Title

Xylem: An Energy-efficient, Globally Redistributive, Financial Infrastructure Using Proof-by-Location

Journal

Distributed Ledger Technologies Research and Practice, 3(3)

ISSN

2769-6472

Authors

Patterson, Donald Jay
Tomlinson, Bill

Publication Date

2024-09-30

DOI

10.1145/3653680

Xylem: An Energy-Efficient, Globally-Redistributive, Financial Infrastructure using Proof-by-Location

DONALD J. PATTERSON*, Westmont College, USA
BILL TOMLINSON*, University of California, Irvine, USA

The Proof-of-Work algorithm that underlies Bitcoin, Ethereum_W[1] and many other cryptocurrencies is well known for its energy-intensive requirements. The Proof-of-Stake algorithm that underlies Ethereum 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. In this paper, we demonstrate that this platform can scale to more than 3.9 trillion transactions per year (more than triple the number of digital payments per year currently occurring). We show a reduction of electricity usage per transaction of 99.9999914% compared to Bitcoin, 99.999905% compared to Ethereum_W, 99.83% compared to Ethereum, and 95.9% compared to the Visa financial services company. We demonstrate that this platform would have a redistributive rather than consolidatory effect on wealth compared to any of these platforms, leading to a source of income for more than 1 billion people around the world, including more than 110 million in the bottom 10-20th percentile by income, with income for that group equivalent to 8.8 million full-time jobs. Finally, this currency provides a positive, non-compulsory mechanism for shaping human habitation patterns in ways that can slow global biodiversity loss and enable ecological restoration. Using Xylem as a global financial infrastructure could lead to significantly better social and environmental outcomes than existing financial platforms.[2]

CCS Concepts: • **Social and professional topics → Sustainability**; • **Information systems → Digital cash**; • **Networks → Location based services**.

Additional Key Words and Phrases: Cryptocurrency, Bitcoin, Ethereum, blockchain, sustainability, wealth inequality, energy use

ACM Reference Format:
Donald J. Patterson and Bill Tomlinson. 2022. Xylem: An Energy-Efficient, Globally-Redistributive, Financial Infrastructure using Proof-by-Location. *Distrib. Ledger Technol.* 1, 1 (March 2022), 29 pages. https://doi.org/XXXXXXX.XXXXXXX

---

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

[1] On approximately Sept. 15, 2022 "Ethereum" using Proof-of-Work consensus transitioned to using a Proof-of-Stake consensus and maintained the original name. A hard fork using the original Proof-of-Work algorithm happened at the same time. We refer to the original system and the hard fork as Ethereum_W (ETHW) and the post-merge Proof-of-Stake system as Ethereum (ETH)

[2] Portions of this article are derived from an earlier conference paper [61].

Authors' addresses: Donald J. Patterson, Westmont College, Mathematics and Computer Science, Santa Barbara, CA, 93108, 955 La Paz Rd, USA, dpatterson@westmont.edu; Bill Tomlinson, University of California, Irvine, Informatics, Irvine, CA, 92697-3440, 5068 Bren Hall, USA, wmt@uci.edu.

2769-6472/2022/3-ART $15.00
https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Broad adoption of state-of-the-art blockchains that employ Proof-of-Work consensus algorithms cause those blockchains to consume large amounts of energy. Critics have noted this issue in academic publications (e.g. [54]) and in news articles (e.g. [35]).

In platforms based on the main alternative to Proof-of-Work, Proof-of-Stake, instead of consuming large amounts of energy, transaction fees reward wealthier 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 benefit from financial incentives and also to influence the ecosystem. Critics have flagged the substantial wealth inequality that exists in cryptocurrencies [71–73], with Bitcoin having a Gini index of 88 [72] and Ethereum having a Gini index of 76-91 [71], compared to an average across the world's nations of 37.6 [102] (with a higher Gini index indicating greater wealth inequality, on a scale from 0 to 100).

This paper proposes a novel 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. The paper also describes a model implementation of a platform, called Xylem, that uses Proof-by-Location to create a global payment system. By redistributing transaction fees to anyone with a smartphone around the world, the platform may provide a valuable source of income for large numbers of people.

While computational currency systems do not share the intrinsic value that commodities such as copper or grain carry, humans have a long history of working with currencies based on trust in a system (fiat currencies based on trust in a government [70], cryptocurrencies based on trust in a computational system [59]) rather than on intrinsic value. There are already contexts around the world where mobile phones provide the underpinnings for the exchange of value [52]. We imagine that Xylem may have an easier time gaining broad global acceptance because it creates a context in which billions of people have an opportunity to earn income through it, differentiated from most human financial systems where billions of people are excluded from it [43].

We propose that Xylem and Proof-by-Location could address key concerns that have been expressed about cryptocurrencies, and could form the basis for a global-scale, environmentally-friendly, economically-redistributive financial platform. This paper describes the details of this platform and reports the results of calculations that support our claims.

2 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.

2.1 General blockchain principles

The fundamental architecture of cryptocurrencies are encapsulated in their blockchain technology, a decentralized and distributed digital ledger employed to record transactions across numerous computers in a way that ensures the security and integrity of the data. Most public blockchains (e.g., Bitcoin and Ethereum) operate on a peer-to-peer network, utilizing cryptographic principles to ensure the authenticity and immutability of the transaction data. Although each system varies in the exact details, frequently the blocks that comprise the chain contain a list of transactions, a reference to the previous block (hence "chain"), and a unique identifier known as a cryptographic hash. Ethereum additionally includes information to define, execute, and validate smart contracts. [14] The decentralized nature of public blockchains is instrumental in eliminating the need for a central authority, thereby fostering a system where trust is established through consensus algorithms such as Proof-of-Work and Proof-of-Stake.

The operational mechanics of the Bitcoin blockchain are underpinned by the process of “mining”, which entails the validation and verification of transactions by network nodes through solving complex, albeit randomized, mathematical problems. [56] A crucial component of this process is the nonce—a random value that miners adjust to find a hash value below a target number set by the network. The Proof-of-Work process, which involves varying the nonce and computing the hash of the block’s contents, is resource-intensive. The first miner to find a hash value below the target broadcasts the new block to the network (using a strategy known as “gossiping"), and upon verification, the block is appended to the blockchain in a linear, chronological order, and the transactions within the block are considered confirmed. The miners are then rewarded with newly created Bitcoins and transaction fees, incentivizing the maintenance and security of the network. The inherent design of the blockchain ensures that once a block has been added to the blockchain, the information it contains is resistant to modification.

A different kind of cryptocurrency and cryptopayment system called Central Bank Digital Currencies (CBDCs) are created and managed by government entities. These CBDCs are similar to fiat currencies but include the audit trail of blockchain-based systems. Decentralization is rarely a feature that CBDCs consider important and alternatively are often implemented as non-public and permissioned systems. This changes the calculus of energy consumption and eliminates the expectation of earning fees for closing blocks. These properties place CBDCs outside the scope of this article. Other complimentary research has examined the impact of CBDCs on the citizens who would be using them [57] Examples of CBDCs include the Bank of Canada’s digital dollar [58], and the Brazilian “DREX" [69]. Similar initiatives which are not strictly CBDCs include a French prototype that examined tracking securities via the Hyperledger system [25] and El Salvador’s official adoption of Bitcoin as legal tender. [2]

2.2 Proof-of-Work

The core functionality of the blockchain underlying Bitcoin [56] 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 [34].

2.3 Proof-of-Stake

Ethereum’s Proof-of-Stake [14] 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 ($\mathrm{Ethereum_w}$) to Proof-of-Stake (Ethereum) has reduced energy usage by 99.95% [5]. 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 in which the staker has invested. However, it also means that Proof-of-Stake-based platforms tend to increase wealth inequality. Wealth inequality leads to negative outcomes, such as food insecurity [81] and lowered population health [20]. Inequality also tends to "go hand in hand with increased ecological degradation." [65]

2.4 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 [29], Proof of Authority [10], Proof of Weight, [10], Delegated Proof of Stake [10], and Proof of Burn [40]. 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 [60], 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., [46, 100]; we build on elements of several of these systems in the Proof-by-Location mechanism described below. Our system intentionally does not attempt to prove the location of participants, but more simply to prove that self-reported locations are not inaccurate given the timing of network communications. We therefore intentionally adopt the terminology Proof-*by*-Location vs. Proof-*of*-Location. An overview of many of the complexities of and adversarial attacks against using network timing to ascertain and prove location can by found in Md Mamunur Rashid Akand's thesis. [1]

2.5 Sustainability Impacts of Blockchain Systems

The sustainability impacts of blockchain systems have been studied extensively over the past years, with a range of concerns having been raised, including energy usage, CO2 emissions, and electronic waste. For a review of such concerns, please see [6, 94]. Blockchain systems have been used to address sustainability concerns in a variety of domains, including agriculture [51], supply-chain management [7], power distribution [41], smart contracts [84], and vehicular networks [93]. There is also recent evidence that some blockchain-based business models may support global sustainability. [32]

Most relevant to this work, the carbon footprint of existing blockchain systems is often very high. [5, 77] Additionally, cryptocurrencies appear to exacerbate wealth inequality, a substantial issue in terms of social sustainability. [71–73] In the work described below, we seek to demonstrate a new model of a blockchain system that provides substantial advantages for both environmental and social sustainability compared to the state of the art.

3 METHODS AND SYSTEM DESIGN

In the process described below, we engaged in an iterative design, prototyping, and evaluation process to produce 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 research unfolded across the course of 16 months from April 2021 through August 2022.

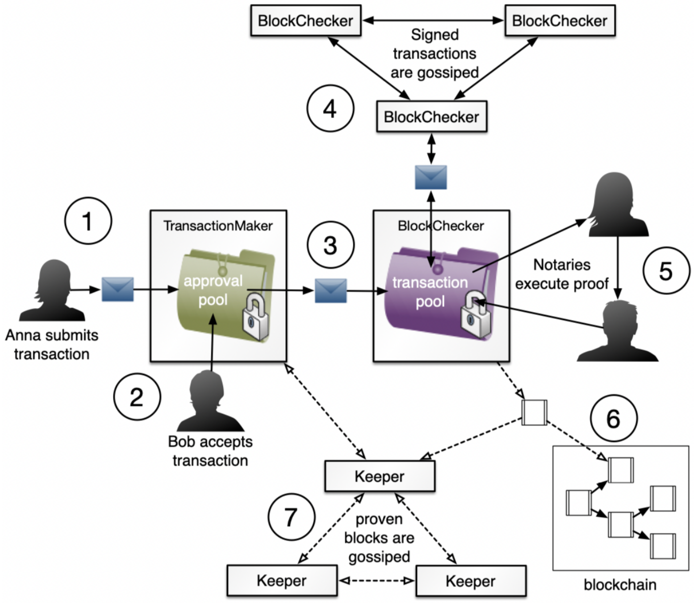

Fig. 1. In the Xylem transaction process, a sender, Anna, initiates a transaction (1) by contacting a TransactionMaker (TM), who confirms that the recipient, Bob, wants to receive it (2). (see Figure 2 for detail.) TM sends it to a BlockChecker (BC) (3) who gossips it out to other BCs (4). A BC works 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).

