

Block Transfer

A Decentralized Stock Transfer Agent Protocol

For Global Financial Markets

John Wooten
john@blocktransfer.io

May 25, 2021

Version A.25

Detailed in US PPA #BTFEJW1P(Mar. 2021)–BTFEJW2P(tbd)

Utility patents extending PPAs in drafting (submission date tbd)

Most recent version at whitepaper.blocktransfer.io

Abstract

Shareholders today widely accept the centralized stock transfer agent model, but it's fundamentally flawed. Transfer agents effectively became six-figure Excel ledgers billed to shareholders after mass digitization forty years ago. In the US public market alone, stock transfer agents waste an aggregate of over 1.44B¹ each year. This expense effectively (although minorly) **hinders the returns of every stock investment on Earth** since fair figures are paid out for transfer agent services rather than meaningful internal corporate investments. Furthermore, transferring securities often takes hours on the phone or computer with unreliable middlemen processing complex owner validation. Not to mention, all systems fall back to one insecure point of accounting trust.² Thus, we propose an open decentralized transfer agent protocol built on blockchain.

1 Centralized Market

1.1 Issuers Are Systematically Underserved & Overcharged

The transition to blockchain today is much like the transition from paper to digital book-entry securities in the 70s and 80s. Central computers offered an obviously faster

¹See Slide 15 & Appendix D

²Think Arthur Anderson/Enron incentives for current firms

service and removed the need for runners and other paper-processing middlemen. For all intensive purposes, digitization saved Wednesdays on the Street. [3]

Likewise, blockchain technology offers a new geometrically-faster service and removes the need for account managers and other computer-processing middlemen. Compared to the current speed, cost, and added benefits of current blockchain implementations, widely-popular centralized transfer agents systematically offer lackluster performance in a market with lax competition and little threat of distribution from previous innovators.

The Block Transfer protocol removes trusted middlemen from CUSIP ownership management and transfer, alongside central shareholder fees. The technology implemented allows for complete public auditability and transparency of ownership distributions. Thus, **anyone can audit the transfer agent ledger** for tax compliance, investor equity stakes, voting representation, and more **at any time** without trusting a central party, enabling recordkeeping at significantly reduced ‘trustless’ costs.

1.2 The Flaw

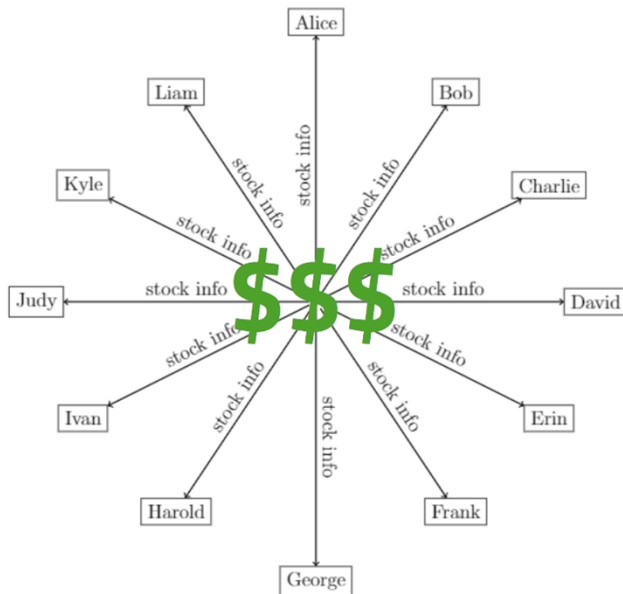


Figure 1: Centralized Transfer Agent Bookkeeping

All shareholder transfer requests, corporate actions, and regulatory reporting flows through the transfer agent. Thus, trust is understandably difficult to achieve in the transfer agent market. Once you have trust, a transfer agent firm can in theory steal the ownership rights of a company’s securities through falsified CUSIP reports.

