# THE FUTURE OF CAPITAL MARKETS

## A Summary of the CoinShares Work-From Home Series

APRIL 2020

Xmargin Paradigm ARWEN

CoinShares

In March of 2020, markets around the world  experienced levels of volatility and turmoil that were unprecedented. The last financial crisis in 2008 resulted in regulation and changes to capital markets and the way our financial institutions and intermediaries in our global financial system function. From trading firms to dealers to large banks, financial services firms across the market and different parts of the asset management ecosystem have been hit hard by recent market events.

While the cryptocurrency trading ecosystem is still nascent, the cryptocurrency market is truly global, with assets that are highly fluid, markets that are open 24/7, and large volumes of trading occurring bilaterally, without intermediaries. At each stage of the trade lifecycle, there are numerous challenges facing market participants.

| The Trade Lifecycle | Challenges in the Crypto Market |
|---|---|
| **Price discovery:** interactions between buyers and sellers in a market to determine price | • Requires a formal or informal market<br>• Function of numerous factors, including market depth, structure, and risk management practices |
| **Execution:** Agreement to buy and sell in a recorded and enforceable transaction | • Requires a formal or informal venue<br>• Few aggregators outside of exchanges and messaging boards – mostly manual |
| **Clearing:** Recording the transaction, updating accounts, margin calculation, and margin management | • No central clearinghouse to net margin positions<br>• Currently managed by counterparties in their own systems or by the trading venue itself |
| **Settlement:** The actual exchange, when assets change hands between buyer and seller and the trade ends | • On-chain settlement happens with finality<br>• Mostly still bilateral with firms using their own infrastructure and procedures for DVP |
| **Reconciliation:** Post-trade activities to ensure trade records match what is recorded on the firm's books | • Entirely internal to the firm's back office<br>• Minimal software automation, as no standard formats for booking trades |

Source: CoinShares Research

One of the themes for our venture investments is that blockchain technology has enabled a fundamental change in the structure and flow of how capital markets operate, including where trades are executed, cleared, and settled. This evolution of market structure can completely transform the role of intermediaries, and enable new market structures to emerge.

In this installment of our series on the Future of Capital Markets, we'll cover the trade lifecycle from start to finish, and talk with three entrepreneurs about the software they're building . While crypto markets may have started out as largely informal and unstructured, the last five years have seen markets become more formalized, more organized, and more sophisticated. At the same time, the unique attributes of cryptocurrencies, the assets themselves, and the networks on which they operate, blockchain networks, have introduced new opportunities in how market participants interact and transact.

*Note: CoinShares invests in innovative companies building the digital asset ecosystem, focusing on making early stage equity investments in financial technology companies. CoinShares is an investor in X-Margin, Arwen, and CoinFirm, and is proposing an investment (subject to commercial negotiations) in Paradigm, all of which are mentioned in this report.*

# The Challenges of Trading Crypto at Scale

The first two components of the trade lifecycle are price discovery and execution. For this discussion, we interviewed Anand Gomes, co-founder and CEO of Paradigm. Paradigm is an institutional-grade messaging platform with embedded workflow automation for digital asset traders. Their vision is to unbundle execution from clearing and settlement.

While much of the talk about crypto markets seems to focus on speculative trading on retail platforms, there's a large and growing cohort of institutional players—lenders, structured product issuers and market makers—in the market as well. Hundreds of millions of dollars of digital assets change hands daily. However, the evolution of a more professional trading ecosystem has been hampered by the difficulty of translating the traditional trade lifecycle into a manageable process.

While the process for spot price discovery is robust and a global price for bitcoin has developed, this is not the case in futures and options markets. Price discovery for small derivatives trades is suitable, but an increase in size or complexity of  an order—like multi-leg option or futures spreads—can make it much harder to execute.

The crypto market is fragmented across a variety of venues including chat and voice, electronic venues like exchanges and other market aggregators, and informal venues like LocalBitcoins and peer-to-peer trades.

With this sort of fragmentation, price discovery becomes a challenging process of hunting for bids and asks. In particular, sophisticated trading strategies can be difficult to execute without building your own trading engine. As a former energy trader, Anand initially began building Paradigm for the energy market but quickly realized it was more powerful for the nascent crypto market. Paradigm is focused on large or complex trades that tend to disrupt traditional order books, suffer from slippage and are difficult to execute efficiently.

