Proof-of-Trade Swapchains:
A Peer-to-Peer Economic Exchange

Aaron Alterman
aa@swapchain.network
www.swapchain.network

Abstract. Barter upends the concepts of 'buyer' and 'seller' for a more equitable method of exchange, allowing economic activity to be directly carried out without financialized vehicles or markets. However, the computational power and availability of information needed to construct socially useful barter chains were not universally available until recently. We propose a distributed infrastructure of algorithmically-generated bartering chains using a novel blockchain mechanism we call "treasure hunt" hashing. Distributing the NP-hard work of optimizing barter chain negotiation[i] over the IPFS peer-to-peer protocol, this system enables ongoing trading of goods and services between parties previously unknown to each other.

1. Introduction

In the 9 years since Satoshi Nakamoto published the Bitcoin whitepaper[ii], cryptocurrency has become the primary use case for the *blockchain* database it describes, and thousands of other cryptocoins have been launched. In attempting to solve the challenges of online commerce, Bitcoin created an algorithmic black hole into which globally significant investment of time, energy and computing power has been poured without substantially affecting the majority of online commerce or providing any truly novel means of economic exchange. As the first response to Nakamoto's paper warned,

> "it does not seem to scale to the required size. For transferable proof of work tokens to have value, they must have monetary value. To have monetary value, they must be transferred within a very large network... if hundreds of millions of people are doing transactions, that is a lot of bandwidth"[iii]

The external costs of blockchain adoption have, so far, outweighed the social utility of any of its applications. The "CPU time and electricity that is expended" identified by Bitcoin as the basis for its intrinsic value has become a primary external concern. Cryptocurrency replicates all of the problems of fiat currency without any central braking mechanism or truly intrinsic value to the speculative assets at the heart of the system. We propose a new truly transformative electronic system, the *swapchain*, to move *beyond* money instead of simply replicating it at high cost and low value.

Created with Master PDF Editor. For non-commercial use only.

Created with Master PDF Editor - For non commercial use only.

2. Observable Consequences of Blockchain Use

At the time this paper is being written, 90% of all possible Bitcoins have already been mined, so we have a fair basis to assess the claims and critiques of the *proof-of-work* (or PoW) blockchain Bitcoin uses. Compare the current use case for Bitcoin with Nakamoto's originally stated motivation in the Bitcoin whitepaper:

> "The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable."

In the attempt to create a currency, "crypto" has instead simply become another speculative asset class instead of a truly useful medium of exchange, and one whose external costs are unsustainable. To wit,

1) The energy consumption of cryptomining has become geopolitically relevant, and the equipment requirements have distorted markets for hardware and created huge amounts of electronic waste.

2) Cryptocurrency's ability to store exchange value is compromised by its volatility. Spending an electronic coin is always an investment decision rather than a routine purchase. Even so-called "stablecoins" are unstable.

3) Fraud is endemic in the cryptocurrency space.

4) Blockchain forensics are rendering guarantees of anonymity obsolete.

5) Transactions can take days to complete because of limited data bandwidth.

6) Prohibitive transaction fees now require "sidechains" be routinely used to bundle many transactions into expensive blockchains such as Bitcoin or Ethereum, having breached sustainability limits for a single blockchain. Linking these assets raises risks of systemic contagion in an economic sense.

7) Cryptocurrencies have not replaced fiat currency, even as several countries have legalized their use as tender. Where nations have poured reserves into crypto, their investments have been fraught.

8) Individuals can no longer mine a single Bitcoin, Ether, or any popular coin on their own, owing to the ever-increasing difficulties of computation. Competition has given way to collusion as all mining is done by large pools of CPU power, whose operators promise steady rates of return on investment to those who join, creating political power from processing power.

By making the coin a store of value, it was inevitable that it became an asset whose practical valuation is measured in fiat currency, rather than as a useful mechanism for fostering socially beneficial exchanges. Famously, the first commercial Bitcoin transaction swapped 10000BTC for two pizzas (ordered by phone and paid in fiat), which could have been valued at a maximum of over 61.35 billion USD (Bitcoin's peak on October 1st 2021). It appears Bitcoin may have hit a ceiling at around 60000USD per coin, at which point miners appear to cash out unused coins for fiat currency. Ironically, the tightening of interest rates by central bankers in the fiat system also profoundly affected the price of Bitcoin as liquidity challenges rose for financialized products such as cryptocurrency.