This challenge is especially emphasized by old transfer agents because they have one central source of bookkeeping trust. That means one rogue low-level employee

able to make it past security checks **could cause millions or more in fraud damages overnight**. This weakness in the central model leads old agents to charge more for their services (for larger firms) to make their accounting seem “more secure,” leveraging the mentality that ‘you get what you pay for’ even though the cost to service most firms is about the same. Over the last forty years, this trend of charging more and more for the false pretense of central accounting security created **one of the highest-margin businesses in all of public finance** at the expense of issuer balance sheets.

Transfer agents got away with this deception for so long because of the lengthy, complex, and sometimes costly regulatory requirements to act as an agent, which were rightfully put in place after much fraud in the 1920s. Likewise, Block Transfer complies, advocates for, and even seeks to assist³ with the regulation in the transfer agent space. However, for so long prior the revelation of blockchain, transfer agents **misused the power of their compliance to charge firms as much as possible**, oftentimes charging smaller issuers \$75 or more for a simple book-entry transfer. At Block Transfer, we’re changing that and approaching the market with a ‘save-money-first’ mentality because we firmly believe that issuer capital should be used in important business projects that benefit all shareholders by creating more corporate issuer value.

For over a century, there has been no clear answer to this dilemma—no definitive way to maintain a transfer agent ledger without a highly trusted middleman, unreasonably costing issuers billions every year that should be put to a higher use.

2 Blockchain—The Solution

In this section, we’ll dive deep into how the Block Transfer protocol works, its two stages of implementation, and some assumptions we made developing its frameworks. We built Block Transfer so that issuers and shareholders alike can leverage our platform while barely realizing that it’s built on blockchain. If you’re a client or issuer shareholder, **you don’t need to understand the Block Transfer protocol** at all to access your account and swiftly execute any daily actions. “Your relationship with it can be like a train passenger’s relationship with the train’s engine: you know it exists, you rely on it to keep working, but you don’t spend your time monitoring it or studying its internals. You’re welcome to study, observe, and even participate in the protocol, but you don’t need to, and most people won’t.” [1]

³Co-founder John Wooten is an aspiring future member of the CFTC/SEC Working Group on Digital Assets pursuant to the Eliminate Barriers to Innovation Act of 2021.

2.0.1 High-Level Premise

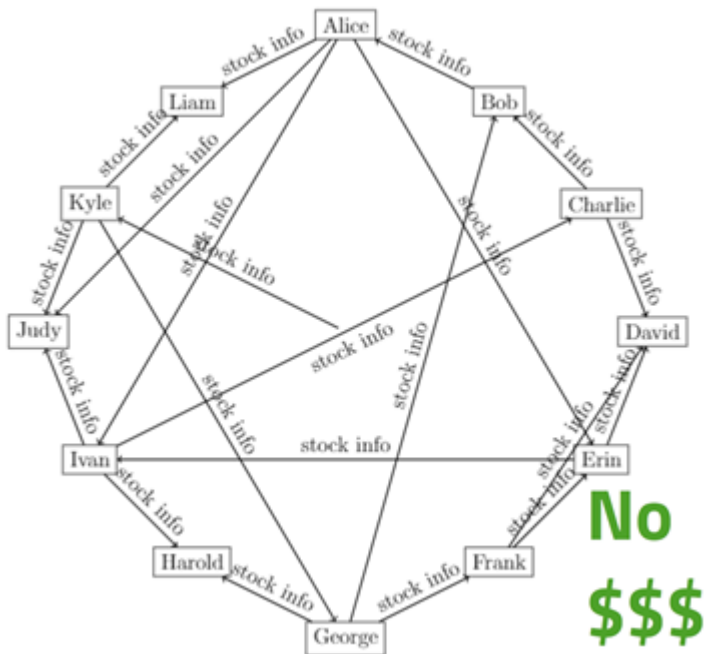


Figure 2: Decentralized Blockchain Bookkeeping

Modern blockchain technology solves the challenge of centralized transfer-agent ledgers by providing an automated way to store and transfer stock ownership records in a secure way that anyone can verify. The Block Transfer protocol uses this technology as the accounting basis for its development of a decentralized stock transfer agent for global financial markets.

