PROBABILISTIC SETTLEMENT FINALITY IN PROOF-OF-WORK BLOCKCHAINS: LEGAL CONSIDERATIONS

Hossein Nabilou[*]

ABSTRACT

The concept of settlement finality sits at the heart of any type of commercial transaction; whether the transaction is in physical or electronic form or is mediated by fiat currencies or cryptocurrencies. Transaction finality refers to the exact moment in time when proprietary interests in the object or medium of transaction pass from one party to his counterparty and the obligations of the parties to a transaction are discharged in an unconditional and irrevocable manner, i.e., in a way that cannot be reversed even by the subsequent legal defenses or actions against the counterparty. Given the benefits of finality in terms of legal certainty and its potential systemic implications, legal systems throughout the world have devised mechanisms to determine the exact moment of the finality of a transaction and settlement of obligations conducted using fiat currencies as a medium of exchange. However, as the transactions involving cryptocurrencies fall beyond the scope of such rules, they introduce new challenges to determine the exact moment of finality in on-chain cryptocurrency transactions. This complexity arises because the finality of the transactions in the cryptocurrencies that rely on proof-of-work (PoW) consensus algorithms is probabilistic. The probabilistic finality makes the determination of the exact moment of operational finality nearly impossible.

After discussing the mechanisms of settlement of contractual obligations in the traditional sale of goods as well as payment and settlement systems - which rather than relying on the concept of

---

[*] *Assistant Professor of Law & Finance, Amsterdam Center for Law & Economics (ACLE), University of Amsterdam, Amsterdam Law School; E-mail: h.nabilou@uva.nl.* *This article was drafted while the author was holding the UNIDROIT – Bank of Italy Chair at the International Institute for the Unification of Private Law (UNIDROIT). The paper has extensively benefited from the discussions with the members of the digital assets and private law group. The author is grateful to UNIDROIT for its generous funding, excellent logistical support, and enriching intellectual environment throughout conducting research on this paper. The author is also thankful to Candida Leone for her invaluable feedback on the earlier drafts of this paper. All errors are those of the author.*

** Editorial note: In this article, "Bitcoin" is capitalized when talking about the concept of Bitcoin but is not capitalized when referencing bitcoin units.

operational finality, rely upon the concept of legal finality - the article argues that even in the traditional payment and settlement systems the determination of operational settlement finality is nearly impossible. This is because no transaction, even a transaction involving a cash payment, cannot be operationally deemed irrevocable as it remains prone to hacks or unwinding by electronic means or mere brute force. The paper suggests that the concept of finality is inherently a legal concept and, as is the case in conventional finance, the moment of finality in PoW blockchains should also rely on the conceptual separation of operational finality from legal finality. However, given the decentralized nature of cryptocurrencies, defining the moment of finality in PoW blockchains, which may require a minimum level of institutional infrastructure and centralization to support the credibility of the finality, may face insurmountable challenges.

TABLE OF CONTENTS

Introduction

Settlement risk has been one of the age-old problems in conventional payment and settlement systems. The main sources of settlement risks are counterparty default risk, operational risks, and uncertainty about the irrevocability of a transaction.[1] Since a settlement failure may result in the failure of a chain of other transactions, it may cause contagion and result in systemic risks if not properly addressed.[2] Due to its potential systemic consequences, such risks have traditionally attracted considerable legal and regulatory scrutiny towards the payment and settlement systems in general and settlement finality in particular.

Various technological, institutional, and legal mechanisms – including judicial, statutory, regulatory, and contractual frameworks – have evolved to address the potential risks stemming from settlement risk. Early examples of such legal mechanisms concern netting, which reduces the settlement risk (i.e., the risk that arises when the payments are not exchanged simultaneously), and close-out netting (which reduces pre-settlement risk such as the risk of default before the settlement date); mechanisms that are mainly applicable in derivative transactions and certain other financial contracts.[3] More recently, various technological and institutional innovations have given rise to different forms of mechanisms that protect the counterparties against settlement risks. Such mechanisms

---

[1] *See* David Mills et al., *Distributed Ledger Technology in Payments, Clearing, and Settlement*, BD. OF GOVERNORS OF THE FED. RSRV. SYS. 31 (2016).

[2] A rather infamous example of the settlement risk is what has come to be known the Herstatt risk, which refers to cross-currency settlement risks in deferred net settlement (DNS) systems resulting from trading across time zones. *See* COLIN BAMFORD, PRINCIPLES OF INTERNATIONAL FINANCIAL LAW 87 (3d ed. 2019) (ebook); BANK FOR INTERNATIONAL SETTLEMENTS, DELIVERY VERSUS PAYMENT IN SECURITIES SETTLEMENT SYSTEMS 14 (1992) [hereinafter DELIVERY VERSUS PAYMENT]; Natalja Westernhagen et al., *Bank Failures in Mature Economies* 5 n.5 (Bank For Int'l Settlements, Working Paper No. 13, 2004).

[3] *See* Barbara C. Matthews, *Capital Adequacy, Netting and Derivatives*, 2 STAN. J.L. BUS. & FIN. 167, 171-72 (1995); Vincent. R. Johnson, *International Financial Law: The Case Against Close-Out Netting*, 33 BOS. U. INT'L L.J. 101, 112-13 (2015).

have been largely successful in protecting the counterparties and financial stability. They have only seldom created problems of systemic significance, making the study of such institutions rather a fringe interest reserved for financial market infrastructure (FMI) aficionados. However, more recently, settlement risk has come into vogue due to the potential settlement issues in the blockchains that use Proof-of-Work (PoW) consensus algorithms.

In studying settlement risks, it is crucial to focus on the two key components of a settlement: the settlement asset (or how settlement is achieved operationally) and legal finality (or how settlement finality is achieved for legal purposes).[4] The settlement asset used in FMIs should have certain properties. It needs to be in the form of an asset bearing the least credit and liquidity risks. This is particularly important within wholesale payment systems, where an otherwise illiquid settlement asset or an asset having counterparty risk would create systemic implications for the systemically important payment systems (SIPS). For example, in Europe and the euro area, SIPS operators must ensure that the final settlements of one-sided payments in the euro are carried out in central bank money (CeBM).[5] The same requirement applies to settling two-sided payments or non-euro one-sided payments, where practicable and available. If CeBM is not used, the operator must ensure that the settlement asset for money settlements has little or no credit and liquidity risks.[6] For settlements in commercial bank money (CoBM), certain conditions are imposed on the SIPS.[7] This paper does not study the price stability or the quality of the settlement asset (such as bitcoin in the Bitcoin Blockchain), instead, it investigates the operational and legal finality aspects of the settlement on certain PoW blockchains.

As major cryptocurrencies carry various degrees of liquidity risks in addition to price volatility, they would not be considered

[4] *See* DELIVERY VERSUS PAYMENT, *supra* note 2 at 15-16.
[5] 2014 O.J. (L 217), *as amended by* 2017 O.J. (L 299), art. 10(1).
[6] 2014 O.J. (L 217), art. 10(3).
[7] *Id.* at art. 10.

reliable settlement assets.[8] In addition, the use of distributed ledger technologies (DLTs) or blockchain for settlement purposes may pose various other risks, such as potential operational and security risks stemming from the use of new technology, lack of interoperability with the conventional FMIs, the potential governance issues in blockchains, and potential issues regarding tamper resistance, privacy, and data integrity.[9] From among all such risks, this paper investigates a specific risk in the payments made by cryptocurrencies. This risk concerns the probabilistic finality of certain cryptocurrencies that use PoW blockchains, such as Bitcoin.[10] The finality of payments and settlements on the Bitcoin Blockchain is viewed as probabilistic due to the likelihood that the most recent transactions embedded in the blockchain may be undone, or bitcoins may be double-spent due to the formation of a fork.[11] The probabilistic finality of Bitcoin has been subject to criticism[12] because the fact that transactions are technically

---

[8] Hossein Nabilou, *Testing the Waters of the Rubicon: The European Central Bank and Central Bank Digital Currencies*, 21 J. OF BANKING REGUL. 299, 302-03 (2019); Hossein Nabilou, *The Dark Side of Licensing Cryptocurrency Exchanges as Payment Institutions*, 14 L. & FIN. MARKETS REV. 39, 41 (2019); Hossein Nabilou, *Bitcoin Governance as a Decentralized Financial Market Infrastructure*, 4 STAN. J. OF BLOCKCHAIN L. & POL'Y 180 (2021) [hereinafter *Bitcoin Governance*]; Hossein Nabilou & André Prüm, *Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies*, 5 J. OF FIN. REGUL. 29, 30 (2019) [hereinafter *Ignorance, Debt and Crytocurrencies*]; Hossein Nabilou, *How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency*, 27 INT'L J. OF L. & INFO. TECH. 266, 286 (2019). Stablecoins may be an exception, but as the history of stablecoins has revealed, the potential flaws in the design may not constitute a great bulwark against price volatility. *See* JP Koning, *End of a Stablecoin*, MONEYNESS (Aug. 22, 2016), https://jpkoning.blogspot.com/2016/08/ [https://perma.cc/A9VL-24GU]; Ben Dyson, *Can 'Stablecoins' Be Stable?*, BANK UNDERGROUND (Mar. 28, 2019), https://bankunderground.co.uk/2019/03/28/can-stablecoins-be-stable/ [https://perma.cc/3Z3W-8RPR].

[9] BANK FOR INT'L SETTLEMENTS, DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENT, CLEARING AND SETTLEMENT 1 (2017) [hereinafter DISTRIBUTED LEDGER TECHNOLOGY].

[10] BANK FOR INTERNATIONAL SETTLEMENTS, ANN. ECON. REP. 101-04 (2018) [hereinafter ANNUAL ECONOMIC REPORT].

[11] *Id.*

[12] *See* Tim Swanson, *Settlement Risks Involving Public Blockchains*, GREAT WALL OF NOS. (Mar. 24, 2016), https://www.ofnumbers.com/2016/03/24/settlement-risks-involving-public-blockchains/ [https://perma.cc/6KEJ-PVVB]; Morten Linnemann Bech et al., *On the Future of Securities Settlement*, BIS QUARTERLY REVIEW 75 (2020). The uncertainty stemming from the settlement finality may be a serious obstacle for the use of certain forms of distributed ledger technologies (DLTs) in the settlement of securities. *See The Use of DLT In Post-Trade Processes*, EUR. CENT. BANK 7 (2021).

vulnerable to forking or potential unwinding is an impediment to Bitcoin's objective of becoming a payment network or a settlement layer for transactions.

Regarding settlement finality in PoW blockchains, there seem to be two main problems. First, in the arrangements relying on consensus algorithms for settlement finality, there may not be a single point in time when the settlement finality is achieved. Furthermore, the legal regime may not expressly recognize finality in such networks, even though the participants in the system may have impliedly been deemed to have agreed on a certain moment for the finality of the transfer.[13] In other words, both in legal and operational terms, we may face difficulty with respect to the finality of settlement under the current legal and regulatory frameworks around the globe.

