Small Transactions with Sustainable Incentives

Fabio Pianese Matteo Signorini Souradip Sarkar
Nokia Bell Labs
first.last@nokia-bell-labs.com

***Abstract*—The design of a successful distributed system for enabling payments and small transactions among Internet users has long been a major challenge in applied computer science. Bitcoin, the first cryptocurrency having reached world-wide popularity, suffers from sustainability problems such as inefficient energy expenditure for its network operation and from perverse incentives that foster speculative hoarding behavior. We propose a digital transfer system based on a variant of the Bitcoin ledger that is meant to support deterministic small payments with enforced proportional transaction fees: to achieve this property, we renounce the persistence of balances expected of a cryptocurrency, thus mitigating currency hoarding. We introduce at the same time a novel external incentive mechanism based on a verifiable third party with the goal of promoting long-term sustainability, adjusting the margins of profitability for contributors to the proof-of-work scheme without stifling the transaction rate.**

I. Introduction

Bitcoin's seminal distributed ledger mechanism is built in a remarkably clever way around a powerful incentive: it encourages membership in the network by rewarding the participation in the distributed agreement protocol. In turn, membership in the network increases the strength of the ledger against malicious subversion (at least as long as no single entity controls a too large fraction of the deployed computing power [12]). The ledger, which records the entire history of transactions, is organized as a chain of subsequent blocks (blockchain). Immutability of the ledger content guarantees the trustworthiness of the system, preventing 'double spending' attacks that would make accounting unreliable.

In Bitcoin, validation is based on a Proof-of-Work (PoW) challenge, where a cryptographic hash function (SHA-256) is computed on a block of pending valid transactions. Solving the PoW requires finding a nonce (random string) that, when concatenated with a block of transactions, yields a hash whose numerical value is smaller than a target value. The difficulty target is adapted iteratively every 2016 blocks so that the expected time for the system to solve a PoW is about 10 minutes. Variable difficulty allows to stabilize the processing delay of transactions against medium-term fluctuations of the available computing capacity.

An incentive system is introduced to compensate successful PoW solutions (marking the achievement of a consensus based on the randomized outcome of this distributed process) with a decreasing amount of newly-minted currency, which tends to zero in the long run. Transaction fees from the solved block are also collected, as a second form of incentive. The total amount of currency that will be generated by the system is fixed to a target quantity of 21 millions, enforced by the minting algorithm. Accordingly, the system designers confided that, at steady state, the collected transaction fees will be sufficient for sustaining the verification activity so crucial for the survival of Bitcoin. However, a clear weakness is the lack of a mechanism capable to extract transaction fees while guaranteeing that small transactions (from cents to few dollars) are still economically viable compared to alternatives available to Internet users. Accordingly, we believe that a payment system that aspires to sustainably enable large volumes of small transactions needs a way to enforce proportional fees.

In this paper, we introduce a new incentive scheme based on a Bitcoin ledger that uses demurrage, or fixed nominal devaluation over time, to enforce transaction fees which are proportional to both transaction volume and processing delay. We illustrate some interesting side properties of this model, such as its forgetfulness, which allows nodes to trim the blockchain and prevents linking of old transactions with newer ones. We then touch upon a definition of incentive sustainability by proposing a simple mathematical model. Finally, we show that the proposed incentive can be made sustainable for a realistic range of external factors (hash rate, energy price, hardware efficiency, rate and volume of transactions) by relying on a *verifiable and not necessarily trusted* third party that controls the exchange rate and compensates miners for lending currency.

II. Related Work

Risk and costs are the main factors influencing the wide adoption of novel payment systems [2], [8]. While the technical and financial risks tied to cryptocurrencies such as Bitcoin have been widely investigated [1], [4], [6], [9], [11], to the best of our knowledge a study of macroeconomic sustainability and its connected risk and costs has not yet been performed. It is clear that cryptocurrencies struggle to survive within strict constraints of cost imposed by competing alternatives. Böhme et al. [4] showed that Bitcoin might not be as cheap as it is perceived as purchases often requires expensive conversion from and to conventional currencies and consumers forgo kickbacks offered by many credit cards. On top of this, Bitcoin users are still encouraged to pay transaction fees to miners as a compensation for their contribution to the distributed consensus mechanism that maintains the resilience and thus the security of the global system. The problem of access costs to a cryptocurrency is integral to the sustainability problem.