Our protocol leverages this triple-entry accounting (double-entry bookkeeping verified by an immutable trustless blockchain network) to record ownership of tokenized public equities. Thus, individual parties can securely sign their own transfers of securities with decentralized cryptographic keys.

2.1 Stage 1

Stage 1 implements Block Transfer on the Ethereum blockchain. We chose to start out on Ethereum because it is the largest, most secure smart-contract-compatible blockchain on Earth. This was of particular importance to us because we feared incumbents trying to deny service to our issuers through 51% attacks or equivalent. By starting out on Ethereum, we make the cost of such an attack economically infeasible. Furthermore, future benefits may accrue as the network transitions to Casper. The vast scale of the Ethereum network simultaneously allows us to represent CUSIP

assets directly on the blockchain network, removing the ability for Block Transfer to manipulate assets due to Ethereum’s robustness.

2.1.1 Protocol Execution

In Stage 1, anyone can validate shareholder records and thus asset ownership by trustlessly querying the Ethereum L1⁴ Merkle Patricia ledger root. [2][1] With this ownership model, no party needs to be trusted for core transfer functionality so long as participants trust the underlying blockchain network and at least one honest Arbitrum validator exists (say Peer *BT*, detailed later).

We execute Block Transfer through a collection of systems and processes coded in a Solidity smart contract. These contracts are then deployed to compliantly maintain transfer agent records for issuers through the issuance of digital tokens representative of underlying asset’s shareholders.⁵ Prior ETH2, we scale these contracts through optimistic rollups and leverage their executive function calls to execute corporate actions submitted by issuers. All contracts are publicly-auditable on Etherscan, and we list the addresses of the contracts for each issuer we service for 24/7 public audit.

We chose to use Arbitrum Rollups in our execution so that shareholders can efficiently have finality in minutes rather than days once transfers reach validators who can leverage trustless finality to extend asset transfer Merkle history despite disputes by verifying the prior states of the L2 chain.

2.2 Stage 2

We plan to implement Stage 2 in Block Transfer Version C.44 once building up a track record as a reliable, compliant transfer agent. Stage 2 executes Block Transfer through its own sovereign Proof-of-Stake blockchain. That means transfer clear in $T + \text{negligible seconds}$ and achieve instant finality directly through our own chain’s validators, rather than relying on Ethereum. Achieving this vision requires Block Transfer to have enough value in the market such that the native currency of the blockchain has enough intrinsic value for validators to act honestly, while also preventing incumbent centralized transfer agents from accruing significant percentages of the currency to execute denial-of-service attacks.

By executing Stage 2, we can have all the issuers Block Transfer services tokenized on one validated blockchain rather than through many smart contracts with independent rollup validators. This means more consensus on state and, given blockchain native value, even more security than already provided with Ethereum.

⁴Ethereum verification net Merkle hashes occurs on ‘Level 1’ of the Ethereum blockchain, whereas Arbitrum Rollups execute on ‘Level 2’ to drastically drop shareholder transfer costs.

⁵Based on pre-IPO cap tables or prior transfer agent ledgers.

2.2.1 Token Economics

In such a future chain, Block Transfer distributed native currency at the beginning as seen fit & then possibly distributes such funds via a faucet for new shareholders so that they can use the token to transfer assets. To submit a transfer, shareholders will pay a nominal amount of the native token to prevent spam denials of service, rather than nominal amounts of ether. Through a pricing stability mechanism, we plan to take the average decentralized exchange rate of the native currency in the past day, determine how much of the currency to charge that's $\simeq 1\text{¢}$ through a consensus DAO or equivalent, and set that as the default transfer rate issued to validators.