One major limitation of the paper is that it only discusses settlement finality in PoW blockchains. Different networks may have different mechanisms for transaction confirmation. PoW and Proof of Stake (PoS) are two main mechanisms. Within the PoW blockchains, various blockchains may use different methods of recording transactions. In general, the recording of transactions in blockchains may rely on two major models: account-based settlement and token-based settlement.[14] Some networks update balances in the ledger that records the positions through debits and credits, while others work based on transferring digital assets in the ledger (namely, the ledger records the transfer of ownership of a given digital asset that is native to the ledger).[15] Although PoW blockchains differ from the PoS blockchains in terms of settlement finality,[16] the method of transaction recording may have little bearing on the debate on settlement finality.[17] This paper only deals with on-chain transactions on the blockchains that rely on the PoW consensus algorithms with probabilistic finality. Off-chain transactions, depending on the methods and the media used, are subject to the relevant rules of exchanges or payment and settlement systems.[18]

---

[13] *See* DISTRIBUTED LEDGER TECHNOLOGY *supra* note 9 at 16.
[14] Aldar C-F. Chan, Utxo in Digital Currencies: Account-Based or Token-Based? Or Both? 1 (Sept. 20, 2021) (unpublished manuscript).
[15] *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 9 at 15 (stating that certain other networks work based on transferring digital representation of physical asset that are held in custody off-chain).
[16] *See id.*
[17] *See id.* at 16.
[18] *See id.* at 15-16.

This paper first explains the concept of probabilistic finality in cryptocurrencies relying on PoW with a special focus on the Bitcoin Blockchain. Second, it highlights the role and importance of transaction finality in traditional commercial and payment transactions. Third, it elaborates on the importance of distinguishing between *legal* finality, as opposed to *operational* finality, in private and commercial law as well as in regulatory law. Fourth, the paper dives deeper into the underpinnings of the concept of settlement finality and its private law as well as regulatory law foundations. In doing so, in addition to discussing the concept of finality in transactions such as the sale of goods, it explores the concept of finality in payments and securities settlement systems and argues that the protections and legal mechanisms that are applicable in payment and settlement systems can also be extended to the PoW blockchain transactions. Fifth, the paper concludes by arguing that not only PoW blockchains, but also conventional settlement systems, cannot ensure technological or operational finality in its strictest sense. Therefore, it is inevitable to rely on legal finality both in traditional payment and settlement systems as well as cryptocurrency networks, however, limitations of legal protections in the PoW blockchains should not be overlooked.

Transaction processing and the problems with settlement finality in the Bitcoin Blockchain

Understanding the reasons behind the probabilistic finality in the PoW blockchains requires studying the main value proposition of such networks. It seems that the main driving force behind the first cryptocurrency was censorship resistance that "allows participants to transact in an environment with minimum social trust."[19] Censorship resistance would mean that there would be no central or single entity in the system that could influence the system in any substantial manner, e.g., by blocking transactions.[20] The way to achieve such censorship resistance is thought to be through decentralization.[21] However, creating and maintaining artificial scarcity in electronic records (assets) in a decentralized manner by preventing duplication (e.g., double spending) has proved to be a substantial challenge that hampered the emergence of digital assets

[19] *Bitcoin Governance, supra* note 8 at 177 (2021); *see also* Nick Szabo, *Money, Blockchains, and Social Scalability*, SATOSHI NAKAMOTO INST. (Feb. 09, 2017), https://nakamotoinstitute.org/money-blockchains-and-social-scalability/ [https://perma.cc/F7GQ-APEJ].
[20] *Bitcoin Governance, supra* note 8 at 177, 186-87.
[21] *Id.* at 186.

for decades.[22] Bitcoin (and its so-called distributed "trust machine"[23]) as a distributed peer-to-peer ("P2P") system eventually solved the age-old double-spending problem by bringing together a decentralized P2P network (the Bitcoin Protocol), a public transaction ledger (the blockchain), a set of consensus rules for independent transaction validation and native asset issuance, and a mechanism for reaching global consensus on the valid chain in a decentralized manner, i.e., the PoW algorithm.[24]

Prior to Bitcoin, even outside the virtual space, addressing the double-spending problem was delegated to trusted third parties with centralized ledgers, who verified and confirmed financial transactions and determined their legal finality.[25] Such intermediaries could, as a matter of course, exert control on the transaction within the bounds defined by law and contract.[26] Bitcoin solved this problem in a secure, *decentralized*, consensus-based, and censorship-resistant manner, without relying on centralized third parties.[27] The PoW algorithm used in the Bitcoin Blockchain, despite being energy intensive, appears to be a secure technique that provides a decentralized and incentive-compatible mechanism for verifying and confirming transactions, as well as securing the Bitcoin Blockchain.[28]

In the Bitcoin network, the user controlling a private key (A), which controls a specific unspent transaction output (UTXO), can

---

[22] *Tokenization: A Digital Asset Déjà Vu*, MCKINSEY & CO. (Oct. 26, 2023, 4:32 PM), https://www.mckinsey.com/industries/financial-services/our-insights/tokenization-a-digital-asset-deja-vu#/ [https://perma.cc/9BCA-A6AJ].

[23] *The Promise of the Blockchain: The Trust Machine*, THE ECONOMIST (Oct. 31, 2015), https://www.economist.com/leaders/2015/10/31/the-trust-machine [https://perma.cc/XLU3-7S3X].

[24] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 1-3 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/BG2S-4VU2]; ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN 2 (Tim McGovern ed., 2d ed. 2017).

[25] *See* Satoshi Nakamoto, *supra* note 24 at 2.

[26] *Id.*

[27] *Id.* at 2-3, 7.

[28] The proof-of-work in principle discourages a 51% attack on the network through certain incentive mechanisms which make hacking the system economically unfavorable to the hacker. *See* Josh Stark, *Making Sense of Cryptoeconomics*, COINDESK (Aug. 19, 2017), https://www.coindesk.com/markets/2017/08/19/making-sense-of-cryptoeconomics/ [https://perma.cc/UB4L-MFMQ]. These incentives counteract early fears of such a 51% attack. *See* Katherine Heires, *The Risks and Rewards of Blockchain Technology*, RISK MGMT. MAG. (Mar. 1, 2016, 6:04 AM), https://www.rmmagazine.com/2016/03/01/the-risks-and-rewards-of-blockchain-technology/ [https://perma.cc/4PAK-JTFA].

send it to another user (B) through the blockchain. When A fills in the amount and fee and sends the instructions, the wallet signs the transaction using A's private key. As soon as the transaction is signed, it is propagated and validated by the network nodes. Then, the miners include the transaction in the next block which is to be mined. The miner who solves the PoW and succeeds in finding the nonce propagates the block to the network. Thereafter, the nodes verify the result and propagate the block.[29] As soon as the result was verified by the nodes, B sees the first confirmation in his wallet indicating that the amount of bitcoin sent by A is received. With each new block, new confirmations appear. Decentralization is achieved in the sense that the network is open and permissionless and unlike traditional centralized payment systems, everyone can join the network to verify and confirm the transaction.

However, such a simplistic overview of the transaction in the Bitcoin Blockchain masks the complexity of the settlement finality in PoW blockchains. There are at least four main reasons that prevent PoW blockchains from guaranteeing the finality of individual payments. First, despite the transparency of the blockchain technology that allows the users to verify whether a specific transaction is included in the ledger or not, there can be rival versions of the ledger or chains of which the parties may not be aware. Simultaneous updates to the ledger by two parties can potentially result in the unwinding of some transactions *ex-post* in spite of the parties' perception that the transaction was final. As ultimately one of the chains or updates to the ledger will survive, the finality of the payments appended to each ledger will remain probabilistic.[30]

The second issue originates from the famous 51% attack.[31] This means that the miners who have substantial computing power can potentially manipulate the ledger, although only to a limited

---

[29] *See, e.g.*, *Proof-of-Work (POW),* ETHEREUM, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/ [https://perma.cc/4K88-QSAP] (last visited Oct. 27, 2023). As soon as the transaction is submitted to the blockchain, it is often picked up by node operators – miners who put the transaction in a block ready for confirmation. The miners confirm those blocks that adhere and conform to the consensus rules and relay them to the node operators.

[30] ANNUAL ECONOMIC REPORT, *supra* note 10 at 101.

[31] Although Bitcoin has never been subject to a successful 51% attack, there have been a few successful 51% attacks to perform double-spends on some cryptocurrencies such as Verge, Bitcoin Gold, and MonaCoin. *See* Cali Haan, *Verge, Bitcoin Gold and Monacoin Hacked*, CROWDFUND INSIDER, (May 25, 2018, 7:41 AM), https://www.crowdfundinsider.com/2018/05/133936-verge-bitcoin-gold-and-monacoin-hacked/ [https://perma.cc/HS58-VKFZ].

extent. The issue arises from the fact that at the time that a transaction is perceived to be settled, it is impossible to ensure the finality of the settlement because the attacker would only reveal the forged ledger once it is sure that its attack was successful.[32] This would have a serious implication for the finality of the settlement in the sense that the finality will remain probabilistic. Although the difficulty with which a successful attack could be performed diminishes as the subsequent updates are added to the ledger, the tamper resistance can never reach 100%.[33]

The third problem with the finality of transactions may arise from forking, which happens if a subgroup of cryptocurrency users may coordinate to use a new version of the ledger or protocol, while other users insist on using the original ledger.[34] This will lead to the emergence of two sub-networks of users resulting in network splitting.[35] Blockchains have split in several historical instances, including a 2013 case whereby an erroneous upgrade to the Bitcoin protocol and its rollback via coordination between developers and miners led to a blockchain fork:[36]

On March 11, 2013, there was an erroneous upgrade to Bitcoin protocol that led to two sets of miners mining legacy protocol and the updated one separately. A chain-split of at least 24 blocks occurred with the new chain having a maximum lead of 13 blocks. Two separate chains were mined for several hours and there had been a successful double-spend. This incident caused bitcoin price to sink by one-third. However, the fork was rolled back by coordination between developers and miners who decided to *ignore the longest chain*, an apparent violation of the Nakamoto consensus. This resulted in some transactions being voided, and raised concerns not only about settlement finality, but also about Bitcoin governance

---

[32] ANNUAL ECONOMIC REPORT, *supra* note 10 at 101-02.
[33] *Id*. at 102.
[34] *Id*.
[35] *A Complete History of Bitcoin's Consensus Forks*, BITMEX RSCH. (Dec. 28, 2017), https://blog.bitmex.com/wp-content/uploads/2017/12/2017.12.28-A-complete-history-of-Bitcoins-consensus-forks-.pdf [https://perma.cc/X8W7-2V94]; *see also* Vitalik Buterin, *Bitcoin Network Shaken by Blockchain Fork*, BITCOIN MAG. (Mar. 13, 2013) https://bitcoinmagazine.com/technical/bitcoin-network-shaken-by-blockchain-fork-1363144448 [https://perma.cc/RA5A-N3C6].
[36] *A Complete History of Bitcoin's Consensus Forks*, *supra* note 35.

and who decides issues concerning upgrades, and how such critical issues should be managed in the future. [37]

The problem with potential coordinated reorganizations, which would compromise the tamper-resistant property of PoW blockchains, would also give rise to concerns about transaction finality. For example, in the immediate aftermath of the Binance hack in 2019, there have been discussions about Bitcoin Blockchain reorganization to reverse transactions and undo the damage. Although such discussions faced immediate and strong resistance from users and developers, leading to the concession by miners and exchanges not to pursue the proposal, such issues are likely to add further questions as to the finality of transactions on blockchains.

Fourth, there remain concerns about Bitcoin's long-term viability – sometimes dubbed a doomsday scenario – due to the issues related to the Bitcoin security model,[38] rooted in its declining block reward or subsidy.[39] Since the Bitcoin block subsidy, which is allocated to successful miners, will stop sometime in the year 2140, in the absence of such a reward, the miners will lack adequate incentives to mine bitcoin and thereby contribute to the security of the blockchain by confirming transactions.[40] Although in theory this concern may be enough to prevent the Bitcoin network from functioning presently by way of backward induction, it seems that market participants anticipate that some solutions will be found for this problem through time, e.g., transaction fees substituting the

---

[37] *Bitcoin Governance, supra* note 8 at 180; *see also* ANNUAL ECONOMIC REPORT, *supra* note 10 at 102; @macbook-air, BITCOIN FORUM *A Successful Double Spent US$10000 against Okpay This Morning* (Mar. 12, 2013, 6:22:02 PM), https://bitcointalk.org/index.php?PHPSESSID=kaoj1mno9enotqmhpvnsj0rue2&topic=152348.msg1616747#msg1616747 [https://perma.cc/X7QZ-ZD6G].