Möser and Böhme [10] published the first longitudinal analysis of Bitcoin fees paid with over 45 million transactions and spanning from the genesis block to the then blockchain

978-1-5386-3662-6/18/$31.00 ©2018 IEEE

head in August 2014. Among their findings, they observe that fees fail to enable a proportional response in terms of processing time. Bitcoin's fee structure attempts to link a concept of priority, capturing the likely delay of a transaction's inclusion in the ledger, with a price per byte of transaction size, reflecting the value of the scarce space available in a block. However, non-homogeneous policies about transaction selection at the miners makes prioritization largely ineffective. Furthermore, they predict issues will arise when transaction fees replace minting as the main reward for miners to maintain the system secure. It is clear that a system entirely based on voluntary fees, even if enforced by popular user agents, cannot offer guarantees to the long term sustainability of the system.

Attempts to revise the incentive model in Bitcoin consider replacing or augmenting PoW with other less costly consensus mechanisms, thus reducing the weight of miner rewards for sustainability. Proof-of-Stake [7] (PoS) rewards the ownership of (and thus the ability to spend) a randomly-chosen atomic currency unit; Proof-of-Activity [3] (PoA) combines PoS with PoW, solving some issues with both systems. PoA increases the fairness and the involvement of the users while reducing the reliance of the network on bulk computational effort for security. Both methods are predicated on the value of ownership of a stake in the network in the form of either the passive holding of a currency amount or the active involvement of users in the verification process. On the other hand, regular users who wish simply to make transactions might find these additional requirements too burdensome to be attractive.

A rich literature exists on the topic of microtransactions, described as massive flows of very small payments that require low latency. Probabilistic schemes for microtransactions involve lotteries [13], *e.g.*, to release 'macropayments' from escrow accounts with much reduced frequency, or established payment channels [14], where a large 'frozen' collateral payment allows the off-blockchain negotiation of state updates with penalties for user misbehavior. The primary focus is on the mechanisms to enable the scalable microtransactions rather than the sustainability of the underlying ledgers.

III. Demurrage Incentives

In Bitcoin two internal incentives coexist. The miners who spend real-world resources to win the PoW lottery expect to receive a minting bonus (indirect, as created by the minting algorithm) plus the sum of the fixed transaction fees collected in a block (direct, as provided by user activity). From a sustainability perspective, we see two problems: *a)* a minting reward encourages hoarding in the early stages of the system's lifecycle. Hoarding is also fueled by the speculation on the rising cryptocurrency value, leading to high volatility in the market valuation that in turn magnifies risk; *b)* typically, fixed transaction fees determine a lower bound to the amount that users will transact over a payment system, which depends on the cryptocurrency value. A likely consequence of this incentive combination is a sluggish growth in the number and volume of transactions, which in turn negatively affects direct miner rewards via a lower rate of fee collection.

TABLE I
Incentives in PoW cryptocurrencies

Incentive	Verification	Transaction
Direct	Trans. fee (int.)	-
Indirect	Minting (int.)	*Demurrage (int.)* *Trans. reward (ext.)*

The former problem cannot be addressed in the context of a *direct* incentive mechanism because of the need to bootstrap the system. Bitcoin initially assigns rewards in a way that is decoupled from the degree of activity and perceived utility of the payment system, both in time (by tolerating positive account balances that do not contribute to the economy) and in value (by way of an exchange rate subject to speculative pressures). The latter, transaction fee proportionality, is notably problematic to enforce: if the marginal cost of accepting a transaction in a block is negligible, then miners will increase their earnings by accepting any non-zero transaction fee, independently of its value [3]. Ultimately, the system ends up penalizing its users, by slowing down their transactions, or alienating them, by requesting large fixed fees to insure prompt service.

A. On Indirect Transaction Incentives

The decreasing minting bonus is a remarkably effective indirect method to both entice the miners and to generate currency that can sustain transactions. However, no such indirect incentive exists that encourages transactions among the holders of the cryptocurrency, which would ensure that the reward given to the verifiers is commensurate with the system's utility as a payment medium. Also, the growing reliance on transaction fees opens new thorny issues for system stability, once the minting reward becomes small enough [5].

