Paradigm

June 2024

Settling the Unsettled

Principal Settlement Risks for Financial Transactions on Public Blockchains

by Natasha Vasan

Policy Lab RH-001

Table of Contents

Regulators,[1] academics,[2] and others[3] often argue that public blockchains can never be used to settle important financial transactions because they do not provide for deterministic settlement finality. We argue that this is not necessarily the case, while highlighting the risk vectors which may create settlement vulnerabilities given the current state of technical and legal infrastructure surrounding public blockchain transactions. We find that settlement risk is most salient in interactions between public blockchains and other (e.g., offchain) settlement systems. Focusing on the Ethereum ecosystem, we present technical, legal, and market-based solutions which can mitigate (and, in many cases, eliminate) the problem of principal settlement risks for financial transactions involving public blockchains.

1. Introduction

Financial primitives are technology neutral, and public blockchains are use-case agnostic. A regulatory framework has been developed to address the operational and financial (e.g., settlement) risks associated with financial primitives and their underlying market infrastructures.[4] While originally developed in the traditional finance context, the high-level tenets of this framework apply regardless of the specific technological makeup of a financial market infrastructure.[5] In some (but not all) cases, public blockchains are used as the means to track, manage, and facilitate the operation of financial primitives, and it is here where we need to think about risk management frameworks and legal protections that exist outside of the technology itself.

In traditional finance, securities trades are generally settled on a "delivery v. payment" (DvP) basis, wherein one leg of a transaction (delivery) is made conditional on the completion of the other (payment) (See Figure 1).[6] When both legs (delivery and payment) of the transaction are complete, which usually (in the US) takes 2 days following the trade's execution and clearing, the transaction is deemed legally and irrevocably settled.

1: Committee on Payments and Market Infrastructures & Board of the International Organization of Securities Commissions, Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements (July 2022), https://www.bis.org/cpmi/publ/d206.pdf (hereinafter, SA/PFMI) at 10 ("the use of distributed ledger technology (DLT) in the [stablecoin arrangement]'s transfer function may create a misalignment between legal (settlement) finality and technical settlement."

2: Hossein Nabilou, Probabilistic Settlement Finality on Proof of Work Blockchains: Legal Considerations (Jan. 31, 2022), https://ssrn.com/abstract=4022676 ; Bumho Son & Huisu Jang, Economics of Blockchain-Based Securities Settlement (Dec. 1, 2022) at 4 ("A public blockchain, however, might not be preferred for securities settlement because of several problems such as scalability, finality, or inefficiency.")

3: See, e.g., Tim Swanson, Great Wall of Numbers, Settlement Risks involving Public Blockchains (March 24, 2016), https://www.ofnumbers.com/2016/03/24/settlement-risks-involving-public-blockchains/ ("Because of how the mining process works – miners can reorganize history (and have) – a public blockchain by design cannot definitively guarantee settlement finality").

4: See, e.g., Committee on Payments and Market Infrastructures & Board of the International Organization of Securities Commissions, Principles for Financial Market Infrastructure (April 2012), https://www.bis.org/cpmi/publ/d101a.pdf (hereinafter, PFMI).

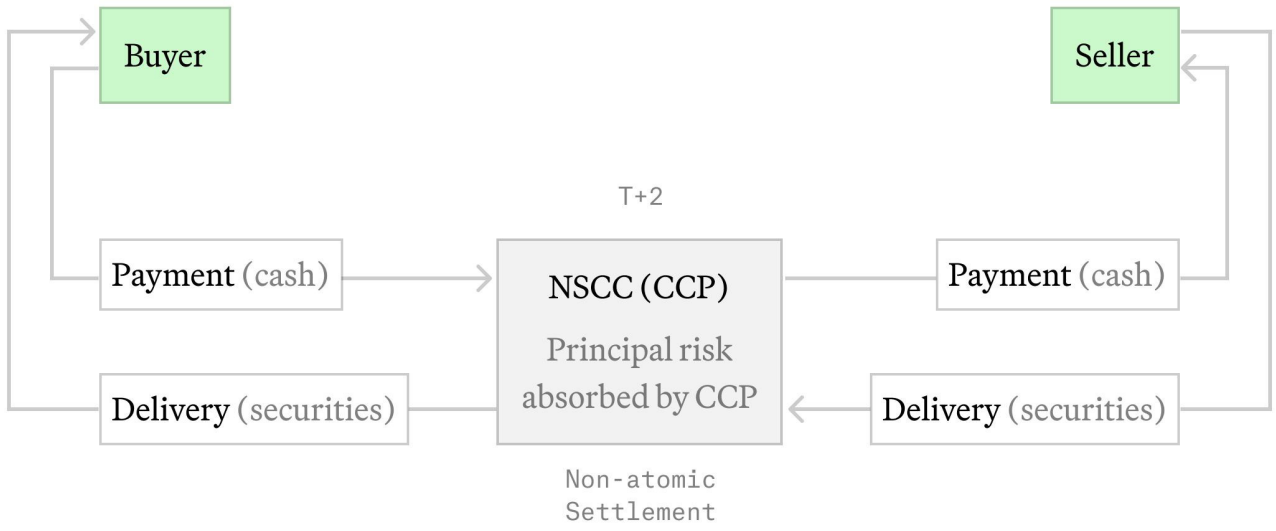
5: PFMI para 1.9 ("There can be significant variation in design among FMIs with the same function"). See also SA/ PFMI para 1.3.3.

6: Similarly, most foreign exchange transactions are made on a "payment v. payment" (PvP) basis.