[38] *See* Raphael Auer, *Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies* 18 (Bank for Int'l Settlements, Working Paper No. 765, 2019) [hereinafter Raphael Auer]; Tim Swanson, *supra* note 12.

[39] Hasu et al., A Model for Bitcoin's Security and the Declining Block Subsidy, UNCOMMON CORE (Oct. 15, 2019), https://uncommoncore.co/research-paper-a-model-for-bitcoins-security-and-the-declining-block-subsidy/ [https://perma.cc/YM9V-JFBG] [hereinafter Hasu]; Raphael Auer, *supra* note 38 at 4.

[40] Dan Held, *Bitcoin's Security is Fine: Fears over the Declining Block Reward are Overblown*, MEDIUM (May 15, 2019), https://danhedl.medium.com/bitcoins-security-is-fine-93391d9b61a8 [https://perma.cc/8UE2-WEHN].

block reward.[41] Thus far, various proposals for dealing with such an issue have been put forward, such as improving block space, perpetual issuance of the block reward, crowdfunding, and adapting the supply of the block space,[42] however, none have been implemented or even tested. The lack of incentive to confirm transactions on the Bitcoin Blockchain – if not an existential threat to the Bitcoin network – will likely increase the time needed for the transaction confirmation and will have a significant bearing on the transaction finality.[43]

Despite such concerns, the probability of transactions being reversed, undone, or ending up in an orphan chain is a function of the block height, meaning that the probability of undoing transactions embedded in the Bitcoin Blockchain depends on how deep the transaction is recorded in the blockchain.[44] As more and more blocks are built on the Bitcoin Blockchain, the lower the probability of undoing the embedded transactions, and as the transaction gets deeper and deeper in the blockchain, the probability becomes infinitesimal.[45] At a certain point, this probability becomes so small that it seems that it has persuaded some authors to suggest that the PoW algorithm of the Bitcoin protocol[46] ensures that the extrinsic investment in expended energy would act as a "thermodynamic guarantee of immutability."[47]

In addition, the concerns about probabilistic finality and the absence of legal protections might be reduced as certain

---

[41] Dillon Healy, *Even Without a Mining Subsidy, These Two Factors Will Protect Bitcoin into the Future*, BITCOIN MAG. (Dec. 29, 2022), https://bitcoinmagazine.com/technical/bitcoin-security-without-mining-subsidy [https://perma.cc/XTC2-AZ4A].
[42] Hasu, *supra* note 39.
[43] *Id.*
[44] *Block Height*, BINANCE ACADEMY, https://academy.binance.com/en/glossary/block-height [https://perma.cc/ZKY5-33K5].
[45] Adam Hayes, *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*, INVESTOPEDIA (Apr. 23, 2023), https://www.investopedia.com/terms/b/blockchain.asp [https://perma.cc/V85F-YESQ].
[46] Satoshi Nakamoto, *supra* note 24; *see also* ANDREAS ANTONOPOULOS, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN (O'Reilly Media ed., 2d ed. 2017).
[47] Cantech TV, *Andreas Antonopoulos Talks Bitcoin, Blockchain and Beyond*, YOUTUBE (Jun. 27, 2016) https://www.youtube.com/watch?v=JulE7xM2CgY [https://perma.cc/AXB2-D8BU].

developments, such as the Lightning Network,[48] may significantly diminish the use of the Bitcoin Blockchain for retail (large volume, low value) transactions. However, it seems that such developments, rather than solving the problem, just transfer it to somewhere else, meaning that they may eventually increase the number of wholesale (large value, low volume) transactions on the Bitcoin Blockchain. Furthermore, most transactions in cryptocurrency exchanges take place through book entries on the books of the relevant exchange rather than using blockchains to transfer tokens. However, inter-exchange and inter-wallet transactions are likely to go through the relevant blockchain. Therefore, at the time of writing, due to transaction batching used for discharging inter-exchange liabilities, which is essentially like the deferred net settlement (DNS) systems in conventional finance, the number of transactions that settle on the Bitcoin Blockchain does not appear to be large, however, the amounts that are settled remain sizeable. In other words, these inter-exchange markets exhibit the attributes of large-value payment systems (LVPS), where systemic risks may become prevalent. If cryptocurrency markets become sufficiently large, these markets would become the Achilles heel of the cryptocurrency industry due to settlement finality risks as well as the volatility and illiquidity of the settlement assets. The next section elaborates on the concept of settlement finality and its legal importance.

The legal importance and implications of settlement finality

Settlement finality – defined as the exact moment in time at which the proprietary interests in the object or medium of transaction pass from one party to another party and the obligations of the parties to a transaction are discharged in an unconditional and irrevocable manner (e.g., in a way that cannot be reversed even by the subsequent legal defenses or actions against each other)[49] – has been one of the most intriguing questions of contract and commercial law and of immense practical as well as intellectual relevance.[50] In law, settlement finality often depends on the type of the contract (e.g., whether the contract involves the exchange of

[48] *See* Joseph Poon & Thaddeus Dryja, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments* SATOSHI NAKAMOTO INST. 1-2 (2016); Aaron van Wirdum, *The History of Lightning: From Brainstorm to Beta*, BITCOIN MAG. (Apr. 4, 2018) https://bitcoinmagazine.com/technical/history-lightning-brainstorm-beta [https://perma.cc/52CP-49UZ].

[49] *See generally* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 9 at 16.

[50] As this definition suggests, the conventional concept of settlement finality is inherently a legal concept meaning that a legal definition of finality necessarily bars certain defences that would otherwise be available to the payer against the payee.

commodities (goods), securities (including derivatives), or funds) as well as the settlement terms embedded in the contract (e.g., the nature of the second leg of the transaction, what private law refers to as price). For instance, in securities transactions when the securities are delivered to the buyer and the funds to the seller, the transaction is said to be final (i.e., settled). In commodity trades, depending on the specific terms of the settlement, the commodities transaction may only involve the settlement of funds, or delivery of financial instruments, other documents, or commodities themselves.[51] In derivative transactions, the settlement depends on the type of the derivative and the terms of the settlement. In such transactions, often the settlement involves settlement of funds (i.e., cash settlement) and only on very rare occasions, the commodity itself.[52]

By definition, each leg of a transaction is considered final when the transfer is irrevocable and unconditional. When there are multiple legs to the transaction, the delivery vs. payment (DvP), delivery vs. delivery (DvD), or payment vs. payment (PvP) mechanisms are often used to coordinate settlement of different legs of the transactions as well as to manage the risk of one leg settling with finality and the other failing to settle.[53] Because depending on the legal nature of the object or medium of exchange the settlement finality may vary, the determination of the nature of the settlement asset is an important consideration in determining the nature of the settlement in cryptocurrency transactions. In addition, in cryptocurrency transactions, depending on the cryptocurrencies being used as a medium of exchange or as the object of exchange, the settlement terms and methods may differ. This paper assumes that cryptocurrencies are being used as media of exchange rather than their object.

The moment of finality is of great significance in commercial and financial transactions as it provides legal certainty to the parties to a transaction as well as the interested third parties to the effect

---

[51] This is the case, for example, in the sale of goods.

[52] JOHN C. HULL, OPTIONS, FUTURES, AND OTHER DERIVATIVES 47 (Pearson, 9th ed. 2018).

[53] David Mills, *supra* note 1 at 6; *see generally* BANK FOR INTERNATIONAL SETTLEMENTS: PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (2012) [hereinafter PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES]; DELIVERY VERSUS PAYMENT, *supra* note 2 at 13; Jan H. Dalhuisen, *Dalhuisen on Transnational Comparative, Commercial, Financial and Trade Law Volume 1: The Transnationalisation of Commercial and Financial Law and of Commercial, Financial and Investment Dispute Resolution* 1 THE NEW LEX MERCATORIA & ITS SOURCES 517-18 (Hart Publishing, 6th ed. 2016) (each source offering concise descriptions of the different models of settlement).

that a transaction that has cleared the moment of finality cannot be successfully challenged in a court of law. As the finality of a transaction bars many of the defenses, which might otherwise be brought by the payer, transferor, or third parties against the payee or transferee to unwind a transaction, the finality of a transaction is essential to commerce as it gives parties and third parties the assurance that the transactions will not be unwound *ex-post*. This means that the parties can take the funds free from any claims and can use them without worrying about the potential challenges to the transactions, which could result in unwinding any future transactions in which the received funds are used. In addition, as settlement finality is relied upon by the parties in updating their own ledgers and determining the amount of their assets and liabilities, it has serious implications for the balance sheets of the participants, rights of their customers and creditors, the assignment of liability to each party, and ultimately for measuring and monitoring risk.[54]

One of the major benefits of having a clear legal regime for determining the exact moment of finality manifests itself in the context of bankruptcy law, where before all the obligations are cleared and settled, the payer becomes subject to an insolvency proceeding. Under such circumstances, the question may arise as to whether the uncleared and unsettled transaction constitutes part of the estate of the insolvent party or belongs to the non-defaulting solvent party. The importance of bankruptcy regimes to transaction finality is not limited to the determination of the bankruptcy estate, as bankruptcy regimes often are intrusive and where the benefits of finality come into conflict with the goals of bankruptcy law, often it is the former that gives way. For example, the bankruptcy estate may be able to unwind certain transactions entered into prior to the liquidation due to the transaction being identified as a transaction at an undervalue, as a voidable preference, or an extortionate credit bargain.[55]

Given its importance in terms of legal certainty, to minimize the uncertainty that may arise from potential *ex-post* legal interventions, special legal protections have been created to achieve legal transaction finality. Traditional commercial law, as well as bankruptcy law, both have created similar approaches to determining the finality of commercial transactions. These mechanisms often rely on specific legal constructs such as a moment or a condition upon the realization of which the transaction is deemed to be final, meaning that it is no longer possible to unwind

---

[54] David Mills, *supra* note 1 at 31.

[55] ALAN DIGNAM & JOHN LOWRY, COMPANY LAW 472-77 (Oxford University Press, 7th ed. 2012).

the transaction. However, given the potential systemic importance of determining the moment of finality and its importance to the orderly functioning of the financial markets, regulatory law has taken a rather different approach to determining the moment of finality in the FMIs by defining the exact moment of transaction finality and moment of irrevocability of transfer orders, which will be reviewed later in this paper.[56]

In addition to the issues that have been dealt with for centuries in conventional commercial and financial transactions regarding their finality, the advent of new payment technologies poses new challenges to determining the finality of transactions and payments made using such technologies. As explained in the prior chapter, this challenge is more significant in the context of blockchains relying on the PoW consensus algorithms as the finality on such blockchains is probabilistic rather than deterministic. In other words, in such transactions, the payer can theoretically never be sure that his payment obligations have been discharged and the payee can never be sure whether he is the rightful owner of the funds, is free of all claims against the payer, and whether subsequent legal action can reverse or unwind the transaction at hand. This means that there always remains a probability of reversibility of the transactions due to either hacks or attacks, forking that may cause the specific transaction to end up in an orphan chain, or potential legal action that might be brought against the payee by the payer or interested third parties (e.g., the creditors of the payer).

