Electronification, trading, and crypto *

Brendan Malone
Paradigm
brendan@paradigm.xyz

Austin Adams
Uniswap Labs
austin@uniswap.org

Maher Latif
Wormhole Foundation
maher@wormhole.foundation

1 Introduction

This paper presents a framework for thinking about the technological change of markets and the characteristics of public blockchains that enable the financial system to be reengineered to be more open, fair, and efficient.

Since 2009, technologists, financiers, academics, and policymakers have speculated about whether blockchain technology is the next truly revolutionary technology to hit finance or just a "solution in search of a problem." We think this framing misses the broader historical relationship between technology and progress. Markets are ultimately human-social phenomena. Our laws and policies influence markets in different ways to better serve their users and broader society — but this does not happen in a vacuum, nor does it happen without friction or resistance.

Technology is inherently subversive, and it's inevitable. Markets are usually resistant to change in the short term, but they are ultimately complex systems that allow for change to occur at multiple timescales in compounding fashion. To some, it might look like crypto has been slow to change how financial markets operate. However, more and more people and institutions from "traditional" backgrounds in finance and engineering are entering the world of crypto everyday. Stablecoins have found product-market fit. Treasuries are trading onchain. And central banks — once anathema to crypto's ethos — are forking popular DeFi protocols for use in cross-border payments. Change is here, if you know where to look.

In future parts of this series, we intend to dive deeper into specific markets and mechanisms to show how public blockchains are a positive force for society and how they can achieve the same or better policy outcomes as more traditional market designs.

2 Historical perspective on technological change

The consumer computing and networking revolutions of the past decades have truly transformed financial markets and banking. Computers and the internet are now fundamental to every interaction we have with the markets. Checks, once flown around the country for physical settlement, can now be accepted and processed electronically using our smartphone cameras. The chaos of the open outcry trading pits have been replaced by the quiet hum of co-located servers sending millions of orders at sub-millisecond frequencies.

*We would like to thank Mary-Catherine Lader, Dan Robinson, Maude Wilson, and Marco Machiavelli

The origins and impacts of these developments in electronification are difficult to parse because technological enhancements reached different markets at different times. **However, one underlying theme is clear: financial markets are often reactive, usually hesitating to embrace change or acknowledge its advantages until a crisis catalyzes — and embeds — innovation and structural change.** Absent shocks, gradual adoption of new technologies is a long and nonlinear process.

We examine two pivotal periods of electronification in the US financial markets as a means to provide contextual framing to understand how and why and how financial markets evolve. This is by no means an exhaustive case study, but rather some historical staging for what we believe is the next step in the evolution of markets.

2.1 The Paperwork Crisis and Electronification of Bookkeeping

In the late 1960s, Wall Street faced a series of crises relating to its ability to record and settle trade-based transactions. This would later be termed the "Paperwork Crisis," and its effects would ultimately stand out as the first consequential push into electronification.

At the time, processes around stock trade clearing and settlement were complex and manually intensive. When a stock trade occurred, the seller had to physically transfer the paper stock certificate to the buyer. This transfer first required the intermediary step of getting the certificate notarized. Once acquired, the purchaser had to physically transfer the certificate to the issuing company's transfer agent to manually record the new ownership for future dividend payments. The transaction was only considered complete once the transfer agent issued a new certificate in the buyer's name. Brokers facilitated these trades on behalf of their clients and had to manage these intensive processes. Some of these processes required more than 60 individual steps, and any error could invalidate the trade or incorrectly log it.

While these processes were adequate for much of the 1950s, a sharp rise in daily trading volumes from 4 million in 1960 to over 12 million by 1968 led to a backlog of paperwork. This culminated in the "Paperwork Crunch," which saw stock exchanges like the NYSE close every Wednesday to give everyone an opportunity to address the week's backlog of paperwork. Although some brokers used mainframe computers, they were prohibitively expensive and offered minimal help in the most cumbersome parts of the process — the physical stock certificate transfer. Under pressure and stress, the number of erroneous trades logged by brokerage clerks skyrocketed. In one now-infamous example, Lehman Brothers discovered "in May 1968 that it had $473 million in securities whose owners it could not locate, and that it owed clients $219 million in securities that it could not find."