The underlying purpose of DvP settlement in inextricably linking both legs of a transaction is to mitigate principal risk – the risk that a seller may "deliver" without ever receiving payment from the buyer, or vice versa, that the buyer may provide payment without ever receiving delivery.[7] Still, principal risk is not totally eliminated unless DvP settlement occurs on a simultaneous basis, such that a seller provides delivery if and only if and at exactly the same time that a buyer makes payment. In other words, where there is a time lag between two legs of a transaction, the risk of DvP settlement fails increases – it remains possible for the first leg to irrevocably deliver value, but never receive payment in return. In the foreign exchange context, this is referred to as Herstatt risk.[8] In traditional finance, DvP settlement is usually attained through centralized intermediaries (e.g., NSCC, the central counterparty for securities trades) who step in to shift the burden of principal settlement risks off the shoulders of individual market participants.

Figure 1

Traditional DvP



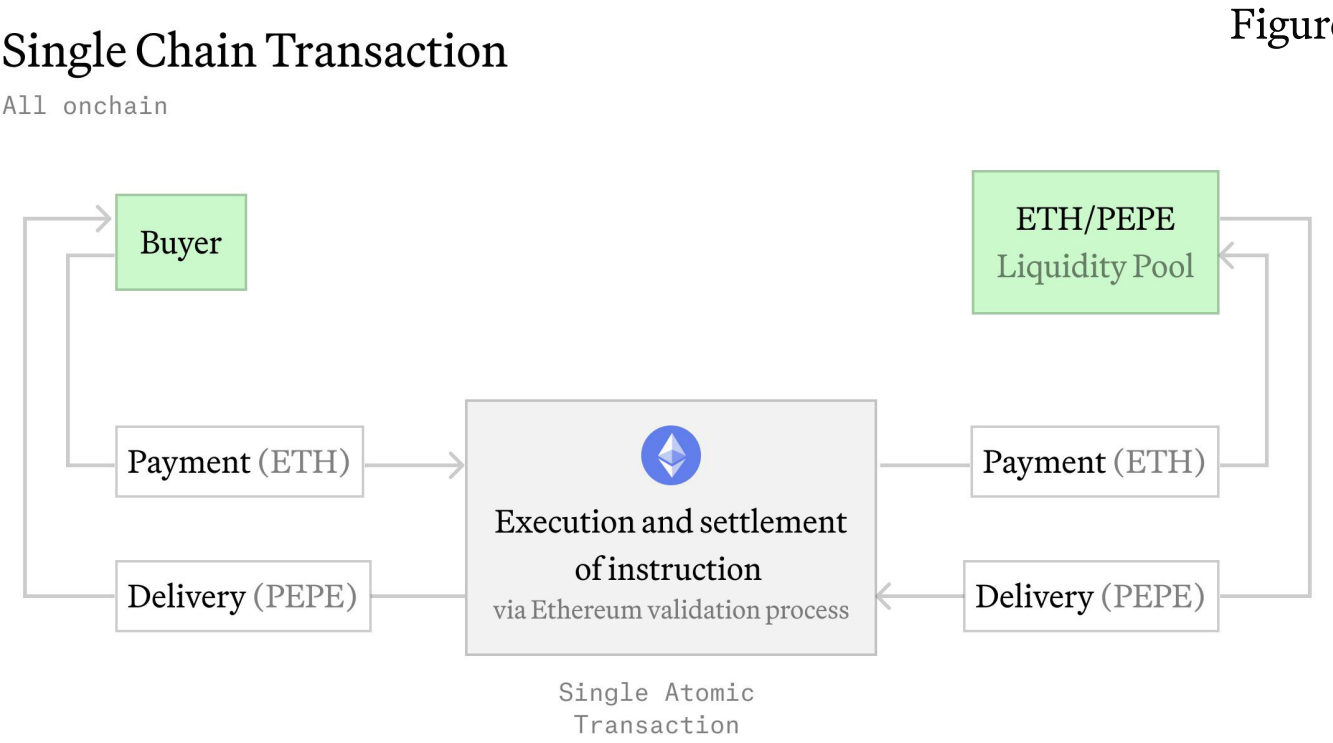
For certain crypto trades – which we call "single-chain transactions" – where both legs of a transaction occur on the same blockchain (say, Ethereum), simultaneous DvP settlement is the norm. Many DeFi protocols – like Uniswap and other DEXs – utilize noncustodial, pre-funded liquidity pool smart contracts to execute transactions. Consider an ETH for PEPE swap on Uniswap – once the payment of ETH is made to the prefunded liquidity pool smart-contract, the smart-contract immediately and deterministically executes delivery of PEPE to the trader (see Figure 2). If something goes wrong (i.e., the trader has insufficient funds in their wallet account to make complete payment, or the pool contains

7: Bank for International Settlements, Delivery versus Payment in Securities Settlement Systems (September 1992), https://www.bis.org/cpmi/publ/d06.pdf.

8: The term "Herstatt risk" is in reference to the infamous failure of Bankhaus Herstatt, a German bank, in 1974. The German financial regulator closed Bankhaus Herstatt in the middle of the German trading day, before the bank had delivered US dollars it had sold to various financial institutions but after it had received payment for those sales in Deutschmarks. The Bankhaus Herstatt incident is the paradigmatic example of disconnects (in the Herstatt case, due to time delays) in settlement of different legs to a transaction leading to principal loss.

insufficient PEPE to fully deliver on the trader's payment), both legs of the transaction will revert because the transaction is atomic. Further, smart-contract enabled innovations like flash loans allow more sophisticated financial activities like margin trading to occur on a simultaneous DvP basis within an atomic, single-chain transaction. For transactional arrangements like these, there is no principal risk.

Figure 2



Single-chain transactions should be differentiated from "hybrid transactions," a term coined by Soubhik Deb et. al. which refers to transactions that "result in both onchain and offchain state changes."[9] Hybrid transactions may involve settlement of each leg on different public blockchains (e.g., a NFT transfer from Ethereum to Solana, see Figure 3), or settlement of one leg onchain and the other totally offchain (e.g., subscription to a tokenized U.S. treasury fund on Ethereum by wire transfer payment, see Figure 4; or a fiat-to-crypto on-ramp transaction on a CEX). Because hybrid transactions involve different systems – with different settlement timelines, security considerations, safety guarantees, etc. –, we generally cannot enable simultaneous DvP settlement for these transactions. In what follows, we explain why this is a problem and propose some potential solutions.