Probabilistic transaction finality in PoW blockchains may have further real and legal implications depending on the specific use-cases of a given cryptocurrency. For example, if a cryptocurrency is used as collateral to secure a transaction in a Decentralized Finance (DeFi) setting, the probabilistic settlement finality might get in the way of determining the exact moment of the perfection of a security interest. One way of creating and perfecting a security interest over a crypto-asset may be that the crypto-asset should come under the *control* of the secured party. The uncertainty regarding the exact moment of the finality of the transaction can have implications to the exact moment of the perfection of security interests and may create problems if between the time of the creation of the security interest and its perfection the debtor becomes subject to an insolvency proceeding or where there are two competing security interests that leave the court struggling to establish the priority between competing secured creditors.

---

[56] *See e.g.,* 1998 O.J. (L 166), art. 3; CAROLE MURRAY ET AL., SCHMITTHOFF'S EXPORT TRADE: THE LAW AND PRACTICE OF INTERNATIONAL TRADE 81 (Sweet & Maxwell, 11th ed. 2007).

Furthermore, operational settlement can become more complicated when the delivery of one asset is against the delivery of another (or against payment) such as the exchange of securities against cash or exchange of one currency for another.[57] Under these circumstances, uncertainty about the finality of one leg of the transaction can prevent the other leg from becoming final. In the FMIs, this risk is important because of the back-to-back transactions and the fact that the counterparties may face funding constraints if their transaction happens to be unwound *ex-post*.[58]

Probabilistic settlement finality could create even more problems when both legs of financial transactions are conducted in a blockchain relying on probabilistic finality. For example, in the DvP systems, the delivery of an asset against payment for that asset is dependent upon the payment.[59] In these types of settlement systems each leg's finality is conditional on the finality of the other leg.[60] Not only must there be a clear moment of finality for both legs of the transaction, but also each leg's finality must be conditional on the finality of the other leg. This interdependency of two sets of probabilistic finality adds more complexity if such networks become widespread as part of decentralized financial market infrastructures (dFMIs).

An even further complicating factor would be the case where the payment and delivery legs of a transaction are conducted in different networks, platforms, or blockchains, and there is no trusted third-party intermediary to provide assurances regarding the finality of settlements.[61] In case of default by a counterparty after the settlement of one of the legs of the transaction, there must be legal clarity as to the status of the transaction.[62] To say the least, in the absence of legal clarity, counterparties should consider extra risk

---

[57] *See* DISTRIBUTED LEDGER TECHNOLOGY, *supra* note 9 at 15-16.
[58] *See* PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES, *supra* note 53 at 154.
[59] *See* DELIVERY VERSUS PAYMENT, *supra* note 2 at 15.
[60] *See* Michael Junho Lee et al., *What is Atomic Settlement*, FED. RSRV. BANK OF N.Y. (Nov. 7, 2022), https://libertystreeteconomics.newyorkfed.org/2022/11/what-is-atomic-settlement/ [https://perma.cc/SPC2-YJHT].
[61] *See* David Mills, *supra* note 1 at 32.
[62] José M. Garrido, *Digital Tokens: a Legal Perspective* 5 (Int'l Monetary Fund Working Paper No. 151, 2023).

management measures for the risks stemming from such eventualities relating to settlement risks.[63]

Probabilistic finality in PoW blockchains may also give rise to serious systemic concerns in the case of potential interconnectedness of conventional payment and settlement systems with DeFi. As the transaction finality cannot be ensured operationally and as the existing legal regimes may not be applicable to the transfers using cryptocurrencies to define the moment of settlement finality, the increasing interconnectedness between conventional payment and settlement systems and the payments using cryptocurrencies may increase the contagion channels between these two sectors. At the moment, it is not clear that if the cryptocurrencies became large enough, whether regulators or even central banks would be able to readily deal with such risks. Therefore, it seems that there is a need for legal intervention to define the finality in the transactions on PoW blockchains. However, before moving forward, there is a need for distinguishing two different concepts of finality, i.e., legal and operational finality.

Legal vs. operational finality

What seems to be a source of major confusion in the debate about the probabilistic finality on the PoW blockchains is that the critiques of transaction finality on the Bitcoin Blockchain often confuse two different aspects of finality: technical, *de facto*, or *operational* finality, and *de jure* or *legal* finality. The operational settlement on the Bitcoin Blockchain is probabilistic, so is the operational settlement with cash and any other means of electronic payments, as there is always a theoretical possibility of taking the

[63] David Mills, *supra* note 1 at 31-32. Although some authors have highlighted the use cases of the blockchain technology for the settlement systems, the analysis in this paper shows that at least certain types of blockchains may not be very suitable for use as the settlement layer. For authors' work highlighting the use cases of the blockchain technology in settlements. *See generally* Eva Micheler, *Custody Chains and Asset Values: Why Crypto-Securities Are Worth Contemplating*, 74(3) CAMBRIDGE L.J. 505, 532 (2015); Eva Micheler & Luke von der Heyde, *Holding, Clearing and Settling Securities through Blockchain Technology Creating an Efficient System by Empowering Asset Owners*, BUTTERWORTHS J. OF INT'L BANKING & FIN. L. 652 (2016); David C. Donald & Mahdi H Miraz, *Restoring Direct Holdings and Unified Pricing to Securities Markets with Distributed Ledger Technology*, THE CHINESE UNIV. OF H.K. FAC. OF L. RSCH. PAPER (2019); David C. Donald, *From Block Lords to Blockchain: How Securities Dealers Make Markets*, 44(1) J. OF CORP. L. 29, 60 (2018); Philipp Paech, *Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty?*, 21 UNIF. L. REV. 612, 613 (2016).

cash back by using brute force, or reversing the transaction due to a technical failure in the payment system, including that of a central bank.[64] However, the near impossibility of operational finality does not necessarily mean that the payment is not *legally* final, in the sense that legal challenges cannot invalidate the payment *ex-post*. In other words, probabilistic *operational* finality does not necessarily imply probabilistic *legal* finality and vice versa,[65] and the impossibility of operational finality does not necessarily put a question mark on the legal finality of a transaction. The difference between settlements with conventional payments vis-à-vis the settlements within a PoW blockchain with probabilistic finality is that the settlements on the conventional payment systems enjoy legal finality, whereas there is no legal protection as to the finality of the settlements on the PoW blockchains.

When the operational mechanisms for settling a transaction cannot theoretically provide 100% bulletproof deterministic finality of a transaction, it would be up to the law to intervene and create presumptions for the finality of a settlement, namely, as soon as certain requirements are met, a transaction would be deemed final. This means that although in the PoW blockchains the actual transfers are not 100% final and immutable, the law may want to presume a certain moment of finality provided certain conditions are met. One major role of legal presumptions has been that where reality cannot provide certainty, the law takes over and acts as a supplier of fictional certainty to meet the demand for it. Such presumptions have been developed for the sale of goods, and in the context of negotiable instruments and money, there seems to be no reason why such judicial, statutory, or regulatory presumptions cannot be developed for the transactions conducted on PoW

---

[64] Although the cash transactions are technically reversible, i.e., by taking back the possession of the cash after the payment (technical probabilistic finality), the law protects such transactions by granting strong legal protections on the settlement by cash. One such reason for the strong protections is ensuring the fungibility of banknotes. *See* Crawfurd v. The Royal Bank (1749) Mor 875 (Scot.).

[65] *See* ANNUAL ECONOMIC REPORT, *supra* note 10 at 101-02. In fact, technically speaking, in most transactions, the real world may not provide a solid 100% certainty; therefore, there is a need for the law to intervene and presume that as soon as certain requirements are met, a transaction would be deemed final. As on the Bitcoin Blockchain, similar to any other payment system, the actual transfers are not 100% final and immutable, but the law may presume that at a certain point in time a transaction becomes final. In other words, the fact that the finality on the Bitcoin Blockchain is not deterministic does not stop the law from presuming the finality of a transaction on its blockchain.

blockchains. For example, following custom, the law may presume that after six confirmations[66] a transaction is legally final.[67]

However, under the current legal framework for payments and settlements, the laws ensuring settlement finality (e.g., the EU Settlement Finality Directive),[68] which require payment and settlement systems to specifically define the moment of entry and irrevocability of the orders and transactions, are not applicable to payments made by cryptocurrencies.[69] The lack of any legal protection for settlement finality in and of itself may create various legal problems for the parties to the transaction and may entail systemic implications if the cryptocurrency markets become sufficiently large, and more sophisticated products and services develop around them. The next section explores the foundation of the concept of legal finality and its emergence from private law, the influence it had on the law of payments, and the concept of settlement finality in regulatory law.

Settlement finality in private and public (regulatory) law

To understand the significance of the settlement finality, the importance of legal presumptions, and how they have come to drive a wedge between the operational aspects of finality and its legal aspects, some flashback to the roots of the concept of settlement finality in private law would be enlightening. From a private law perspective, the debate on finality is rooted in two main contractual freedoms. First, freedom to choose the method and medium of payment as a means of discharging obligations.[70] According to this principle, the parties are free to choose whatever they want as a medium of exchange. As payment is only one method of discharging

---

[66] Despite the fact that some merchants even accept zero-confirmation transactions for small payments, such transactions, as far as they are not included in the blockchain, carry certain levels of risks and the transferee would only accept such transactions at his own peril. *See* Raphael Auer, *supra* note 38 at 6, 14.

[67] Although the case law may evolve and presume settlement finality after six confirmations for private-law purposes, given the potential for systemic risk arising from the ambiguity as to the finality of payments, such issues may better be dealt with *ex-ante* within a *regulatory* framework, as is the case with conventional payment and settlement systems. *Id.*

[68] 1998 O.J. (L 166).

[69] *See id.* at arts. 1-2.

[70] Although the creditor is entitled to require the payment in legal currency, the parties may substitute a different obligation from that originally undertaken. *See* HUGH BEALE, CHITTY ON CONTRACTS, 1577-78 (31st ed. 2012). The legal tender laws should not be confused with the freedom to select a specific means of payment (which is probably an extension of the freedom of contract).

obligations, the parties to a transaction may even choose to settle obligations through countertrade (e.g., goods for goods, goods for services, services for goods, or services for services) or other arrangements of their own choice. In addition to the freedom to choose the method and medium of payment, from a purely private law perspective, the parties to a transaction are free to choose the moment of the finality of their transaction. [71]

When parties choose to pay with a given medium of exchange, the legal status of the medium of exchange plays an important role in discharging the obligations of parties to a contract. Such a medium should desirably have two important features. First, it should be immediately available for onward transfers in future transactions. Secondly, it should be free from any adverse claims, which is a prerequisite for the first feature. In other words, the payment should be made with freely transferable funds.[72]

Payments in currency (i.e., legal tender) satisfy both conditions of having immediate availability and of being freely transferable funds. This is because there are well-established and clear rules regarding the moment at which the legal tender settles the obligations.[73] This clear legal regime rests on three sets of rules:

---

[71] "The position is different under the laws of Netherlands, Spain, Germany, the Argentine, Brazil, Chile, and Colombia where the property passes only if the intention of parties is supported by the actual delivery of the goods." Carole Murray, *supra* note 56 at 76-77. As many jurisdictions afford some flexibility on the separation of delivery and the legal construct of passing of property, certain jurisdictions afford the flexibility to parties so that they modify the applicable laws on the passing of the property in the goods sold to be modified by special arrangements between parties to a transaction. Under the UK laws, there are two fundamental principles: (1) If parties contract for the sale of unascertained goods, the property does not pass unless and until the goods are ascertained; and (2) If the contract is for the sale of specific or ascertained goods, the property passes according to the intention of the parties (when the parties intend it to pass). *See id.* at 78. "If the goods are ascertained, under an f.o.b. contract, property in them passes when they are shipped unless the passing of title is postponed by express or implied stipulation; thus, the seller may have reserved the right of disposal of the goods until the contract terms of payment have been complied with." *Id.* at 30.