**30% of all crypto trades cannot be executed on screen**

These trades tend to be negotiated and executed over chat. This includes multi-leg option trades and futures spreads, as well as outright options and futures. These types of trades generally have no standard contract, may not be quoted anywhere and therefore have no accessible market for price discovery, and thus suffer from significant execution risk.

The Paradigm vision is simple: trade anything, with anyone, and clear and settle it anywhere using a single point of access. They can do this at scale, because unlike a traditional venue, Paradigm has decoupled the execution layer from the clearing and settlement layer.

At CoinShares, we think there is a massive opportunity to transform the structure of markets outside crypto in the same way. Offering this degree of choice at these different layers has never been done before, even in the traditional markets.

In Paradigm, you will soon be able to write your own contract, collect quotes, and execute a bilateral trade, where you can use a decentralized settlement protocol to settle your trade from a cold storage wallet or third-party custodian directly without ever touching a trading venue or exchange, and subsequently, without ever exposing yourself to that counterparty risk.

The folks at Paradigm argue that there are many asset classes outside of crypto that have unique structural characteristics that make them especially suitable to this RFQ model. One of the biggest challenges in legacy markets is that it's very difficult to quantify and qualify risk. We saw this in 2008 and are potentially seeing it again now.

There are many analogies between the systemic risk in legacy markets and what's happening in the crypto space. Just like legacy markets, structural weakness in the crypto market highlights where systemic fixes are needed. The market will force more systemic fixes in the crypto market like increased capital and margin requirements, a push towards better, more standardized liquidation methodologies and systems, circuit breakers, and general best practices at the infrastructure layer.

## Building a Distributed Clearinghouse

In part two of the series, we were joined by Darsh Vaidya, founder and CEO of X-Margin, to discuss the middle of the trade lifecycle: clearing. X-Margin has built a zero-knowledge calculation agent that allows for cross-margining without a central counterparty or clearinghouse.

**The derivatives market is by far the largest sector of the financial market**

According to a BIS report dated June 2019, the notional amount of OTC derivatives in the market were $640 trillion at end-June 2019, the highest level since 2014. The industry's largest clearing house, the Options Clearing Corporation (OCC) reported 4.9 billion trades cleared in 2019.

In crypto, nothing is centrally cleared. Clearing is venue-specific, and rules vary between platforms. Margin requirements are far stricter than in legacy capital markets. Margin calls have much tighter windows, can happen 24/7, and liquidations can occur swiftly.

Margin must be managed separately for each venue or broker, and there is no trusted third-party to calculate margin requirements. Crypto exchanges have different ways of allowing users to 'borrow' margin and in many cases, they utilize pooled insurance funds which act as the collateral behind the margin.

Most traders have positions across multiple venues. But without a central clearinghouse to verify there is an offset, they need to post new collateral at each venue. This is capital inefficient and limits the overall volume of trade.

Moreover, trading firms need to deposit their collateral on exchange, opening them up to security concerns and solvency risk. Because digital assets settle with finality when transferred, a trader posting margin to an account with another firm is effectively settling the trade on the blockchain before it has been completed, and then performing additional settlement when posting more margin, or finally liquidating the position. While some platforms attempt to provide "proof of solvency" or maintain an "insurance fund" to avoid socializing losses, the industry still suffers from the challenges associated with centralization of clearing, and the unique characteristics of cryptocurrencies which settle with finality on the blockchain when transferred.

X-Margin has built a proprietary zero-knowledge calculator, that does aggregate calculations on data without revealing it.

For cryptographic validity, it produces proof of computation and proof of encryption, meaning one can verify that the computation is doing what it's supposed to be doing, and verifies that no information is leaked in that process.

In its first product, X-Margin is focusing on margining. It receives private trade data, aggregates the risk and calculates margin across venues, enabling cross-margin without that central counterparty. This reduces collateral requirements and is a much cheaper and more scalable solution than a central clearinghouse.

While X-Margin is starting with the crypto market, the vision is much larger, and the solution could be applied to other asset classes that have no affordable, scalable clearing solution. At CoinShares we believe ultimately, a solution like this will scale quickly across multiple asset classes and venues and introduce a new model for how firms calculate and manage margin, enabling traders to optimize capital efficiency.

