Each transaction will share the characteristics of a Bitcoin transaction (sender signature, recipient public key, inputs, and outputs, typically 300-400 bytes in total), with additional space for recipient signature, TransactionMaker signature, and a note field.

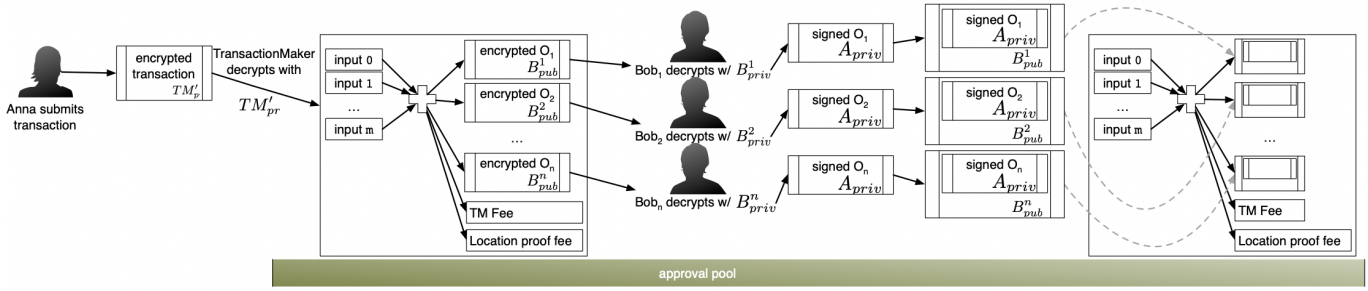

Fig. 2. How a Xylem transaction receives approval from recipients.

B. Approval Pool

The approval pool consists of the set of transactions that a TransactionMaker is holding while it waits for the recipient(s) of a transaction to approve the exchange.

When Anna creates her transaction, she signs each element of her output set with her private key. Then she encrypts each element of her output set with the public key of the recipient(s), embeds it in the transaction T, and then encrypts T with the public key of the TransactionMaker TM. See Figure 2.

The result is a transaction that must first be received and decrypted by TM. TM validates the inputs and still partially encrypted structure of the transaction and returns to Anna a set of URLs that she can provide to the output recipient(s). The TM then adds the transaction to its approval pool.

The output recipient(s), $B_0 \dots B_{n-1}$ use the URLs to receive their encrypted output, O_i from TM. Each recipient decrypts the output and returns it to TM. TM replaces the encrypted output, O_i, with the decrypted output. Because the decrypted output originated with Anna and was encrypted by her, it can be digitally signed by her as well, ensuring that the decrypted output is what Anna intended.

Once all recipients have provided the decrypted output, the TransactionMaker can then completely validate the transaction to ensure that the inputs are unspent, and that the sum of the inputs is greater than the sum of the transaction outputs (with the remainder providing a later Block Fee).

C. Location Pool

After receiving approvals from each of the recipients, TransactionMaker TM sends the signed transaction to a BlockChecker BC. BC stores the transaction in its location pool. The location pool consists of the set of transactions that are waiting to be assembled into blocks by BlockCheckers and notarized by Notaries.

BC then gossips the transaction to other BlockCheckers, who store it in their own location pools.

D. Block Notarization

Each BlockChecker takes the hashes from the previous blocks in the blockchain and converts them into a set of latitude and longitude locations at various targets points around Earth, $T_0 \dots T_{m+n-1}$ (see Section IV-G).

The n BlockCheckers closest to targets 0 through n-1, and the m Notaries closest to targets n through n+m-1 form a "subcommittee" that is responsible for notarizing the next block. BlockChecker BC_0 who is closest to target T_0 is the "lead BlockChecker" for the next block. Hereafter, we call this BlockChecker T_0BC_0, meaning the BlockChecker closest to T_0. Similarly, the closest BC to target T_1 will be called T_1BC_0, the BC second-closest to target T_0 will be T_0BC_1, etc.

Having a shared, comprehensive model of which BlockCheckers and Notaries are available to validate blocks (based on which were previously registered on the blockchain) allows for only a single optimal notarization pipeline to exist, thus removing the need for competition (as there is in the Proof-of-Work process underlying Bitcoin) that might otherwise lead to a proliferation of energy use. See Section IV-F below for how the platform recovers if T_0BC_0 is unavailable or dishonest.