9: Bank for International Settlements, Delivery versus Payment in Securities Settlement Systems (September 1992), https://www.bis.org/cpmi/publ/d06.pdf.

Figure 3

Hybrid Transaction

Crosschain

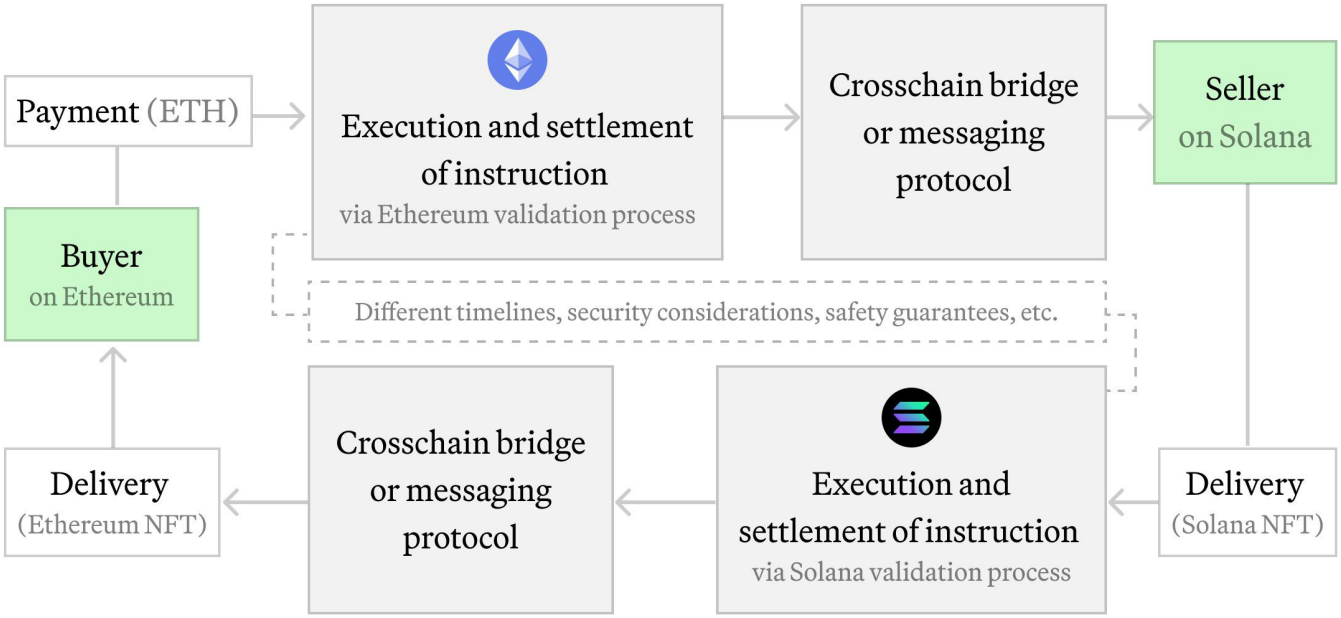
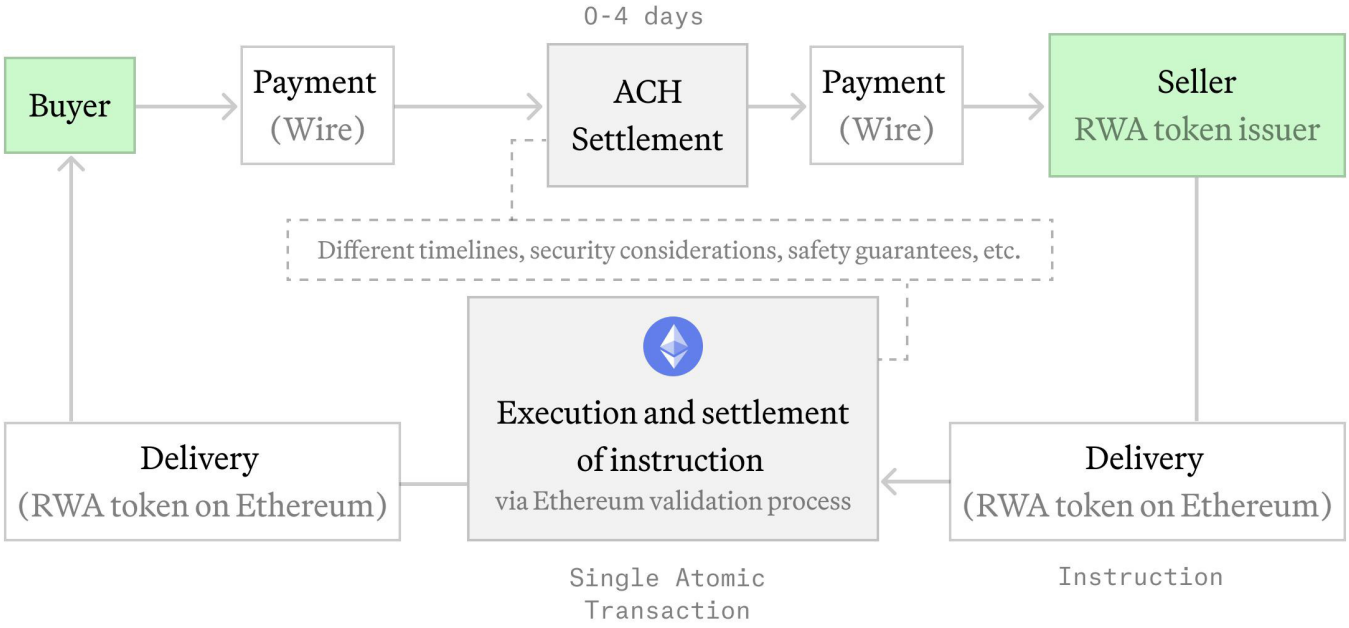