Proof-of-stake[1] (or PoS) mining was proposed as a more efficient alternative to proof-of-work blockchains in 2011[iv]. However, adoption has been glacial, even with the advent of hybrid PoW/PoS systems: the proof-of-work market is valued roughly nine times the proof-of-stake market[v]. Additionally, proof-of-stake systems require financial resources similar to those needed to buy enough specialized proof-of-stake mining equipment. The network functions only to exacerbate inequalities between participants.

3. Bartering vs. Currency-based exchange

In the classic 1998 paper[vi] by Federal Reserve researcher N. Kocherlakota entitled "Money is Memory," the problem of currency's functioning is described as follows:

> Memory is defined as knowledge on the part of an agent of the full histories of all agents with whom he has had direct or indirect contact in the past. Money is defined as an object that does not enter utility or production functions, and is available in fixed supply. The main proposition is that any allocation that is feasible in an environment with money is also feasible in the same environment with memory. ...[A]ny allocation that is achievable using money alone could be achieved instead by allowing agents costless access to a historical record of past actions that I term memory; I conclude that the role of money is to serve as a (typically imperfect) form of memory.

This makes clear the potential of a well-developed technology (capable of performing the functions of both memory and allocation) to not only equal, but surpass money's utility. Kocherlakota goes on to explain that "memory dominates money" in environments with a random matching of a large set of potential traders because

> [T]he set of incentive-feasible allocations in an environment with memory is always a superset of the set of incentive-feasible allocations in the same environment with money.

[1] Proof-of-stake requires nodes to freeze a minimum number of their cryptoassets during "minting" and randomly awards a new coin from a lottery weighted by how many coins are 'staked,' i.e., the more existing coins one stakes, the better the chances of being awarded the next free one.

Created with Master PDF Editor. For non-commercial use only.

When and how barter first arose as a means of economic exchange is beyond the scope of this paper, but we can safely say that bartering has a long history as a tool of economic exchange. Bartering is not limited to humans; there are numerous examples in the animal kingdom of barter economies in both primates and non-primates[vii]. What we do know is that at some point between the emergence of gift economies and the first surviving coinage from Lydia in the 7th century BCE, metallic trade emerged. First recorded in ancient Sumerian texts around 3000 BCE, using metals as standard units of value was common practice. Sumerians traded discrete amounts of gold and silver, as well as barley and cattle[2], as standard fungible units within a larger economy with both barter and standardized metallic trade (e.g., scales weighing talents of silver, before coinage).

Barter will reliably arise in post-monetary systems where access to currency is limited.[3] Currency's strength against barter as a tool to engender economic exchange is that the price is fixed and easy to understand in simple terms, e.g., the number of dollars and cents something costs. In order for barter to scale, the exchanges each need to have similar value in voluntary exchange for each party at the time of any given swap.

Where currency allows for easy bilateral trade (money for commodity), barter allocates goods most efficiently when more than two agents are involved in an exchange. For any *two*-way transactors unable to find mutual satisfaction, a more complex *n*-way circular exchange can be constructed: such multilateral barters are called *barter chains*.

Barter chains do not have to maintain the same quantitative value for each trade from beginning to end, and they do not necessarily need to be circular[4]. This allows for better matching of valuations in real time, because access to commodities is not restricted to a single fungible good (i.e., currency), but according to the present wants and needs of the transactors at the time of trade. Hermit crabs line themselves up in order of size when they find a large shell, waiting until an appropriately sized crab will complete the chain (standing between the large, empty shell and the line of smaller-shelled crabs), at which point each crab crawls into the shell vacated by its larger neighbor. One famous barter chain began with a single paperclip and ended with a house[viii].

A well-known example of barters in computational theory is the national kidney exchange, typically involving tens of thousands of pairs of recipients and donors who need to be matched according to medical and distance requirements. It is illegal to pay for kidneys in most countries, barring this type of medical trade from money-based markets. The establishment of algorithmic pair-matching programs like the National Kidney

[2] The Sumerian word for 'interest' is the same as the word for 'calf,' indicating that animal husbandry was an early avenue toward financialization, and Sumerian debt records are well-attested.

[3] For this reason, barter is an effective (a historically proven) strategy against inflation.

[4] Altruism in barter is an important aspect which is beyond the scope of this paper, but deserves attention when establishing the norms and conventions of a coordinated barter system. See section 10.

Created with Master PDF Editor. For non-commercial use only.

Registry show that software-assisted bartering is already saving lives today; if the problem of coordinating barter exchange is, at the very least, non-polynomially 'hard' to solve algorithmically, human intervention and a wide enough array of inputs into the system should render the problem solvable for chains of a certain length.