All BlockCheckers in the subcommittee perform speed-of-light confirmation on the locations of all other entities in the subcommittee. The BlockChecker sends a network message to each member of the subcommittee and expects a reply within 1.25-3.33 times the time it would take light to travel to that entity and back. (This range was established based on typical network latencies between major cities of the world [16].) All BlockCheckers then exchange "EigenTrust" reports, assessing their degree of trust in the location of all other subcommittee members [17]. Based on the results of the location validation, all BlockCheckers then calculate EigenTrust values for all members of the subcommittee.

T_0BC_0 then decides on a proposed allocation of block fees among the subcommittee members and creates a transaction with no inputs and one output per honest subcommittee member. Entities get paid in proportion to their EigenTrust score. This payment process provides an incentive for all entities to report their location correctly on the blockchain; if they misrepresent themselves, they will fail in the location validation process, and will not get paid. A zero fee output is given to any entity below an agreed-upon EigenTrust threshold (i.e., an entity that was non-responsive or at the wrong spot), equivalent to being mistrusted by at least 30% of the subcommittee BlockCheckers. If an entity is the recipient of 3 zero-value outputs in Block Fee transactions in the blockchain

("three strikes"), it is permanently excluded from future block notarization efforts.

E. Notarization Chain

To produce a notarization chain, T_0BC_0 determines an ordered series of other subcommittee members (to optimize signatures in as short a time as possible), and sends it out to the each of the BlockCheckers in the subcommittee as block B. T_0BC_0 sends B to each of subcommittee BlockCheckers, with each BlockChecker signing it and sending it out to the Notaries nearest to them, who in turn sign the block and return it to that BlockChecker, who then returns it to T_0BC_0[1]. The lead BlockChecker must accumulate signatures from at least half of the subcommittee members. Since these subcommittee members are located all over the world, his step creates a delay that functions to prevent competing blocks from being viable alternatives in the blockchain history. This delay is similar to the one in Bitcoin that prevents double-spending attacks.

Each of these BlockCheckers decides if T_0BC_0's allocation of fees is close enough to their own EigenTrust calculations. If they support it, they sign the block and forward it to the next entity in the notarization chain as described above. If they oppose it, they send a message to T_1BC_0, who is next in line to be the lead BlockChecker, to let that BlockChecker know that they could potentially support an alternative block proposed by T_1BC_0.

F. Recovery Modes

If T_0BC_0 fails at any aspect of the above, T_1BC_0 may also run its own notarization process. The process is identical to the above, but T_1BC_0's timestamp must include a 0.5s lag (which will be checked by other Keepers in the gossip process). Since T_1BC_0 has real-time information about whether T_0BC_0's notarization is likely to succeed (since it's part of the EigenTrust process and gets messages from non-supporters of T_0BC_0's notarization chain), it can decide whether or not to spend its time on a competing chain, thus reducing the frequency of redundant computational activity. Continuing this premise, any T_NBC_0 may start a chain, as long as they include a lag of length $N/2$ seconds. T_0BC_1 may start a chain as well, involving $T_1BC_1...T_NBC_1$, but it must include a 1 second lag. Similarly, T_NBC_M may begin a chain with $delay = (N/2 + M)$. And if T_0BC_0 was not able to assemble a 50% quorum from among the subcommittee, it may also proceed with a 40% quorum and a 1 second lag. These various possible pathways ensure that there is a single preferred notarization chain (T_0BC_0 + 50% quorum), and hence there is minimal competition and easy agreement in the gossip process, but that there are nevertheless a very large number of possible ways for the system to recover if one or more entities are missing or lying.

[1]The block is returned to a BlockChecker between every Notary to avoid firewall restrictions.

G. The Geographic Hash Function

An important part of Proof-by-Location is the ability to randomly choose a point on the Earth. To achieve this goal we use a one-way hash function that resolves to geographic locations. This "geographic hash function" takes a set of bytes as input and outputs a latitude and longitude pair. Our hash function has the following properties: All decentralized participants algorithmically agree on a choice of inputs so that the outputs will be consistent; in order to prevent precomputing, the inputs are unknowable before the completion of the previous block; and the hash function deterministically selects N different locations.