[72] "In the case where payment must be made 'in freely transferable funds' the payment will normally be made when the funds are freely available in the hands of the recipient, and this will not normally be the case until the funds have been credited to the account specified for receiving payment so that the payee has control over the money following payment." Hugh Beale, *supra* note 70 at 1617.

[73] The moment of finality is not an independent topic in the private law. Finality is largely a regulatory concept, which is mainly discussed and studied in relation to SIPS. *See* 2014 O.J. (L 217), *as amended by* 2017 O.J. (L 299), art. 10(1). However, the basic concepts rely on private law concepts of passing the property or proprietary interests from one party to his counterparty.

take-free rule, shelter rule, and the defenses such as good faith and the purchase for value rule. However, such a determination, i.e., whether the medium of exchange can be deemed to be immediately available and free of any adverse claims, is not straightforward in the case of the transactions in which cryptocurrencies are intended to function as a medium of payment in discharge of obligations. In addition to the concerns about fungibility, this is partly because the finality in the Bitcoin Blockchain cannot be operationally ensured.[74] Seen through this lens, the probabilistic finality in the Bitcoin Blockchain can hardly meet the first criterion, i.e., the immediate availability for onward transfers.

Regarding the second criterion (i.e., take-free rule), due to the uncertainty about the legal nature of bitcoin, especially, whether it can be recognized as property or could benefit from a more precise recognition as money, it is not obvious whether, which, and to what extent the adverse claims of third parties to a given bitcoin, which is used as a medium of exchange, can travel with it. Therefore, there is considerable uncertainty as to whether the freely transferable funds condition can be met. This means that, from a private law perspective, Bitcoin may not be a suitable candidate for becoming a medium of exchange.

Despite Bitcoin's legal handicap, parties may still choose to use it as a medium of exchange according to the above-mentioned freedom that allows the parties to contractually agree on the moment of finality. When a bitcoin is contractually used as a medium of exchange, and not the object of exchange, a great number of private law rules traditionally applied to money, such as the take-free rule, shelter rules, as well as the defenses such as good faith and purchase for value, may be applicable to such a transaction.[75] This means that private ordering can effectively make the traditional defenses, which are available to money, applicable to Bitcoin as well. In this case, for example, if defenses such as good faith and purchase for value are defeated, there would be a need for requiring a party to a transaction to send bitcoins or their equivalent value off-chain back to his counterparty, because it may not be practically feasible to technically unwind the transaction. As such contractual agreements

---

[74] *What Is Finality In Blockchain, and Why Does It Matter?*, COINTELEGRAPH, https://cointelegraph.com/explained/what-is-finality-in-blockchain-and-why-does-it-matter [https://perma.cc/VJ7A-7SMW] (last visited Oct. 30, 2023).

[75] *Blockchain & Cryptocurrency Laws and Regulations 2024*, GLOB. LEGAL INSIGHTS, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa#:~:text=The%20sale%20of%20cryptocurrency%20is,MSB")%20under%20Federal%20law [https://perma.cc/MA2L-2ZTS] (last visited Oct. 30, 2023).

could be cumbersome for the parties to cryptocurrency transactions, especially if such currencies gain considerable adoption, the way forward may be through giving legal effect and recognition – either judicially or by legislation – to the industry standards by developing a legal or regulatory concept of settlement finality in blockchains relying on probabilistic settlement finality.

The private law origins of legal finality

One of the main concerns in private law is the potential impact of the insolvency of a party to a transaction on settlement finality. The insolvency concern has been of great significance in all areas of business law, however, it is of special importance to the settlement finality and the time at which the property passes unconditionally and irrevocably from one party to another, because the party making an advance payment may find himself in a precarious position if the seller becomes insolvent before the passing of property in the goods sold under the contract.[76] Determining the moment of finality in private law where the obligations of parties to a trade are discharged could increase legal certainty in trade and could function as a circuit breaker of potential chain reactions that unwinding of a single transaction in a chain of transactions could create. In the next section, the paper first analyzes the origins of the concept of finality in private law and then it investigates the regulatory concept of finality before venturing into its extension to the cryptocurrencies with PoW blockchains.

Passing of proprietary interests under private law

In private law, the transaction finality depends on the type and the terms of the contract as well as the nature of the medium of payment. In contract law, one of the most important moments in a transaction is the moment at which the property or proprietary interest passes from one party to another. This moment determines the rights and obligations as well as potential liabilities of the parties to a transaction, which is of great importance in case of insolvency of one party to a transaction. The general principle under the private and commercial law of many jurisdictions such as the U.S., the UK, and certain civil law countries is that the property (or the proprietary interest in goods) passes when the parties intend it to pass irrespective of the actual delivery of the physical goods.[77]

---

[76] *See* Carole Murray, *supra* note 56 at 80.
[77] *See id.* at 78-79.

This means that in commercial law, the passing of proprietary interests to goods sold may often be separate from the actual delivery of those goods. The traditional decoupling of the finality of transfer of ownership in commercial law from the physical possession and delivery or transfer of the goods is rooted deep in the foundations of property law where, due to exigencies of commerce, such a separation had to be recognized.[78] Documentary sales in international sales of goods present an interesting case where the decoupling of the delivery of physical goods and the legal passing of property reaches its pinnacle. In the law of documentary credits, the property only passes when the bill (of lading) is delivered to the buyer irrespective of the actual delivery of the goods.[79] This decoupling presents many benefits such as allowing the buyer to resell the goods that are in transit, practically functioning as a source of funding and liquidity in international trade.[80]

---

[78] *Id.* at 81; *see also* Henry Hansmann & Reinier Kraakman, *Organizational Law as Asset Partitioning*, 44 EUR. ECON. REV. 807, 814 (2000). The separation of physical goods from the rights attached to the goods has manifestations in all areas of law from property to contracts, and from company to financial law. For example, stock ownership, contrary to popular belief, does not indicate that the owner of the stock actually owns part of the premises of the company, it only means that the owner has a bundle of rights regarding the legal entity that is called a company. *See generally* Dignam & Lowry, *supra* note 55. In addition, in modern securities law and regulation, the concept of separation of the legal ownership from the beneficial ownership is based on such a decoupling. In property law, and in secured transactions, the floating charge (where a charge is placed on a floating/changing inventory of goods), is a manifestation of this phenomenon. The decoupling of physical possession and transfer of goods from their legal construct of passing of property or being subject to a security interest is what has allowed the development of the effective markets in such property and has been a great impetus for growth. *See* HERNANDO DE SOTO, THE MYSTERY OF CAPITAL: WHY CAPITALISM TRIUMPHS IN THE WEST AND FAILS EVERYWHERE ELSE (Basic Books, 2003).

[79] This is applicable to the situations in which it is the seller's duty to deliver the bill. If no such duty exists, such as in Ex Works or Free on Board (where the buyer contracts with the carrier) or free delivered contracts, the physical delivery of the goods to the buyer or to the carriers is presumed to be the time at which the property passes to the buyer. *See* Carole Murray, *supra* note 56 at 81.

[80] *See* Daniel E. Murray, *History and Development of the Bill of Lading*, 37 U. MIAMI L. REV. 689, 706 (1983). As it is well known in international trade, the banks do not deal with the goods, they only deal with the documents (containing certain rights to goods). This means that such decoupling of right to the goods from the goods themselves allows banks to extend credit to the buyer (by opening a line of credit in his favor). This also happens in many secured transactions where the secured party's rights to the personal or real property is detached from the owner of the real property allowing the items of which the security is created to be used by the owner (obligor) while a security interest in favor of an obligee (secured party) is created. The big chunk of expansion and contraction of credit relies upon the secured financing, facilitated by the developments in property and contract laws.

Such practices are also recognized under the standard practices in international sales. For example, under the cost, insurance, and freight (C.I.F.) term, the goods are deemed to be delivered to the buyer once the bill of lading is delivered to him (or to the bank).[81] This means that the property under the C.I.F. passes at the delivery of the bill of lading to the buyer or to the bank when the payment by a letter of credit is arranged.[82] Under such terms, the risk of loss passes to the buyer on shipment of the item sold, however, the property to such goods does not pass upon shipment. Therefore, under C.I.F., not only the passing of property is kept separate from the delivery of the goods, but also the passing of the risk and passing of the property are kept separate by the legal system (using legal fictions). However, such transfers of property and risk should be kept separate from the strict sense of legal finality in this paper. Under a C.I.F., Cost and Freight (C. and F.), or Free on Board (FoB) contract, where the seller receives the bill of lading from the shipowner, the delivery of the bill to the buyer or his agent is thought to pass the proprietary interests to the buyer *only conditionally*, meaning that the property in the goods sold will revert to the seller if the goods are found to be nonconforming with the contract.[83]

The decoupling of the legal treatment of the moment of the passing of proprietary interests from the moment of the delivery of physical goods (akin to operational finality) has wider implications in legal and financial systems. The entire apparatus of title(-based) finance including seller finance (such as retention of title to goods or conditional sales, and securities lending), buyer finance (such as factoring and discounting, securitization, and sale and repurchase (repo)), and lessor finance (such as finance leasing, hire purchase and sale and lease-back) are directly or indirectly built on the concept of separation of the (physical) possession of goods from the property rights to goods.[84] For example, in the retention of title, the English law allows a clause providing that the seller retains the property in the goods sold until he received the purchase price in

---

[81] CLIVE M. SCHMITTHOFF, SCHMITTHOFF'S EXPORT TRADE: THE LAW AND PRACTICE OF INTERNATIONAL TRADE, 41-42 (9th ed. 1990).
[82] Carole Murray, *supra* note 56 at 44.
[83] *Id*. at 81-82.
[84] PHILIP R. WOOD, LAW AND PRACTICE OF INTERNATIONAL FINANCE 292-99 (2008) (explaining title financing). In the modern securities markets with immobilized and dematerialized securities, the concept of control is taken to be equivalent of the concept of possession, especially for the purposes of creation and perfection of security interests. *See* 2002 O.J. (L 168), arts. 1(5), 2(2); s*ee also* Case C-156/15, Private Equity Insurance Group v. Swedbank, judgment, ¶¶ 36-37, 44 (Nov. 10, 2016).

cash. Such a clause is deemed to be effective and defeats the general presumption that the property in the goods sold passes when the bill of lading passes from the seller to the buyer. In this respect, such a clause is believed to make the passing of property conditional upon a specified event.[85]

This section briefly discussed how property passes from the buyer to the seller – which is akin to the transaction finality in our discussion – in transactions the object of which is goods (sale of goods). The objective of the section is to demonstrate that even where the transaction involves physical goods, due to commercial reasons, certain legal constructs have been designed to decouple the moment of the finality of a transaction (passing of proprietary interests) from the actual delivery of the goods. The next sections study the transactions in which either negotiable instruments or cash (funds or money) is the medium of exchange in a trade and where the finality of payments is determined not by the actual transfer of funds, but by the legal constructs such as the delivery of a payment instrument.

Private law and negotiable instruments

Although the initial forms of money that seemed to function as the settlement layer for trades were in the form of commodity money (i.e., precious metals), the exigencies of (international) trade and recurring ebbs and flows in the supply of the medium of settlement (i.e., gold and silver) gave rise to the creation of (debt) instruments as a medium of exchange that largely came to replace the settlement asset in routine trade transactions. The passing of such instruments from one party to another established a presumption that the proprietary interests in goods subject to trade settled the obligations with finality. Negotiable instruments are a case in point. A common feature to all negotiable instruments is that they are concerned with a promise to pay in the ultimate medium of exchange, clearing, and settlement in the underlying layer of centralized payment system wherein tendering the medium of exchange immediately discharges all the obligations of the parties to a transaction.[86]

---

[85] Carole Murray, *supra* note 56 at 83.