To assess these prototypes, we conducted a series of numerical calculations and agent-based simulations to confirm the viability and likely impacts of Xylem if deployed at scale. We researched the associated academic literature, independent analyses, news reports, and whitepapers to determine the relevant parameters for the calculations of the prototypes and several existing financial platforms. Our calculations for the final prototype can be seen in detail here: https://docs.google.com/spreadsheets/d/1NuzAro7FSX-xRFWpyi7ePsGUIeFqva88ur3XBJ3jTeU.[3]

Our approach necessarily is limited in its generalizability because it is, at its core, a model-based approached. Any system that is implemented as a real-deployment will encounter unexpected design challenges that weren't accurately assessed in the modelling process, weren't considered at all, or more perniciously, didn't exist until a deployed system is deployed (e.g., any range of potential adversarial technologies like the Bitcoin Dust attack[4]). Nevertheless, before proceeding with a real-world deployment of this system, it is prudent to analyze the parameters of the design as we do in this article.

Here, we present a description of 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

---

[3] the source code is available on request.

[4] A dust attack sends many small quantities of cryptocurrency to an address in an attempt to break anonymity or decrease system efficiency in various ways.

on 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).

3.1 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 unspent transaction outputs (UTXOs) from previous transactions 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 [22] and reduces implicating recipients in a financial exchange without their consent).

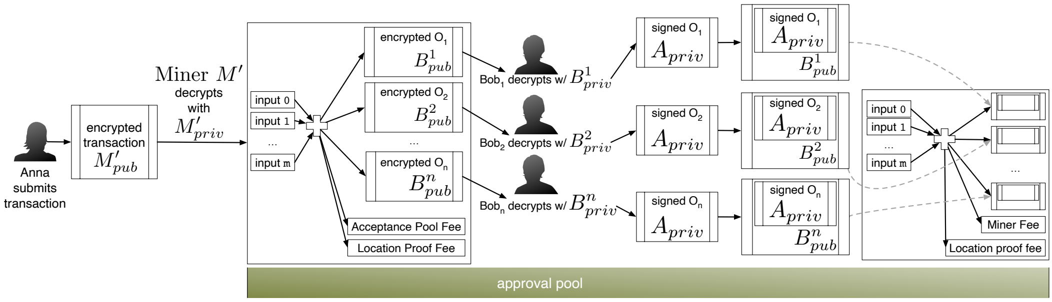

Fig. 2. How a Xylem transaction receives approval from recipients.

Xylem has a transaction size of 1KB. Each transaction shares 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.

3.2 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), $B_0 \dots B_{\beta-1}$ use the URLs to receive their encrypted output, O_i, from TM. Each recipient decrypts the output and returns it to TM. TM replaces 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, TM 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).

3.3 Transaction Pool

After receiving approvals from each of the recipients, TM sends the signed transaction to a BlockChecker, BC. BC stores the transaction in a “transaction pool". The transaction 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 transaction pools.

3.4 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 3.11).

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 3.6 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 [99] and was also supported by [49], which claimed most transmission media peak at $\frac{2}{3}c$. We designed the algorithm to calculate time inclusive of digital signing but exclusive of block verification execution, which slightly impacts the latency.) All BlockCheckers then exchange location confirmation information and, based on the communicated results, they then calculate “EigenTrust" values for all members of the subcommittee [39].

T_0BC_0 then decides on a proposed allocation of block fees among the subcommittee members, proportional to their EigenTrust scores, and creates a transaction with no inputs and one output per subcommittee member. This payment process provides an incentive for all entities to report their location correctly on the blockchain (see Section 3.7); 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 three zero-value outputs in Block Fee transactions in the blockchain (“three strikes”), it is excluded from future block notarization efforts.

3.5 Notarization Chain

To produce a notarized block for the blockchain, the lead BlockChecker (T_0BC_0) determines an order of the subcommittee members to query and sends the block out to each of the BlockCheckers$_{\mathrm{i}}$ ($i \in \{1 : n - 1\}$) in the subcommittee. Each BlockChecker$_{\mathrm{i}}$ signs it and sends it out to the Notaries nearest to them, who in turn sign the block and then return it to BlockChecker$_{\mathrm{i}}$. BlockChecker$_{\mathrm{i}}$ then sends it to BlockChecker$_{\mathrm{i+1}}$. The block is returned to a BlockChecker between every Notary signature to avoid firewall restrictions under the assumption that BlockCheckers are globally accessible on the Internet. The lead BlockChecker must accumulate signatures from at least half of the subcommittee members. Since these subcommittee members are located all over the world, this step creates a delay that functions to prevent competing blockchain forks from being viable alternatives in the blockchain history. This delay is similar to the one in Bitcoin that prevents double-spending attacks.

T_0BC_0's incentivized strategy for choosing subcommittee members is to optimize for receiving signatures in as short a time as possible. Signatures are cumulative to prevent the process from being conducted in parallel – bypassing the intended delay.

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.

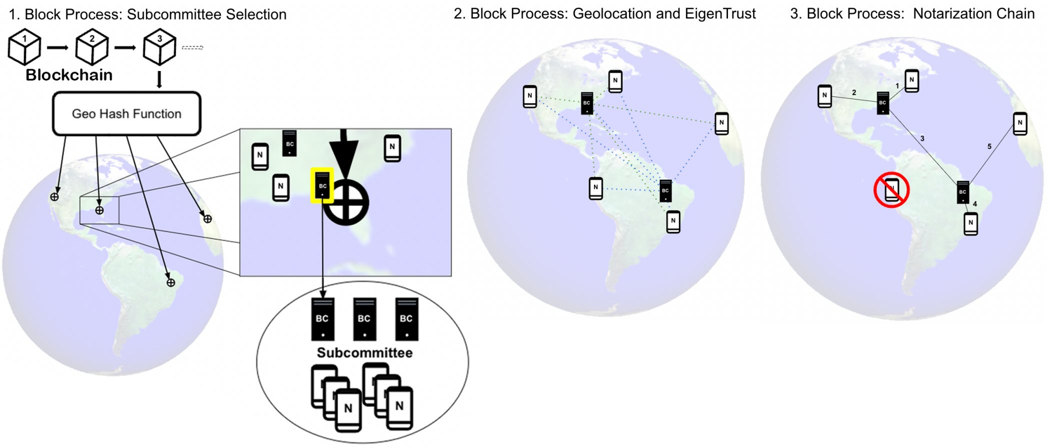

Fig. 3. In Step 1, all Notaries perform a Geographic Hash Function to identify agreed-upon Targets ($T_0 ... T_{n+m-1}$) located around the world. The closest BlockCheckers ("BC" in diagram) to each of the first n targets, and the closest Notaries ("N" in diagram) to each of the later m targets, all 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).

3.6 Recovery Modes

If T_0BC_0 fails at any aspect of the above (for example, due to network delay, device failure, etc.), 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 sequence), it can decide whether or not to spend its time on a competing block, thus reducing the frequency of redundant computational activity. Continuing this premise, any T_NBC_0 may start notarizing a competing block, 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. While the multiple alternatives for notarization allow for temporary forking of the blockchain, the blockchain consensus mechanism would allow the overarching system to converge on a single winner based on the positive-feedback nature of that process, as is the case with Bitcoin. Also, we recognize that this process for dealing with delays and missing nodes will increase the latency of the verification process somewhat; however, given that exact location is not needed for the verification process to proceed, we do not anticipate that this increased latency will compromise the functioning of the system.

3.7 Platform setup

When a node (Notary, TransactionMaker, or BlockChecker) wants to join Xylem, it sends itself a transaction (see 3.1) of 0 Xyla, including in the notes field its GPS coordinates, mobile phone number[5], public key, and whether it is just a Notary, or a TransactionMaker or BlockChecker as well. The Notary's device does not need to have GPS capabilities; they may simply look up their coordinates on a map, or ask someone with a GPS-enabled device, and enter their coordinates based on that information. To preserve a degree of privacy for the Notaries, the GPS coordinates include only one decimal place (11.1km accuracy). In the notarization process, if there are multiple people in the same GPS location, one will be chosen pseudorandomly based on the numerical closeness of their public key to the hash of the previous block, with the most similar being selected first.

To bootstrap the system and transition from a no-cost transaction model to a 1.7% cost transaction model (born by the user), a gradual subsidy is put in place as follows: it starts at 2% and transitions linearly to 0.3% over the first 1,000,000 blocks. At which point, each transaction will entail a 1.7% fee to the user and a 0.3% subsidy to the nodes that participate in forming and validating the block. (See Section 3.10 for more discussion of this ongoing stable subsidy.) This process is analogous to the reward halving algorithm in Bitcoin, where we use the term “subsidy" instead of “reward".

If a Notary changes its location significantly (e.g., moves to a different country), it may send itself a new 0-value transaction with its new location. Only the most recent location registration is used in the block notarization process.

The amount of fees that nodes receive varies based on the number of participation nodes. The fees are fixed and arranged in such a way that the expected cost of running a node and the fees

---

[5] The mobile phone number may be replaced by some other non-free real-world communication mechanism in futures where mobile phones are no longer readily available; see 3.12.2 for more detail on the role of mobile phones in reducing pseudospoofing

the nodes receive would be equal when there are approximately four orders of magnitude more Notaries than Keepers.

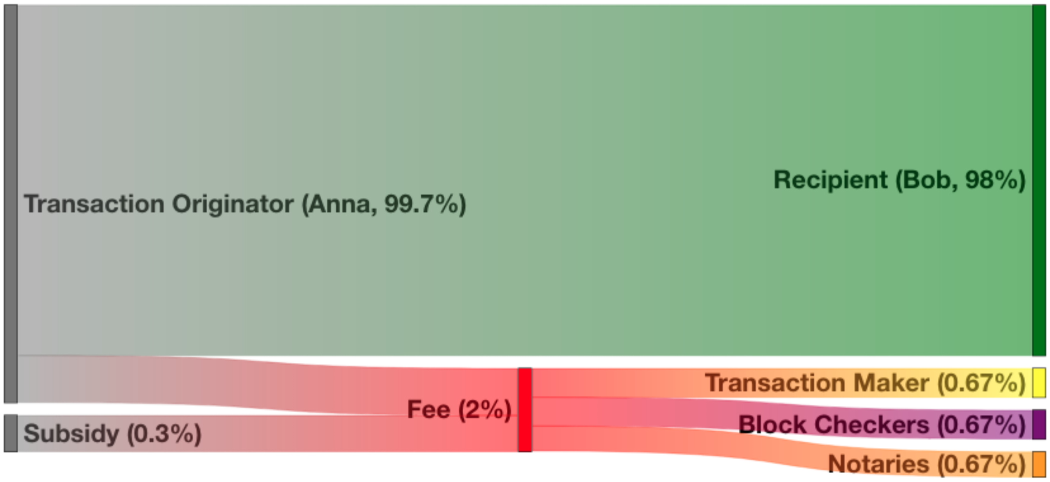

Fig. 4. A Sankey diagram showing how the transaction originator, Anna, sends money to the recipient, Bob, a portion of which combines with a subsidy to fund the fees that go to the TransactionMaker, the BlockCheckers, and the Notaries. The TransactionMaker fee goes to one entity, the BlockChecker fee is split across the 10 BlockCheckers on the subcommittee, and the Notary fee is split across the 40 Notaries on the subcommittee. This diagram shows the post-bootstrapping stable subsidization rate. There are additional subsidies during the bootstrapping phase.