When "Money is Memory" was written, the computing power to run a centralized system fulfilling money's crucial functions with a ledger system already existed. Several generations of software and hardware advances later, the ability to run such a system in a distributed and decentralized way is within our grasp.

Economists often postulate that barter is the original form of trade, preceding money and even the state. However, all available anthropological and historical evidence is that barter only arises after standardized metallic trade, which arise only after states allowed interdependence on a societal scale, freeing households from the need for self-sufficiency and allowing them to specialize beyond subsistence hunting and farming. Trade arises from surplus, and surplus is very difficult to achieve alone. Interdependence requires trust, which a zero-trust system will never achieve. To replace money with memory in the form of a blockchain, we cannot be satisfied merely to record irreversible payments.

Forseeable challenges arise around the issue of trust at three levels:

1) trust in the system overall,
2) trust between direct transactors previously unknown to each other, and
3) trust between indirect transactors, e.g., fellow members of the chain not directly involved in your trades.

Interacting with any previously unknown party requires contextual trust, whether at a trading post on an ancient road or in a virtual casino. Since swapchains will prefer first-time interactions, we are simply solving this problem every time: transactors must reasonably believe the value of their trades will be borne out upon delivery regardless of the identity of the potential transactors.

If we propose the swapchain as a more Kocherlakotan-complete substitute for memory than either fiat or digital currency, we must prove that it is capable of retaining useful information. Where all parties are known not only by experience but by local reputation, we use narratives to tell us about a person's trustworthiness. Merely placing a history of transactions for a particular cryptocurrency wallet within a zero-trust system has proved a poor substitute for face-to-face trust-based systems.

Created with Master PDF Editor. For non-commercial use only.

We propose a barter and transactional record-keeping system whose agents allow for unfinancialized voluntary exchanges between peers, coordinated cryptographically. If the power of currency is its ease of use in making trades, a *smart barter* (compare to "smart contract") system will have to provide commensurate dexterity in meeting the needs of its users. Fortunately, managing interface complexity is well within the scope of software.

Decentralized barter systems require distributed data storage, listing (among other information) all previous transactions involving either a known commodity or a scope-bounded IOU for service (hereinafter referred to as a *quality*), and its exchange value in that transaction (hereinafter, a *quantity*). This allows the tracking of the exchange values of any previously traded quality over time, fulfilling (with unmatched precision) money's memory function.

We propose to use the peer-to-peer IPFS[5] protocol to store transactional records, *offers* (advertised qualities), *wants* (advertised searches for qualities). These items are stored (or at least described) as human-readable JSON[6] document files on a public but specialized IPFS network. File URLs are created by a SHA-256 hash[7] of their contents on IPFS (known as *content-based addressing*) and hosting is distributed in a fashion similar to BitTorrent. Each *node* is identified by its cryptographic *public key*, and we use 'nodes' interchangeably with 'users,' 'participants,' or 'transactors.'

We call the barter chains created through these mechanisms *swapchains*, which are generated using *treasure hunt hashing*. We call the cryptographic exchange medium a *credit* (as opposed to a coin) and the system for creating and using them *proof-of-trade*.

4. Treasure-Hunt Hashing

The most useful innovation in the Bitcoin paper is idea of storing information in an otherwise irreversible hash by manipulating a "nonce" (or *salt*) within the text to be hashed.[8] In a proof-of-work blockchain, the numerical value of this hash becomes a mathematical boundary, past which future hashes will not be valid. This is done to create artificial scarcity by increasing computational difficulty, as Nakamoto explains:

[5] IPFS ("InterPlanetary File System") is a decentralized file storage network using a content-based addressing scheme to locate data.

[6] JSON ("JavaScript Object Notation") is a data format which is both human- and machine readable.

[7] That both Bitcoin and IPFS systems use the same SHA-256 algorithm to produce 32-character hexadecimal hashes is likely due to the fact that their whitepapers were released 5 years apart. For ease of comparison, this paper suggests the same hashing scheme, but one could easily use any other strong hashing algorithm or combination of weak ones and achieve the same network functions.

[8] Hash functions compress any input into a very large number with a fixed number of hexadecimal digits. Cryptographic hashes are designed to be extremely difficult to reverse: finding the hash from a given value is easy, but finding the original value given a hash is almost impossible.

Created with Master PDF Editor. For non-commercial use only.

> "Proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash. ...we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits."

Fortunately, the address space in hashes such as SHA-256 are wide enough[9] to allow us to store far more information at a far lower computational cost than proof-of-work. Salting a transaction record to create a *directed* one-way hash, we can implement any number of arbitrary requirements on hash values to store information (of course, each additional requirement adds to the computational cost of hash guessing). Simple constraints for acceptable hashes might include requiring the hash to contain a certain sequence of characters, or producing a certain modulus when divided by certain value, or even place those constraints on a secondary hash of the first hash.