Figure 4

Hybrid Transaction

On & Offchain



2. Why is this a problem? Addressing the "worst case" scenario

At the outset, it is important to note that trade settlement is a fundamentally legal construct. In the Ethereum context, the word "settlement" is often used in reference to the technical and economic notion of transaction or block "finality" – a moment (e.g., the next finalized checkpoint) after which it becomes economically irrational for any malicious actor to try and remove a transaction from the blockchain ledger. However, even the strong technical finality guarantee provided by Ethereum under the CASPER-GHOST consensus protocol is not enough to satisfy financial regulators, who demand *deterministic* settlement finality.[10] This is because even such "finalized" Ethereum transactions are theoretically subject to reversion in the "worst case" scenario.

The law is concerned about this worst case scenario because legal settlement finality is heavily relied upon by market participants, such that disruptions to transactions following settlement cause widespread market distress. While the law does not purport to totally eliminate the possibility of settlement failures or disruptions, it must be prepared with tools to provide redress for those harmed in the case that such settlement problems occur. In practice, this effectively means that individual market participants should never be subject to principal risk.

Established settlement systems in traditional finance exemplify this dynamic. Clearing and settlement for most traditional securities occurs through a central counterparty (CCP) that acts as a middleman, engaging in a process called novation to replace the original contract between buyer and seller with two contracts interposing the CCP as buyer to every seller and seller to every buyer. In so doing, the CCP shifts the burden of counterparty credit risk (which can be a form of principal risk) from individual traders to itself. The CCP engages in legally mandated risk-management practices, like collecting margins from its institutional clearing members and keeping a minimum capital buffer in order to mitigate the chances of its failure, given the fact that it absorbs and concentrates all counterparty risk in the system. Still, the risk of a CCP's failure is present and widely known, so legal and institutional mechanisms (e.g. the CCP's access to emergency central bank liquidity facilities) exist so that market participants can trust that their personal balance sheets will not be harmed by any black swan event interfering with the CCP's settlement function.[11]

By contrast, under the status quo, DeFi market participants have no guarantee that transactions they view as "final" would continue to be recognized (by the protocol, the law, or other network participants) following a black swan event. It is common that the likelihood of a malicious validator acquiring 67% of the network and engaging in a long-term blockchain reorganization is brushed off as infeasible due to the exorbitant expense of such an attack,[12] but such a remote but possible contingency is exactly what is meant by a "worst case" scenario or "black swan event". Somewhat more likely is the potential for a consensus or execution client used by a supermajority of validators to contain some software bug (either unintentional or intentional) causing finalized transactions to be disrupted. In either of these cases,

10: SA/PFMI paragraph 3.4.3 and 3.4.4.

11: For an analysis of the Federal Reserve's role in ensuring the continued operation and solvency of CCPs during the 1987 "market break" (a black swan event), see Ben S. Bernanke, Clearing and Settlement During the Crash, 3 Review of Financial Studies 133 (1990).

12: One estimate suggests that, given the price of ETH, total amount of ETH staked, and validator count on December 31, 2023, it would cost an attacker 34.39 Billion USD and take over 5 months to engage in a 34% attack on the network. Lucas Nuzzi, Kyle Waters, & Matias Andrade, Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum at 26 (Feb. 2024), https://ssrn.com/abstract=4727999.

DeFi market participants whose transactions are reversed have no recourse – there is a discrepancy between the record of transactions they reasonably viewed as final and, accordingly, may have relied on, and the actual state of the blockchain ledger.

This doesn't pose too much of an issue for single-chain transactions. Given that both (delivery and payment) legs of single-chain transactions settle simultaneously, a blockchain reorganization would either reverse both legs of the trade or neither. The worst that could happen is that traders suffer the "replacement-cost" of having to replace their transaction at current – potentially less favorable – market prices.[13] Again, there's no principal risk for single-chain DeFi transactions.

However, things are not so simple for hybrid transactions. In any case where one leg of a transaction is on Ethereum and another is not (whether it be on a different blockchain, or offchain entirely), the possibility remains that one leg of a transaction will settle irrevocably elsewhere but the Ethereum leg will become reversed following confirmation (because of a blockchain reorganization). On the other hand, for certain hybrid transactions involving an onchain leg and an offchain (i.e., traditional finance) counterpart, issues with offchain confirmation also pose settlement risks. The 2021 Gamestop incident exemplifies this dynamic – as Gamestop's stock price experienced a rapid, Reddit fervor-induced spike, NSCC significantly increased its collateral requirement on Robinhood's clearing account, causing Robinhood to halt trades between execution and settlement. Where a token (RWA or DeFi-native) is traded in exchange for offchain consideration (e.g., fiat wire transfer), the token transfer could be finally executed onchain – and several subsequent onchain actions could be made reliant on its validity – before clearing and settlement take place for the corresponding leg on the "real world" ledger. This leaves open the possibility that in the time between onchain and offchain settlement, something (like the Gamestop incident) can go wrong such that offchain settlement never actually occurs. Both of these realities create a source of principal risk in public blockchain-based infrastructure for financial primitives, which global financial regulators, financial institutions, and general public sentiment will not tolerate if left unaddressed.