Since Notaries do not have a copy of the full blockchain, they can't validate that the transactions that they sign appropriately generated income for themselves without additional support. On the one hand, BlockCheckers are expected to make sure that fees are appropriately awarded to Notaries that sign transactions, because they may find their blocks rejected in the gossip process if they have not done so. While Notaries can, in principle, check the blockchain to see if they were appropriately paid and thereafter refuse to notarize future blocks from those BlockCheckers, this by itself does not prevent BlockCheckers from colluding against Notaries. Notaries can also develop simple techniques for gossiping information about fraudulent BlockCheckers in order to collectively refuse their work and further incentivize good behavior, akin to digital unionization processes such as Turkopticon [37].

3.8 Transaction Fees

The transaction fee for the platform will be set at 2% of the value of the transaction. Senders may add additional transaction fees to ensure completion of their transaction (for example for low-value transactions that might otherwise be ignored by Keepers).

This rate is well below the average rates for Bitcoin (1.04 USD to 62.79 USD, which would amount to 12.9% to 781% on an 8.04 USD transaction[6]) [76] and Ethereum (1.65 USD to 196.68 USD, which would amount to 20.5% to 2446% on an 8.04 USD transaction) [9]. It is on par with Visa fees (1.15% + 0.05 USD to 2.40% + 0.10 USD) [47]. While the percentage fee rather than a flat fee runs the risk of prioritizing high-value transactions over low-value transactions, the high throughput of the

---

[6] We estimate that the average value per digital payment is 8.04 USD (based on 839.5B payments [19] in 2021 with a total value of 6.75 trillion USD [68]).

platform makes it likely that all transactions will be processed quickly regardless of their value, since BlockCheckers will typically be able to add all available transactions to each block (since the system can handle 3.9 trillion transactions per year, and the annual demand for transactions is projected to be 1.09 trillion trillion in 2023[19], less than 1/3 the capacity that Xylem can handle).

3.9 Baseline Transactions

Xylem also includes a novel piece of functionality to enable the system to scale across long periods of time. Currently, blockchain systems typically rely on miners having a full copy of every transaction since the platform's beginning. As such, the total size of the blockchain scales in proportion to the number of transactions (which, under ongoing usage, is a multiple of both users and time). In Xylem, there is an ongoing process through which the total size of the necessary chunk of blockchain that each Keeper needs to manage is constrained to scale only based on the number of users rather than either time or number of transactions. Every 1 minute, all transactions for 1/65536 of all users (based on the first four hexadecimal digits of their public keys) are reconciled and embedded into a set of "Baseline Transactions," one per user. This process consolidates all previous UTXO's into one UTXO with an equivalent amount of Xyla. These transactions produce a baseline for each user that means that all of their past UTXOs are no longer relevant to future transactions (even though they may still be stored if a Keeper is so inclined). Over a period of approximately 46 days (65,536 minutes), all users go through this process. By the time all users have undergone the process, all transactions prior to each user's last Baseline Transaction are no longer necessary to produce a full representation of all funds on the platform. In essence, the same consensus mechanism that allows for universal agreement among many distributed Keepers will also enable the Baseline Transactions to obviate the need for most Keepers to keep track of all transactions that have ever existed, but rather just tracking those transactions since a user's most recent Baseline Transaction.

For example, imagine a Xylem deployment with 5 billion users. To process Baseline Transactions for all users, approximately 76,000 users must be processed every minute. Since the platform can process 125,000 transactions per second, the reconciliation process would take 0.61 second per minute. This delay of less than a second would not significantly effect most users' experience using the platform. But it would mean that the total size of the blockchain would not become untenably larger over time. Imagining these 5 billion users produced 1.09 trillion transactions per year (one transaction per user every 1.8 days), the total size of the Xylem blockchain at steady state would be 137 TB. While currently a 100 TB SSD drive costs 40,000 USD [4], SSD price per TB is projected to fall to 6 USD by 2030 [28] (the soonest we could reasonably expect to achieve >1 trillion transactions), for a total cost of 822 USD for disk space (411 USD/year, assuming replacement every other year), well within the 2000 USD in income slated for each Keeper.

3.10 Inflation

Xylem will have a low, consistent rate of inflation, enacted through transaction and block subsidies that are added to transaction fees to incentivize Keepers and Notaries. This rate of inflation will mirror the low, consistent rate of inflation that is the explicit policy goal of the US Federal Reserve and similar organizations in other governments around the world [26]. It will be enacted in two ways: as a gap between the transaction fee rate charged to the sender and the transaction fee rate received by the nodes, and also to pay for the fees for the Baseline Transactions described above.

With the velocity of money in the US varying between 4.4 and 8.8 annually [27], we project that the velocity of money in the Xylem ecosystem will be ~6.6 annually. With a 2% rate of inflation being desirable [26], we propose that each transaction should be subsidized by 0.3% (2/6.6). Therefore, the 2% transaction fee will be composed of 1.7% provided by the sender and 0.3% provided by an ongoing subsidy.Since Notaries are selected randomly and widely distributed, it is unlikely that a group would be able to “game the system” to take advantage of the 0.3% subsidy.

The amount needed to fund Baseline Transaction fees will be smaller than the amount needed for the subsidizing of regular transaction fees; at 0.05 Xyla for each Baseline Transaction, these fees will amount to 17% of the total annual subsidies.

In addition to mirroring the best practices of global governments, Xylem’s inflation will also address a concern about cryptocurrencies with a capped amount of total money: money is gradually lost but never created. For example, because of lost passwords (including user error, hardware failure, or even death) all Bitcoin will eventually disappear.

3.11 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 $i \in N$ different locations.

3.11.1 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, i, 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[7]. 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 to such a position would 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 is 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

---

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

goals [98]). Without loss of generality, however, such a function serves to randomly choose locations on the Earth.

3.12 Attacks

Xylem builds on many properties of existing cryptocurrencies: decentralization, SHA256 hashes, public/private key encryption, etc, that help to resist attacks on the integrity of the system. Nevertheless, any platform passing around large amounts of money is going to be threatened. 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.

3.12.1 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 blockchain already held by most of the Keepers following the first-spend.

3.12.2 Pseudospoofing (collect fees). One key attack that is relevant to the Xylem ecosystem is pseudospoofing[8]. Pseudospoofing is a known concern in location-based systems [38, 42].

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 process 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.

3.12.3 Pseudospoofing (flash). A second variant of a pseudospoofing attack (and related to the 51% attack) involves trying to double-spend by *rapidly* becoming a majority of nodes on the Xylem platform [50]. 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.

3.12.4 Pseudospoofing (playbook). A playbook attack entails creating a large number of entities over time, and having them participate as valid actors in the ecosystem [50] but then, in concert, changing behavior and acting maliciously. Xylem prevents this type of attack by permanently

---

[8] We use the term “pseudospoofing" attack to replace an equivalent term, “Sybil” attack [50], because it avoids associating an inherently malicious behavior with a medical condition, Dissociative Identity Disorder.

banning any Notary that has been part of past subcommittees and been identified as a liar on three separate occasions. While 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, responsiveness is a necessary precondition to participate. So, while not necessarily malicious, a repeated lack of responsiveness predicts an inability for a Notary to participate in the future. Regardless, even a Notary "banned" in this sense, 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 sequence.

4 EVALUATION

In this section, we perform quantitative evaluations[9] to evaluate the following three hypotheses:

- Xylem can scale to process all current digital payments around the globe on par with or above the rate provided by several existing digital currency platforms.
- Xylem will use less energy per transaction than several existing digital currency platforms.
- Xylem will reduce wealth inequality more than several existing digital currency platforms.

4.1 Assumptions

To enable a high level of service, we assume that all Keepers (TransactionMakers and BlockCheckers) will have at least gigabit upload and download speed. With 7.95B people in the world [103], and with 19% of people having access to Gbps internet access [90], and with 24.74% [90] using fiber for that access (which we use as a proxy for symmetrical upload and download speed), we calculate that more than 370M people have access to gigabit upload speeds. At more than 4% of the world population, this number represents an ample community to provide services as Keepers for the Xylem platform.

We further assume that all Notaries will have access to smartphones. While they do not need gigabit networking speed, they nevertheless need to be able to run an app and send and receive network messages. With more than 6.5B smartphone subscribers in the world projected for 2022 [83], more than 80% of the world's population currently has the technology necessary to serve the role of Notaries. This number is expected to rise to 90% by 2025, with 7.33B smartphones [87] and a projected population of 8.18B [103] in 2025. These numbers mean the large majority of the world's population can serve as Notaries.

Throughout the calculations below, we set global demand for digital transactions at 1.09 trillion transactions per year, based on projections for 2023 [19]. At 8.04 USD per transaction (see Section 3.8), these transactions would total ~8.80 trillion USD in value. We acknowledge that the rebound effect [86] may make this a conservative estimate, because once most people have easy access to digital transactions, they may make more of them.

We conducted the calculations below with 100,000 Keepers (50,000 TransactionMakers and 50,000 BlockCheckers) and 1 billion Notaries. The Xylem platform could readily operate using more or fewer of each of these entities. Larger numbers of Keepers would make the platform more decentralized, make it more secure, use more energy, and slow the gossip process slightly.

---

[9] We note that varying methodologies can make it challenging to collect accurate data about cryptocurrencies. To offer an example, Blockchain.com reports that the total estimated transaction value of Bitcoin is 3.314B USD across 271.04k transactions [11]. These figures suggest that the average Bitcoin transaction is ~12.2k USD. The figures above are at odds with another source, BitInfoCharts [8], which reports that the average transaction value was 3.69 BTC (177k USD). Interestingly, that source reports a median transaction value that is substantially lower: 0.016 BTC (774 USD). The fact that two different sources offer a spread greater than two orders of magnitude demonstrates that there is often not a shared consensus on key factors of the calculations we are seeking to conduct.

Larger numbers of Notaries would enable the platform to enact a greater reduction in global wealth inequality (see Section 4.5 below) but would also use more energy.

4.2 Transaction Throughput

The total number of transactions that a given infrastructure is able to handle in a particular period of time is critical to its potential for achieving global-scale adoption. In this section we perform analyses to determine if Xylem can scale to process all current digital payments around the globe on par with or above the rate provided by several existing digital currency platforms. A more in-depth discussion of real-world challenges of using network transmission times as input data for algorithmic analysis can be found in [1].

There are two rate-limiting steps in transaction throughput in the Xylem pipeline: the gossiping of blocks among Keepers, and the number of Notaries who are needed to sign a block.

4.2.1 Gossip Speed. The gossiping of blocks among Keepers is a function of Keeper networking speed, transactions per block, and transaction size.

We assume that the gossip itself takes $O(logN)$ steps to reach N Keepers [74], but each step only needs to involve the hash of the block rather than the full content of the block, so each recipient can decide if they have already encountered the block and only download those that are new to them. The downloading of the block content itself can be parallelized via a service such as IPFS [45].