The technical choices embedded in Bitcoin jeopardize the long-term sustainability of the system. We propose an incentive system in which ownership is discouraged and proportional transaction fees are levied indirectly (Table I). By taking the block as a time unit, we enforce a negative interest rate during the transaction verification process on the value of all existing balances in the network. With minor technical modifications to support this feature, called *demurrage*, the resulting cryptocurrency system acquires interesting properties:

- fees are enforced by demurrage in proportion to transaction amount and expected execution time
- at steady state total monetary mass is known and fixed, loss of coins is not a systemic issue
- forgetfulness: the blockchain can be trimmed as unspent transaction outputs become devalued
- timeliness: guaranteed lifetime based on fees before a transaction is known as accepted or rejected

B. Rationale and Implementation

At block creation, a set amount q of currency is generated by the algorithm by minting. At the same time, existing currency loses nominal value at fixed rate $0 < r < 1$ (e.g., if the demurrage is 1% per block, $r = 0.99$). At

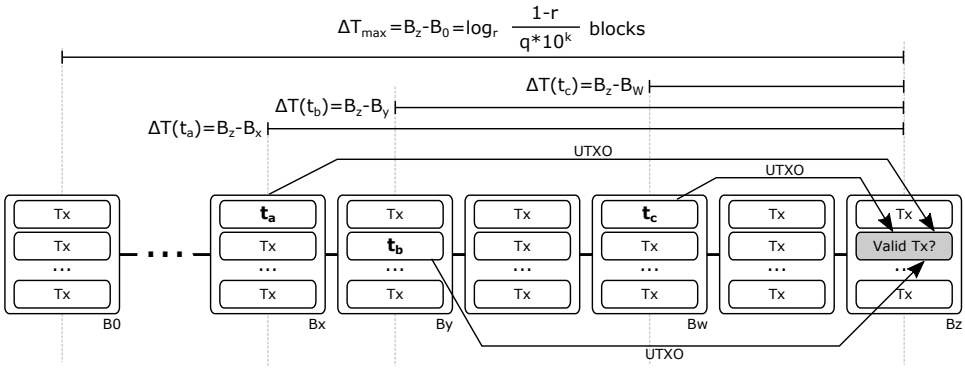

Fig. 1. Effects of demurrage on block lifetime and transaction validity

steady state, the outstanding monetary mass $\mathcal{Q}$ is constant: $\mathcal{Q}(b) = \sum_{i=-\inf}^{b} q_i = q + qr + qr^2 + ... = \frac{q}{1-r}$. As a transaction is published in the network, verifiers must make sure that the account from which the funds are drawn contains enough funds at the current block b by appropriately factoring in the depreciation of the amount A originally stored in the blockchain at block b_0: $A(b) = A(b_0)r^{b-b_0}$, $b > b_0$. In case of insufficient available balance, the transaction is disregarded, otherwise it is accepted and included in the current block b. Similar to Bitcoin, as soon as the PoW for a block is completed, it is published and circulated in the network and work begins on a new transaction block.

Standard transactions specify a number of inputs (credits being consumed) and outputs (credits being created). Transaction outputs are uniquely identified by an ID and, as each one of them can be spent once, can be either classified as *unspent* (UTXOs) or *spent*. Furthermore, excluding the case of coinbase transactions, the sum of the outputs must not exceed its inputs lest the transaction be rejected. Any excess in input values, on the other hand, is collected as a transaction fee by the miner who solves the block in which it is included.