The period forced one of the most consequential reevaluations of securities trade clearing and settlement systems and the technology they relied on. In 1971, the world would see the launch of the "first electronic stock market" — the NASDAQ. In 1973, the Depository Trust Company (DTC), was founded to immobilize certificate transfers by custodying them in a single depository and simplify settlement with a unified accounting ledger.

2.2 Sept 11th and the Electronification of Check and Securities Settlement

Exogenous events also played a significant role in the adoption of innovation. Despite the consumer computing revolution in the 1990s, electronification was slow to come to the clearing of physical checks only until after 9/11. When the U.S. government grounded air travel, paper checks could not be transported around the country to facilitate clearing and reconciliation (the requirement at the time was that checks had to be returned to the paying bank). It was not until the passage of the Check Clearing for the 21st Century Act (Check 21) that the market was able to leverage technological improvements to speed and efficiency by making it legally permissible to clear images of paper checks instead of the paper copy itself.

Similarly, in 2012, the move to dematerialize (e.g., make electronic representations of paper certificates) securities was turbocharged after the DTCC, which houses the majority of U.S. stocks and bonds, found one of its securities vaults flooded during Hurricane Sandy. In total, nearly 1.7 million security certificates stored in a lower Manhattan skyscraper had been damaged.

3 Decomposing the trading stack

Technology and market structure are intertwined. In many cases, technological adoption conforms to an existing market structure. **In other cases, new technologies allow for new actors to disrupt a market's existing structure, radically altering the underlying organization of the market and the actors that trade in it.** This makes it difficult to parse the effect of market changes that derived purely from technological changes, on the margin.

Unpacking the independent components of technology and market structure design that make trading possible — the "trading stack" — is one way to analyze the impacts of technological changes.

So, what makes up the trading stack?

- **Network.** The collection of people, relationships, and technology that allow for the exchange of information between multiple parties in a financial transaction.
  - *Examples: phones, face-to-face, electronic messaging, etc.*
- **Custody and settlement.** The technologies or media that allow for the recording, transfer, and custody of assets.
  - *Examples: paper ledgers, paper bearer instruments, digital ledgers, tokens, etc.*
- **Coordination and process.** The set of rules, norms, or business logic that describe — and enforce — how a transaction occurs.
  - *Examples: norms, enforced rules/regs, business logic, smart contracts, etc.*
- **Price discovery.** The form and mechanism that allow for assets to be priced.
  - *Examples: form (electronic vs. analog) and mechanism (RFQ, CLOB, AMM)*

This is obviously an imperfect and (mostly) theoretical exercise. Depending on the specific instantiation of the trading stack it can be almost impossible to cleanly disaggregate overlapping and often codependent components. However, we believe there is still value from an analytical perspective in having the ability to "toggle" different technological and organizational assumptions at different layers of the stack and assess the implications on the overall system. We therefore use this framework for thinking through the past, present, and future of trading with a particular focus on recent market designs made possible thanks to public, permissionless blockchains.

4 Real-world RFQ Trading Stack (c. 1700)

Imagine a remote-trading system that uses an RFQ mechanism to price securities issued to fund frontier exploration projects. The system is accessible to traders across Europe, who use it regularly to buy and sell securities. This sounds like some bond-trading platforms that are currently used today. However, in our hypothetical example, it is 1700 and computers, the Internet, and phones have not yet been invented. The trading stack is as follows:

- **Network.** An exchange in Amsterdam with traders in Amsterdam, London, and Paris. Assume for the sake of the example that the fastest and most-reliable form of communication between London, Paris, and Amsterdam is by homing pigeon. Pigeons can fly roughly 60 mph across a distance of up to 600 miles.
- **Custody and settlement.** Paper certificates held in self-custody by traders. These are too large to fly by homing pigeon, so physical settlement of trades occurs 14 days after trade execution.
- **Coordination and process.** The Amsterdam Stock Exchange (ASE), which is open from 9:30am - 4:30pm CET, Monday through Friday. Once a trade is submitted, that trade is valid until a subsequent trade is received from the same trader or the end of the day, whichever happens first.
- **Price discovery.** Analog system using the RFQ mechanism where prices are manually submitted to the exchange, where they are matched and routed accordingly.