Most importantly, X-Margin's model can help reduce systemic risk, as it's custody agnostic and doesn't require margin to be posted on an exchange or with a trading counterparty. Traders can work with an escrow agent, their custodian, or even a multi-sig cold storage wallet, to verifiably post margin without transferring it with settlement finality to a third party. Effectively, X-Margin becomes a technology and software layer that performs all of the traditional functions of a centralized clearinghouse without holding assets or holding proprietary trade information.

The benefits of this model are:

- Cheaper to run
- No central counterparty
- Real-time
- Scalable
- Risk methodology agnostic
- Custody agnostic

The theme here is similar to that discussed with Paradigm - breaking out the clearing layer and abstracting it into software. Software is eating capital markets.

**The crypto derivatives market traded roughly $3.1 trillion of notional value in 2019**

Traditional markets are more than 100 times larger. Coming out of the financial crisis, there was a significant push for OTC derivatives to move to central clearing. According to ISDA's 2013 paper on The Value of Non-Cleared OTC Derivatives, the non-cleared derivatives segment of the OTC derivatives market includes "many important products with significant value to the economy". As a result of this demand, the non-cleared segment of the OTC derivatives market is expected to remain significant in size. According to an IMF study, 25% of the interest rate derivatives market, 33% of the credit default swaps market, and significant percentages of other types of OTC derivatives will remain uncleared.

While the first phase of X-Margin's roadmap is focused on the cryptocurrency derivatives market, the team sees opportunity in covering a wide range of legacy financial OTC derivatives, given many bespoke services in traditional finance are still completely bilateral with no scalable or affordable clearing solution, and cross-margin requires OCC membership.

With the introduction of stablecoins suitable for use in regulated capital markets and the increasing acceptance of the "digitization" of new types of collateral using tokenization by regulators, there's a massive opportunity to build a new model for helping traders apply leverage while maximizing security, minimizing centralization and systemic risk, and providing better risk oversight and risk management policies and procedures.

## The Challenges of Settling a Crypto Trade

Finally, we chatted about the final stage of the trade lifecycle—settlement—with Sharon Goldberg, co-founder and CEO of Arwen. Arwen has built a secure settlement solution for digital assets. Arwen's technology eliminates risk and friction associated with moving coins across custodians.

Settlement is when the actual exchange of assets takes place and the trade is finalized. If Meltem agrees to sell Sharon one token for $10, we would swap these to settle the trade. The question is, how do we do this, and who goes first?

If Meltem sends Sharon the token before Sharon pays, she'll have Meltem's token and can just flake on her side of the trade. Likewise, if Sharon goes first and sends Meltem dollars before Meltem sends her token, Meltem could take Sharon's dollars and never deliver. In other words, this process has significant counterparty risk.

Now, maybe we can phone the bank and reverse or cancel the wire, but if payment is made via a stablecoin, it settles with finality on the blockchain. So how do trades in the crypto market settle today?

### In today's crypto market, trades settle in two ways.

On exchanges, the exchange effectively plays the role of an escrow agent. Each party to a trade first posts its assets or funds on the exchange. The exchange then makes a book entry noting the change in ownership, or moves the funds from wallet to wallet, depending on whether the exchange co-mingles funds or has dedicated wallets.

In the OTC market, the trade settles bilaterally, where the two parties hopefully have some degree of trust or rely on reputation or existing relationships and take turns going first. Typically, the party with more leverage can dictate settlement terms (i.e. who goes first and thus takes on all of the counterparty risk).

Neither of these options is particularly appealing to a trader looking to manage risk and optimize capital efficiency.

On the exchange side, counterparty risk exists in every trade, but cryptocurrency exchanges have had a poor track record here, starting with Mt Gox in 2014. The blockchain analytics firm CoinFirm estimates that in 2019, exchange and wallet exploits resulted in $230M of damages. Typically these exploits are a result of:

- Poor management: General incompetence, insolvency, poor operational security, and more.
- Hacks: Exploiting vulnerabilities, stealing private keys, and hacking wallets.

We've seen an explosion of projects tackling the problem of non-custodial trading via "decentralized exchanges" or DEXs. These seek to realize the promise of non-custodial trading by creating a messaging board and order matching system and leaving settlement to the counterparties to coordinate amongst themselves. However, DEXs have struggled with bad UX, regulatory complexity, lack of liquidity, and a host of other issues.

On the OTC side, ironically, the market is entirely dependent on reputation and trust despite dealing in an asset that is meant to minimize trust. While some companies have built centralized escrow agents to act as the middleman to receive funds/crypto from both sides and then settle once delivery has been confirmed, this model is not riskless either.