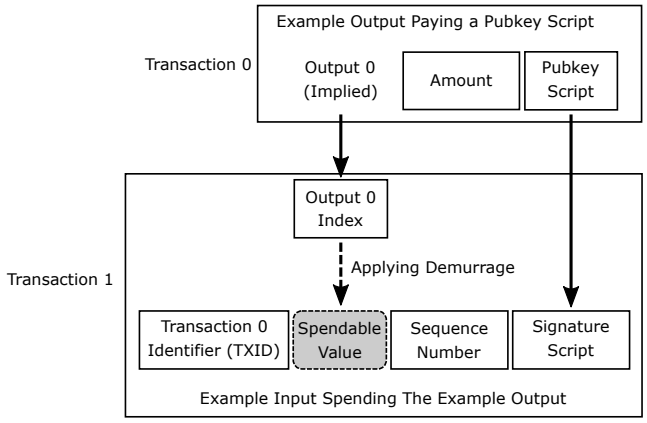

Fig. 2. Tx Spending overview with demurrage

Under demurrage, UTXOs lose value over time at a constant rate r. Demurrage determines a set of block lifetime windows (ΔTs in our notation) during which the various outstanding balances in the system are non-zero, as shown in Figure 1. The maximum lifetime of any transaction in the system $\Delta\mathrm{T}_{max}$ is thus computed as the time required for the largest sum available in the system $\mathcal{Q}$ to decay to zero. It is defined as:

$$\Delta\mathrm{T}_{max} = \log_r \frac{1-r}{q \cdot 10^k} \quad \text{blocks}$$

where k is the precision in decimal digits of the currency unit representation (in Bitcoin, $k = 8$). In practice, most of the balances in the system will decay much faster than $\Delta\mathrm{T}_{max}$. This feature results in a much smaller storage overhead in both the blockchain data structure and in the content of memory pools at every node, which allows to tune important parameters (such as block size and target periodicity) to help accommodate increased transaction workloads.

The way in which peers can retrieve information to compute the demurrage and validate UTXOs does not require any alteration of the Bitcoin standard protocol. Indeed, in order to check for double spending attacks, miners browse the blockchain starting from the UTXO block up to the new block which has to be created. As such, during such operation, the miner calculates ΔT as the number of blocks elapsed since each UTXO's inclusion in the blockchain. It then applies to each input value a $r^{\Delta T}$ devaluation factor and checks whether the amount is still positive. It then verifies that a non-negative transaction fee is associated with the transaction before validating it. Newly-minted coins that compensate for the decayed ones, plus collected transaction fees in excess of demurrage loss, are introduced in the system via a coinbase transaction in accordance with the Bitcoin protocol.

Figure 2 depicts an overview of a single transaction spending where each input, referring to a previous transaction's output, does not have access to the whole output but to a portion of it. Code shown in Listing 1 synthesizes the relevant changes made to the *Bitcoin-core* source code to support demurrage calculation. The devalued amount to be considered when a transaction is executed is computed via the *InputDemurrage()* function as *txout.nValue * demurrage* where the demurrage is computed by *pow(1-rDemurrage, age)*. The *age* value here is the difference between the current block height and the block height of the referenced UTXO.

```
double getDemurrage(unsigned int
    pastBlockHeight, unsigned int
    currentBlockHeight){
  int age = currentBlockHeight -
      pastBlockHeight;
  double demurrage = pow(1-rDemurrage, age);
  return demurrage;}

CAmount InputDemurrage(const CTransaction&
    tx,int n,const CTxOut& txout){
  const CAmount amount(txout.nValue *
      getDemurrage(n,
      chainActive.Height()));
  return amount;}
```

Listing 1. Calculating demurrage on unspent outputs during validation

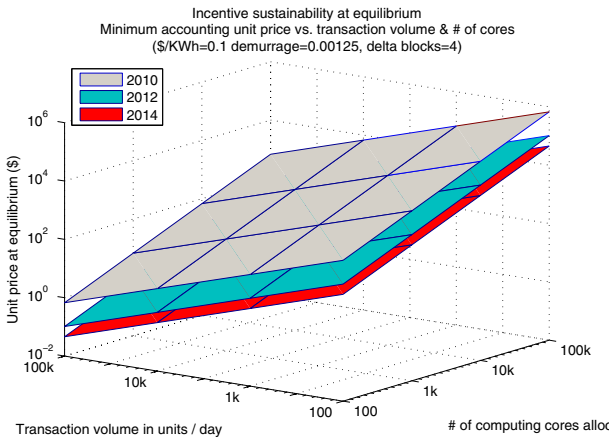

Fig. 3. Sustainable equilibria: accounting unit price vs. verifier population and transaction volumes in three operating scenarios

