NBER WORKING PAPER SERIES

BLOCKCHAIN FOR TIMELY TRANSFER OF INTELLECTUAL PROPERTY

Dongling Cai
Yi Qian
Ning Nan

Working Paper 30913
http://www.nber.org/papers/w30913

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
February 2023, Revised March 2025

The authors would like to thank Leyao Tan and Ethan Chiang for excellent research assistance, thank colleagues for reading the manuscript and sharing thoughts, thank the SSHRC IG for support. This work was supported by the SSHRC CIDE Small Grant for Innovation Research (2018), the SSHRC IG (grant number # 435-2018-0519, 2018-2023), and the SSHRC Insight grand (# 435-2017-0138). All three grants are from the Canadian government in supporting academic research only, with no conflicts of interests. This work was also supported by NSFC (Grant No.72001221) and CPSF (grant No.2020M672911). Both grants are from the Chinese government in supporting academic research only, with no conflicts of interests. The views expressed herein are those of the authors and do not necessarily reflect the views of the National Bureau of Economic Research.

NBER working papers are circulated for discussion and comment purposes. They have not been peer-reviewed or been subject to the review by the NBER Board of Directors that accompanies official NBER publications.

© 2023 by Dongling Cai, Yi Qian, and Ning Nan. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

Blockchain for Timely Transfer of Intellectual Property
Dongling Cai, Yi Qian, and Ning Nan
NBER Working Paper No. 30913
February 2023, Revised March 2025
JEL No. O3, O31, O33, O36, O39

ABSTRACT

This article examines how blockchain technology can facilitate innovation by streamlining the licensing process of intellectual property (IP). In the traditional world, there can be tension between inventors and developers when it comes to licensing IP before a patent is granted. Developers need more information about the IP in order to estimate its value, while inventors are hesitant to disclose too much information for fear that developers will use it to develop and commercialize the IP without licensing it. The blockchain's ability to create a transparent and secure record of the inventing process can alleviate these concerns. On the one hand, blockchain's traceability helps protect IP from infringement, encouraging inventors to disclose more information about their high-value IP. On the other hand, developers have more incentive to license IP rather than infringe on it because of the risk of punishment. The size of the community maintaining the blockchain is a crucial factor in ensuring the validity of the blockchain. A community that is too large or too small would not be able to reach equilibrium. These findings provide insights into how blockchain can be used to improve the economics and marketing of IP.

Dongling Cai
University of Waterloo
dongling.cai@uwaterloo.ca

Yi Qian
Sauder School of Business
University of British Columbia
2053 Main Mall
Vancouver, BC V6T 1Z2
Canada
and NBER
yi.qian@sauder.ubc.ca

Ning Nan
Sauder School of Business
University of British Columbia
2053 Main Mall
Vancouver, BC V6T 1Z1
Canada
Ning.nan@sauder.ubc.ca

1. INTRODUCTION

The development of COVID-19 vaccines puts the spotlight on the tension between intellectual property (IP) protection and timely sharing of inventions (Nature, 2020; Shores, 2020; The Washington Post, 2021). IP is non-exclusive and non-rival (Bhattacharya and Guriev, 2006; Boldrin and Levine, 2002). It is therefore impossible to protect its value once information regarding the IP is shared. IP laws, the prevailing form of IP protection, seek to provide incentives for innovation through ex-post grant of monopoly rights. However, with the average patent grant lag of 28 months (Popp et al., 2004), law protection can be too time-consuming for incremental contributions to a collaborative project such as vaccine development or for maximizing the welfare gains from technological idea trading (Gans et al., 2008). Blockchain technology has been proposed as a new solution to balance IP protection, innovation cultivation, and information dissemination in marketing and advertising activities (van der Waal et al., 2020; Peres et al. 2022; Joo et al. 2023).