Implications

- **Institutional adoption of DeFi:** For large financial institutions engaging in high-value transactions, the probabilistic settlement guarantee of public blockchains like Ethereum may be a significant deterrent, absent additional safeguards. These institutions are most likely to place value on extremely strong settlement guarantees for blockchain-related activities, particularly as they are sometimes required to do so by regulation.[14] Accordingly, the uncertainty surrounding legal settlement on Ethereum may push such institutions to favor (by launching and/or participating in) tokenization projects on private permissioned blockchains, rather than public permissionless blockchains like Ethereum.
- **Cross-chain MEV:** Asynchronous settlement cycles across public blockchains are inherent to most cross-chain MEV extraction opportunities. For instance, CEX-DEX arbitrage opportunities expose traders to principal risk in both legs of the transaction - a transfer on an Ethereum DEX may be reversed following irrevocable payment to the CEX due to a blockchain reorganization, or the CEX may become insolvent and therefore unable to honor trade instructions after the corresponding leg is settled via the Ethereum blockchain. Akin to inventory risk, this

13: The degree of replacement-cost risk for a particular transaction depends on the time elapsed from trade execution to settlement, as well as the volatility of the traded asset.

14: See Basel Committee on Banking Supervision, Prudential treatment of cryptoasset exposures (Dec. 2022), https://www.bis.org/bcbs/publ/d545.pdf (requiring legally recognized settlement finality as a precondition for bank's tokenized asset projects to receive favorable capital treatment).

this heightened principal risk may mean that profitable cross-chain MEV opportunities are only available to highly resourced market participants, creating a distinct centralization vector.[15]

- **Limitations on interoperability with a tokenized world:** Outside of the DeFi context, tokenization projects on permissioned blockchains – by private institutions and national governments alike – have seen significant advances in popularity and sophistication. While a legitimate criticism of these projects thus far has been their siloed and disconnected nature, we are seeing significant movement towards better integration and interoperability between permissioned blockchain networks in terms of not only technology, but regulatory, governance, and operational standards.[16] The lack of a strong and legally recognized guarantee of settlement finality for transactions involving public blockchains could stand in the way of DeFi becoming an integrated part of the future of finance these developments represent, causing DeFi to become its own "walled garden" inconveniently segregated from the rest of the tokenized world. Without matching the legal and technical protections for settlement attained (or required) by other tokenized systems, DeFi will be unable to successfully interoperate with those systems. This would give regulators one more reason to exclude DeFi from their vision of a tokenized future of finance.
- **Public confidence in the system:** Market participants – institutional and retail – want certainty that the transactions they view as final will always be recognized as such. The mere possibility of an attack on transaction finality occurring, in conjunction with the reality that there really is currently no recourse for market participants in the event that their transactions are reverted, may deter participation in the network. Even for single-chain transactions, replacement-cost risk following an attack on finality may itself constitute a significant deterrent for DeFi market participants given the time-sensitive nature of many trading strategies and high degrees of token-price volatility. This is not to say that the goal should be to eliminate any and all possibility of such an attack, but the burden should not be on individual traders to bear the costs of settlement risks. With increasingly significant centralization vectors on Ethereum,[17] more value flowing through all public blockchain ecosystems (creating more incentives to exploit the blockchain record, potentially to capture various forms of MEV), and omnipresent threats of cybersecurity exploits and hacks, promoting public trust in the integrity and credibility of DeFi markets should be highly prioritized.

3. Solutions: Technical, legal, & market-based

As noted, hybrid transactions are no homogenous beast – both legs might be on different blockchains, or one leg might be onchain and the other totally offchain (e.g., recorded on a bank's internal ledger). What's more, in either case, the assets transacted may be digitally native or tokenized representations of real-world assets (RWAs). These details

15: Evmos, Youtube, Asynchronous Settlement and Cross-Chain MEV (May 9, 2023), https://www.youtube.com/watch?v=VOZ1qlc4KXg.

16: See Ananya Kumar et. al., Atlantic Council, Standards and Interoperability: The future of the Global Financial System (April 10, 2024), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/standards-and-interoperability-the-future-of-the-global-financial-system/; see also Bank of Canada and the Monetary Authority of Singapore, Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies (2019), https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf (discussing HTLC for interoperable interbank blockchain payment settlement); Bank of International Settlements, BIS Annual Economic Report 2023, Blueprint for the future monetary system: improving the old, enabling the new (2023), https://www.bis.org/publ/arpdf/ar2023e3.pdf (discussing the "Unified Ledger" proposal).

17: e.g., gETH execution client is used by 62% of Ethereum validators, Ether Alpha, Client Diversity, https://clientdiversity.org/ (accessed May 10, 2024).

should inform the range of solutions we consider when addressing the question of how to deal with principal risk for hybrid transactions– different solutions make sense in different transactional contexts. While external legal intervention through public law mandates may be appropriate where there are offchain dependencies, crypto-native technical interventions are likely more effective when transactions are confined to the public blockchain ecosystem.

This notion – that different risk management frameworks are appropriate in different contexts – is also a core principle of traditional finance. For instance, retail traders who purchase securities via the public capital markets are provided more robust legal protections than institutional market participants who purchase securities in private placements directly from an issuer/ their intermediary. Likewise, the settlement systems for different traditional asset classes – like securities, derivatives, and bank liabilities (i.e., funds transfers) – have different settlement timelines (T+2 v. RTGS),[18] settlement methods (DvP v. PvP),[19] and operational mechanics (CCP novation v. electronic interbank payment systems, like ACH). These settlement systems carry different risk profiles, reflecting the nature of the transactions they facilitate and preferences of the market participants they serve. This is to say, there are multiple ways to transact, all of which come with different tradeoffs in terms of safety and efficiency. The same idea applies when we talk about managing risks for hybrid transactions on public blockchains .

Additionally, different approaches to solving for principal risk – technical, legal (public law and private contracts), market-based – can be composable, rather than mutually exclusive. Industry self-regulation is exemplary here. Baseline standards and best practices to ensure strong and interoperable finality guarantees across systems can be developed through industry collaboration, and these standards/practices can be normalized through public law mandates, private agreements, and/or market incentives.