Given the assumptions above, we project that Keepers could theoretically gossip 1,000,000,000 bits per second / 8 bits per byte / 1,000 bytes per transaction = 125,000 transactions per second. The small amount of additional content that must be gossiped with each block for the block notarization process is trivially small compared to the size of the transactions themselves; signatures by 25 BlockCheckers and Notaries, and outputs to the same 25 entities, would compose 0.0026% of the total size of a full block. With 1 block per second (125,000 transactions per second), Xylem will accommodate ~125,000 transactions per block. Note that many transactions will be smaller than 1,000 bytes, which will mean that more transactions may potentially be processed in a full second.

4.2.2 Notaries per Block. Based on a simulation we conducted with Notaries and targets located randomly around the globe, using a non-optimized selection algorithm where all Notaries communicate solely with $T0BC0$, notarization chains with 5 out of 10 BlockCheckers and 20 out of 40 Notaries took an average of 2.4 seconds, whereas an equivalent chain in which Notaries reported to the subcommittee BC nearest to them took an average of 0.77 seconds. The notarization chain combined with the 0.2 seconds that is required for the initial location verification round will take ~0.97 seconds, or just under the desired 1 second block time.

4.3 Transaction Rate

Here we draw on previous research and our own analyses to compare the maximum transaction rate for Xylem and several other financial infrastructures.

In Bitcoin, a transaction is often deemed to be complete after 6 blocks have been closed that build on the block that includes the transaction [67]. After this point, the difficulty of undoing all the blocks that rely on that transaction is prohibitively great [56]. However, with Bitcoin blocks closing on average every 10 minutes, an hour typically passes before six blocks have closed that build on the transaction in question. This amount of time is untenably long for many payments that people may want to make. For example, needing to wait an hour to pay at the end of a 5 minute trip to a nearby food store is well too long for most people to adopt a new payment model.

Existing blockchain systems deployed in the real world have much shorter block times. For example, Solana features a block time of ~0.625 seconds [104], Algorand currently features a 2.5 second block time [53] and the Bitcoin Lightning Network can be resolved in under a minute [3]. Xylem's requirement that Keepers (the only entities that need to manage a full copy of the blockchain) will have symmetrical gigabit upload and download speed allows for a faster block time to be viable.

In Xylem, in order for the user experience to maintain a rapid completion of transactions, there will be 1 block per second. Given the same 6-block rule that Bitcoin users often employ, this block rate will mean that users have access to their funds within 6 seconds of their transaction being included in a block. We believe that this speed will be acceptable to most users.

While the system will seek to achieve 1 block per second, there are several factors that may cause a lower block rate. First, if there is not a transaction that needs to be propagated at a particular time (e.g., in the early stages of adoption, when there are relatively few transactions), there is no need for any BlockCheckers to create a block, and the whole system will wait until there is a transaction that needs to be processed. Second, if the lead BlockChecker fails to respond when it is its turn to lead the block checking process, there may be a delay while other BlockCheckers take over the process. Neither of these occurrences should significantly compromise the experience that users have with the system.

Since there are ~30 million seconds per year and 125,000 transactions per second (as described above), Xylem's maximum transaction rate is greater than 3.9 trillion transactions per year, well in excess of the total number of credit card transactions in 2018 (369 billion) [75], and well above the total number of global non-cash transactions as well (projected to be 1.09 trillion in 2023) [19]. Therefore Xylem's potential throughput is well in excess of the world's current demand for digital payments, and hence we expect the actual data throughput to be much lower than the theoretical maximum. Nevertheless, this theoretical maximum is several orders of magnitude greater than BTC (~3 transactions/second [12]) and Ethereum_w (~15 transactions/second, [15]), well ahead of Visa (7,400 [92] transactions/second), and slightly ahead of Ethereum (100,000 [15] transactions/second). [10] Figure 5 shows, on a logarithmic scale, how Xylem compares to these other currency platforms.

We do agree that "[t]here's a big difference between operating a testnet on a bunch of Amazon servers and a mainnet distributed around the globe." [78] Without having deployed Xylem at global scale, we acknowledge that its true number of transactions per second is likely to be lower than its theoretical maximum. Nevertheless, based on these calculations, and in particular the fact that most transactions will be less than 1,000 bytes and that the total demand for payments is currently only ~1/3 of the rate Xylem could handle even if all transactions were a full 1,000 bytes, we believe Xylem can scale to process all current digital payments around the globe on par with or above several existing digital currency platforms[11].

4.4 Energy Impact

In this section we perform an analysis to determine how Xylem's energy per transaction relates to existing digital currency platforms.

It is challenging, for a platform such as Xylem, to define the scope of analysis to assess its energy impact. Nevertheless, scoping is a key component of life cycle analysis [66], and essential to conducting fair comparisons among different platforms. Certain infrastructures such as a global communications network are necessary for rapid, digital, global financial transactions. However, existing analyses of other financial platforms do not typically include such infrastructures in their calculations, nor do they include the end-user devices used in transactions [5, 77, 82]. We scope our analysis in a way that is similar to how other cryptocurrencies have been analyzed, by including

---

[10] We note that Ethereum is a hypothetical maximum as well, whereas the other values are those deployed in practice.

[11] Note that as internet speeds increase, the Xylem platform will dynamically increase transactions per second, thereby potentially accommodating correspondingly larger throughput of transactions and larger numbers of transactions per block.

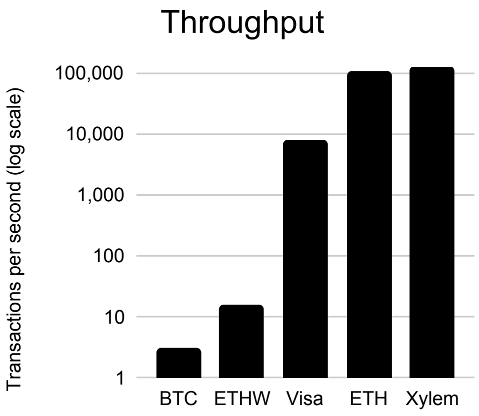

Fig. 5. Xylem has greater throughput than Ethereum (ETH), Bitcoin (BTC), Ethereum$_W$ (ETHW), and Visa.

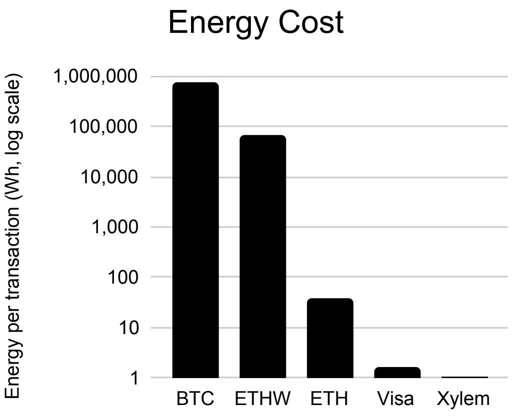

Fig. 6. Xylem uses less energy per transaction than Bitcoin (BTC), Ethereum$_W$ (ETHW), Ethereum (ETH), and Visa.

the energy consumed by all the devices involved in *maintaining the blockchain infrastructure*. Since Xylem invites participants to include their end-user devices in the blockchain infrastructure, we include them when analyzing Xylem.

We calculate here the total energy cost of running the full platform (1.09 trillion transactions per year) for one hour. The 100,000 Keepers would consume 200 Watts each [80], for a total of 5.6 MWh in that hour. Each Notary would consume 0.02W while idling (based on estimates that an Android device uses a mean of 6.06 joules in idle mode waiting for WhatsApp messages [64]). With 1 billion Notaries, that amounts to 2.0 MWh during that hour. In addition to all of the Notaries idling, the subcommittee of 40 Notaries for each block would need to receive and reply to 11 network messages, consuming an additional 8.2 KWh. Combining these values, the full Xylem platform would consume 7.6 MWh in that hour. Dividing that amount by 125 million transactions per hour produces a result of 0.061 Wh per Xylem transaction. We direct the reader to the full calculations supporting this summary.[12]

Bitcoin requires 707 KWh per transaction [77], Ethereum$_W$ requires ~64.2 KWh [77], Ethereum requires 35 Wh [5], and Visa requires 1.48 Wh [82]. As such, Xylem is 99.9999914% less impactful than Bitcoin, 99.999905% less impactful than Ethereum$_W$, 99.83% less impactful than Ethereum, and 95.9% less impactful than Visa. Figure 6 shows these values on a log scale.

We recognize that financial platforms such as Xylem encourage the movement of financial transactions from non-digital media such as paper money and coins to digital media such as mobile phones. As such, they are implicated in the proliferation and growing ubiquity of digital devices in myriad human contexts. However, this proliferation is being driven by many other forces in industrial civilization as well—telephony, photography, ubiquitous information access, social media, etc. We see Xylem as "hitching a ride" on the growing ubiquity of mobile devices (with 90% of the

---

[12] Please see specifically rows 109 and following in column E of this document:
https://docs.google.com/spreadsheets/d/1NuzAro7FSX-xRFWpyi7ePsGUIeFqva88ur3XBJ3jTeU
We also note that these figures are based on numerical simulations, and a real-world deployed system would likely vary from these numbers. Nevertheless, these numerical simulations offer an important first step toward a viable real-world deployment.

world's population projected to own smartphones by 2025 in the absence of Xylem [87]), rather than a major driver of this shift.

In summary, Xylem has a smaller energy footprint per transaction than the platforms analyzed above, and as such could provide a medium for financial transactions with dramatically lower environmental impacts.

4.5 Wealth Inequality

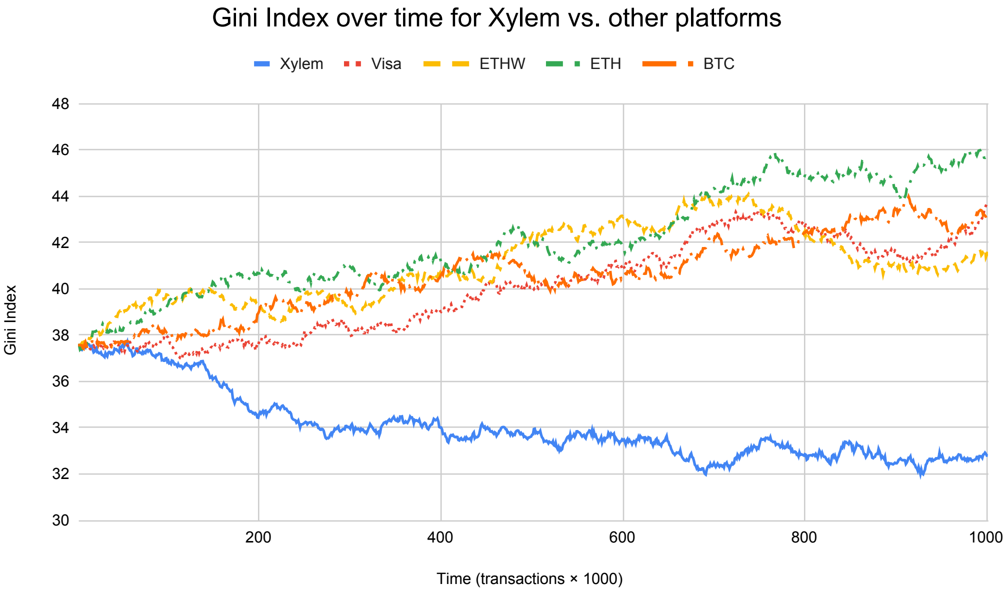

Fig. 7. This chart shows the effect of Xylem vs. other financial platforms on wealth inequality in a simulated world. It displays the Gini index, a measure of wealth inequality, for the community over time. A higher Gini index connotes a world with greater wealth inequality.