Blockchain is a distributed ledger running on devices of a community of record keepers (Tapscott and Tapscott, 2016). It relies on decentralized consensus of record keepers rather than centralized records maintained by authoritative institutions to prove activities around anything of value such as ownership or transactions of money, titles, deeds, or creative work (Cong and He, 2019). The time lag for adding or verifying records in a blockchain system ranges from seconds to hours, which is a negligible delay compared with the 28-month lag of obtaining patent protection. Due to its potential to serve as a timely, immutable, and scalable public ledger, blockchain technology has been considered as a potentially more accessible and efficient solution to represent the latest state of IP creation and ownership (van der Waal et al., 2020). Such capacity has already been extensively utilized in IP ownership identification by leading digital media, art, and luxury companies to combat IP infringements (Blockchain Bitcoin News, 2021; Forbes, 2017; LVMH, 2021; SiliconANGLE, 2020) and even to have NFT-based virtual luxury (Bao, et. al., 2024). The trusted and timely authorization capabilities of blockchain have also attracted significant attention in the medical industry. Blockchain has been applied to enhance the efficiency of vaccine and drug development and distribution (Sonoco, 2020; Chaban, 2021; Trehan et al., 2020).

Nevertheless, as a community- and algorithm-based system, blockchain is subject to the impact of record keeper behaviors and the threat of security breaches. Such behavioral and technological concerns can have significant implications for the potential of blockchain systems to fully substitute for or effectively complement prevailing forms of IP protection. The objective of our study is to use theoretical modeling to gain a systematic understanding of the promise and limitations of blockchain in balancing IP protection and timely development and transfer of innovations. Our model integrates the bargaining process entailed in IP transfers and strategic behaviors involved in the decentralized consensus in blockchain. It therefore helps to fill the research gap regarding the causality between the non-exclusive, non-rival nature of IPs and community- and algorithm-based blockchain systems.

Our analysis begins with a baseline model of IP transfer and protection in the traditional world (see Section 3.1). Model analysis indicates that IP protection in the traditional world does not have a Pareto-optimal solution for the two parties involved in IP transfer: a research entity that creates the invention and a developer firm that commercializes the invention. Timely transfer of IP depends on a few key parameters, including the probability for the developer firm to successfully commercialize the IP without licensing, the proportion of research entities with high-value inventions in a market, the value gap between the high- and low-value inventions, and the value loss due to delayed IP transfer. The basic model analysis concretizes the tension between IP protection and timely transfer by fleshing out cost-benefit tradeoffs from the research or developer firm's perspective.

We then consider IP protection and transfer with the mediation of a blockchain system. In Section 3.2, our analyses show that a blockchain system with perfect consensus brings a Pareto-optimal solution for research and developer firms involved in an IP transfer. It therefore has the potential to expedite IP transfer without compromising IP protection. This idealized blockchain model formalizes the rationale for IP-intensive industries to invest in blockchain applications.

We then make the more realistic assumption of imperfect consensus in blockchain and incorporate outside security threats (see Section 4). In such a model setup, IP transfer becomes a multi-party game among the research and developer firms, blockchain record keepers, and outside hackers. The Pareto-optimal solution for the idealized blockchain model no longer applies. Achieving favorable IP transfer

outcomes requires firms to consider blockchain-specific factors such as the accuracy of a firm's estimation of consensus quality and the size of the blockchain record keeper community. Furthermore, our model analysis formalizes the cost-benefit tradeoffs from a record keeper's or hacker's perspective and shows how these tradeoffs influence the research or developer firm's decisions about blockchain-based IP transfers.

Through these model analyses, we gain a systematic understanding of the traditional and blockchain-specific tensions between IP protection and timely IP transfer. Our study therefore provides some theoretical clarity into the benefits and caveats of using blockchain for IP economics. It lays foundations for guiding applications and potential regulatory policies. We discuss the most recent blockchain applications by IPwe (PRNewswire, 2021) and the Nigerian government (PRNewswire, 2022) in the context of our theoretical predictions. We further relate to the marketing applications of blockchains (Ding and Wang, 2023; Peres et. al., 2023; Marthews and Tucker, 2023). Our model propositions provide direct theoretical prescriptions and guidance to stakeholders in cautiously managing their IPs with blockchains.