Technical

- **Cross-chain messaging:** We are seeing a lot of innovation working to enable seamless transfers across public blockchains. Cross-chain messaging protocols like Wormhole [20] and bridges are the starting point. Bridges enable messages (transactions) to be transferred across public blockchain networks with varying degrees of security, decentralization, and ecosystem compatibility. However, while bridges make possible cross-chain transactions, they do not address the asynchronicity in settlement cycles and varying settlement guarantees across blockchains. Bridges can mitigate principal risk by waiting until a transfer on the source chain is confirmed according to the consensus rules of the source chain prior to executing the corresponding leg of the transaction on the destination chain – effectively, this is non-simultaneous DvP. In addition to adding latency to cross-chain communications, this does not totally eliminate principal risk for transactions involving transfers on public blockchains like Ethereum where finality can be disrupted even after "confirmation" as defined by the protocol.[21] The Crosschain Risk

18: The settlement cycle for derivatives contracts is often much longer than that for securities or interbank funds transfers, potentially extending multiple weeks.

19: While both securities and exchange-traded derivatives settlement occur on a DvP basis, securities transactions are generally physically-settled while some derivatives transactions are cash-settled.

20: Wormhole is a "generic message passing protocol" which enables decentralized applications to integrate cross chain functionalities. Wormhole is not itself a cross-chain token bridge, but effectively enables cross-chain bridging functionalities on all dApps using Wormhole using "Core Contracts" deployed on all blockchains in its ecosystem. See Wormhole Documentation, https://docs.wormhole.com/wormhole (accessed May 12, 2024).

21: The Ethereum protocol uses the CASPER FFG confirmation rule, which defines "finality" with respect to a transaction as the moment the transaction is followed by two checkpoints with a "supermajority link." Ethereum Docs, Proof-of-Stake, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (accessed May 10, 2024).

Framework labels "network consensus risk" a key category of risk associated with cross-chain communication technologies, noting that "such risks are often beyond the control boundary of cross-chain infrastructure and likely represent a fundamental security limitation to bridging across independent sovereign chains."[22] Still, it is worth noting that settlement disruptions following protocol-defined finality on Ethereum are highly unlikely given the exorbitant expense they entail. Accordingly, non-institutional market participants may view the benefits of cross-chain trading opportunities to justify potential risks arising from the, admittedly remote, possibility of settlement disruptions.

- **Public-private blockchain communication:** Most bridges address cross-chain communications between public blockchains, but, as we move towards an increasingly tokenized future, a solution is needed to enable public and private blockchains to communicate with each other. Public-private blockchain communications constitute a different type of hybrid transaction, with different considerations involved in addressing associated risks. Specifically, private blockchains are primarily used and managed by highly regulated financial institutions or even national governments, who may demand greater settlement guarantees and legal protections.

  Chainlink's Cross-Chain Interoperability Protocol (CCIP) is currently being used in a collaboration between SWIFT and several major financial institutions (including DTCC, Euroclear, BNP Paribas, BNY Mellon, and more) to test the feasibility of such private-public blockchain communications.[23] In its Report discussing the findings of this collaboration, SWIFT noted that regulatory compliance would require a "designated depository" (a central account keeper or bookkeeper) to confirm settlement finality in a transfer system involving public-private blockchain communications.[24] This underscores the fact that, for certain transactions, an overlay of rules and practices external to the technological system itself (that is, offchain) may be necessary for regulatory compliance.

  Similarly, hashed time-lock contracts (HTLCs) have been explored by Central Banks – specifically, the Monetary Authority of Singapore and the Bank of Canada– as an experimental technical solution to facilitate atomic (though non-simultaneous) swaps across permissioned blockchain networks.[25] However, HTLCs have not seen widespread adoption as a vehicle for interoperability across private blockchains, potentially given certain fundamental economic and technical problems associated with HTLCs.[26]

22: See Cross Chain Risk Framework, Categories of Risk, https://crosschainriskframework.github.io/framework/20categories/categories-of-risk/ (accessed May 10, 2024).

23: Macaulay Peterson, Blockworks, Banks can '10x the Blockchain Industry" Saus Chainlink Co-Founder (June 6, 2023), https://blockworks.co/news/banks-can-10x-the-blockchain-industry-says- chainlink-co-founder, see also Chainlink Labs, An Industry Case Study: Cross-Chain Settlement of Tokenized Assets Using Chainlink CCIP (Sept. 2023), https://pages.chain.link/hubfs/e/anz-ccip-cross-chain-tokenized-asset-settlement-case-study.pdf.

24: Swift, Swift unlocks potential of tokenisation with successful blockchain experiments (Aug. 31, 2023), https://www.swift.com/news-events/press-releases/swift-unlocks-potential- tokenisation-successful-blockchain-experiments.

25: Bank of Canada and the Monetary Authority of Singapore, Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies (2019), https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf; Yunyoung Lee et. al., Atomic Cross-Chain Settlement Model for Central Bank Digital Currencies (Sept. 2021), https://www.sciencedirect.com/science/article/pii/S0020025521009713/.

26: See Cyber Initiative, Youtube, HTLCs Considered Harmful - SBC'19 (Feb. 6, 2019),

https://www.youtube.com/watch?v=qUAyW4pdooA (Dan Robinson on HTLCs).

Legal

Technological innovations can go a long way in providing the settlement guarantees and risk mitigation we seek for hybrid transactions. However, particularly for hybrid transactions involving transfers wholly outside of the blockchain context and/or on private blockchains, they may not go far enough. For public blockchains which lack deterministic settlement finality on a technical level, external legal intervention may be necessary to generate institutional adoption, public trust, and regulatory acceptance where such blockchains are used as a settlement layer for financial primitives. Likewise, legal mandates on specific actors may be more feasible and effective where a centralized manager (of an offchain ledger, or private blockchain) is involved in one - or both - legs of a transaction and is easily identifiable. There are a number of avenues for such legal intervention, which vary in their degree of intrusiveness on public blockchain infrastructure. As highlighted above, different avenues may be appropriate depending on the nature of the transaction at issue and preferences of the transacting parties.