3 Technical Description derived from generalized Patents

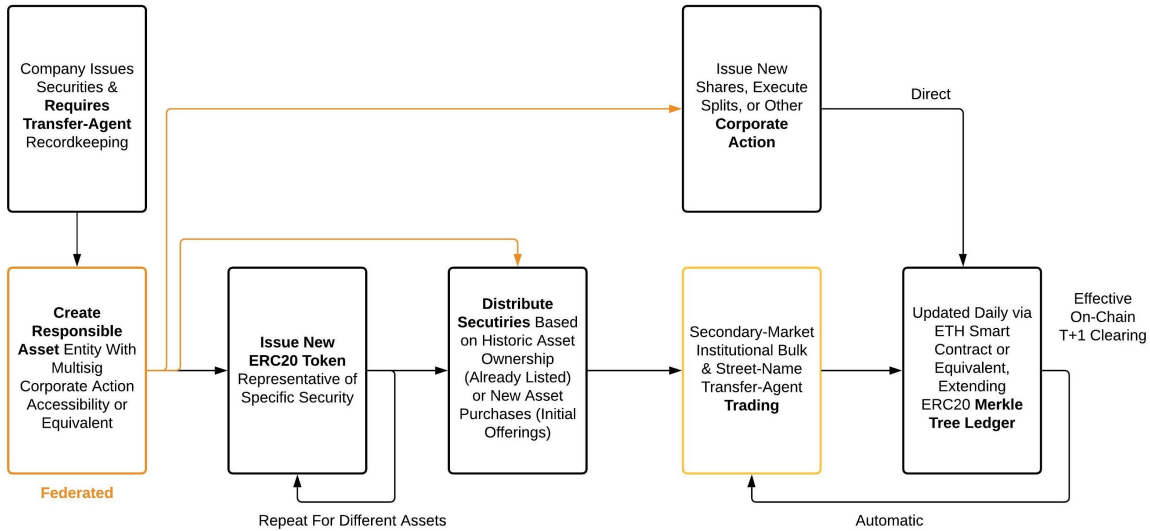


Figure 3: Block Transfer Federated Protocol

Per Figure 3,⁶ issuers that require transfer agent services can leverage Block Transfer to easily, compliantly keep track of their securities on a distributed ledger at minimal cost. The following subsections explain each step of this process in detail.

3.0.1 Create Responsible Asset Entity With Multisig Corporate Action Accessibility or Equivalent

First, issuers onboard with a transfer agent registered in their jurisdiction willing to back the statements of the distributed ledger with the proper infrastructure, regu-

⁶This figure is from A.12 and does not take into account the T+minutes scalability we've additionally implemented through optimistic rollups. We're finalizing our protocol testing and audits, and will update this transfer time accordingly in A.27.

latory approvals, industry connections, compliant certificates, accounting overhead, technical expertise, insurance, etc. (referenced herein as Peer \mathcal{BT}). Peer \mathcal{BT} then securely generates a network wallet, following the details of a contractual obligation with the issuer to act as their transfer agent.

This cryptographic wallet requires collective issuer Board approval for executive actions.⁷ For deployment contract purposes, these actions cover stock splits, new CUSIP issuance, and transfer from authorized to unrestricted shares or equivalent. Tender offers with proper SEC registration or equivalent are executed through on-chain smart contracts deployed at the time of receiving a registered tender offer by Peer \mathcal{BT} . Peer \mathcal{BT} also handles dividend distribution in US dollars (legally required in US, or equivalent) through internal direct deposit with shareholders registered by prior transfer agent or through KYC onboarding. These distributions are reported to shareholders through applicable tax forms each year. Restricted shares are implemented through contract sub-functions requiring necessary conditional approval. Warrants (given separate CUSIPs) are handled through separate contracts and redeemable at expiration or SEC-approved forced redemption through provisions in Subsubsection 3.0.5's Lemma proof alongside Peer \mathcal{BT} .

Post-agreement with the issuer, Peer \mathcal{BT} connects to and queries the underlying network and begins the issuance or transfer process of said issuers' securities through Block Transfer contract constructors and mint functions.⁸

3.0.2 Issue New ERC20 Token Representative of Specific Security

Peer \mathcal{BT} compliantly deploys the Block Transfer protocol with initialized parameters representative of the issuer's securities, and the blockchain network creates a new decentralized token. **The new distributed ledger is the legally-binding representation of ownership in the underlying** per Peer \mathcal{BT} 's transfer agent agreement with the issuer. Process repeated as needed for other issuer securities.