We propose a new blockchain consensus mechanism we call a *treasure hunt*, where nodes look for the *location* of the next block (i.e., the SHA-256 hash of an update to the chain) on the IPFS network[10], where this hash is the URL of the swapchain document listing all proposed barters within the chain. Nodes discover the next block either by publishing their proposed addition to the chain (with a new block and salt added) to IPFS[11], or by simply waiting for the next block to be published to the other nodes in the chain, (e.g., if your swap has already been settled).

Given the wide address space, few if any nodes will come up with the same hashed address for the same block, so the lowest arithmetic valued hash (collisions are fine) will be preferred where there are multiple valid hashes for the same information. There is no algorithmic reward for being first, since the purpose of this blockchain is to reach consensus rather than to narrowly restrict rewards for the comparatively trivial work of coming up with a directed hash. The reward for having a block accepted is in the content of the block (i.e., trades which meet with the approval of peer nodes), and the work to certify the block is performed by all nodes equally in order to advance the chain.

At each step, the swapchain document is hashed anew, with the location of the previous step recorded as the offer chain ID. No Merkle trees are needed to constrain the data size because the amount of information each chain contains should never reach beyond human readability, as all nodes must approve of all chained trades.

[9] SHA256 hashes compress any text input into a practically unique number between 0 and 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129, 639,936 (usually represented as 32 hexadecimal digits).

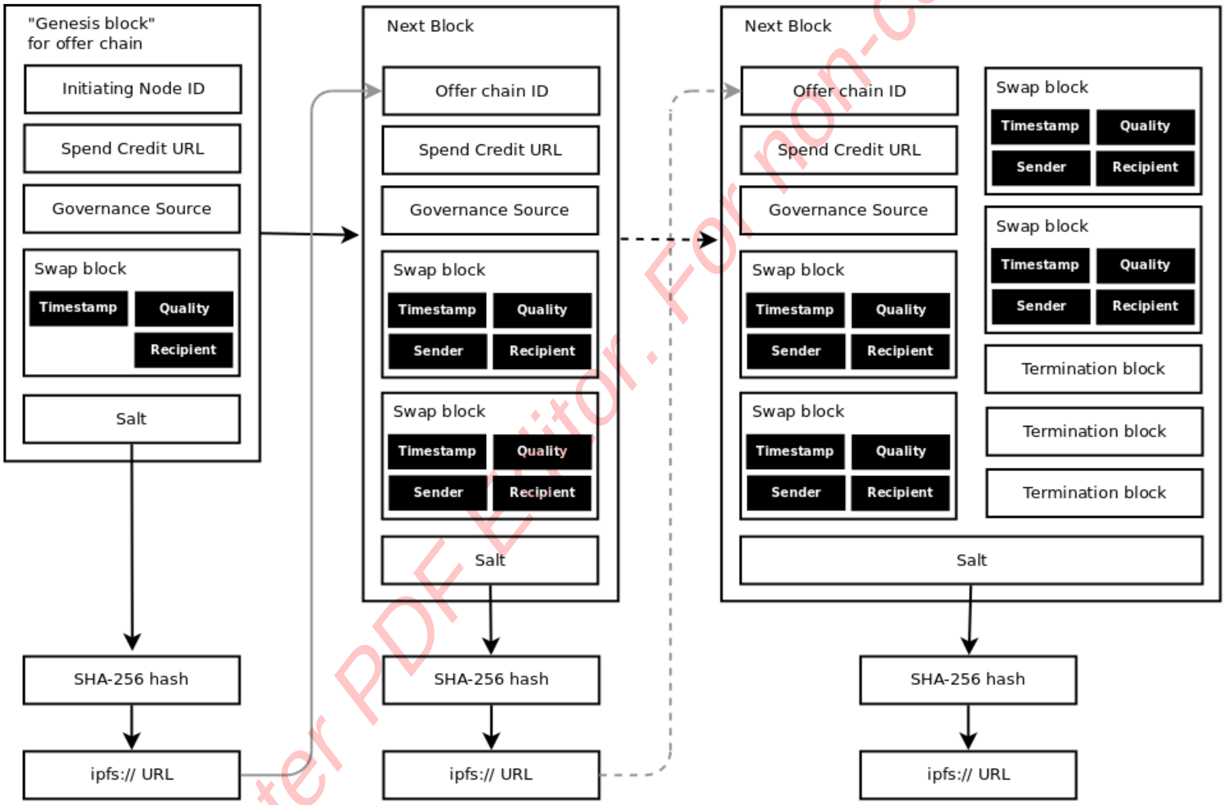
[10] IPFS' main function is to reverse the 'irreversible' hashes created by its content addressing scheme.