[86] This is why the creditor has no obligation to accept a negotiable instrument (bill, note, or check) in payment of a debt, unless he has expressly or impliedly agreed to do so. *See* Hugh Beale, *supra* note 70 at 1433. In addition, where an agent is authorized to receive payment, he has the authority to receive the payment only in cash. The principal cannot be bound by the agent accepting a bill of exchange without the principal's express authority. *Id*. at 1427.

But what makes some instruments act as negotiable instruments is a legal construct called the concept of negotiability. Under English law, a payment medium should have at least three characteristic features to be considered negotiable:

1. If made payable to the bearer, it is transferable by delivery; and if made payable to order by endorsement and delivery enabling the transferee to sue upon it in his own name;
2. There is a presumption of consideration; and
3. Good title is acquired by the transferee who takes the instrument in good faith and for value, even though the transferor did not have a good title or did not have the title at all.[87]

The third feature of negotiable instruments is the most important feature of such instruments for the purpose of this study. This feature means that the classic doctrine of *nemo dat quod non habet*[88] is not applicable to such negotiable instruments if the good faith purchase-for-value conditions are met.[89] Even within the negotiable instruments, there is a more granular hierarchy between different kinds of negotiable instruments. For example, the negotiability of bills of lading is different from that of bills of exchange. A holder of a bill of lading (unlike the holder in due course of a bill of exchange) cannot acquire a better title than that of his predecessor. In other words, the holder of a bill of lading cannot acquire it free of equities. This means that if a negotiable bill of lading is acquired by fraud and endorsed to a *bona fide* endorsee for value, the *bona fide* endorsee will not acquire title to the goods. However, under the same circumstances, the endorsee of a bill of exchange acquires all the rights arising under the bill of exchange.[90]

---

[87] JAMES S. ROGERS, THE EARLY HISTORY OF THE LAW OF BILLS AND NOTES: A STUDY OF THE ORIGINS OF ANGLO-AMERICAN COMMERCIAL LAW 3 (Cambridge University Press, 2004) (quoting WILLIAM S. HOLDSWORTH, A HISTORY OF ENGLISH LAW 113-14 (8th ed. 2023). Despite this, money could be recovered from a bad faith payee or a payee who received it for no consideration. Money cannot be recovered by means of an action for wrongful interference with goods unless the specific notes and coins can be identified. *See* CHARLES PROCTOR, MANN ON THE LEGAL ASPECT OF MONEY 44 (7th ed. 2012).

[88] Latin phrase meaning "No one can give what he has not got" OXFORD REFERENCE https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100228794 [https://perma.cc/P8WU-ZP7A] (last visited Oct. 26, 2023).

[89] In other words, an important exception to the generally applicable rules of derivative transfer of title is the defense of good faith purchase for value, recognized both in common law and equity. David Fox, *Cryptocurrencies in the Common Law of Property, in* CRYPTOCURRENCIES IN PUBLIC AND PRIVATE LAW, 159 (David Fox & Sarah Green eds., 2019).

[90] Carole Murray, *supra* note 56 at 310. In other words, the shelter rule applies, and innocent acquirer and any onward transferee are protected from competing claims.

This effectively means that bills of exchange are one step closer to being money than bills of lading.

When it comes to cash, i.e., notes and coins, the *nemo dat* doctrine has never applied. Notes and coins pass by delivery and are not recoverable from a person who obtains possession in good faith.[91] The disapplication of this principle is mainly due to commercial reasons because money is the medium by which all other forms of value change hands.[92] The disapplication of the *nemo dat* doctrine to cash makes it the most efficient medium of exchange in the economy.[93] Based on this principle, stolen money cannot be recovered if it is paid for a valuable consideration to a *bona fide* third party.[94] This rule is also applicable to banknotes as they are considered cash and not goods or securities.[95] Therefore, the banknotes and coins are essentially negotiable chattels if received in good faith and for valuable consideration. This means that the transferee acquires good property (good title), even though the transferor did not have a good title or property.

As there are only two conditions for the disapplication of the *nemo dat* doctrine (i.e., good faith and valuable consideration),[96] when money or banknotes are offered in the discharge of a debt, the payee is not required to inquire about the title as the recognition as a currency of such chattels and changing of hands of such currency not only passes the possession but also the property.[97] In addition, payment in cash enables the payee to use it immediately. In other

---

[91] *See* Proctor, *supra* note 87 at 43-44 (citing Higgs v. Holiday [1600] Cro. Eliz. 746; Miller v. Race [1758] 97 Eng. Rep. 398, 401; Wookey v. Poole [1820] 106 ER 839; *but compare* German Civil Code BGB § 935, ¶ 2).

[92] *Id*.

[93] Because it removes the uncertainty regarding potential third party rights as well as liquidity and counterparty risks. In other words, such mechanism essentially transforms money into an information-insensitive asset. *See Ignorance, Debt and Cryptocurrencies, supra* note 8 at 15; Tri Vi Dang et al., *Ignorance, Debt and Financial Crises* 22 (Working Paper, July 20, 2020); Gary Gorton, *The Development of Opacity in U.S. Banking,* 31 YALE J. ON REGUL. 825, 827 (2013); Gary Gorton et al., *The Safe-Asset Share*, 102 AM. ECON. REV., 101, 102 (2012).

[94] Proctor, *supra* note 87 at 44 (citing Miller v. Race [1758] 97 Eng. Rep. 398, 401).

[95] Proctor, *supra* note 87 at 44. The same rule was developed in the U.S. *See* Newco Rand Co. v. Martin, 213 S.W.2d 504, 509 (1948) (stating "[m]oney is currency, is not earmarked and passes from hand to hand. . . . One may give a bona fide transferee for value a better title to money than he himself has.").

[96] *See* Banque Belge v. Hambrouck [1921] 1 K.B. 321, 329; *see also* R. v. Curtis, exp A-G (1988) 1 Qd R 546, 548; Grant v. The Queen (1981) 147 CLR 503, 506; Sinclair v. Brougham [1914] AC 398, 418.

[97] *See id.*

words, the transferee has the unrestricted right to immediate use of the transferred funds.[98] This feature of cash is what differentiates it from negotiable instruments, such as bills of exchange, checks (and drafts), notes, and negotiable letters of credit, which are built upon the underlying payment layer, and consist in promises to pay in the ultimate medium of clearing and settlement (i.e., cash or CeBM).

Private law and finality in cryptocurrencies

Given the above description, the legal treatment of finality in transactions involving PoW cryptocurrencies ultimately depends on the legal categorization of the cryptocurrency in question. In the context of private law under the common law regimes, if bitcoin is recognized as a type of intangible property (a type of personal property),[99] its transfer would be subject to the rules of derivative transfer of title. This would mean that the *nemo dat* doctrine would apply. Suppose that A passes 5 bitcoins to B, B will only get an indefeasible right to ownership in coins if A was the rightful owner of the 5 bitcoins and the transaction was valid. Under this rule, A cannot give a better title to B than A has originally had.[100] The law of tracing allows the defects in A's title to be traced back to B's title.

As explained in the previous sections, in common law, an equitable title to personal property is extinguished against the purchaser if the latter purchases for value (valuable consideration) and without notice of the competing equitable title. This defense seems to be applicable to cryptocurrency transactions, regardless of their characterization as money or some other type of property or interest.[101] Under this rule, if B is a good faith purchaser for value of the cryptocurrency that he has received from A, who has stolen the crypto from C, then B defeats proprietary claims by C to recover the cryptocurrency or their traceable proceeds.[102] However, this defense has been traditionally only available to money and negotiable instruments such as bills of exchange and promissory notes.[103] This means that the common law rule of good faith

---

[98] *See* Hugh Beale, *supra* note 70 at 1581, n.279.
[99] *See* Daniel Carr, *Cryptocurrencies as Property in Civilian and Mixed Legal Systems*, *in* CRYPTOCURRENCIES IN PUBLIC AND PRIVATE LAW 177, 179-80 (David Fox & Sarah Green eds., 2019) (discussing the treatment of cryptocurrencies as property in civilian and mixed systems).
[100] *See* David Fox, *Cryptocurrencies in the Common Law of Property, in* CRYPTOCURRENCIES IN PUBLIC AND PRIVATE LAW, 139, 156 (David Fox & Sarah Green eds., 2019).
[101] *Id*. at 159
[102] *Id*. at 160.
[103] *Id*.

purchase for value only applies if the cryptocurrencies are characterized as money for the purpose of the rule and if the parties choose to treat them as money exempting them from the full application of the *nemo dat* doctrine.[104] If this rule is applied, an indefeasible legal title in a transferee who has received the money in good faith and for value is created.[105]

To summarize, the moment of the finality of a transaction or payment is significant in private law because, unless otherwise indicated or required, it can determine who owns what at a particular moment in time. In a commercial transaction, the passing of the physical possession of goods does not necessarily signify the passing of title to those goods. The opposite is also true; the passing of title may not necessarily signify the passing of possession of the goods. For example, in documentary credits, the passing of title happens when the documents of shipment (bills of lading) are passed from the seller to the buyer. And there is no need for taking the actual possession of goods by the buyer. It is a legal construct that decouples the actual possession and control (physical) of an asset from its legal concept for the facilitation of trade between two parties. The same principle can apply to the cryptocurrencies with PoW blockchains, meaning that the passing of proprietary interest or title to cryptocurrencies could be independent of the passing of the cryptocurrency on the blockchain (constructive transfer).

Despite being problematic, the probabilistic finality may not be a huge cause for concern in the contractual and non-systemically important retail payment settings. However, uncertainty about the finality of transactions may eventually halt trades in cryptocurrencies or even may create systemic risks if such cryptocurrencies are used for wholesale payments. As in the context of wholesale payments where funds are constantly and immediately reused and reinvested, the absence of deterministic finality – be it legal or operational – would introduce new risks in the financial system stemming from the linked exposures of counterparties and potential unwind of all linked transactions.[106] This may mean that the private law alone may not be able to provide a bullet-proof deterministic legal finality. Therefore, if, for some legal reason such as the absence of valuable consideration of good faith, the transaction could be voided, such transaction cannot be considered final. Therefore, given the systemic implications of certain systems (e.g., FMIs), there has been a need for additional regulatory measures that have aimed to achieve finality by creating certain

---

[104] *Id*.
[105] *Id*.
[106] ANNUAL ECONOMIC REPORT, *supra* note 10 at 111 n.26.

legal presumptions for the moment of finality. In such systems, a transaction would be final according to the rules of the system even if there might be legal grounds to revoke the transactions. As will be seen shortly, the residual remaining legal risks to the finality of transactions in the conventional FMIs have been managed by additional institutional mechanisms such as liquidity facilities, the introduction of central clearing counterparties (CCPs), and the mandatory buy-in tool in securities settlement systems.

Transaction finality in payment and securities settlement systems legal framework

The concept of transaction finality in the context of financial instruments, money, and fund transfers[107] is slightly different from the concept of transaction finality in the context of the sale of goods. To say the least, money constitutes one leg of any trade other than the countertrade (e.g., barter) and its prevalence as a medium of exchange in commercial transactions has necessitated a special legal treatment which has led to special judicial and legal protections regarding its settlement finality. As previously mentioned, one such special protection is the disapplication of *nemo dat* doctrine in private law.