A key factor in the Xylem platform is paying Notaries for their work on the platform. In this section we perform analyses of the effect that Xylem and other financial platforms will have on wealth inequality. This section includes two main analyses: first, a numerical analysis of the effect that Xylem would have on the incomes of the people who serve as Notaries, and second, a simulation comparing the effect of Xylem vs. the effect of other platforms on wealth inequality.

With a 2% transaction fee, ~176 billion USD in fees will be distributed among Keepers and Notaries. To maintain approximately 100,000 Keepers, each of whom would need to earn ~2,000 USD/year to maintain a constantly-running, reasonably modern desktop computer with wired Gigabit fiber ethernet [13], approximately 2 billion USD of fees will need to go to the Keepers. The remaining 174 billion USD will be split among the Notaries.

We expect that a share of 174 billion USD would incentive large numbers of people to participate as Notaries. However, as the number of Notaries increases, the amount each Notary earns and

---

[13] Note that the fees are structured to incentivize the participation of no more than 100,000 Keepers, with the remainder of the fees distributed among Notaries.

the frequency with which they are paid both decrease. We perform the calculations here with the expectation that approximately 1 billion people would be willing to install an app and allow it to run in the background on their smartphone in exchange for 174 USD per year, even if the platform only paid them randomly. Nevertheless, in a real-world deployment, the ratio of transaction fees to Notaries may be higher or lower.

We expect that supply-and-demand will set the value of participating as a Notary at no more than the cost of mobile phone service at a particular location. For example, in the US at the time of writing, the lowest mobile phone service was 10 USD per month (120 USD per year) [31] and the cheapest used smartphone was 120 USD [16]. Amortizing the smart phone across four years is 30 USD per year. Including another 25 USD per year for electricity, repairs, and other ancillary expenses brings the total cost per year to 175 USD, just above the 174 USD that we hypothesize users may earn. If the total amount of transaction fees that may be collected via a single device exceeds this rate per currently-participating Notary, we expect that additional Notaries will join the platform (likely without benefiting people in poverty, since rich people will be incentivized to open large numbers of mobile phone accounts simply to collect the fees). (Note that this price point may go up or down as these costs inevitably change over time. Nevertheless, the core analysis remains the same. Additionally, supply-and-demand may set different price points in different regions, since US phone service would only be economically viable for earning Notary fees in the US; a phone with service in a different country would be needed to collect fees in an economically viable way in that region. Essentially, the amount earned from Xylem could offset up to the amount of an individual's total phone bill, but is unlikely to rise above that level due to the economic factors described here.)

We also anticipate that there will be some level below which the value of participating will not fall, since if the value is less than this rate, Notaries will not have sufficient incentive to install the app or to make sure it continues running. Nevertheless, among low SES individuals, the marginal utility of a few dollars is higher than for high SES individuals, and will create a greater incentive for people in that demographic to participate.

4.5.1 Numerical Analysis of Payments to Notaries. Assuming that much of the bottom 10% of the world's population will not have enough income to own a smartphone (based on projections for 2025 above), we perform the following analysis based on the SES segment of world population just above that level. Those in the 10-20 percentile range of global income earn approximately 2212 USD per year [96]. An increase in salary of 174 USD would represent an ~8% increase in their annual salary, equivalent to more than 20 full days of work. Another way to look at this platform is as a societal intervention that creates income for those in the 10-20 percentile of global wealth equivalent to 80 million full time jobs, as well as opportunities for hundreds of millions of other people in low SES contexts to supplement their income. This app would run in the background on their phone, and require only a fraction of 1 USD of electricity per Notary per year [24].

There are many ways in which low-income populations and Xylem are well matched. For those at the margins of being able to afford a smartphone, installing Xylem could offset a significant portion of their phone bill. Further, alternative currencies are more compelling in regions where fiat currencies are unstable. Mobile phones have been shown to lead to benefits for people in poverty [89]. Enabling potentially millions of people to access mobile phones more easily could have substantial corollary benefits. We also recognize that unstable civil contexts may not support a reliable, global communications network; nevertheless, one of the benefits of decentralized systems is their ability to handle disruptions to individual nodes or entire regions.

4.5.2 Simulation. To explore the effect of Xylem vs. other financial platforms (Bitcoin, Ethereum$_{\mathrm{w}}$, Ethereum, and Visa) on wealth inequality, we created an agent-based simulation. In this simulation, several hundred people engage in repeated financial transactions, paying transaction fees to other members of the population. What differs between the Xylem condition and the conditions representing other financial platforms is that, with Xylem, each transaction fee is distributed to a random member of the community, whereas with the other financial platforms, the fee is distributed in proportion to community members' existing wealth. These different modes of 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 [87]), whereas transaction fees in the other platforms are distributed to people who control expensive computing power (Bitcoin, Ethereum_w), who have Ether to stake (Ethereum), or proportional to their ownership in a publicly traded company (Visa). All of these are wealth-intensive positions.

We then ran a simulation of 1,000,000 transactions, and measured the Gini Index [102] that resulted from each run. The Gini Index is a measure of the level of wealth equality in a given population.

At the start of both simulations, the agents were given a distribution of wealth consistent with the average Gini value of all countries in the world today [102][14].

The simulation reveals the dramatically different effect that Xylem would have on wealth inequality compared to the other financial platforms. By redistributing fees among large numbers of the population, regardless of their pre-existing wealth, Xylem increases financial equality. The other platforms, on the other hand, act to increase wealth inequality. Figure 7 shows these results.

Essentially, if deployed at global scale as described in this analysis, Xylem will lead to the creation of income opportunities for large numbers of low-income individuals all around the world. This effect is in line with other efforts to use mobile money systems to address poverty [85].

While the poorest 10% of people in the world will not have access to smartphones and will therefore not have access to the Xylem fee payments, we anticipate that an additional 174 USD per year could profoundly affect the lives of millions of people.

4.6 Effect on Biodiversity

Anthropogenic climate change is reshaping the world in deeply harmful ways [63]. The World Bank projects 216 million climate migrants by 2050 [101], the IEP projects 1.2 billion by 2050 [36], and the UN International Organization for Migration projects 1.5 billion in next 30 years [91]. Non-human species are greatly affected as well, with nearly 3 billion animals killed or displaced by the 2019-2020 Australian wildfires [33], and a billion animals killed by the British Columbia heat wave of 2021 [79].

The first way that Xylem could support biodiversity is via the reduction of wealth inequality. As Oxford economist Kate Raworth puts it: "The more unequal a county is, the more likely is the biodiversity of its landscape to be under threat." [65] The relationship between wealth inequality and threats to biodiversity comes largely from the lifestyles of the very wealthy. As Weidemann et al. write in Nature Communications, "the affluent citizens of the world are responsible for most environmental impacts." [97] The harms that result from over-consumption by the wealthy have been documented elsewhere as well. [88] By reducing wealth inequality globally, Xylem could potentially reduce the threat to biodiversity globally.

A second way Xylem could support biodiversity is via its potential effect on human habitation patterns. The late ecologist Edward Wilson proposed that half of the Earth should be left uninhabited by humans [98], to allow biodiversity to recover and thrive on the planet. This goal is aligned with

---

[14] Interestingly, aside from the unequal allocation of fees, to *maintain* the existing level of wealth inequality the simulation needed to have the recipients of the majority of the transactions be wealthy individuals. As this was a necessary requirement for maintaining the status quo, both experimental conditions also chose the recipients of 99.5% of transactions from a weighted list where individuals are represented proportional to their existing wealth.

policies under way in the US and elsewhere [18] to preserve large amounts of the Earth's ecosystems. Nevertheless, this approach to conservation is not without criticism [17, 44, 62]. The goal of causing humans to occupy less space on Earth appears to be aligned well with conservation goals, and ultimately with the long-term well-being of humanity, which relies heavily on the continued existence of diverse non-human species. Xylem can provide a non-compulsory mechanism for reshaping human habitation patterns. While a small change in income models may not create a large or rapid response, it may nevertheless create a pervasive, gentle incentive that influences relocation decisions. By using the same kernel mechanism that prevents location targets in the ocean, location targets can also be redirected away from environmentally-sensitive regions. Xylem notary locations create financial incentives to be in some regions but not others. Opportunities for income have long been a force affecting where people move; Xylem provides a landscape of income potential that can be aligned with conservation goals.

We considered several mechanisms for how to constrain the locations of targets in the Xylem platform. We considered making a fixed map, in consultation with stakeholders in environmental and humanitarian organizations, and then hard-coding it into the technical infrastructure. But we decided this approach would be too rigid and unable to adapt to changing circumstances across decades or centuries. We contemplated allowing particular accounts to control the map for certain areas and sending login credentials for those accounts to the heads of each government, but were concerned that the environmental and humanitarian ends we desired would be compromised by self-dealing. We recognize that the social aspects of this topic, in particular which stakeholders get to make the relevant decisions about where to put targets, are challenging.

Our current solution is to encourage urbanization using current population distribution as a benchmark – allowing targets to be placed where Notaries sign up (a proxy for population distribution). Urbanization is beneficial in some ways and harmful in others [23], but tends to lead to a reduction in *per capita* emissions [55], and frees up space in which biodiverse species may thrive more effectively [98]. In its current instantiation, the platform only creates targets in the 50% of the globe's land area where Notaries are most strongly represented.[15] We anticipate that, if there were a non-trivial amount of income (e.g., \$174, as mentioned above) to be earned simply by living in a particular area while maintaining mobile phone service and running an app, that income could cause people to move from other locations into locations where such income could be earned. There are numerous instances where governments and other institutions pay people to relocate, e.g. [95]; while the amounts that would be provided by Xylem would likely be substantially lower than those offered by countries, the SES status of those being incentivized by Xylem to move would be lower as well. Even if the effect were less pronounced and more gradual, there would be a slight financial incentive to move.

4.7 Effect on Electronic Waste

Cryptocurrencies are often critiqued for the large amounts of electronic waste (e-waste) that they produce [21]. E-waste from the Xylem platform will be much lower than other cryptocurrency platforms, since beyond the required capabilities (gigabit ethernet for Keepers and the ability to run an app and exchange messages for Notaries), there is no incremental benefit to larger capabilities. By supplanting Proof-of-Work-based platforms such as Bitcoin, Xylem would reduce the financial sector's overall per-transaction e-waste footprint.

---

[15] Specifically, the system places all targets within the area defined by the set of circles with centers at the locations of the first 1M non-excluded Notaries, and with radius defined as SQRT(Area of Earth / (2 * MAX(Number of Notaries, 1000000) * PI)). In practice, this mapping will lead to a bit less than 50% total area coverage, since some of the circles will overlap, and avoids placing targets in the ocean.