[11] We suggest "treasure hunch" as an additional neologism for treasure hunt hash guesses.

Created with Master PDF Editor. For non-commercial use only.

When all transactors arrive at the same location, they include this block in their version of the chain and move on to finding the next acceptable block of trades to complete the loop of transactions. Nodes in the swapchain continue adding blocks until all parties have added their own countersigned termination request block to the chain.

Each offer chain is a list of pointers to IPFS URLs so that all information can be independently verified off-chain. Documents begin with the public key of the offerer (i.e., the initiating node ID), the URL of a valid spend credit document (whose content points to all of the burn credits needed to complete the transaction), and links to the open-source code of governance software which will distribute tokens once the swapchain is complete.



Created with Master PDF Editor. For non-commercial use only.

5. Proof-of-trade credits

We define an electronic credit as a chain of signatures on a series of transactional records within a peer-to-peer content-hashed distributed data storage scheme. The swapchain credit is a medium of exchange, but not a store of value.

By manipulating salts we can control the address resulting from IPFS' content-hashing scheme such that the first two characters denote 1 of 256 attributes describing the type of document. Reserving the first x digits of the hexadecimal hash requires an average of 16^x guessed hashes. Generating 256 random hashes is fairly trivial for today's computers, and leaves plenty of addressable space for collision-free content hashing, letting us immediately distinguish between the types of documents needed to make the system work without having to inspect the contents first.

Proof-of-trade uses two key aspects of the blockchain (manipulating irreversible hashes to store human-readable information, and the mechanism of determining the order of operations based on a rolling sequence of such hashes) and the native content hashing functions of IPFS[ix] to distribute the NP-hard computational task of constructing an optimized barter chain, while requiring human review before and after the execution of those chained exchanges.

Proof-of-trade credits are a medium of exchange, but they do not store value. The value of any particular voluntary exchange within a barter chain is negotiated by the nodes during the course of the swaps engineered by the action of the network. **The credit is a tokenized, atomized measure of trust.** Proof of one satisfactory trade is both bar to entry and price of admission to the market for another unique transaction.

Cryptocurrency's zero-trust model extends only as far as first-time payments. Unfortunately, the irreversible nature of transactions in that system make questions of post-purchase satisfaction irrelevant, which is why fraud is so rampant in the space. The theory of the blockchain is that all transactions being public and immutable is a viable substitute for conventional reputation; anyone can verify that a particular public key has transacted with so-and-so, but no information is available about the aftermath of the transaction going forward.

Swapchains have a different view of trust and its value within an economic system, because the credit itself is a tokenized, atomized measure of trust. Trust is earned by satisfying others; each credit spent is verification that at least one other person (but likely two) benefitted from trading with you. However, this trust is fleeting: when spent, it becomes irrelevant. Past transactions are available and part of a public, if decentralized record; however, when a credit has cycled through both burn and spend for all transactors, the likelihood of that record persisting on the network wanes.

Created with Master PDF Editor - For non-commercial use only.

In the swapchain, you're only as good as your last trade[12], and reputation functions as a binary gate: if you have proof of a satisfactory trade, you can enter the market again, but only once. Obviously, you may accrue more than one credit at a time, but each transaction requires the sacrifice another token. Chains are linked, but not linear; each individual chain will be linked to many more individual chains, and data may persist, but swapchains do not require a single immutable blockchain.

6. Transactions

Each transaction is collaboratively constructed and countersigned by all parties. After the swapchain has been certified and countersigned by all nodes, the offer chain is run through the governance code referenced in the swapchain document. This creates a piece of open-source software called a decentralized autonomous organization (or *DAO)* capable of issuing credits. DAOs are run cooperatively, with members voting via *governance tokens*.

When all nodes have locked in their signatures, credits are awarded to each node in the form of an IPFS document. Two types of credits are created from that chain of signatures for each node: *spend* credits and *burn* credits. Each node in the swapchain receives one spend credit, one burn credit for every other node, and a preset number of governance tokens for the DAO. To spend a credit, a simple majority of the holders of your associated burn credits must agree to unpin your burn credit and cryptographically sign your new swapchain (which references the burn credit). After a swap has been certified, each transactor is still required to fulfill certain duties which should be specified in the swap contract (e.g., delivery of goods, pinning/signing burn credits).