However, given the commercial and systemic importance of payment and settlement systems, the lawmaker has taken an extra step forward and has required the operators of the payment and settlement systems to define certain moments in the life of a transaction for the purposes of the finality of the transaction by clearly defining a point in time where transactions become final and by outlining the legal implications of finality.[108] The reason behind the special legal protections for transfer orders is not very different

[107] For a definition of the concept of funds under the European Union law, *see* Hossein Nabilou, *The Dark Side of Licensing Cryptocurrency Exchanges as Payment Institutions*, 14 L. & FIN. MKTS. REV., 39, 42 (2019).

[108] In the context of FMIs, including payment and securities settlement systems, finality denotes the moment in time when the transfer order or the transfer itself becomes unconditional and irrevocable. In this context, finality can be used both in the legal and technical sense. When used in its legal sense, it means that the transfer discharges the obligations, and it cannot be revoked by the counterparties or other third parties. When it is used in its technical sense, it refers to the making of entries in accounts. *See* EUROPEAN CENTRAL BANK, THE PAYMENT SYSTEM: PAYMENTS, SECURITIES AND DERIVATIVES, AND THE ROLE OF THE EUROSYSTEM 145 (Tom Kokkola ed., 2010). Although making debit or credit entries in the accounts triggers the settlement finality, it is not the crediting or debiting of the accounts that are irrevocable as the financial intermediary has the power to change the ledger, but making such a debit or credit entry makes the transactions final in the eyes of the law.

from the finality concept in the sale of goods discussed in previous sections. According to the European Central Bank, "[b]etween the time a transfer order is accepted for settlement by the payment operator and the time the order is actually settled [in the books], participants are subject to credit or liquidity risks, as the transfer order can be revoked or a participant could become insolvent."[109]

In addition to special protections to the transfer orders, to increase the certainty about the finality of transactions in a payment system, the legal systems in major jurisdictions, such as in the EU, have slightly diverged from the private law concept of finality. They take a different approach to determining the moment of finality. Under the current payments and securities settlement systems, a final settlement is only possible under the settlements conducted by the payment and securities settlement systems.[110] This means that such settlements should be conducted within a securities settlement system that is designated by a Member State under the Settlement Finality Directive (SFD).[111] Only in this case will the parties be protected against insolvency proceedings initiated by other participants.

Under such regulatory frameworks, the settlement finality concept in payment and settlement systems has taken a more granular shape, and a fine distinction between the settlement finality concept applicable to 'transfer orders' (or settlement instructions) and the one applicable to actual 'transfers' (i.e., entries in securities and cash accounts) has emerged.[112] Accordingly, the SFD is mainly about the 'moment of entry' and the 'moment of irrevocability' of transfer orders and not the actual transfer of assets.[113] In the EU, article 3(1) of the SFD, states that even in the event of insolvency proceedings against a participant, transfer orders and netting shall be legally enforceable and binding on third parties if they were entered into a system before the moment of opening of such insolvency proceedings.[114]

Under European regulations, a securities settlement system,

---

[109] *Id.*
[110] Summary Report of the Targeted Consultation on the Review of the Directive on Settlement Finality in Payment and Securities Settlement Systems, EUR. COMM'N 3 (2021).
[111] 1998 O.J. (L 166).
[112] *Id.*
[113] EUROPEAN POST TRADE FORUM, *EPTF Report - Annex 3: Detailed Analysis of the European Post Trade Landscape*, 73-74 (2017) [hereinafter EUROPEAN POST TRADE FORUM].
[114] 1998 O.J. (L 166).

such as a central securities depository (CSD) is required by the Central Securities Depository Regulation (CSDR)[115] to define three distinct definitions of settlement finality that grant protection against insolvency proceedings of other participants in the securities settlement system. Settlement Finality I occurs at the exact moment of the entry of a transfer order into the system. If a transfer order is entered into the system before the opening of an insolvency proceeding, it is protected against insolvency proceedings.[116] Article 3 of the SFD stipulates that the moment of entry of a transfer order into a system should be defined by the rules of that system.[117] Settlement Finality II is the moment after which the transfer order becomes irrevocable and neither a participant of the system, nor a third party can revoke it. Settlement Finality III is the moment after which the transfer orders are binding and enforceable against third parties, even in case of opening of an insolvency proceeding.[118]

Similarly, and in compliance with the SFD, under the TARGET2-Securities (T2S) operational framework, Settlement Finality I (moment of entry) is achieved at the moment of validation of the settlement instruction on the T2S platform. Settlement Finality II (irrevocability) is achieved at the matching of the instruction on the T2S platform, and finally, Settlement Finality III (finality of transfer) is achieved at the moment at which the cash account is credited if the transfer concerns cash, or when the securities account is credited or debited if the instruction relates to a securities transfer.[119]

It is important to note that such a moment of finality, despite being recorded and operationalized in the books and records of the intermediaries and the parties, should essentially be characterized as legal finality as it is the rules applicable to the system or the operator (which is required by the law to define the moments of finality) that define the moment of finality. Overall, the payment and settlement finality even in the centralized FMIs remain operationally probabilistic, but it is the touch of the law that attempts to transform the probabilistic operational finality to a deterministic legal finality.

---

[115] 2014 O.J. (L 257), amending 2012 O.J. (L 86), 1-72.
[116] *Id.*
[117] 1998 O.J. (L 166).
[118] EUROPEAN POST TRADE FORUM, *supra* note 113 at 73-74; 2014 O.J. (L 257). Furthermore, tools such as the buy-in tool have been introduced to deal with potential settlement failures. *See* 2014 O.J. (L 257), art. 7(3); 2018 O.J. (L 230), art. 16; *see also Eddy Wymeersch, Central Securities Depositories and Reform of the Settlement Process*, 14 J. SEC. OPERATIONS & CUSTODY (2021); *How to Survive in a Mandatory Buy-in World: A Discussion Paper by the ICMA Secondary Market Practices Committee*, INT'L CAP. MKT. ASS'N 4 (June 2018).
[119] EUROPEAN POST TRADE FORUM, *supra* note 113 at 73-74.

However, to say that the law provides for a completely deterministic finality would be inaccurate, in particular if we adopt a definition of finality based on the irrevocability of the transaction (or transfer order) even in cases of bankruptcy. This is because even the transactions that are deemed to be final in a legal sense could be unwound in exceptional circumstances. For example, in the EU, article 3(1) of the SFD, states that even in the event of insolvency proceedings against a participant, transfer orders and netting shall be legally enforceable and binding on third parties if they were entered into a system before the moment of opening of such insolvency proceedings.[120] *However*, if transfer orders are entered into a system *after* the commencement of the insolvency proceeding and are carried out on the day of the opening of such proceedings, they will be enforceable and binding on third parties *only if* "after the time of settlement, the settlement agent, the central counterparty or the clearing house can prove that they were not aware, nor should have been aware, of the opening of such proceedings."[121] This means that under such circumstances if the settlement agent was aware or should have been aware of the opening of such proceedings, the transaction could be challenged and eventually unwound. To ensure that remaining risks would not threaten the safety and soundness of the overall settlement system, institutional arrangements have emerged that are to be briefly discussed in the next section.

Institutional arrangements and the settlement discipline regimes

A judicial stamp of approval on the current practices, or a legislative or regulatory measure protecting the settlement finality on PoW blockchains, may be seen as an easy solution for the problem of settlement finality, however, merely introducing the

---

[120] This provision effectively disapplies the 'zero-hour' rule (ZHR) or midnight hour rule. The ZHR entails the retroactive application of the insolvency proceedings from 00:00 hours of the day when the insolvency is declared, or the insolvency proceedings are commenced. *See also* 2014 O.J. (L 257), art. 6(1); 2014 O.J. (L 257), art. 7; 2002 O.J. (L 168), art. 8 (stating it also disapplies the ZHR for financial collateral). For more details, *see* MATTHIAS HAENTJENS, FINANCIAL COLLATERAL: LAW AND PRACTICE 289-95 (2020).

[121] Article 3(2) of the SFD pre-empts the law and regulations of member states that are related to the transactions concluded before the moment of opening of insolvency proceedings that would otherwise lead to the unwinding of a netting. *See* 1998 O.J. (L 166) 48; *see generally* Diego Devos, *Legal Protection of Payment and Securities Settlement Systems and of Collateral Transactions in European Union Legislation* INT'L MONETARY FUND (Oct. 2006).

concept of legal finality would be hollow if it is not supported by the mechanisms and institutional arrangement that would credibly enable the participants in the network to ensure the finality of payments and settlements. In the conventional FMIs, sophisticated and complex mechanisms have emerged to prevent settlement fails, protect settlement finality, and in case of settlement fails, remedy them. Such measures – constituting the settlement discipline regime – consist of a set of rules and mitigation techniques aimed at preventing fails and protecting the settlement layer of a payment and settlement system.[122] These mechanisms include market rules, regulations, and best practices at the trading level or pre-settlement level as well as the institutions and mechanisms to ensure settlement finality, including the following non-exhaustive list:[123]

1. Fail monitoring and reporting mechanisms;
2. Technical pre-settlement measures;
3. Hold-release mechanism encouraging early matching and allowing for matching to be separated from the availability of cash or securities;
4. Other technical measures for facilitating settlement and reducing liquidity risks and securities needs, such as queue management facilities, settlement optimization techniques, and multiple settlement cycles during the day;
5. Existence of central clearing counterparties (CCPs) and the methods they use to avoid settlement fails, including stringent membership requirements;[124]
6. Arrangements for reducing liquidity risks such as access to credit and liquidity facilities (of central banks), securities lending arrangements,[125] transaction shaping mechanisms and partial delivery solutions; and
7. Mechanisms similar to a mandatory buy-in tool.[126]

From among the above-mentioned arrangements, CCPs occupy a relatively *sui generis* position in FMIs. CCPs mitigate systemic risk by acting as a circuit breaker when risks of defaults

---

[122] *See generally* Daniela Russo & Simonetta Rosati, *Short Selling, Clearing, and Settlement in Europe: Relations and Implications*, *in* HANDBOOK OF SHORT SELLING 159-62 (Greg N. Gregoriou ed., 2012) [hereinafter SHORT SELLING].
[123] *Settlement Fails – Report on Securities Settlement Systems (SSS) Measures to Ensure Timely Settlement*, EUR. CENT. BANK (April 2011).
[124] *Id*.; Hossein Nabilou & Ioannis Asimakopoulos, *In CCP We Trust ... Or Do We? Assessing the Regulation of Central Clearing Counterparties in Europe* 9 (Faculty of Law, Economics, and Finance, Working Paper No. 13 2019).
[125] FINANCIAL STABILITY BOARD, SECURITIES LENDING AND REPOS. 6 (2012); SHORT SELLING, *supra* note 122 at 151; Joanna Benjamin et al., *The Future of Securities Financing*, 1 L. & FIN. MKTS. REV. 47 (2013); MATTHIAS HAENTJENS, FINANCIAL COLLATERAL: LAW AND PRACTICE, 114-23 (2019).
[126] For a definition of mandatory buy-in, *see CSDR Settlement Discipline, Mandatory Buy-Ins,* INT'L CAP. MKT. ASS'N (2019).

leading to settlement fails tend to propagate from one counterparty to another. This is made possible through either novation or open offer. Novation extinguishes the original contract between the buyer and the seller and replaces it with two new contracts: one between the buyer and the CCP, and the other between the seller and the CCP. This way, the CCP interposes itself between the original buyer and seller and becomes the buyer to the seller and the seller to the buyer. In contrast, under open offer, as the CCP immediately interposes itself between the buyer and the seller in a transaction at the very moment of its inception, no contractual relationship between the buyer and the seller is created *ab initio* and two separate contracts are formed: one between the buyer and the CCP and the other between the CCP and the seller.[127] This way, a CCP insulates both buyers and sellers from the credit risk of the counterparties to a trade.