1) Hash Input: Our input is derived directly from the blockchain. When $block_m$ is being confirmed, the algorithm relies on a SHA256 double hash of $block_{m-2}$ concatenated with a 16-bit integer index and finally concatenated with a SHA256 double hash of $block_{m-1}$. The resulting bytes are together double-hashed and the result is interpreted as a 256-bit integer[2]. We then create a uniformly distributed random number on $[-90°, 90°)$ by scaling it by $INTMAX_{256}$.

$$\begin{aligned} a_i &= SHA256(SHA256(block_{m-2})) \\ b_i &= SHA256(SHA256(block_{m-1})) \\ c_i &= SHA256(SHA256(a_i \cdot i \cdot b_i)) \\ lat_i &= (c_i/INTMAX_{256} - 0.5) * 2 * 90° \end{aligned}$$

In a similar way we can obtain a longitude that varies between $[-180°, 180°)$. We reverse the block order for this quantity.

$$\begin{aligned} d_i &= SHA256(SHA256(b_i \cdot i \cdot a_i)) \\ long_i &= (d_i/INTMAX_{256} - 0.5) * 2 * 180° \end{aligned}$$

This result is a one-way hash function that produces the same outputs given the same inputs.

Using Archimedes' Hat-Box Theorem we can then use these two random numbers to choose a location coordinate randomly on a sphere. Those coordinates can be mapped to a physical location using the WGS-1984 projection model.

Since ∼71% of the planet is ocean, choosing a random location on the planet would frequently end up in the ocean, and the nearest Notary would typically be on the coast of the nearest land mass, thus heavily biasing the algorithm in favor of coastal locations. Therefore, in practice passing this location through a kernel function that remaps the uniform spherical location to a human-centric distribution will likely be necessary. In addition, the kernel may also remap target locations for environmental purposes (e.g., preventing targets from appearing in locations with low population densities (determined by the density of Notaries), which would align with ecological restoration goals [18]). Without loss of generality, however, such a function serves to randomly choose locations on the Earth.

[2]Like bitcoin we use double SHA-256 hashes, but recognize that the rationale for the choice of *double* hashes is not clearly settled.

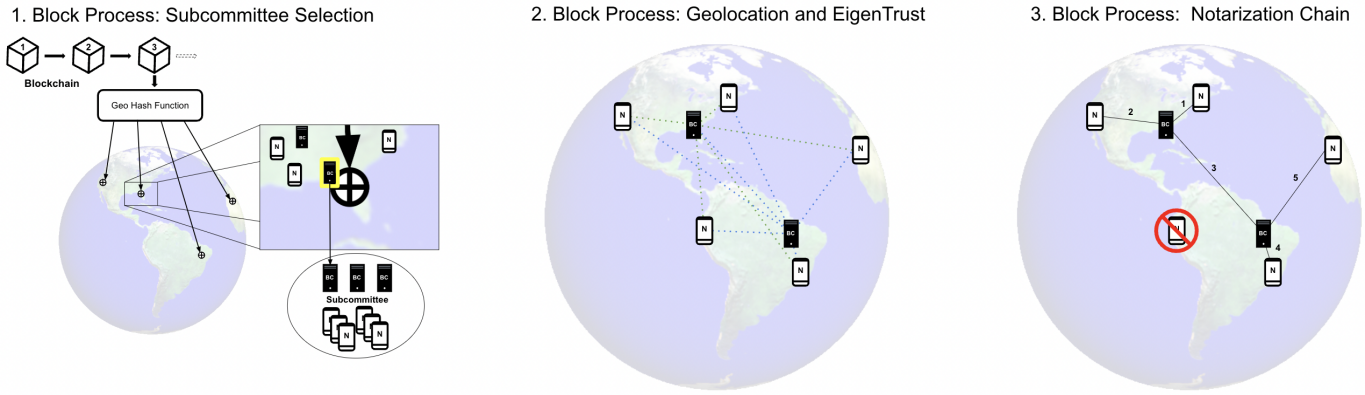

Fig. 3. In Step 1, all Notaries perform a Geographic Hash Function to identify agreed-upon Targets ($T_0 ... T_N$) located around the world. The closest BCs to each of the first several targets, and the closest Notaries (N) to each of the later targets, all become members of the subcommittee. In Step 2, the BCs in the subcommittee perform location verification on all other members of the subcommittee, and use the EigenTrust algorithm to determine if any subcommittee members are lying about their location. In Step 3, the subcommittee BCs work together to have a block of transactions signed by each non-lying subcommittee member in turn. Thereafter, the closed block is gossiped to all other Keepers (TMs and BCs).

V. Evaluation

We have conducted initial quantitative analyses and simulations of the impacts of Xylem and they support the theorized results described below.

The environmental impacts of the real system promise to be greatly reduced compared to Bitcoin and other Proof-of-Work-based system for two reasons. First, the design of the system eliminates the need for quintillions of hashes to happen every second [19]. Second, electronic waste from the Xylem platform will be much lower than other cryptocurrency platforms, since beyond the baseline required capabilities, there is no incremental benefit to larger computational capabilities.