In practice, the DAO should be able to handle these functions seamlessly for users. To spend a credit, one need only submit a swapchain document to the DAO containing their corresponding burn credits, and the DAO should handle all required notifications and pinning/unpinning requests, and so forth. This DAO exists until all credits issued by that swapchain are spent, and it may decide to issue additional credits to parties exclusively outside the DAO's membership for the purpose of trade fulfillment, (e.g., logistics; insurance; dispute arbitration; IPFS pinning services).

Swapchains are *forward trusting*, and trust can be revoked post-exchange if some fraud occurs. The other transactors act as a de facto jury to arbitrate claims of dissatisfaction; if you are dissatisfied with your trade, you can appeal to others to withhold their burn credits from the offender until a resolution can be reached.

[12] It is conceivable that at some point, convention will push the required number of spend credits per transaction beyond one for a variety of reasons, some of which are discussed in Section 13.

Created with Master PDF Editor. For non-commercial use only.

7. Network

Transactions, offers, wants, qualities, spend credits, burn credits, contracts, governance tokens, open-source discovery algorithms, and even the software needed to run the system itself all exist as immutable documents within an IPFS network. Each type of document would be denoted by the first two hexadecimal digits of its directed hash, which we call a *mask*.

Each transaction document is a list of IPFS addresses and the hashes of their contents, requiring that data to be "live" within the system as a further means of checking the authenticity of requests. Running the network entirely on IPFS results in a number of efficiencies over traditional blockchain architecture:

1) Hashing is predictable and native.

2) IPFS' garbage-collection functions obviate the need for traditional blockchains' concerns about reclaiming disk space.

3) Storing all assets including code on the network allows low-power nodes to enter the system without penalty.

4) Not all nodes need be online to complete transactions.

5) IPFS' pinning functionality allows uptime guarantees for data.

6) Immutable open source code is tamper-resistant.

7) True neural networking can be integrated into algorithms for discovery, negotiation, arbitration, etc.

8. Distributing costs

All manner of incidental costs may become crucial to satisfactory trade: shipping, insurance, arbitration, etc. How these costs are distributed is to be decided by convention among transactors, and one size may not fit all. Consider some predictable scenarios:

1) damages during shipping or delivery;
2) in a chain of n length, 1/n trades involves an outsize shipping cost;
3) a transactor refuses to accept delivery of an item;
4) a service rendered is later revealed to have been criminally negligent; etc.

At some point a single transaction may require multiple spend credits to cover such additional costs. The scope of this paper precludes us from describing in detail conventions which should arise organically from the (often negative) experiences of transactors over time. We must allow fair practices to evolve within a framework which demands fairness as a bar to entry, but does not prescribe how to achieve it (or by what means). Each swapchain is an opportunity to tweak these conventions anew.

Created with Master PDF Editor. For non-commercial use only.

9. Swapchains

The steps to complete a swapchain (as outlined above) are as follows:

1) Your offer chains are published on the IPFS network.
2) Any node wishing to add a block of swaps to your chain notifies you of a new IPFS document whose location's first two digits identify it as a *counter-offer*.
3) To accept the counter-offer and complete the chain, send a termination block as your next block. Otherwise, publish a counter-offer. Counter-offers will continue until all parties send a termination block.
4) When all nodes implicated in a chain have sent a termination block, each node publishes a counter-signature document containing:
   a) a cryptographic signature of the final transaction document;
   b) the location of a spend credit from a previous transaction;
   c) the location of burn credits validating that spend credit;
   d) a cryptographic signature of the concatenation of all of the above; and
   e) a salt giving the signature document the appropriately-masked hash for a counter-signature.
5) Burn credits are created when each countersignature is itself countersigned by all other nodes with a salt giving the counter-countersignature document the appropriately masked hash for a burn credit.
6) The spend credit document consists of:
   a) your original countersignature;
   b) an array of the locations of each published countersignatures (i.e., burn credits);
   c) a cryptographic signature of the concatenation of all of the above; and
   d) a salt giving this document the appropriately-masked hash for a spend credit.
7) Pin the burn credits upon satisfactory receipt of the traded quality (or qualities).
8) The offer chain reconstitutes itself as a DAO, generating a new keypair to countersign (and salt) each spend credit to issue a pre-agreed number of unique governance tokens per transactor.
9) This DAO may also exchange resources from node members for services such as logistics, inspection, insurance, etc. Conceivably, a reusable swapchain could be constructed such that it always results in the assembly of a number of inputs (i.e., resources and labor) into a certain quality, spontaneously creating an enterprise governed by the DAO which creates new offer chains and a potential income stream for the participating nodes.