3.0.3 Distribute Securities Based on Historic Asset Ownership (Already Listed) or New Asset Purchases (Initial Offerings)

Completed proprietorially by BlockTrans Syndicate, a Delaware corporation. We'll update the Whitepaper with further specifications post-patent issuance.

3.0.4 Issue New Shares, Execute Splits, or Other Corporate Action

Using the secure blockchain account established in Subsubsection 3.0.1, Peer \mathcal{BT} ⁹ calls pre-assigned contract functions or internal operations to process corporate ac-

⁷Amendable should the issuer's Board of Directors change

⁸Ideally on a weekend with little book-entry trading activity when transferring from old agent.

⁹May be the issuer's Board through a multisig wallet given collective autonomous control over executing forward or reverse stock splits, dividend or coupon distributions, further offerings or buybacks said wallet, or cancellation of tokenized ownership for debenture securities, as matured.

tions as directed and signed by the Board. The automated security built into the implemented blockchain network ensures that (assuming trust in the underlying MPC and distributed ledger technologies used) the Board is the only organization that ever controls the executive ‘msg.sender’ caller that controls the smart contract provided by Peer \mathcal{BT} (or equivalent). This remains true so long as the private keys used to generate the multisig account or equivalent depending on the blockchain network are generated, stored, and accessed securely.

3.0.5 Secondary-Market Institutional Bulk Street-Name Transfer-Agent Trading

This stage is handled by the DTCC side of the share registrar, under Cede & Co.’s wallet address on the transfer agent ledger, per agreements and connections as the DTC maintained by Peer \mathcal{BT} . Further detailed in proofs.

3.0.6 Updated Daily via ETH Smart Contract or Equivalent, Extending ERC20 Merkle Tree Ledger

As transfers take place, they are recorded on a perpetually-updated pseudonymous Merkle tree. The confirmation times of these transfer agent book transfers are as equivalently small as the cryptographic validation confirmation speed on the underlying blockchain. This Subsubsection will be updated for Patricia Merkle Tree specifications in A.26 with lower transfer times per our developmental improvements to the Block Transfer protocol in A.25.

4 Regulatory Compliance

For the Block Transfer protocol to function, Peer \mathcal{BT} , as stated in its definition, must register with the SEC alongside other significant market participants (or equivalent) and comply with such regulations regarding the maintenance of transfer agent ownership reports of public securities. Additionally, Peer \mathcal{BT} must comply with SEC Section 17(c) and 17(d)-15 insofar as validating and standing liable for all CUSIP transfers approved by the Block Transfer protocol.

To comply with these regulations, we automatically and securely records a snapshot of the blockchain transfer agent ledger after traditional market close and reconciles it with federated shareholder information equivalent to peer address information. This pull is done by having a function call to the smart contract that pulls the latest Merkle Patricia header and thus sum Merkle tree of shareholder ownership records

To be implemented in B.31. Since the stock transfer agent is not responsible for enforcing trading halts, there is no need for Peer \mathcal{BT} to have overruling multisig access to this federated wallet and thus the issuer has complete independent control of implemented corporate actions and executive decisions regarding their CUSIPs or the state of Peer \mathcal{BT} .

(in Stage 1). This pull is imported into Peer *BT*'s IPFS node as a collected ledger. Security of this ledger is unimportant and can thus be public since it records the same information as available by a simple analysis of the previously defined blockchain.

Once a Merkle root is created, anyone can access the ledger and verify their or other market participant's shareholder ownership similar to how it is displayed in the perpetual network. Furthermore

Peer *BT* then automatically pulls shareholder information through calls to its IPFS node and reconciles the public addresses with regulatory-required holder information. This report is accessible at any time and on demand by the issuer. Then, through simple API calls, Peer *BT* can automatically submit this ledger to the SEC for simple regulatory compliance. Annual reports can be similarly automated securely since all form TA-2s are formatted identically. Peer *BT*'s reporting truthfulness can be audited by anyone since their submitted document is hashed to an IPFS pin, and anyone can access the published reported SEC documentation to verify its hash against said file alongside the validity of its claims and ownership distributions per comparison with the public chain and hashed history.