Perhaps the most relevant example here is the legacy of Bankhaus Herstatt, a German bank who in the 1970s became insolvent and was closed mid-day before completing settlement of foreign exchange transactions. Herstatt risk has become the moniker for settlement risk in legacy capital markets, and crypto capital markets are not immune to this.

One area of development in crypto finance has been the growth of non-exchange custodians, or so-called "institutional custodians." While these platforms allow traders and firms alike to hold their funds in a segregated, dedicated wallet - almost like a digital vault - they don't resolve the issues created by centralization and aggregation of coins. As Sharon points out centralized escrow agents or depositories effectively become a massive honeypot for attackers.

CoinShares has previously published research on the risk of centralizing bitcoin custody in exchanges and custody platforms.

**According to our research, exchanges, asset managers, and custodians currently hold at least 20% of all bitcoin**

When the DAO was hit by a smart contract exploit in 2016 and 15% of all Ethereum in circulation was drained from the smart contract, the Ethereum community rolled back the Ethereum blockchain to restore funds. At CoinShares, we worry that without solutions like Arwen, it's only a matter of time until a large custodian or exchange is hacked and results in a catastrophic event.

An exciting feature of software like Arwen is that it can be utilized as a standalone solution, or it can be incorporated into existing platforms like exchanges, OTC desks, and custodians. For exchanges, Arwen's settlement technology can enable non-custodial trading. With non-custodial trading, users no longer have to deposit their coins at a centralized exchange. User coins remain housed in users' own wallets, instead of trusting the exchange's wallet with custody. Exchange operators can add Arwen's settlement technology to mitigate risk from hacks, unexpected technical issues, and reduce the impact of malicious actors.

We could see the creation of an exchange like the one being built by Paradigm that is purely a software layer for price discovery and trade execution, where all settlement is done on-chain via Arwen. In this instance, custody would be the sole responsibility of the asset holder (being their own bank) and the exchange, clearinghouse, and settlement agent would never touch the funds - they would only provide software.

## Conclusion

If we zoom out and look at the bigger picture, it doesn't make sense to style cryptocurrency markets after legacy markets.

**Bitcoin cannot be a systemic hedge if holders are beholden to large financial institutions**

Building new custodial intermediaries in the same manner as after existing legacy precedents obviates the most compelling features of digital assets entirely.

With the introduction of stablecoins suitable for use in regulated capital markets and the increasing acceptance of the "digitization" of new types of collateral using tokenization by regulators, there's a massive opportunity to build a new model for markets where intermediaries are both software-based and more secure than those in traditional markets.

Although Paradigm, X-Margin, and Arwen have all initially launched products aimed at crypto, it's clear from our conversations that there are applications far beyond that ecosystem, and that although many challenges remain (especially on the regulatory side) what we're potentially seeing is crypto as a kind of "sandbox" for the re-making of the legacy financial system. We call this theme both "revolution" and "evolution" occurring concurrently.

To learn more, we encourage you to visit www.coinshares.com.
If you are interested in discussing with our team, please contact investments@coinshares.com.

# DISCLOSURE

Please note that this document is provided on the basis that the recipient accepts the following conditions relating to provision of the same (including on behalf of their respective organisation). This document has been prepared for informational purposes only and does not contain, or purport to be, a financial promotion of any kind and is not intended to constitute an offer, solicitation or invitation for any securities and may not be distributed into jurisdictions where it is unlawful to do so.

Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of the CoinShares Group, which is the issuer of this document, as of the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and / or obtained from sources believed to be reliable; however, the CoinShares Group does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the  date indicated. Any forward-looking statements speak only as of the date they are made, and the CoinShares Group assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time.

Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances. Crypto assets are a highly volatile asset class. Your capital is at risk. The value of crypto assets can go down as well as up and you can lose your entire investment.

CoinShares (Jersey) Limited ("CSJL"), a private limited company incorporated in Jersey, Channel Islands (#102184), is regulated by the Jersey Financial Services Commission in the conduct of AIF Services Business and certain classes of Fund Service Business and Investment Business pursuant to the Financial Services (Jersey) Law 1998, as amended. The registered office address of CSJL is 2 Hill Street, St. Helier, JE2 4UA, Channel Islands.

The CoinShares Astronaut is a trademark and service mark of CoinShares (Holdings) Limited.