Created with Master PDF Editor. For non-commercial use only.

10. Scaling

Swapchains should scale as well as any other IPFS network without any need for exponential resources devoted to investing tokens with value. Because artificial scarcity is not valued in the proof-of-trade system, the issuing of credits does not require increasing amounts of energy (as in PoW) or to be an accredited crypto investor (PoS). Though both traditional blockchains and swapchains both use a bit of brute force to work, the computational requirements of swapchains are much lower and stay lower over time, even though limiting the amount of time any swapchain will create credits is another important part of the system design.

By relying on a robust, open source storage network like IPFS as its backbone, swapchains can preserve artifacts from blockchains no longer actively processing transactions. Issuing a limited number of credits per chain keeps the processing requirements for operating the system low; the limits of human readability probably max out at chains with dozens or hundreds of exchanges, and machines may be able to do exponentially more, but certainly not on the scale where calculations become too difficult for a mobile CPU to process.

At the time this paper was written, the computing power of the Bitcoin network was over 80 zettaFLOPS. The top 8 supercomputers in the world don't even reach 900,000 petaFLOPS all combined. Over 200 quintillion hashes are currently being generated per second, and with blocks being rewarded approximately every ten minutes, only 1 of every 120 sextillion calcutations gets a virtual reward for the "correct" answer.

Swapchains would rather the multitude of CPUs on the network collaborate toward a common and equitably distributed reward for their work, although the nature of algorithmic discovery means the actual efficiency of all network calculations cannot be guaranteed. However, since the discrete discovery mechanisms of the swapchain described above are not intrinsic to its functioning (i.e., this paper describes the infrastructural layer over which human decisions about trades are arranged), each node is able to run their own discovery algorithms to fine tune their performance.

Blockchains assume the longest chain is the most correct. The social utility of a barter chain increases with length, but this is limited by the time it takes to compute and execute these trades. If all nodes come up with the same transactions in the same order, this mechanism could be used not only to generate and confirm consensus, but naturally distribute the computational work of constructing an optimally efficient chain of trades.

Created with Master PDF Editor - For non-commercial use only.

11. Fungible Qualities

History predicts that in markets where access to currency is limited and barter arises as a substitute, a certain fetishized commodity or small set of commodities typically assume the role of currency in order to provide a standard valuation for trades. We propose that if anything become such a type of universally fungible quality by convention, it should be stored electrical energy, for several reasons:

1) Energy is infinitely useful, even used within the system itself to run nodes.
2) Energy can be stored and transmitted with existing infrastructure.
3) Renewable energy is easy to produce sustainably (and cheaply enough if you can barter for equipment).
4) Energy must be consumed to have value, lowering the incentives to hoard it.

The model of cryptocurrency inverts the genius of Dwork and Naor's work[x] to lock up energy: this is vastly inefficient, considering the system could be engineered to distribute energy instead of paying people to negate it. The results of such perverted incentives are plain to see in the global impacts of crypto mining: in 2021, bitcoin alone consumed an average of 141 Terawatts/hour; 132TWh of new solar panel capacity was installed worldwide. In the same year, Bitcoin mining rigs cost an average of 7000USD for a machine which consumed an average of 3 kilowatts per hour. A rooftop solar panel array producing 6 KW/h per hour at peak costs about the same (not including installation). The global impact of swapping energy-negative mining equipment for an energy-positive solar array or wind turbine—at scale—is left as an exercise for the reader.

Created with Master PDF Editor. For non-commercial use only.

12. Risks

Where Bitcoin aimed only to replace fiat currency and guarantee payment, it failed by becoming a store of purely speculative value and created an ecosystem of energy waste and fraud. The risks of adopting another blockchain technology to replace the idea of money itself is certainly a more ambitious goal with unknown unintended consequences. Much of how any system operates in reality has to do with the conventions and practices of end users in contrast to the intentions of the system's designers. However, some obvious forseeable risks can be addressed in this paper.

As with currency-based commerce, the layer above purchase, i.e., the inspection and use of the qualities received, lies within the realm of humanity and is ripe for all sorts of human exploitation. **Swapchains attempt to enclose the possibilities of systemic abuse by requiring satisfaction from fellow nodes before credits can be expended.** Because proof-of-trade is subject to human approval, it becomes much harder to game the system in a meaningful way. In addition, truly random sortition, pseudonymity, fair matching algorithms and a sufficient number of nodes in per chain might guard against various types of fraudulent practices. However, if a convention becomes commonplace, it reflects some systemic need, whether expressed 'legitimately' within the proscribed confines of that system.