Legal requirements applicable to settlement infrastructures supporting certain types of financial transactions – like those by regulated financial institutions,[27] and/or on financial market infrastructures deemed "systemically important"[28] – mandate certain and legally enforceable settlement finality. That is, no amount of technical innovation will be adequate without an external legal basis for settlement finality.[29] This suggests that, in order to maximize the potential for public blockchains to be used as settlement layer for a diverse array of financial activities, a moment of settlement finality following which transactions are perpetually recognized as final should be defined and consistently recognized by DeFi market participants, institutional players, and the law. For instance, settlement finality on Ethereum could be legally defined as the moment when a transaction is followed by a finalized checkpoint. Alternatively, settlement finality could also be defined as some later point where the finality guarantee is even higher.

Such a legal basis for settlement finality could be codified by contract between, for instance, an offchain issuer of a RWA token and purchasers of the token, providing that the offchain issuer will recreate any transactions reversed following the contractually defined moment of settlement finality at original prices or reimburse the purchaser for any amount lost. In this way, the costs of principal settlement risks for hybrid transactions involving an offchain transfer could be allocated ex-ante by contract, enhancing certainty for market participants that their transactions will be recognized economic effect following the moment of settlement finality, even if the network ceases to recognize their transaction.

Additionally, a defined moment of settlement finality could become incorporated in public law or industry self-regulation. This could provide a legal cause of action for a trader financially harmed by a settlement disruption following legal settlement finality against the misbehaving actor (byzantine validator, or negligent / intentionally malicious client software developer) whose conduct caused the blockchain reorganization. Further, technological solutions like protocol-enshrined insurance mechanisms (e.g., slashing insurance[30]) could work in concert with such legal rules to provide for certain recompensation for victims of blockchain reorganizations whose "reasonable expectations" of settlement finality (as legally defined) are breached.

27: Basel Committee on Banking Supervision, Prudential treatment of cryptoasset exposures (Dec. 2022), https://www.bis.org/bcbs/publ/d545.pdf.

28: PFMI.

29: In the SWIFT experiment above involving public-private blockchain hybrid transactions, this external legal basis was provided by the centralized "designated depository" who confirmed when transactions were finally settled. Swift, Results Report, Connecting Blockchains: Overcoming Fragmentation in Tokenised Assets (Aug. 2023), https://www.swift.com/swift-resource/252093/download.

30: Soubhik Deb, Robert Raynor, and Sreeram Kannan, STAKESURE: Proof of Stake Mechanisms with Strong Cryptoeconomic Safety (Jan. 11, 2024), https://arxiv.org/pdf/2401.05797.pdf.

We have yet to discuss the risks associated with settlement delays (rather than reorganizations) resulting from network latency, congestion, or inefficient gas pricing. This can be classified as an operational risk affecting transaction execution, in contrast to principal risk which - as we have discussed - affects trade settlement. Still, in the context of hybrid transactions involving Ethereum transfers, settlement delays pose significant problems – in addition to making trade processing slower, by increasing the time between trade execution and settlement, settlement delays increase the likelihood that a transacting party will face a total loss of principal. To address this problem, the law could impose obligations on an offchain agent involved in a hybrid transaction (e.g., a transfer agent or "designated depository"[31]) to "do their best" to ensure timely inclusion of transfers they instruct on a public blockchain – this might look like gas fee minimums, privately negotiated agreements with block-builders or relay providers (e.g., purchasing blockspace futures),[32] and/or trade limitations in periods of high network congestion.

Market-based

According to the Bank of International Settlements (BIS), one of the main drawbacks of public blockchains is that they lack the "settlement finality that comes from central bank money residing in the same venue as other claims."[33] It appears that this is a criticism of the fact that in a decentralized financial environment, there is no clear analogue to the "full faith and credit" of the government that underlies public trust in traditional financial markets.

Should NSCC fail tomorrow, there is a general acknowledgment that the U.S. government would probably bail them out (or create a monetary situation wherein they are very likely to be bailed out by private actors), which creates a general sense of confidence that securities will continue to be settled without principal risk borne by individual market participants even in the event of a huge market shock. The security of a government backstop is even more explicit in the traditional banking sector, where the Federal Deposit Insurance Corporation (FDIC) – created after the Great Depression, the most infamous black swan event – automatically insures all bank deposits up to $250,000. However, it is unclear what would happen if a malicious validator acquired 67% control of Ethereum's network tomorrow, and chose to rewrite the history of the blockchain. There is a chance that the Ethereum community, through social governance, would decide to hard fork the blockchain (see the DAO) to restore any reversed transactions, but this is far from a foregone conclusion. In effect, there remains some likelihood that individual market participants would have to bear the principal risk of settlement failures in the event that they occur, which is a source of uncertainty that the entire DeFi industry shares an interest in putting to rest.

To conclude, we consider some ways in which DeFi markets could evolve to provide stronger guarantees of settlement finality and protection in the case of a "black swan" event, without losing the potential for true decentralization:

1. **Decentralized settlement insurance** – In their recent paper, Soubhik Deb, Robert Raynor, and Sreeram Kannan of Eigenlayer proposed a mechanism to utilize slashed funds (which are currently burned) as a means to compensate victims of settlement disruptions.[34] A settlement insurance mechanism could also operate in a manner somewhat analogous to the depository insurance scheme for banks in the traditional financial system, wherein participants pay regulator assessments to the insurance fund in exchange for coverage. An important difference, however, could be

31: See note 25.

32: Drew Van der Warff and Alex Matthews, Opportunities and Considerations of Ethereum's Blockspace Future (July 26, 2023), https://frontier.tech/ethereums-blockspace-future.