This system is arbitrarily inefficient.

If a trader in London wants to execute a trade, they first have to send a homing pigeon to Amsterdam. At 223 miles straight-line distance, it would take the pigeon roughly 3 hours and 45 minutes to reach the ASE. Upon arrival, the ASE will manually match the trader with Amsterdam-based market makers who can provide a quote for the trade the trader is looking to execute. Additional back-and-forth communication (w/ standard pigeon-message latency) is required for the trader to receive and conditionally accept a quote, which again requires additional communication for trade settlement and reconciliation.

You can see from this example how market structure and technology are mutually reinforcing. With a single trader and multiple market makers centrally located at the ASE, it is already difficult to imagine this system working in practice. There are numerous places where the technologies used circumscribe the market structure possibilities and introduce inefficiencies and risk (e.g., what if a pigeon goes down over the English Channel?). That said, the underlying price-discovery mechanism (i.e., RFQ) requires relatively little in the way of complicated infrastructure. The ASE serves as a central routing hub for matching traders to market makers, but it does not need to maintain an order book or keep track of trader/dealer inventories.

How would technological improvements change these dynamics?

Electronification of the **Network** layer would reduce latency in message routing, but without attendant electronification of the **Custody and settlement** layer of the stack, paper certificates would still need to change hands 14 days after trade execution. Digital databases coupled with electronic messaging would improve pre-trade and post-trade activities, but may not be enough to structurally alter the design of the market: due to the double-spend problem, a centralized entity, such as the ASE, is still required to facilitate asset transfer, even if settlement itself is as simple as updated electronic records in a database. This is more or less how the first wave of electronification unfolded in the fixed-income securities space (as described above) with electronic trading venues offering a better way to coordinate at the pre-trade and execution levels, while custody and settlement remained centralized and paper-based.

ASE could conceivably use a CLOB or CFMM to calculate prices without any additional changes to technology or market structure. Of course, this heavily constrains subsequent market structure designs (i.e. requires institutional intermediation) and places a high degree of responsibility on ASE.

- ASE is required to manage technical infrastructure, including physical hardware and exchange software, which requires significant upfront capex. Any automation or interoperability between ASE systems and external systems depends on ASE making them compatible, and physical proximity to ASE's systems has implications for latency and trade execution.
- Market participants need to trust that ASE will operate the market in a predictable manner in accordance with predefined rules, which likely allow significant management discretion.
- Market participants are exposed to counterparty risk as a result of the role that ASE plays as custodian.

Much of the story of electronification to date has involved making existing processes digital but not dramatically altering the shape of the trading stack. This limits the subsequent market structure design space due to its continued heavy reliance on intermediation (of assets, technology, and communications) by specific institutions.

5 Enter: Blockchain Trading Stack

Permissionless blockchains enable new structures not previously possible with the traditional trading stack. To grok this point, imagine trying to implement an AMM like Uniswap v3 using homing pigeons in the 1700s and the market layout described in the previous section. De-electronifican by analogy. Conceptually, you have the modular components necessary to make it work in a narrow sense, but it would not be efficient or extensible. **One technological advantage of public blockchains comes from the fact that the entire trading stack is integrated into a single cohesive system that is participant agnostic.**

Anyone can make a market for any asset, because the entire trading stack is public infrastructure that is not owned or controlled by any one person:

- **Network.** Nodes running blockchain protocol client software, which lets them communicate with each other and the underlying data structures.
- **Custody and settlement.** Tokens representing digital assets that can be transferred between users and held in custody by users and smart contracts.

- **Coordination and process.** The blockchain protocol, which forms the base layer for communication and coordination, and the smart contract protocol that executes the basic business logic of the exchange mechanism.
- **Price discovery.** A simple formula (e.g., xy=k) that leverages the smart contract logic and underlying pool of tokens held in smart contracts.

Let's go back to our previous example of the homing pigeon-based market structure.