2. LITERATURE REVIEW

2.1 IP Transfer and Protection:

The realization of economic and welfare gains from IPs often requires the transfer of an invention (we use IP and invention interchangeably hereafter) from a research/innovative entity (individual or firm, we use entity and firm interchangeably hereafter) to a developer firm (Teece, 1986; Arora et al., 2001; Gans et al., 2008). The prevalence of IP transfer is driven by two forces. First, the separation of research and developer firms and thereby the need for IP transfer can bring cost reductions associated with enhanced specialization (Arora et al., 2001; Mowery, 1983; Williamson, 1991). Second, the sequential nature of innovation requires the sharing of basic, preliminary inventions with subsequent developers. Scotchmer (1991, p. 24) notes, "most innovators stand on the shoulders of giants, and never more so than in the current evolution of high technologies, where almost all technical progress builds on a foundation provided by earlier innovators." Such sequential innovation is exemplified by

pharmaceutical research and development. It is estimated that a quarter to 40% of the revenues of major pharmaceutical companies are accounted for by in-licensed products (Bhattacharya and Guriev, 2006).

The prevalent practice of IP transfer gives rise to the concern about IP protection. A key concern is that innovation entails considerable uncertainties and information asymmetry (Baysinger et. al., 1991; Jia et. al. 2019, Shavell and Van Y. 2001). As intangible assets, IPs are essentially ideas or information that can be duplicated and disseminated at a minimal cost. Therefore, once a research firm discloses some information about an invention to a developer firm, the developer firm can immediately gain values from the shared information. This so-called non-exclusive nature of IP lowers the research firm's bargaining power in IP transfer and ultimately hurts the research firm's incentive for innovation. Meanwhile, the research firm can disclose the same information about an invention to many developer firms and obtain economic gains from the same IP multiple times. This non-rival nature of IP compromises a developer firm's incentive to commercialize an invention (Bhattacharya and Guriev, 2006; Boldrin and Levine, 2002; Forbes, 2015). Overall, the non-exclusive and non-rival nature of IP causes a conflict of interest: the developer firm would prefer to verify the quality of an invention before paying for it, which requires the research firm to disclose information about the invention as far as possible; yet the more invention-related information is disclosed by the research firm, the less incentive the developer firm would have to pay for the invention (Arrow, 1962).

To date, the conflict of interest is mainly reconciled by IP protection provided by authoritative institutions in the forms of patents, trademarks, or copyrights (Lev 2001). A research firm needs to apply for formal IP protection for its inventions. Once the IP protection is granted, a developer firm is required to pay for the use of the invention and the research firm is prevented from selling the same IP multiple times. However, the reliance on a central institution creates a bottleneck effect, which manifests as extensive delays from the IP application to the grant of IP protection. The delay is especially prominent for patents. For example, Popp et al. (2004) find that the average patent grant lag (inclusive of provisional applications and patent continuance) is 28 months, with a standard deviation of 20 months.

The time delay associated with institution-based IP protection erodes the innovation incentives of both research and developer firms. On the research firm's side, recent research shows that some inventors forgo IP protection in order to avoid the detrimental effect of time delay on their performance (Romer 2002; Wen et al., 2016; Zhang 2018). Such decisions can ultimately compromise the research firm's gain from innovation (Bechtold and Hoffler 2011). For example, the proposal to waive IP protection of COVID vaccines has caused concerns that the waiver will dissuade pharmaceutical companies from creating cutting-edge technologies in the future (The Washington Post, 2021; WTO, 2021). On the developer firm's side, the delay affects their decisions on when to require an IP transfer. This strategic trade-off is highlighted in Gans et. al. (2008). With an empirical data set, Gans and colleagues find that the timing of licensing—a common form of IP transfer—is significantly associated with the timing of patent allowance. Such delay is only justifiable for inventions with sufficient market potential. For incremental inventions that are not immediately marketable but are crucial to sequential innovations, the time delay of patents becomes a significant barrier to innovation.

In sum, research to date has identified the tension between institution-based IP protection and timely sharing of inventions as a key barrier to effective realization of the economic and welfare gains of IPs (e.g., Arora et al., 2001; Gittelman and Kogut, 2003; Gans et al., 2008). Authoritative institutions become a bottleneck in information sharing between researcher and developer firms and in the transfer of inventions that are foundational to further development (such as the development of COVID-19 vaccines). Blockchain has been proposed as a new solution to balance IP protection, innovation cultivation, and information dissemination (van der Waal et al., 2020).