The systemic risk of fraud producing counterfeit credits itself is fairly low: there is no systemic incentive to limit the number of available credits, unlike blockchains used to create artificial scarcity. Fraudulently creating a spend credit not only implies creating a exponentially expanding set of false burn credits and transactions; it doesn't solve the problem of needing to exchange actual goods or services with another human being. The computational cost of automatically tracing the transactional history of the spend credits offered in the fourth step of the transaction described in §9 should be reasonable.

In fact, every effort should be made to make credits easy to acquire for new entrants, such as giving them away on a regular basis, offering them in exchange for surveys, or by trading them for fungible qualities in exchange for services rendered to a DAO in fulfillment of the terms of an existing swap, like shipping and insurance.

Because the swapchain credit is designed as a medium of exchange rather than a store of value, increasing the supply of credits shouldn't have an inflationary effect the way a traditional currency might. But what making credits trivial to acquire could do is devalue the very trust they tokenize. If it's too easy for malicious actors to start over within the system (having been denied the use of their existing credits by angry transactors), participants won't feel secure swapping with a random stranger on the network.

Created with Master PDF Editor. For non-commercial use only.

Another likely exploit would be a ghost exchange, where two or more parties collude to certify a fictitious trade. This is functionally indistinguishable from an eventual bilateral return of merchandise, provided there is mutual satisfaction[13]. The system is designed to try to deliver equivalent value to what you offer; if a ghost exchange is viewed as a service for whatever reason, the most each malefactor can get away with is a credit and a single trade only by providing additional incoming and outgoing swaps. We assume that in trading between jurisdictions where an item is common in one but prohibited in another, some subterfuge might be employed to use swaps to advertise those qualities.

A ghost trade simply expands the chain, but hopefully not in such a way as to make it prohibitively inefficient. To counterbalance small frauds, swapchains should be large and randomly assembled. A related problem to 'ghost exchange' is that any offers of services are simply IOUs, and cannot be as effectively evaluated as material goods at the point of exchange; some of this risk might be limited by curtailing the number of times a service quality can be exchanged, lest these IOUs become a permanent store of value.

13. Conclusion

The actual work of creating a mutually agreeable swapchain is a monumental computational task, worthy of a distributed network's processing power. However, this paper describes only the proof-of-trade/swapchain system, which constitutes a layer underneath the actual negotiation of the trade. The swapchain only certifies those voluntary exchanges suggested by collaborative algorithms.

The precise mechanisms and algorithms through which equitable, sustainable voluntary exchange on the human level may be achieved through the use of swapchains are beyond the scope of this paper. With so much free CPU time and interconnectivity on their hands, nodes on the network could run a neural network tasked with more efficient barter chain construction: helping smooth out the rough patches in searching for offers (managing distances and shipping costs, finding close alternatives to a desired quality and/or basket of qualities, implementing the personal preferences and experience of node operators, etc).

Ultimately, economic exchange is a human activity, and using technologically aided barter has the potential to create a truly transformational model of economic exchange with greater value to humanity than mere speculative currency.

[13] Altruism (narrowly defined here as exchanging something for nothing) should be rewarded by some convention, whether algorithmically through some governance function, or by an expectation from other transactors.

Created with Master PDF Editor. For non-commercial use only.

References

i Abraham, David J., "Clearing Algorithms for Barter Exchange Markets:Enabling Nationwide Kidney Exchanges" http://www.cs.cmu.edu/~sandholm/kidneyExchange.EC07.withGrantInfo.pdf

ii S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", www.bitcoin.org, 2009

iii Donald, James A. "Bitcoin P2P e-cash paper"

iv https://bitcointalk.org/index.php?topic=27787.0

v https://coincodex.com/cryptocurrencies/sector/proof-of-stake/

vi Kocherlakota, N., "Money is Memory", Journal of economic theory 81, 232251, 1998 https://cpb-us-w2.wpmucdn.com/sites.uwm.edu/dist/8/268/files/2019/01/Kocherlakota-1998-JET-11a7m8w.pdf

vii https://www.youtube.com/watch?v=f1dnocPQXDQ

viiiOne Red Paperclip http://oneredpaperclip.blogspot.com/

ix Benet, Juan. "IPFS - Content Addressed, Versioned, P2P File System" https://raw.githubusercontent.com/ipfs/papers/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf

x Dwork, C., Naor, M. "Pricing via Processing or Combatting Junk Mail" https://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf

Created with Master PDF Editor - For non-commercial use only.