To point to a specific market structure improvement enabled by technology, we will highlight a feature that is fundamental to the blockchain space. A problem (just one of many) with the pigeon-based market structure is that an adversarial market maker can send pigeons to the ASE imitating their competition's orders (spoofing). In blockchain-based markets, the nodes ensure that the transaction came from the specified user by using various cryptographic protocols. For example, Ethereum validators use signatures based on Elliptic Curve Digital Signature Algorithm (ECDSA).

To ensure that this trade was not spoofed by an adversarial market maker, the homing pigeons could transport ECDSA-compliant signatures between London and Amsterdam. However, even with a team of trained abacus users, it would take multiple days to calculate the signature, which would be invalid with any error. The calculations needed are far from trivial as well. On the other side, ASE abacus users must also verify the signature before any action can be taken, which also extends the time until the market actions can be confirmed. Technological improvements enable these signatures to be generated and verified to be correct nearly instantly inside your browser. Creating and verifying these signatures are the bedrock of the blockchain-based markets because they obviate the need for multiple layers of institutional intermediation. Additional utility comes from the fact that the protocol can, on its own, execute complex business logic, such as calculating (in near real-time) the price of an asset.

This shift is not without consequences. Blockchain-based markets must charge for the amount of compute that is used, which is a dramatic shift from how traditional finance markets have evolved. This has led to the general acceptance of automated market makers, which attempt to maximize market efficiency for relatively small levels of compute. Of course, this is just one application of permissionless blockchains to market design and does not even consider the benefits that stem from having embedded clearing and settlement infrastructure.

6 Conclusions and potential areas of future exploration

We are still in the early days of blockchain-enabled financial innovation, but it is clear (to us) the coming wave of change will transform markets in profound ways.

Today, most financial markets operate in a suboptimal equilibrium, having arrived at their current structure through a series of organic processes as opposed to thoughtful, deliberate engineering. Regulation and competitive dynamics play a significant role in the ability and willingness of market participants to change their practices, but so too does the availability and applicability of existing technologies. The U.S. Treasury market is one such example.

Putting the U.S. Treasury market on a blockchain would not solve all of the market's woes, but it would open a new design space by making it possible to create a single market that retains the modular interoperability necessary for customization for specific segments and use cases. **The same**

pool of tokenized securities can be used across a wide range of market participants and protocols.

For example, the U.S. Treasury market is often described as the most important financial market in the world. However, the U.S. Treasury market is not functionally a single market, but rather a complicated collection of multiple sub-markets that serve different users and employ different technologies. Government officials have proposed a number of reforms that would reduce fragmentation in the market, which could improve market functioning by reducing the need for trade intermediation. Of course, this is not without challenges. Depending on the market segment, trade execution happens via anonymous RFQ, CLOB, match auctions, or by streaming quotes. Clearing and settlement may involve any number of entities, including the Federal Reserve, the DTCC, or the Bank of New York Mellon. Integrating the market into a single trading stack is a tall task, both in terms of technology and coordinating challenges — but it is made easier by the blockchain stack.

The opportunities become even more apparent when you consider the benefits of composability. **A payment stablecoin can be used as the cash-leg of a repo transaction with a DeFi protocol and a tokenized Treasury security, and neither the issuer of the stablecoin, developer of the protocol, tokenizer of the Treasury, nor the network validators need to coordinate with (or trust) each other in order for the transaction to work.** This would be a sea change in both digitization, interactivity, and customization. We would go from markets that most users must accept as they find them to ones where everyone can begin customizing their tech stack.

The market structure shifts enabled by blockchains is something that we will delve into more deeply in coming posts. Through this lens we can begin to ask a number of questions related to the design of better markets.

For example:

- What does settlement look like in a world where it can be fine-tuned, so it no longer has to conform to market conventions around specific times or intervals? Is it possible to build primitives that let you choose settlement time, and what implications would such designs have on market functioning?
- What systems could we build if we started from scratch with modern technology, as opposed to the skeuomorphic adoption process that currently dominates the world? Should we bring blockchains to markets that do not currently use them? Should we combine blockchains with more traditional market designs to leverage the benefits of both?
- How might blockchains enable a move from price-time priority markets to markets based on fees and competition, and what might that mean for market structure (and consumers)?

If these questions excite you, please let us know. Efficient market structure and design is of critical importance to capital formation and international competitiveness and is an important component of effective public policy.