5 Future Work

Other technical implementation details for regulatory-compliant shareholder voting commitment schemes, similar to TrueBit, Maker, and federated voting DAOs.

References

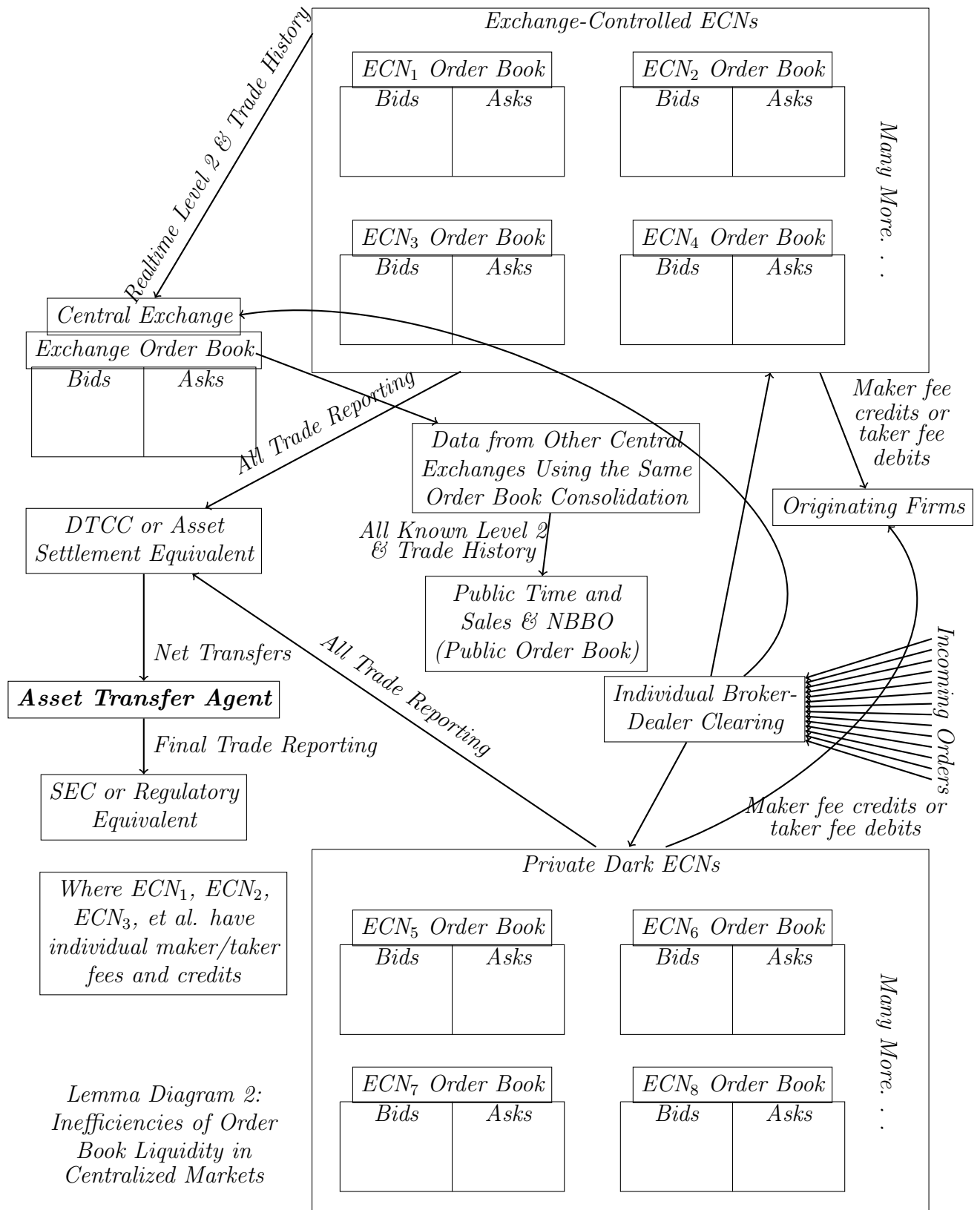
- [1] Ed Felten, Steven Goldfeder, H. K. L. B. J. C. R. F. (2021). Protocol Deep Dive. *Offchain Labs, Inc.*
- [2] Foundation, E. (2020). Patricia Tree. *Ethereum Wiki*.
- [3] Gray, N. (2017). The New York Stock Exchange Used to Be Closed Every Wednesday. *Medium*.
- [4] US Congress ([1934] 2012). Securities Exchange Act of 1934. *The United States of America*.