The platform should also work as a force to reduce wealth inequality rather than exacerbate it. The modes of fee distribution are consistent with the nature of each platform: the large majority of transaction fees in Xylem goes to Notaries, that is, anyone with a smartphone (90% of the population by 2025 [20]), whereas transaction fees in the other platforms are distributed to wealthy people who control expensive computing power (Bitcoin), who have Ether to stake (Ethereum2), or proportional to stock ownership in a publicly traded company (Visa). Since Xylem essentially distributes fees to random participants it works toward ameliorating wealth inequality.

VI. Discussion

Xylem builds on many properties of existing cryptocurrencies: decentralization, SHA256 hashes, public/private key encryption, etc. Nevertheless, any platform passing around large amounts of money is highly likely to be the target of attacks. Here we detail a selection of common attacks and misbehavior that may occur in a large-scale Xylem deployment, and how Xylem protects against them.

A. 51% attack (reorg)

To perform a 51% attack on a Proof-of-Work platform, one must take control of 51% of the computing power in the financial network, a challenging task. To perform a 51% attack on a Proof-of-Stake platform, one must take control of 51% of the financial assets in a system, also difficult. To perform a 51% attack on a Proof-by-Location platform, one must take control of computers in 51% of the unique locations around the world. We argue that, given the difficulties of real-world logistics: navigating local politics, local regulations, and various other local conditions, it is more difficult to perform a 51% attack on Proof-by-Location than either Proof-of-Work or Proof-of-Stake. To create an alternative sequence of blocks rooted in a common ancestor (the classic "double-spend" attack), a bad agent would need to take control of the specific set of BlockCheckers and Notaries randomly chosen by the Geographic Hash Function. They would also have to control 51% of all Keepers (TransactionMakers and BlockCheckers) to succeed in propagating an alternative block history that was at odds with the more advanced block-chain already held by most of the Keepers following the first-spend .

B. Pseudospoofing (collect fees)

One key attack that is relevant to the Xylem ecosystem is pseudospoofing[3]. Pseudospoofing is a known concern in location-based systems [22], [23].

In a pseudospoofing attack, one entity presents itself as multiple entities. Without appropriate defenses, a pseudospoofing attack on a Proof-by-Location-based platform could allow an attacker to collect fees for each of their virtual identities by claiming that they are geographically distributed. The Proof-by-Location system, using speed of light location verification within the subcommittee, and EigenTrust to merge the verifications across BlockCheckers, arrives at a shared decision grounded in real-world physical phenomena. This allows the platform to converge on an accurate consensus about which identities are lying about their location. Once identified, the malicious agents' identities can be excluded.

[3]We use the term "pseudospoofing" attack to replace an equivalent term, "Sybil" attack [21], because it avoids associating an inherently malicious behavior with a medical condition, Dissociative Identity Disorder.

C. Pseudospoofing (flash)

A second variant of a pseudospoofing attack (and related to the 51% attack) involves trying to double-spend by rapidly taking over the majority of nodes on the Xylem platform [21]. To address this issue, after the first 1,000 blocks, the platform requires at least 80% of BlockCheckers in the notarization chain to have notarized before. If that doesn't happen through the default subcommittee selection process, the Keepers must go back through the targets and identify the second closest BlockChecker for any targets where the initially-selected subcommittee member has not yet performed a successful notarization, until the 80% threshold is reached. This requirement prevents rapid introduction of new BlockCheckers.

D. Pseudospoofing (playbook)

A playbook attack entails creating a large number of entities over time, and having them participate as valid actors in the ecosystem [21] but then, in concert, changing behavior and acting maliciously. Xylem prevents this type of attack by permanently banning any Notary that has been part of past subcommittees and been identified as a liar on three separate occasions. This feature disadvantages participants with intermittent network availability, since not responding to a location verification request for any reason is treated as a strike against the Notary. However, since the Xylem platform relies on rapid responses from its Notaries, repeated lack of responsiveness is problematic in itself for a Notary's future participation. Additionally, Notaries may still spend past earnings, and may re-add themselves with a different account; the only harm they will experience is that they will not count toward the 80% threshold described in the previous section until they have succeeded in participating successfully in a notarization chain.

VII. Conclusion

This paper has presented a novel mechanism for enabling a distributed global consensus to confirm the integrity of digital financial transactions. The associated platform, Xylem, is designed to have lower environmental impacts than existing financial infrastructures such as Bitcoin, Ethereum, Ethereum2, and Visa. Notably, it is also designed to distribute transaction fees geographically to support broader global participation. The tendency for existing Proof-of-Stake algorithms to support wealth centralization is a critical and underappreciated shortcoming of previous approaches that our system corrects.