By standing in between counterparties, CCPs reduce the risk of a panic reaction to solvency problems of a single counterparty and decrease the likelihood of a sudden failure of chains of counterparties. Additionally, they enhance transparency regarding counterparty credit risk, which enables both market participants and regulators to have a better assessment of counterparty risks in the financial system.[128] CCPs also monitor and ensure the uniform application of collateral requirements on all clearing members.[129] Furthermore, central clearing with fewer CCPs lowers the average counterparty risk through netting.[130]

Given CCPs' role in the financial markets, they are considered too-big, too-interconnected, or too-important to fail. In addition, their incentives would not be aligned with those of society due to the moral hazards arising from being recognized as such.[131] This is

---

[127] BANK FOR INT'L SETTLEMENTS, RECOMMENDATIONS FOR CENTRAL COUNTERPARTIES 13 (2004) [hereinafter RECOMMENDATIONS FOR CENTRAL COUNTERPARTIES]; *see generally* Jo Braithwaite & David Murphy, *Central Counterparties (CCPs) and the Law of Default Management*, J. CORP. L. STUD. (2017); *Got to Be Certain: The Legal Framework for CCP Default Management Processes*, BANK OF ENG. (2016).

[128] RECOMMENDATIONS FOR CENTRAL COUNTERPARTIES, *supra* note 127 at 16 n.3.

[129] Darrell Duffie, *Replumbing Our Financial System: Uneven Progress*, INT'L J. CENT. BANKING 9 (2013).

[130] Darrell Duffie & Haoxiang Zhu, *Does a Central Clearing Counterparty Reduce Counterparty Risk?*, REV. ASSET PRICING STUD. 74, 75 (2011).

[131] Hossein Nabilou & Alessio Pacces, *The Law and Economics of Shadow Banking*, *in* RESEARCH HANDBOOK ON SHADOW BANKING: LEGAL AND REGULATORY ASPECTS 7, 17 n.48 (Iris H.Y. Chiu & Iain G. MacNeil eds., 2018).

why CCPs are subject to strong and harmonized regulatory minimum margin standards.[132] In addition, systemic liquidity events necessitate extending central bank liquidity facilities to CCPs, and in many jurisdictions, such a liquidity backstop has been made available to CCPs. In Europe, Article 85(1)(a) of EMIR opens up the possibility for CCPs to have access to central bank liquidity facilities by mandating the Commission to assess, in cooperation with the members of the European System of Central Banks (ESCB), the need for any measure to facilitate the CCPs' access to central bank liquidity facilities.[133] In some jurisdictions, such as the U.S., banks (depository institutions) used to have almost exclusive access to central bank liquidity facilities, with limited opportunities for non-bank financial institutions.[134] Although the Dodd-Frank Act does not expressly allow access to the Federal Reserve liquidity facilities to CCPs, currently in the U.S. (and likewise in the UK), such access is granted.[135]

The reason for highlighting the importance of institutional arrangements that help ensure the settlement finality is mainly because the law is unable to provide for 100% bulletproof settlement finality. In other words, technical limitations and the requisites of justice and fairness in the traditional FMIs do not allow for a deterministic finality in its strictest sense. Therefore, to remedy such a shortcoming, a whole host of institutional arrangements to ensure settlement finality in conventional FMIs have emerged, without which the legal as well as operational risks in the payment and settlement systems could destabilize the financial markets.

The same line of reasoning could apply to the PoW blockchains. As such networks cannot provide for the deterministic finality of the transactions, it is imperative to have legal mechanisms in place to provide for a moment of finality in such transactions if such networks ever want to be used as a reliable medium of exchange or a settlement layer for upper layers of a payment network (as is the case with the Lightning Network). For example, various moments could be defined as the moment of settlement finality. One way of defining such a moment is to defer to the long-established tendency in the law to be reliant on the practice of

---

[132] Darrell Duffie, *supra* note 129 at 9, 254.
[133] European Market Infrastructure Regulation (EMIR), art. 85(1)(a).
[134] Darrell Duffie, *supra* note 129 at 253, 255, 257.
[135] Marc Dobler et al., *The Lender of Last Resort Function after the Global Financial Crisis* 13, 14 (Int'l Monetary Fund, Working Paper No. 16/10 2016).

merchants (e.g., a law merchant).[136]

Currently, on the Bitcoin Blockchain, a number of confirmations are required by the industry practices to deem a bitcoin transaction final. These numbers vary from zero to six.[137] On the extreme low, traders and merchants accepting unconfirmed transactions is not unheard of, however, the most conservative approach seems to be accepting a transaction as final when that transaction has had six confirmations. This is because undoing six blocks requires a very high investment in energy.[138] To reduce the uncertainty about the settlement finality especially within the first sixty minutes, the industry has developed its own commercial customs. Depending on the wallet used, as soon as a transaction is broadcast to the Bitcoin Blockchain, the receiving wallet receives a notification confirming the receipt of payment, but the payment is only considered final after six confirmations. However, even such legislation or regulation will, at best, import the two most important traditional exceptions to the generally applicable rules of derivative transfer of title, i.e., the defenses of good faith and purchase for value, eventually making 100% deterministic finality impossible. Even in the unlikely scenario that the laws and regulations would adopt the most accommodating approach to cryptocurrencies by offering the strongest protections to cryptocurrency transactions akin to the regime applicable to fund (money) transfers, such a law would not be able to guarantee a deterministic finality.

In the absence of such a deterministic finality, the role of institutional arrangements akin to the settlement discipline regime becomes important. However, such institutional arrangements can hardly be applied or imposed on PoW cryptocurrencies. Given the anti-institutional and libertarian ethos of PoW blockchains, adapting

---

[136] Indeed, one of the well-established conceptions of the common law has been the fact that the judges find the law rather than make it. *See* Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 PA. L. REV. 1643-96 (1996). In the spirit of this tradition, it would be reasonable for legal systems, at least for private law purposes, to presume settlement finality after 5 blocks are built on the block containing the transaction.

[137] Since an unconfirmed transaction could be reversed, accepting an unconfirmed transaction as payment is a very risky practice. Daniel Zarifpour, *Money & Motivation against a Decentralized System*, MEDIUM, https://zarifpour.medium.com/money-motivation-against-a-decentralized-system-e4cc85b4afe9 [https://perma.cc/VQ8X-53H4].

[138] This is not to say that it amounts to complete immutability. Theoretically complete immutability cannot be achieved. *See Bitcoin is Not Immutable – An Atheist Perspective*, MEDIUM, https://medium.com/@alchimista/bitcoin-is-not-immutable-an-atheist-perspective-4444a1224410 [https://perma.cc/FDP7-K88W].

the technology to the established institutional constraints of settlement regimes would go deeply against the raison d'être and the main value proposition of such cryptocurrencies. As it is highly improbable that such institutional arrangements could be transplanted in the PoW blockchains, the use of such blockchains for payment purposes will inevitably carry certain levels of finality risk. Thus far, there have been no system-wide realization of such risks and only the future will tell how finality risks in PoW blockchains will be dealt with if such cryptocurrencies gain wider acceptance.

Conclusion

The settlement finality has been one of the most controversial aspects of the cryptocurrencies that rely on PoW consensus algorithms for their transaction confirmations. The main critique is that since the PoW blockchains rely on probabilistic finality, they would be unsuitable for payment processing. However, it seems that the critiques of the probabilistic finality on PoW blockchains often confuse *operational* finality with *legal* finality. The main contribution of this paper is to identify the real source of concern about the probabilistic finality in the PoW blockchains. As it turns out, the real cause of concern has little to do with the operational or even legal finality but originates from the incompatibility of PoW blockchains with the institutional arrangements (akin to the settlement discipline regime) that deal with the remaining risks that neither legal nor operational finality can address.

To identify the root of the problem, this paper highlighted the key distinctions between legal finality and operational finality. It argued that since the operational finality cannot be realistically ensured in any payment and settlement system, ultimately it is the law that should intervene and fill the gap by devising the concept of *de jure* or legal finality as opposed to operational finality.[139] However, after studying the concept of legal finality in conventional trade of goods (tangible goods) and payment and settlement systems, this article argues that the concept of settlement finality in

[139] For example, the draft UNIDROIT principles on digital assets states that, "The law should specify the requirements for a transferee to qualify as an innocent acquirer (IA) of digital assets and derivative digital assets and the rights obtained by an IA (e.g., requirements and rights akin to those found in good faith purchase, finality, and take-free rules)." Issues Paper, Study LXXXII, Working Group 3, INTERNATIONAL INSTITUTE FOR THE UNIFICATION OF PRIVATE LAW (UNIDROIT) 18 (June 2021). Although this is a first step toward recognizing legal finality, it is far from ensuring the complete finality of the transactions as it may require various other regulatory actions.

law is, at best, a non-deterministic concept, and neither the law nor technology can provide a bulletproof 100% deterministic finality. Even in the most systemically important FMIs, the law may not provide for complete certainty and finality as the exigencies of certainty, finality, efficiency, and financial stability may give way to the requisites of justice and fairness ingrained in the insolvency laws.[140] Accordingly, legal systems have gone as far as the law can go to provide for as much finality as possible through using legal presumptions and rules to provide certainty to the parties to a transaction and to avoid potential systemic implications of settlement fails in the payment and securities settlement systems.

Therefore, rather than taking a strong position to provide completely deterministic finality, in the case of the most systemically important FMIs, the law aims to provide the maximum achievable degree of finality. To manage the risks stemming from the remaining degree of uncertainty, the law requires alternative institutional mechanisms that could mitigate the risks that would emanate from the potential unraveling of transactions. These mechanisms include those employed by the CCPs or other systems and operators of the payment and settlement systems, such as having access to central bank liquidity facilities, stringent membership requirements, and the buy-in tool in case of settlement failure in CCPs and central securities depositories (CSDs).[141]

This paper argues that this institutional backstop for the finality of transactions is what differentiates the PoW blockchains from the conventional financial systems. As the law may be unable to provide a deterministic finality, it resorts to alternative mechanisms to require the participants to remedy the issue by establishing arrangements that could minimize the instances of settlement fails, and in case of settlement fails, such fails could be remedied as soon as practicable. However, establishing such institutional mechanisms to deal with the remaining risks of settlement finality requires a certain level of centralization in the

---

[140] The level of optimal certainty and precisions of law have been subject to a great scholarly debate under the rubric of the debate on the rules versus standards. *See* Isaac Ehrlich & Richard A. Posner, *An Economic Analysis of Legal Rulemaking*, 1 J. LEGAL STUD. 257 (1974); Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 3 DUKE L.J. 557 (1992); Hans-Bernd Schaefer, *Legal Rule and Standards*, *in* The Encyclopedia of Public Choice 347-48 (Charles K. Rowley & Friedrich Schneider eds., 2004); Cass R. Sunstein, *Problems with Rules*, CAL. L. REV. 953, 984 (1995); Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 414 (1985).

[141] Such a requirement is introduced in the EU in its short selling regulation as well as the CSDR. *See* 2012 O.J. (L 86), 1-72; 2014 O.J. (L 257).

PoW blockchains. In the absence of such mechanisms, and centralized control, the law may be unable or unwilling to extend its traditional protections for the settlement finality in PoW blockchains, and such PoW networks may continue to suffer from the finality issues in the absence of any market-driven mechanisms to remedy the potential settlement fails. Along with other reasons,[142] this may be a legitimate reason for pessimism about the potential use-cases of decentralized PoW blockchains in traditional post-trade processes.

[142] *See The Use of DLT in Post-Trade Processes: Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments*, EUR. CENT. BANK 29 (2021).