A Centralized Markets

Lemma 1. *Relying greatly on centralized transfer-agent trust enables incumbents to, (i) behind closed doors and for their own profit's sake, manipulate the lending practices of long-term untouched book-entry CUSIP shares with very low need for immediate liquidity to profit internally by lending out securities to shorts without shareholder knowledge or consent in violation of the Securities Exchange Act of 1934 Sec. 8;¹⁰ [4] (ii) pass fraudulent corporate actions such as illicit secondary offerings to create widespread shareholder dilution for the sake of extremely large profitable shorts; and (iii) in a complete worst case scenario, fraudulently steal book-entry securities and dump them on the open market behind closed doors and likely without consequence for a reasonable amount of time given the public opaqueness of current transfer agent books (large risk if burning the books and shutting down operations could produce a short-term profit greater than the long-term value of providing transfer agent service).*

Lemma 2. *To increase your understanding of where transfer agents fit in the market, we'll look at the process most stock trades go through. There's a lot of information preceding this diagram regarding incoming orders omitted due to a lack of significant involvement with the transfer agent. Furthermore, there's a lot of additional information about Electronic Communication Networks and central-exchange mechanisms that effectively bear no impact on the transfer agent. Not to mention, there are a lot of nuances not fully captured by this diagram that again bear no impact on transfer agent functions. Please don't read too much into Lemma Diagram 2, but rather use it to understand the comically complex current state of trading middlemen. This complexity, combined with a lack of clear information on the functions of transfer agents, enabled old firms to charge so much for a reasonably simple service.*

¹⁰See Block Transfer's work as lead plaintiff in *Shareholders v. The Vanguard Group, Inc.* (DE)



*Notice that the transfer agent in practice only interacts with the Depository Trust & Clearing Corporation¹¹ and Securities & Exchange Commission (alongside book-entry shareholders and public clients) (or equivalent). Notably, the DTCC effectively handles all trade settlement off the direct transfer-agent book through one commingled ownership record under Cede & Co. (**C**entral **D**epository) such that no shares move on the book when net broker trade consolidation occurs. Thus, the share balance of Cede & Co. only changes through offerings, splits, or movement from a brokerage account to/from the book-entry ledger. 80–90% of US equities are held by the DTCC through Cede, enabling the complex market participants in Figure 2 and beyond to increase profits at your expense through three-week settlement leniency.¹²*