Financial systems are an important part of the global sociotechnical infrastructure and any changes to them should be justified from both a social and a technical perspective. We therefore propose the Xylem platform as a step toward providing a better user experience, a better economic infrastructure, and a better social mechanism by which people engage in payments around the world.

Acknowledgments

We thank Ethan Bañez, Evelyn Chin, Hayden Freedman, Nicole Sullivan, and Ishan Varney for their contributions, and Adrien Berthelot and the reviewers for their feedback.

Disclaimer

The authors hold positions in several crypto- and fiat currencies.

References

[1] C. Mora, R. Rollins, K. Taladay, M. Kantar, M. Chock, M. Shimada, and E. Franklin, "Bitcoin emissions alone could push global warming above 2 C," *Nature Climate Change*, vol. 8, no. 11, 2018.

[2] J. Huang, C. O'Neill, and H. Tabuchi, "Bitcoin uses more electricity than many countries. how is that possible?" *The New York Times*, 2021. https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," May 2009. http://www.bitcoin.org/bitcoin.pdf

[4] J. Hinsdale, "Cryptocurrency's dirty secret: Energy consumption," *State of the Planet*, 2022. https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy

[5] V. Buterin, "Ethereum whitepaper," 2014. https://ethereum.org/en/whitepaper/

[6] C. Beekhuizen, "Ethereum's energy usage will soon decrease by 99.95%," *Ethereum Foundation Blog*, 2021. https://blog.ethereum.org/2021/05/18/country-power-no-more/

[7] K. Simpkins, "Amid climate change and conflict, more resilient food systems a must, report shows," *CU Boulder Today*, 2022. https://www.colorado.edu/today/2022/07/15/amid-climate-change-and-conflict-more-resilient-food-systems-must-report-shows

[8] M. Curran and M. C. Mahutga, "Income inequality and population health: A global gradient?" *Journal of Health and Social Behavior*, vol. 59, no. 4, pp. 536–553, 2018, pMID: 30381957. https://doi.org/10.1177/0022146518808028

[9] Foamspace Corp, "FOAM," 2022, accessed August 7, 2022. https://www.foam.space/

[10] Bitstamp, "You've heard of Proof-of-Work and Proof-of-Stake. What else is there?" 2021. https://blog.bitstamp.net/post/youve-heard-of-proof-of-work-and-proof-of-stake-what-else-is-there/

[11] K. Karantias, A. Kiayias, and D. Zindros, "Proof of burn," 2020. https://iohk.io/en/research/library/papers/proof-of-burn/

[12] R. Oppliger, *Contemporary cryptography*, ser. Artech House computer security series. Artech House, 2005.

[13] S. Laki, P. Mátray, P. Hága, T. Sebők, I. Csabai, and G. Vattay, "Spotter: A model based active geolocation service," in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 3173–3181.

[14] B. Wong, I. Stoyanov, and E. G. Sirer, "Octant: A comprehensive framework for the geolocalization of internet hosts," in *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation*, ser. NSDI'07. USA: USENIX Association, 2007, p. 23.

[15] Dow Jones, "Understanding the Steps of a "Know Your Customer" Process," 2022, accessed August 19, 2022. https://www.dowjones.com/professional/risk/glossary/know-your-customer/

[16] WonderNetwork, "Global Ping Statistics," 2022, accessed August 7, 2022. https://wondernetwork.com/pings

[17] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," in *Proceedings of the 12th International Conference on World Wide Web*, ser. WWW '03. New York, NY, USA: Association for Computing Machinery, 2003, p. 640–651. https://doi.org/10.1145/775152.775242

[18] E. Wilson, *Half-Earth: Our Planet's Fight for Life*. Liveright, 2016. https://books.google.com/books?id=gft1CQAAQBAJ

[19] coinwarz.com, "Bitcoin hashrate chart," 2022, accessed August 31, 2022. https://www.coinwarz.com/mining/bitcoin/hashrate-chart

[20] A. Turner, "How many smartphones are in the world?" 2022. https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[21] B. Levine, C. Shields, and N. Margolin, "A Survey of Solutions to the Sybil attack," *Technical Report of Univ of Massachussets Amherst*, vol. 2006–052, 11 2005.

[22] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," 05 2014, pp. 1232–1239.

[23] P. Jiang, H. Wu, and C. Xin, "DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network," *Digital Communications and Networks*, 2021. https://www.sciencedirect.com/science/article/pii/S2352864821000663