IV. Sustainability

In a perspective of long-term survival of the system, especially after the minting bonus fades and transaction fees fund the verifiers' reward, we need to find a set of conditions for which the collected transaction fees cover or exceed the verification costs. Bitcoin's network-wide cost and reward functions can be approximated as:

$$C = \frac{H}{\xi_H} P_W t \qquad R = (\kappa + \Phi T) P_X$$

Where H is the total hashrate of the network, ξ_H is the average hashing efficiency (in hashes/J), P_W is the price of electricity, and t the time expectation for a reward to be created; κ is the minting reward, Φ the fixed transaction fee, T the number of transactions, and P_X the currency exchange rate. To work under consistent sets of assumptions, we looked into the historical developments of Bitcoin and of its supporting ecosystem. In Table II we define three scenarios, corresponding to distinctive phases of Bitcoin's life: an early stage circa 2010, in which the prevalent technology used for validation was CPU; a time of rapid growth circa 2012, when GPUs became the standard platform; and a maturity stage circa 2014, when off-the-shelf ASIC-based devices became available. For our calculations we set energy price at 0.1 $/KWh. We observe that, while the minting incentive guarantees a succulent payoff under the recent scenarios, transaction fees alone would not be sufficient to sustain the system in any of these configurations. A complex tangle of trade-offs exists between the currency exchange rate P_X, the transaction fee value and its enforcement policy the transaction volume S, the number of transactions T, and the resilience of the system against PoW attacks. The energy price is ultimately the deciding factor of whether the incentive is sustainable, as the cost of performing validation is proportional to the hardware resources engaged in the process (for a given technology).

A. Analysis and Results

To estimate the sustainability boundaries of our proposed demurrage incentive, we model the value of P_X that yields the economic equilibrium condition ($R = C$) for the entire network. In Figure 3 we represent the equilibrium price $\overline{P_X}$ across a large spectrum of conditions, including the size of the V population, the daily transaction volume S, and the technology platform of choice (derived from the Bitcoin scenarios in Table II). The cost function used in this Figure implements the demurrage incentive in the form of a demurrage rate of 1.25‰ per block ($r = 0.99875$) and a conservative duration of a transaction cycle (i.e., from V to U, among members of U, and from U back to V) of 4 blocks.

We observe that there is a smooth dependency between $\overline{P_X}$ and the independent variables of the system. Given an initial value of $P_X > \overline{P_X}$ enforced by M to sustain the system at a low transaction rate, we expect that the incentive will drive the system towards a stable equilibrium: the increased revenues from a larger transaction volume will attract a larger population of verifiers until $C \sim R$, at which point any increase in the verifier population will be discouraged, unless called for by a larger transaction volume. The fact that M retains control of P_X and can adapt it over time allows to fine-tune the balance between difficulty of the PoW (which protects the ledger from attacks) and overall energy footprint of the system (to prevent wasteful derives of the previously unbridled verifier population).

B. Implications: External Mining Incentives

A currency that cannot retain its value over time is an unlikely target for hoarding, and therefore has negligible value *per se*. Accordingly, if the mere ownership of the currency received as reward for the verification work cannot be monetized externally, it is unlikely that the mining incentive as a whole would work as intended.

We address this point by introducing a novel form of *external* incentive that compensates the lending of currency units by stakeholders to fund transactions among the users. The external incentive is administered by a market M, a third party entity that facilitates the issue of funds to the users from the verifiers. The reward is paid by M to miners in an external currency, in order to to compensate them of the losses incurred

TABLE II
BITCOIN REFERENCE ECOSYSTEM SCENARIOS (AVERAGES, FROM BLOCKCHAIN.INFO & EN.BITCOIN.IT)

Year	Tech	ξ_H (Mh/J)	H (Gh/s)	T/block	S/T	Φ	P_X ($)	mint/block	$\frac{R}{C}$(mint)	$\frac{R}{C}$(~~mint~~)
2010	CPU	0.050	14.895	4	37.7	0	0.1	50	1.0	~ 0
2012	GPU	3.855	$17 \cdot 10^3$	149	19.37	.0001	10	25	6.7	0.002
2014	ASIC	1429	$149 \cdot 10^6$	448	7.64	.001	400	25	5.8	0.10
2016	ASIC	10182	$1.36 \cdot 10^9$	1450	15.14	.00025	550	12.5	3.1	0.09

by demurrage while users were performing transactions. The reward may correspond to the interest on the nominal value borrowed $I(b) = A(b_0)(1 - r^{b-b_0})$, $b > b_0$, multiplied by the exchange rate[1] of the cryptocurrency P_X.