| Name | Address | Shares | Date Issued | Date Cancelled |
|---|----------------------------|-------------|-------------|----------------|
| Cede & Co. | 120 Somewhere Street, Fers | 869,420,821 | 3/29/2018 | |
| Hillhouse Capital Advisors Ltd. | 121 Somewhere Street, Fers | 38,648,477 | 3/29/2018 | |
| Morgan Stanley | 122 Somewhere Street, Fers | 31,838,451 | 3/29/2018 | |
| Credit Suisse Ag/ | 123 Somewhere Street, Fers | 25,220,152 | 3/29/2018 | |
| Goldman Sachs Group, Inc. | 124 Somewhere Street, Fers | 24,780,889 | 3/29/2018 | |
| UBS Group AG | 125 Somewhere Street, Fers | 20,151,665 | 3/29/2018 | |
| Nomura Holdings Inc. | 126 Somewhere Street, Fers | 15,946,694 | 3/29/2018 | |
| Blackrock Inc. | 127 Somewhere Street, Fers | 10,446,752 | 3/29/2018 | |
| Vanguard Group, Inc. (The) | 128 Somewhere Street, Fers | 8,913,516 | 3/29/2018 | |
| Canada Pension Plan Investment Board | 129 Somewhere Street, Fers | 6,970,111 | 3/29/2018 | |
| Bank of America Corporation | 130 Somewhere Street, Fers | 5,563,347 | 3/29/2018 | |
| Vanguard International Stock Index-Total Intl Stock Inc | 131 Somewhere Street, Fers | 3,457,929 | 3/29/2018 | |
| Vanguard International Stock Index-Emerging Markets | 132 Somewhere Street, Fers | 3,075,937 | 3/29/2018 | |
| KraneShares CSI China Internet ETF | 133 Somewhere Street, Fers | 2,493,773 | 3/29/2018 | |
| iShares Core MSCI Emerging Markets ETF | 134 Somewhere Street, Fers | 2,168,732 | 3/29/2018 | |
| iShares MSCI Emerging Markets ETF | 135 Somewhere Street, Fers | 819,963 | 3/29/2018 | |
| Delaware Group Global & International Funds-Emergi | 136 Somewhere Street, Fers | 700,000 | 3/29/2018 | |
| iShares MSCI China ETF | 137 Somewhere Street, Fers | 593,721 | 3/29/2018 | |
| Amplify Online Retail ETF | 138 Somewhere Street, Fers | 413,142 | 3/29/2018 | |
| Vanguard Intl Equity Index Fds-FTSE All World ex U.S | 139 Somewhere Street, Fers | 405,198 | 3/29/2018 | |
| Wells Fargo Emerging Markets Equity Fd | 140 Somewhere Street, Fers | 375,339 | 3/29/2018 | |

Figure 3: Example of Top \$1Q Class A Shareholders
(inaccurate due to opaqueness of transfer-agent ledger)

¹¹Also interacts with OTC Markets Group when applicable for transfer-agent share verification

¹²The DTCC which, through special documentation outside the scope of this whitepaper, can effectively empower brokers to transact more shares than issued through 21-day failure-to-deliver periods. A prime example includes the rampant short selling of Overstock in 2008. Generally, a very small portion of shareholders (maybe 25% on the high end) vote at annual meetings. Because the so many people shorted the stock through laxly-settled trades routed through the DTCC, significantly more people ‘owned’ the stock than the number of shares issued. Around 200% of outstanding stock voted by broker-delegated proxy at the Overstock annual meeting, showcasing just how many investors bought thin air thinking it was stock. For more on this phenomenon, see minute two here.

B Decentralized Markets

Lemma 3. Subsubsection 3.0.5. *At this stage, a vast bulk of share transfers come from (i) large funds directly entering a debit equity position through book-side registration, transacting with the corporate multisig account itself (if shares allocated) or simply moving onto the transfer agentbook after executing a block-size acquisition on dark ECN(s); (ii) consolidated settled order flow from the DTCC on behalf of member firm brokers and subsequent clearinghouses from clients moving from their broker to the transfer agent ledger; and (iii) transferring direct share purchase plans or corporate stock bonus incentives from the transfer agent ledger to a broker dealer through the DTCC ledger (also implementable through the issuance of new shares or transfer of authorized but not issued shares from an corporate multisig account to fulfill options and warrant contracts along related tax reporting standards, as generally used to satisfy outstanding in-the-money warrants).*

Lemma 4. *Institutional entities can interact with Block Transfer protocol through (i) direct wallet access (or custodial equivalent) as a peer computer node on the underlying network or (ii) through a more traditional federated contact with Peer \mathcal{BT} who can automatically process authorized secure SWIFT directions to transfer shares¹³ and deemed authenticated by Peer \mathcal{BT} who accepts the risk of default upon fraudulent securities transfers against their insurance*

Lemma 5. *Though not feasible in a traditional centralized transfer agent which often simply offers to dispose of shares at random market prices on behalf of book-entry shareholders through brokerage or issuing-firm agreements, the Block Transfer protocol furthermore allows for direct peer-to-peer transfers of issued tokens across the blockchain network, enabling compliant atomic swaps between two or more registered peers for some other for of value (say USDC).*

¹³When securely signed and verified by a STAMP certificate seal alongside necessary surety-bond insurance