33: Bank of International Settlements, BIS Annual Economic Report 2023, Blueprint for the future monetary system: improving the old, enabling the new (2023), https://www.bis.org/publ/arpdf/ar2023e3.pdf.

34: Soubhik Deb, Robert Raynor, and Sreeram Kannan, STAKESURE: Proof of Stake Mechanisms with Strong Cryptoeconomic Safety (Jan. 11, 2024), https://arxiv.org/pdf/2401.05797.pdf.

that the settlement insurance treasury is held in smart contracts and managed through a system of decentralized governance.

A decentralized settlement insurance framework, however structured, could operate in conjunction with external legal requirements in the context of financial transactions– for instance, the law could require regulated financial institutions to purchase coverage before engaging in financial transactions involving public blockchains.

2. **Central counterparty for hybrid transactions** – While "centralized" in traditional financial markets, central counterparties (CCPs) do not inherently require centralized management and operation. The core function of a CCP is to pool resources and risk exposure into one entity, so that individual market participants do not have to worry about things like the credit risk posed by their counterparty (who may be a complete stranger given the anonymous nature of today's trading markets). In the case of U.S. securities clearing, that "entity" is the Depository Trust Corporation (DTC), a centralized financial institution. But, it is worth considering whether that "entity" could be, say, a DAO.[35]

   For single-chain transactions, automated market makers (AMMs) serve a functionally similar role to a CCP, providing a pre-funded pool of assets against which market participants can trade without credit risk. However, credit risk may remain for hybrid transactions like those involving centralized cryptocurrency exchanges or traditional financial institutions, who may default on their obligations in the event, for instance, of insolvency. In such cases, a system of central clearing (which could be governed by a decentralized network) could work to spread losses from counterparty default across many market participants. Likewise, this CCP could also be obligated (contractually or by public law) to provide compensation to participants harmed by a settlement disruption, thereby addressing the problem of principal settlement risk in these transactions.

   One implication of this arrangement could be that certain transactions – like fiat-to-crypto onramp transactions – would no longer need to be cleared and settled in-house at the individual centralized exchange where they are executed. Such a shift to central clearing, where exchange execution is separated from clearing/ settlement, could enable efficiencies like the economies of scale associated with CCP netting and enhanced competition among centralized exchanges.

3. **Standardized legal contracts** – While this may sound like it belongs in the "legal" solutions section, the development of a standardized contractual framework to govern certain categories of hybrid transactions is both within the ambit of private sector action and carries significant implications that are not purely legal but economic, technical, and transactional. The ISDA Master Agreement for over-the-counter derivatives transactions, first introduced in 1985, transformed OTC derivatives markets – decreasing transaction costs and enhancing market integrity – by providing a consistent, predictable, and legally enforceable foundation for derivatives transactions. A similar approach may offer significant benefits in the context of certain hybrid transactions – a standardized contractual framework could define the moment of settlement finality for both legs of a transaction, specify how parties should behave and remedies available in the event of settlement disruptions (potentially eliminating principal risk for traders), and even integrate certain aspects of contract logic into the operations of smart contracts.[36]

35: A variant of this proposal has been articulated in Sara Feenan et. al., Decentralized Financial Marekt Infrastructures: Evolution from Intermediated Structures to Decentralized Structures for Financial Agreements, 1 J. of FinTech 2 (2021), https://www.worldscientific.com/doi/epdf/10.1142/S2705109921500024.

36: ISDA, Legal Guidelines for Smart Derivatives Contracts: The ISDA Master Agreement (Feb. 2019), https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf (describing how principles of ISDA documentation may be codified through computer code in "smart derivatives contracts").

With enough adoption, a standardized contractual framework to govern certain hybrid transactions – like those involving tokenized RWAs, stablecoins, etc. – could provide greater legal certainty, institutional credibility, and transactional efficiencies to the use of public blockchains as a settlement medium in these markets and for high-value finance generally.

4. Conclusion

In sum, while the settlement concerns surrounding public blockchains like Ethereum voiced by regulators and the like are often far overstated, there remains a benefit to thinking deeply about systemic vulnerabilities and risk-vectors which could arise before they actually do. Much of traditional finance has been shaped by a patchwork of reactionary responses to "black swan" events – like the great depression, the back office crisis of 1968, the global financial crisis, to name a few. This is like putting bandaids on cracking pipes. By taking a proactive, rather than reactive, approach to enshrining resiliency (through technological, as well as legal and market-based adjustments) in the plumbing of financial markets built on public blockchains, we can build a stronger foundation for a robust, trustworthy, and efficient next-generation financial system.

In this paper, we have identified settlement discrepancies and the resulting principal risks in certain hybrid transactions as a potential systemic vulnerability, and have noted various potential mitigants to this problem. We hope that future technical, legal, and economic research further investigates these (and, hopefully, others in addition to those outlined here) solutions.

Appendix - Table of transaction settlement characteristics

	Example	Intermediary	Simultaneous DvP?	Risks
Traditional DvP	Purchase of securities against payment in cash	Central counterparty (e.g. NSCC)	Sometimes	Replacement cost risk; Principal risk (absorbed by CCP, does not affect traders)
Single Chain DeFi DvP	DEX swap of ETH for PEPE	Decentralized network participants (i.e. validator set)	Always	Replacement cost risk
Hybrid Transaction	Cross-chain (e.g. Solana to Ethereum) NFT sale	Decentralized network participants (i.e. validator set) on both chains + cross-chain messaging contract (e.g. Wormhole)	No	Replacement cost risk; Principal risk (affecting traders)
Hybrid Transaction (On & Offchain incl. private blockchains)	RWA token purchase by wire transfer; centralized exchange fiat-to-crypto onramp transaction	Centralized intermediary for off-chain leg (e.g., ACH; "designated depository" for CCIP) + Decentralized network participants (i.e., validator set) for on-chain leg	No	Replacement cost risk; Principal risk (affecting traders)