A first remark about the scheme sketched above is that the value of the exchange rate parameter P_X is now irrelevant to the successful execution of a transaction. The receiver of a transaction can claim its value, diminished by demurrage since the transaction's block creation, by exchanging it back on M against external currency, or can use it to perform new transactions via the payment system. The brokerage by M enforces a "limited-convertibility" rule on the positive account balances in the system, which cannot be redeemed into an external currency unless the initial transaction in a chain was also performed through M. Since P_X can be controlled by M and determines the amount of reward received by miners, it provides a powerful means to control the system-wide incentive with which to drive the system to a point of sustainable equilibrium.

A second remark is that the role of M is not too dissimilar from the role of present-day currency exchanges, at least as far as users are concerned. By guaranteeing stability in the value of P_X, M eliminates the volatility risk associated with trading in a fully-convertible cryptocurrency. From the miner's point of view, the reward collected from minting becomes tightly coupled with the activity level and volume of transactions being conducted over the network. In the best case, supposing a continuous stream of transactions is executed using the q balance minted by V, he will receive from M a total value of qP_X over the entire lifetime of the reward. The miner can easily verify that he's not being cheated by M by examining the transaction record in the blockchain to check when (and how much of) his balance was borrowed from his account. By making the reward value proportional to transaction volume, a link is created between external utility of the payment system and its total cost of operation, fostering a sustainable growth in the miner population as long as the system's adoption and usefulness expands.

Throughout this discussion, we considered M as a single logical entity for clarity, but it could easily be implemented as a distributed system managed by multiple tenants. In this case, M would operate as a multilateral (pool) clearing system [15] and its members should be bound to cooperation by technical and legal agreements (e.g. to prevent arbitration on the value of P_X across members and to ensure that account imbalances are periodically settled and commitments honored).

[1]M ensures its own sustainability with traditional means, e.g. controlling the spread between buy and sell prices of currency units transacted by the users and/or applying flat exchange fees.

V. CONCLUSIONS

We proposed and analyzed an incentive model for ledgers based on PoW mining providing a sustainable reward to miners by way of an indirect transaction incentive, based on the principle of demurrage, and an external mining reward provided by a verifiable third party. By rewarding miners based on the amount of transactions carried over the network in a way that can be externally controlled and is not patently threatened by strategic manipulation of users and miners, we showed that equilibria can be reached that guarantee the sustainability of the payment system across a large spectrum of internal and external system parameters.

ACKNOWLEDGEMENT

This paper has been accepted for publication in Blockchains and Smart Contracts workshop (BSC'2018).

REFERENCES

[1] R. Ali, J. Barrdear, R. Clews, and J. Southgate. Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, 54(3):262–275, 2014.

[2] Ross Anderson. Risk and privacy implications of consumer payment innovation, 2012.

[3] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Proof of activity: Extending bitcoin's proof of work via proof of stake. In *ACM NetEcon*, 2014.

[4] R. Bohme, N. Christin, B. Edelman, and T. Moore. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2):213–238, may 2015.

[5] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan. On the instability of bitcoin without the block reward. In *Proc. of ACM SIGSAC CCS Conference*, pages 154–167, 2016.

[6] Ghassan O. Karame. Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. In *Proc. of ACM CCS*, 2012.

[7] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake, 2012.

[8] William J. Luther. Cryptocurrencies, network effects, and switching costs. *Contemporary Economic Policy*, 34(3):553–571, 2016.

[9] T. Moore and N. Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *Financial Cryptography and Data Security*, pages 25–33. Springer, 2013.

[10] M. Möser and R. Böhme. Trends, tips, tolls: A longitudinal study of bitcoin transaction fees. In *Financial Cryptography and Data Security*, pages 19–33. Springer, 2015.

[11] M. Möser, R. Böhme, and D. Breuker. Towards risk scoring of bitcoin transactions. In *Financial Cryptography and Data Security*, pages 16–32. Springer, 2014.

[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org, 2008.

[13] R. Pass and A. Shelat. Micropayments for decentralized currencies. In *ACM CCS*, 2015.

[14] J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf.

[15] E. F. Schumacher. Multilateral clearing. *Economica*, 10(38):150–165, May 1943.