Transactions/year	1,000	1,000,000	1,000,000,000	1,094,000,000,000
Total energy (kW)	4.51	8.64	30.44	25,758.72
Notaries	100	10,000	1,000,000	1,000,000,000
Keepers	10	100	1,000	100,000
Energy/transaction (Wh)	39,549.82	75.68	0.27	0.21
Cost of energy/year (USD)	$1,898.39	$3,632.44	$12,798.07	$10,831,026.08

Fig. 8. This figure shows various factors of the Xylem ecosystem as it increases in scale. While the energy per transaction starts out high, the total energy at that point is still quite low.

4.8 Ramping Up

Xylem's operating costs and impact are proportional primarily to the number of Keepers and Notaries rather than number of transactions. As with Bitcoin or Visa, Xylem could process large numbers of transactions per year with a very small number of devices, for example, one Keeper (which could serve as both TransactionMaker and BlockChecker) and two Notaries. However, the system would not be very secure at this scale, because only three entities would need to conspire to take over the entire financial ecosystem. The security of the system scales with the number of devices. Therefore, one of the goals in ramping up the system is to increase the number of devices over time, thereby increasing security and increasing the number of people who benefit from the system. Figure 8 shows the relationship between the number of Keepers, the number of Notaries, and the environmental and financial cost of energy. It also shows approximate numbers of transactions that we might see going through the system each year at those various scales.

We expect that the number of transactions will be correlated with the number of devices participating as Keepers or Notaries because the more transactions there are, the more transaction fees there are, and therefore the greater financial incentive there is for people to participate in the platform. To support broad adoption of this platform, we plan to release open source implementations of Xylem both to serve as TransactionMakers and BlockCheckers and also iOS and Android apps to allow large numbers of people to serve as Notaries. Xylem also has built-in incentives, described above, to help bootstrap early participation in the platform. While we recognize that large numbers of Keepers and Notaries will lead to environmental impacts, we believe these costs are offset by the benefits in terms of replacing existing more harmful platforms and providing income to people all over the world.

5 IMPLICATIONS FOR RESEARCH AND PRACTICE

The ideas presented in this article have substantial implications for the research community and that of practitioners.

Xylem offers a novel model for how a cryptocurrency could be designed. The cryptocurrency domain has a long-standing issue with sustainability, given the high energy costs associated with Proof-of-Work and other consensus mechanisms. This work could help shift the scholarly discussion toward more sustainable models of cryptocurrency. Similarly, cryptocurrencies have been indicted for their inegalitarian impacts [71–73]; Xylem points in a direction whereby both research and practice could engage cryptocurrencies in efforts to foster greater financial equity.

On a longer term, if Xylem were to become established as a currency in use around the world, it could lead to substantial wealth redistribution, which would itself influence both the research and practitioner communities. If Xylem were to become established, the location data that it would make available (even at 11.1km accuracy) would likely become a resource for both researchers and practitioners as well. Finally, it could lead to novel directions for privacy and security researchers and practitioners, as they develop new approaches to geography-based consensus mechanisms.

6 LIMITATIONS

There are a number of different limitations that constrain this work. For example, the limited amount of income that any one user can earn means that it will not single-handedly fix global poverty. Nevertheless, we hope that a large-scale deployment would help improve the income, and thereby the living conditions, for large numbers of people near the bottom of the wealth spectrum.

This system is also limited by its reliance on mobile devices. While mobile devices are currently ubiquitous in many contexts, there are still contexts where mobile devices are beyond the financial reach of many individuals. Additionally, just as mobile devices weren't ubiquitous in any contexts just a few decades ago, it's possible that they will not be ubiquitous a few decades from now, either due to technological progress brought about by advanced research and development, or due to economic contraction brought about by environmental challenges or other factors [13].

There are likely to be challenges that emerge as this project moves from a simulation to the real world, as well. For example, as discussed earlier, various factors may constrain the accuracy of location validation that underlies Proof-by-Location. Also, any system that transacts large amounts of money is likely to be subjected to a wide array of attacks by adversaries. We sought to address several of these attacks above; nevertheless, adversaries are innovative, and both technical and social factors involved in deployment may impede the system's effectiveness.

This system is proposed as a global intervention, which implies its deployment in a wide variety of social environments. Access to mobile phone devices and the networks that they rely on can be restricted dynamically in response to geopolitical changes, civil disorder, and natural disasters of various kinds. This could include a direct response to this system itself, which could become the target of political attention. Additionally, changes in the monetary environment, changes in the business models of mobile phones and data networks, and changes in the control of energy generation and consumption could all limit the successful deployment of Xylem.

7 CONCLUSION

This paper has presented a novel mechanism for enabling a distributed global consensus about financial transactions. It has presented a platform based on this mechanism that could potentially process three times the number of digital payments that currently occur in the world. This platform would have lower environmental impacts than existing financial system including Bitcoin, Ethereum$_w$, Ethereum, and Visa. And it would combat wealth inequality, which is a critical and underappreciated shortcoming of all of the systems.

This platform has five main benefits. First, it can scale to handle 125,000 transactions per second, more than triple the total number of digital payments currently occuring around the world (see analysis below). This number exceeds the observed throughput of Bitcoin (~3 transactions per second [12]), Ethereum$_w$ (~15 transactions per second [15]), and Visa (~7,400 transactions per second [92], and Ethereum's theoretical maximum (~100,000 transactions per second [15]).

Second, Xylem is more energy efficient than those other platforms. It is 99.9999914% less energy intensive per transaction than Bitcoin, 99.999905% less intensive than Ethereum$_w$, 99.83% less intensive than Ethereum, and 95.9% less intensive than Visa.

Third, Xylem can help address wealth inequality. If deployed at a global scale, Xylem could provide a mechanism similar to a universal basic income for 1 billion or more people. These fees would provide digital currency to more than 110 million people in each decile of global income except the bottom 10% (who typically do not have enough capital to own smartphones [87]). The fees would produce the income equivalent of 8.8 million full-time jobs for people in the second lowest decile and millions more full-time job equivalents in other deciles. As such, it could alleviate human suffering and enable financial inclusion [52].

Fourth, by shaping the infrastructure in ways that allow governments to require the use of *particular* Notaries, Xylem becomes a financial platform that is more effectively aligned with democratic uses than most cryptocurrencies. While this design choice may be at odds with the libertarian leanings prevalent in the cryptocurrency community [30], it also provides mechanisms (albeit outside the scope of this paper [48]) for creating non-financial incentives for pro-social behavior as well.

Finally, by weighting geographic locations in the consensus algorithm, Xylem may provide a positive, non-compulsory incentive for people to adopt less environmentally harmful habitation patterns.

We believe the Xylem platform will be better than Bitcoin for several reasons. The primary reasons are improved performance and the greatly reduced environmental footprint that Xylem provides. In addition, Xylem has other characteristics, such as its ability to distribute wealth widely among global populations and its potential impacts on human habitation patterns that allow it to be more socially engaged than the more libertarian Bitcoin [30].

We believe this platform will be better than Ethereum$_{\mathrm{w}}$ for the same reasons described above regarding Bitcoin, and will be better than Ethereum and Visa primarily due to its effect on wealth inequality. There will be a greater relative incentive for lower income individuals to participate in the Xylem platform (as Notaries) compared to the other platforms, which has the possibility of resulting in greater social good.

While a financial system will not be able to cure all of the world ills, we nevertheless hope that the Xylem platform may provide a better user experience, a better economic infrastructure, and a better social mechanism by which people engage in payments around the world.

https://www.overleaf.com/project/651c7ca78b48378fe3234b6e

ACKNOWLEDGMENTS

The authors thank Ethan Bañez, Evelyn Chin, Hayden Freedman, Nicole Sullivan, and Ishan Varney for their contributions to the project, and Adrien Berthelot for his useful feedback.

REFERENCES

[1] Md Mamunur Rashid Akand. 2023. *Contribution to Proof-of-Location Systems.* Doctoral Thesis. University of Calgary, Calgary, Alberta, Canada. https://prism.ucalgary.ca/handle/1880/116173 Retrieved from PRISM Repository, University of Calgary.

[2] Fernando E. Alvarez, David Argente, and Diana Van Patten. 2022. *El Salvador's Experiment with Bitcoin as Legal Tender.* https://www.nber.org/digest/202207/el-salvadors-experiment-bitcoin-legal-tender NBER Digest No. 7.

[3] Andreas M. Antonopoulos. 2014. *Mastering Bitcoin: Unlocking Digital Crypto-Currencies* (1st ed.). O'Reilly Media, Inc.

[4] Desire Athow. 2022. At 100TB, the world's biggest SSD gets an (eye-watering) price tag. (2022). https://www.techradar.com/news/at-100tb-the-worlds-biggest-ssd-gets-an-eye-watering-price-tag Accessed August 26, 2022.

[5] Carl Beekhuizen. 2021. 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/

[6] Jocelyn Cranefield David Johnstone Markus Luczak-Roesch Donald J. Patterson Bill Tomlinson, Jens Boberg and Shreya Kapoor. 2021. Analyzing the sustainability of 28 "Blockchain for Good" projects via affordances and constraints. *Information Technology for Development* 27, 3 (2021), 439–469. https://doi.org/10.1080/02681102.2020.1828792 arXiv:https://doi.org/10.1080/02681102.2020.1828792

[7] Michael Wang Fangyi Wang Peng Xiangli Bill Wang, Zhiyu Lin and Zhi Li. 2023. Applying blockchain technology to ensure compliance with sustainability standards in the PPE multi-tier supply chain. *International Journal of Production Research* 61, 14 (2023), 4934–4950. https://doi.org/10.1080/00207543.2022.2025944 arXiv:https://doi.org/10.1080/00207543.2022.2025944

[8] Bitinfocharts.com. 2021. Bitcoin (BTC) price stats and information. (2021). https://bitinfocharts.com/Bitcoin/ Accessed September 16, 2021.

[9] Bitinfocharts.com. 2022. Ethereum Avg. Transaction Fee historical chart. (2022). https://bitinfocharts.com/comparison/ethereum-transactionfees.html#3y Accessed August 24, 2022.

[10] Bitstamp. 2021. 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] Blockchain.com. 2021. Estimated Transaction Volume. (2021). https://www.blockchain.com/charts/estimated-transaction-volume Accessed September 16, 2021.

[12] Blockchain.com. 2022. Transaction Rate Per Second. (2022). https://www.blockchain.com/charts/transactions-per-second Accessed Sept 16, 2021.

[13] Marshall Burke, Solomon M. Hsiang, and Edward Miguel. 2015. Global non-linear effect of temperature on economic production. *Nature* 527, 7577 (nov 2015), 235–239. https://doi.org/10.1038/nature15725

[14] Vitalik Buterin. 2014. Ethereum Whitepaper. (2014). https://ethereum.org/en/whitepaper/

[15] Andrew Button. 2022. Ethereum: 100,000 Transactions per Second Coming Soon! *Yahoo Finance* (2022). https://ca.finance.yahoo.com/news/ethereum-100-000-transactions-per-183200856.html

[16] Best Buy. 2023. Samsung - Pre-Owned Galaxy A11 32GB (Unlocked) - Black. (2023). https://www.bestbuy.com/site/samsung-pre-owned-galaxy-a11-32gb-unlocked-black/6497042.p?skuId=6497042

[17] Bram Büscher, Robert Fletcher, Dan Brockington, Chris Sandbrook, William M. Adams, Lisa Campbell, Catherine Corson, Wolfram Dressler, Rosaleen Duffy, Noella Gray, and et al. 2017. Half-Earth or Whole Earth? Radical ideas for conservation, and their implications. *Oryx* 51, 3 (2017), 407–410. https://doi.org/10.1017/S0030605316001228

[18] Campaign for Nature. 2022. More than 100 Countries Commit to Protect at Least 30% of Land and Oceans by 2030. (2022). https://www.campaignfornature.org/more-than-100-countries-commit-to-protect-at-least-30-of-land-and-oceans-by-2030 Accessed August 25, 2022.

[19] Consultancy.uk. 2020. Global market size of digital payments industry soares. (2020). https://www.consultancy.uk/news/25975/global-market-size-of-digital-payments-industry-soares

[20] Michaela Curran and Matthew C. Mahutga. 2018. Income Inequality and Population Health: A Global Gradient? *Journal of Health and Social Behavior* 59, 4 (2018), 536–553. https://doi.org/10.1177/0022146518808028 arXiv:https://doi.org/10.1177/0022146518808028 PMID: 30381957.

[21] Alex de Vries and Christian Stoll. 2021. Bitcoin's growing e-waste problem. *Resources, Conservation and Recycling* 175 (2021), 105901. https://doi.org/10.1016/j.resconrec.2021.105901

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

[23] T. Elmqvist, E. Andersson, T. McPhearson, X. Bai, L. Bettencourt, E. Brondizio, J. Colding, G. Daily, C. Folke, N. Grimm, D. Haase, D. Ospina, S. Parnell, S. Polasky, K. C. Seto, and S. Van Der Leeuw. 2021. Urbanization in and for the Anthropocene. *npj Urban Sustainability* 1, 1 (Feb. 2021), 6. https://doi.org/10.1038/s42949-021-00018-w

[24] EnergyUseCalculator.com. 2022. Electricity usage of a Cell Phone Charger. (2022). https://energyusecalculator.com/electricity_cellphone.htm Accessed August 24, 2022.

[25] Euroclear. 2023. *Settlement of French Government Bonds in Central Bank Digital Currency (CBDC) with Blockchain.* Technical Report. Euroclear. https://www.euroclear.com/content/dam/euroclear/news%20&%20insights/Format/Whitepapers-Reports/settlement-french-government%20bonds-in-cbdc-with-blockchain.pdf Accessed: 2023-10-19.

[26] Federal Reserve. 2022. Why does the Federal Reserve aim for inflation of 2 percent over the longer run? https://www.federalreserve.gov/faqs/economy_14400.htm Accessed August 25, 2022.

[27] Federal Reserve Bank of St. Louis. 2022. Velocity of M2 Money Stock. (2022). https://fred.stlouisfed.org/series/M2V Accessed August 20, 2022.

[28] David Floyer. 2021. QLC Flash HAMRs HDD. (2021). https://wikibon.com/qlc-flash-hamrs-hdd/ Accessed August 26, 2022.

[29] Foamspace Corp. 2022. FOAM. https://www.foam.space/ Accessed August 7, 2022.

[30] David Golumbia. 2016. *The Politics of Bitcoin: Software as Right-Wing Extremism.* Number 15 in Forerunners: Ideas First. University of Minnesota Press, Chicago. https://www.upress.umn.edu/book-division/books/the-politics-of-bitcoin

[31] Quinlan Grim. 2023. 6 Best Cheap Cell Phone Plans of 2023. (2023). https://money.com/best-cheap-cell-phone-plans/

[32] Samet Gunay, Mohamed M. Sraieb, Kerem Kaskaloglu, and Mehmet Emin Yıldız. 2023. Cryptocurrencies and global sustainability: do blockchained sectors have distinctive effects? *Journal of Cleaner Production* 425 (2023), 138943. https://doi.org/10.1016/j.jclepro.2023.138943

[33] Jack Guy. 2020. Nearly three billion animals killed or displaced by Australia's fires. (2020). https://www.cnn.com/2020/07/28/asia/australia-fires-wildlife-report-scli-intl-scn/index.html Accessed August 25, 2022.

[34] Jeremy Hinsdale. 2022. Cryptocurrency's Dirty Secret: Energy Consumption. *State of the Planet* (2022). https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy

[35] Jon Huang, Claire O'Neill, and Hiroko Tabuchi. 2021. 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

[36] Institute for Economics and Peace. 2022. Over one billion people at threat of being displaced by 2050 due to environmental change, conflict and civil unrest. (2022). https://www.economicsandpeace.org/wp-content/uploads/2020/09/Ecological-Threat-Register-Press-Release-27.08-FINAL.pdf Accessed August 25, 2022.

[37] Lilly C Irani and M Six Silberman. 2013. Turkopticon: Interrupting worker invisibility in amazon mechanical turk. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 611–620.

[38] Peng Jiang, Hongyi Wu, and Chunsheng Xin. 2021. DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. *Digital Communications and Networks* (2021). https://doi.org/10.1016/j.dcan.2021.09.006

[39] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. 2003. The Eigentrust Algorithm for Reputation Management in P2P Networks. In *Proceedings of the 12th International Conference on World Wide Web* (Budapest, Hungary) *(WWW '03)*. Association for Computing Machinery, New York, NY, USA, 640–651. https://doi.org/10.1145/775152.775242

[40] Kostis Karantias, Aggelos Kiayias, and Dionysis Zindros. 2020. Proof of Burn. (2020). https://iohk.io/en/research/library/papers/proof-of-burn/

[41] Abdullah Ayub Khan, Asif Ali Laghari, Mamoon Rashid, Hang Li, Abdul Rehman Javed, and Thippa Reddy Gadekallu. 2023. Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review. *Sustainable Energy Technologies and Assessments* 57 (2023), 103282. https://doi.org/10.1016/j.seta.2023.103282

[42] Samer Khanafseh, Naeem Roshan, Steven Langel, Fang-Cheng Chan, Mathieu Joerger, and Boris Pervan. 2014. GPS spoofing detection using RAIM with INS coupling. 1232–1239. https://doi.org/10.1109/PLANS.2014.6851498

[43] Paul Sergius Koku. 2015. Financial exclusion of the poor: a literature review. *International Journal of Bank Marketing* 33, 5 (Jan. 2015), 654–668. https://doi.org/10.1108/IJBM-09-2014-0134 Publisher: Emerald Group Publishing Limited.

[44] Helen Kopnina. 2016. Half the earth for people (or more)? Addressing ethical questions in conservation. *Biological Conservation* 203 (2016), 176–185. https://doi.org/10.1016/j.biocon.2016.09.019

[45] Protocol Labs. 2022. IPFS powers the Distributed Web. (2022). https://ipfs.tech/ Accessed September 23, 2022.

[46] Sándor Laki, Péter Mátray, Péter Hága, Tamás Sebők, István Csabai, and Gábor Vattay. 2011. Spotter: A model based active geolocation service. In *2011 Proceedings IEEE INFOCOM*. 3173–3181. https://doi.org/10.1109/INFCOM.2011.5935165

[47] Kimberlee Leonard and Cassie Bottorff. 2022. Credit Card Processing Fees (2022 Guide). (2022). https://www.forbes.com/advisor/business/credit-card-processing-fees/ Accessed August 24, 2022.

[48] Lawrence Lessig. 2009. *Code 2.0* (2nd ed.). CreateSpace, Scotts Valley, CA.

[49] Dave Levin, Youndo Lee, Luke Valenta, Zhihao Li, Victoria Lai, Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee. 2015. Alibi Routing. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, SIGCOMM 2015, London, United Kingdom, August 17-21, 2015*, Steve Uhlig, Olaf Maennel, Brad Karp, and Jitendra Padhye (Eds.). ACM, 611–624. https://doi.org/10.1145/2785956.2787509

[50] Brian Levine, Clay Shields, and N Margolin. 2005. A Survey of Solutions to the Sybil attack. *Technical Report of Univ of Massachussets Amherst* 2006–052 (11 2005).

[51] F. Dal Mas, M. Massaro, V. Ndou, and E. Raguseo. 2023. Blockchain technologies for sustainability in the agrifood sector: A literature review of academic research and business perspectives. *Technological Forecasting and Social Change* 187 (2023), 122155. https://doi.org/10.1016/j.techfore.2022.122155

[52] Bill Maurer. 2012. Mobile Money: Communication, Consumption and Change in the Payments Space. *The Journal of Development Studies* 48, 5 (2012), 589–604. https://doi.org/10.1080/00220388.2011.621944 arXiv:https://doi.org/10.1080/00220388.2011.621944

[53] Silvio Micali. 2020. Algorand 2021 Performance. https://www.algorand.com/resources/algorand-announcements/algorand-2021-performance Accessed August 25, 2022.

[54] Camilo Mora, Randi Rollins, Katie Taladay, Michael Kantar, Mason Chock, Mio Shimada, and Erik Franklin. 2018. Bitcoin emissions alone could push global warming above 2 C. *Nature Climate Change* 8, 11 (2018).

[55] Pablo MuÃ±oz, Sabrina Zwick, and Alisher Mirzabaev. 2020. The impact of urbanization on Austria's carbon footprint. *Journal of Cleaner Production* 263 (2020), 121326. https://doi.org/10.1016/j.jclepro.2020.121326

[56] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (May 2009). http://www.bitcoin.org/bitcoin.pdf

[57] Neha Narula, Lana Swartz, and Julie Frizzo-Barker. 2023. CBDC: Expanding Financial Inclusion or Deepening the Divide? (Jan 2023).

[58] Bank of Canada. ND. *Digital Canadian dollar.* https://www.bankofcanada.ca/digitaldollar/ Accessed October 20, 2023.

[59] Future of Money Research Collaborative:, Taylor C. Nelms, Bill Maurer, Lana Swartz, and Scott Mainwaring. 2018. Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. *Theory, Culture & Society* 35, 3 (2018), 13–33.

https://doi.org/10.1177/0263276417746466 arXiv:https://doi.org/10.1177/0263276417746466

[60] Rolf Oppliger. 2005. *Contemporary cryptography.* Artech House.

[61] Donald J. Patterson and Bill Tomlinson. 2022. Proof-by-Location as a Socially Responsible Financial Infrastructure. In *IEEE Global Emerging Technology Blockchain Forum.*

[62] Stuart L. Pimm, Clinton N. Jenkins, and Binbin V. Li. 2018. How to protect half of Earth to ensure it protects sufficient biodiversity. *Science Advances* 4, 8 (2018), eaat2616. https://doi.org/10.1126/sciadv.aat2616 arXiv:https://www.science.org/doi/pdf/10.1126/sciadv.aat2616

[63] Hans O. Pörtner, Debra C. Roberts, Helen Adams, Carolina Adler, Paulina Aldunce, Elham Ali, Rawshan Ara Begum, Richard Betts, Rachel Bezner Kerr, Robbert Biesbroek, Joern Birkmann, Kathryn Bowen, Edwin Castellanos, Gueladio Cissé, Andrew Constable, Wolfgang Cramer, David Dodman, Siri H. Eriksen, Andreas Fischlin, Matthias Garschagen, Bruce Glavovic, Elisabeth Gilmore, Marjolijn Haasnoot, Sherilee Harper, Toshihiro Hasegawa, Bronwyn Hayward, Yukiko Hirabayashi, Mark Howden, Kanungwe Kalaba, Wolfgang Kiessling, Rodel Lasco, Judy Lawrence, Maria Fernanda Lemos, Robert Lempert, Debora Ley, Tabea Lissner, Salvador Lluch-Cota, Sina Loeschke, Simone Lucatello, Yong Luo, Brndan Mackey, Shobha Maharaj, Carlos Mendez, Katja Mintenbeck, Mariana Moncassim Vale, Mike D. Morecroft, Aditi Mukherji, Michelle Mycoo, Tero Mustonen, Johanna Nalau, Adrew Okem, Jean Pierre Ometto, Camille Parmesan, Mark Pelling, Patricia Pinho, Elvira Poloczanska, Marie-Fanny Racault, Diana Reckien, Joy Pereira, Aromar Revi, Steven Rose, Roberto Sanchez-Rodriguez, E.L.F. Schipper, Daniela Schmidt, Davis Schoeman, Rajib Shaw, Chandni Singh, William Solecki, Lindsay Stringer, Adella Thomas, Edmond Totin, Christopher Trisos, David Viner, Maarten van Aalst, Morgan Wairiu, Rachel Warren, Pius Yanda, and Zelina Zaiton Ibrahim. 2022. *Climate change 2022: impacts, adaptation and vulnerability.* IPCC.

[64] Stylianos Rammos, Mansi Mundra, Guijin Xu, Chuyi Tong, Wojciech Ziolkowski, and Ivano Malavolta. 2021. The Impact of Instant Messaging on the Energy Consumption of Android Devices. *2021 IEEE/ACM 8th International Conference on Mobile Software Engineering and Systems (MobileSoft)* (2021), 1–11.

[65] Kate Raworth. 2017. *Doughnut Economics: Seven Ways to Think Like a 21st-Century Economist.* Random House.

[66] G. Rebitzer, T. Ekvall, R. Frischknecht, D. Hunkeler, G. Norris, T. Rydberg, W.-P. Schmidt, S. Suh, B.P. Weidema, and D.W. Pennington. 2004. Life cycle assessment: Part 1: Framework, goal and scope definition, inventory analysis, and applications. *Environment International* 30, 5 (2004), 701–720. https://doi.org/10.1016/j.envint.2003.11.005

[67] Nathan Reiff. 2021. How does a block chain prevent double-spending of Bitcoins? (2021). https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp Accessed August 28, 2022.

[68] Renub Research. 2022. Digital Payment Market, Size, Global Forecast 2022-2027, Industry Trends, Impact of COVID-19, Opportunity Company Analysis- Product Image Digital Payment Market, Size, Global Forecast 2022-2027, Industry Trends, Impact of COVID-19, Opportunity Company Analysis. (2022). https://www.researchandmarkets.com/reports/5521693/ Accessed July 15, 2022.

[69] Reuters. 2023. *Brazil central bank names its digital currency 'Drex', scheduled for 2024 launch.* https://www.reuters.com/technology/brazil-central-bank-names-its-digital-currency-drex-scheduled-2024-launch-2023-08-07/ Accessed: yyyy-mm-dd.

[70] Joseph A. Ritter. 1995. The Transition from Barter to Fiat Money. *The American Economic Review* 85, 1 (1995), pp. 134–149. http://www.jstor.org/stable/2118000

[71] David Rosenthal. 2018. Gini Coefficients Of Cryptocurrencies. (2018). https://blog.dshr.org/2018/10/gini-coefficients-of-cryptocurrencies.html

[72] Nouriel Roubini. 2018. Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs On "Exploring the Cryptocurrency and Blockchain Ecosystem": Crypto is the Mother of All Scams and (Now Busted) Bubbles While Blockchain Is The Most Over-Hyped Technology Ever, No Better than a Spreadsheet/Database. (2018). https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf

[73] Ashish Rajendra Sai, Jim Buckley, and Andrew Le Gear. 2021. Characterizing Wealth Inequality in Cryptocurrencies. *Frontiers in Blockchain* 4 (2021). https://doi.org/10.3389/fbloc.2021.730122

[74] Gokay Saldamli, Charit Upadhyay, Devika Jadhav, Rohit Shrishrimal, Bapugouda Patil, and Lo'ai Tawalbeh. 2022. Improved gossip protocol for blockchain applications. *Cluster Computing* 25, 3 (01 Jun 2022), 1915–1926. https://doi.org/10.1007/s10586-021-03504-z

[75] Erica Sandberg. 2020. The Average Number of Credit Card Transactions Per Day & Year. *CardRates.com* (2020). https://www.cardrates.com/advice/number-of-credit-card-transactions-per-day-year/ Accessed September 22, 2022.

[76] Arijit Sarkar. 2022. Bitcoin average transaction fees lowest in two years at $1.04. (2022). https://cointelegraph.com/news/bitcoin-average-transaction-fees-lowest-in-two-years-at-1-04 Accessed August 24, 2022.

[77] John Schmidt. 2022. Why Does Bitcoin Use So Much Energy? *Forbes* (2022). https://www.forbes.com/advisor/investing/cryptocurrency/Bitcoins-energy-usage-explained/

[78] Kai Sedgwick. 2018. No, Visa Doesn't Handle 24,000 TPS and Neither Does Your Pet Blockchain. *Bitcoin.com* (2018). https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/

[79] Deepa Shivaram. 2021. Heat Wave Killed An Estimated 1 Billion Sea Creatures, And Scientists Fear Even Worse. (2021). https://www.npr.org/2021/07/09/1014564664/billion-sea-creatures-mussels-dead-canada-british-columbia-vancouver Accessed August 25, 2022.

[80] Sibelga. 2022. How much power does a computer use? And how much CO2 does that represent? *Energuide.be* (2022). https://www.energuide.be/en/questions-answers/how-much-power-does-a-computer-use-and-how-much-co2-does-that-represent/54/ Accessed September 22, 2022.

[81] Kelsey Simpkins. 2022. 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

[82] Statista. 2022. Bitcoin average energy consumption per transaction compared to that of VISA as of April 25, 2022. (2022). https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/ Accessed August 23, 2022.

[83] Statista. 2022. Number of smartphone subscriptions worldwide from 2016 to 2027. (2022). https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ Accessed July 14, 2022.

[84] Quinten Stokkink and Johan Pouwelse. 2023. A Local-First Approach for Green Smart Contracts. *Distrib. Ledger Technol.* (jul 2023). https://doi.org/10.1145/3607196 Just Accepted.

[85] Tavneet Suri and William Jack. 2016. The long-run poverty and gender impacts of mobile money. *Science* 354, 6317 (2016), 1288–1292. https://doi.org/10.1126/science.aah5309 arXiv:https://www.science.org/doi/pdf/10.1126/science.aah5309

[86] Joan Thiesen, Torben S. Christensen, Thomas G. Kristensen, Rikke D. Andersen, Brit Brunoe, Trine K. Gregersen, Mikkel Thrane, and Bo P. Weidema. 2006. Rebound effects of price differences. *The International Journal of Life Cycle Assessment* 13, 2 (2006), 104. https://doi.org/10.1065/lca2006.12.297

[87] Ash Turner. 2022. How many smartphones are in the world? (2022). https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

[88] UNICEF. 2023. *Over-consumption in the world's richest countries is destroying children's environments globally, new report says.* https://www.unicef.org/press-releases/over-consumption-worlds-richest-countries-destroying-childrens-environments-globally Accessed: 2023-10-21.

[89] USAID. 2015. Mobile Phones Tackling Poverty. (2015). https://www.usaid.gov/infographics/50th/mobile-phones-tacking-poverty Accessed August 24, 2022.

[90] VIAVI. 2022. Gigabit Monitor. (2022). https://gigabitmonitor.com/ Accessed July 14, 2022.

[91] Gaia Vince. 2022. The century of climate migration: why we need to plan for the great upheaval. (2022). https://www.theguardian.com/news/2022/aug/18/century-climate-crisis-migration-why-we-need-plan-great-upheaval Accessed August 25, 2022.

[92] Visa. 2022. Visa Fact Sheet. *The New York Times* (2022). https://usa.visa.com/dam/VCOM/global/about-visa/documents/aboutvisafactsheet.pdf

[93] Yuntao Wang, Zhou Su, Jiliang Li, Ning Zhang, Kuan Zhang, Kim-Kwang Raymond Choo, and Yiliang Liu. 2022. Blockchain-Based Secure and Cooperative Private Charging Pile Sharing Services for Vehicular Networks. *IEEE Transactions on Vehicular Technology* 71, 2 (2022), 1857–1874. https://doi.org/10.1109/TVT.2021.3131744

[94] Moritz Wendl, My Hanh Doan, and Remmer Sassen. 2023. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of Environmental Management* 326, Part A (2023), 116530. https://doi.org/10.1016/j.jenvman.2022.116530

[95] Cassie Werber. 2023. *More countries are paying people to move out of their overgrown cities: Remote work might incentivize moves, but will digital nomads really help revive the countryside?* https://qz.com/more-countries-are-paying-people-to-move-out-of-their-o-1849943791 Accessed: 2023-10-21.

[96] WID.world. 2022. World Inequality Database. (2022). https://wid.world/data/ Pre-tax national income, P10-20. Accessed August 1, 2022.

[97] T. Wiedmann, M. Lenzen, L.T. Keyßer, and Julia K. Steinberger. 2020. Scientists' warning on affluence. *Nat Commun* 11 (2020), 3107. https://doi.org/10.1038/s41467-020-16941-y

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

[99] WonderNetwork. 2022. Global Ping Statistics. (2022). https://wondernetwork.com/pings Accessed August 7, 2022.

[100] Bernard Wong, Ivan Stoyanov, and Emin Gün Sirer. 2007. Octant: A Comprehensive Framework for the Geolocalization of Internet Hosts. In *Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation* (Cambridge, MA) *(NSDI'07)*. USENIX Association, USA, 23.

[101] World Bank. 2021. Climate Change Could Force 216 Million People to Migrate Within Their Own Countries by 2050. (2021). https://www.worldbank.org/en/news/press-release/2021/09/13/climate-change-could-force-216-million-people-to-migrate-within-their-own-countries-by-2050 Accessed August 25, 2022.

[102] World Bank. 2022. Gini Index. (2022). https://data.worldbank.org/indicator/SI.POV.GINI Accessed August 24, 2022.

[103] Worldometer. 2022. World Population Projections. (2022). https://www.worldometers.info/world-population/world-population-projections/ Accessed August 1, 2022.

[104] Anatoly Yakovenko. 2022. Solana: A new architecture for a high performance blockchain v0.8.13. https://solana.com/solana-whitepaper.pdf Accessed August 18, 2022.