2.2 Blockchain Technology and Applications

A blockchain system preserves and verifies records by decentralized consensus among distributed record keepers (Tapscott and Tapscott, 2016). The decentralized consensus can be programmed to trigger the execution of actions such as sending a payment from one account to another (Cong and He, 2019). Smart contracts are a common type of application to realize such programmable decentralized consensus in blockchain (Bartoletti and Pompianu, 2017). They can be consistently executed by a

network of mutually distrusting nodes owned by distributed record keepers, without the arbitration of a trusted central authority. In this distributed and trustless way, smart contracts can automatically store records and certify the provenance of records such as IP ownership.

The technical capabilities of blockchain have inspired a stream of studies to depict potential applications of the technology (Abadi and Brunnermeier, 2018; Batista et al., 2021; Xu et. al., 2017; Yaga et. al., 2018; Yiannas, 2018). For example, Cong and He (2019) develop a theoretical model to explicate the implications of the decentralized consensus and smart contracts in a blockchain system to industry organization and competition. Their model analysis indicates the potential for blockchain to mitigate information asymmetry and improve social welfare and consumer surplus. Our paper further incorporates the specificity of IP and licensing properties and concerns. Chod et al. (2020) argue that blockchain technology can make monitoring mechanisms more efficient than traditional methods. With a signaling game model, they show that the adoption of blockchain makes it possible for a firm to signal through its inventory, which is more cost-efficient than signaling through loan requests. Firms can therefore secure favorable financing terms at lower signaling costs. Yermack (2017) treats blockchain as a novel technology to a classic problem of trading and tracking the ownership of financial assets. They argue that the transparency of ownership offered by blockchain will change corporate governance in many ways. Chod and Lyandres (2021) examine the financing of entrepreneurial ventures with an initial coin offering, which is an application of blockchain technology. Building on these but also recognizing the differences in IP and traditional financial products, our study addresses the role of blockchain in securing trust and reputation in a bargaining model of IP, and contributes to this emerging literature on market concentration and regulation in the blockchain industry (e.g., Ferreira, Li, and Nikolowa, 2019; Cong, He, and Li, 2020; Alsabah and Capponi, 2020; Lehar and Parlour, 2020; Amiram et al., 2022; Cong et. al., 2022).

With respect to IP protection, the unreliability of the current IP system is shown as the number of intellectual property disputes increases year by year – from about 5,000 infringements to 40,000 in 2017 (Yang et. al. 2019). Blockchain has given clear advantages in the field of IP. The immutability of the data being entered ensures high-level security. This is because information is stored using hash

pointers, which are linked from one block to another, forming a chain. It would be difficult to change any data without being noticed in this decentralized system, since digital copyright infringement can be traced much more effectively. Blockchain technologies allow anyone who claims to secure the rights to an IP object to do this, thus the registered IP objects become publicly available and significantly accelerated. This solves the problem with the current convention as the process of verifying and approving inventions is slow-paced.

A few papers have commented on the potential of blockchain to relieve the tension between IP protection and timely sharing of inventions. For example, Catalini and Gans (2016) develop a theoretical model to show how blockchain can reduce the cost of verification and networking. Subsequently, they envision blockchain-based IP registration and content licensing. In their vision, payments for the use and remix of IPs or digital content can be tracked in a granular and transparent way by all market participants, especially parties with conflicting interests (such as the research and developer firms involved in IP transfer). Following a similar logic, blockchain has been suggested as a cost-effective way to protect IPs in the fashion industry such as fashion designs and trademarks (Burstall and Clark, 2017). The urgent need to develop COVID-19 vaccines motivates further attention to the applications of blockchain to IP protection. Scientists see significant potential of blockchain in overcoming barriers in vaccine development such as time-consuming procedures for clarifying ownership and difficulties in tracing invention sharing (van der Waal et al., 2020). While Catalini and Gans (2016) envision full transparency and trackability, our model dissects into the payoffs and tensions among the different parties that are often present in the real marketplace, and analyzes the tradeoffs between values from successful IP transfer by releasing early to increase the chances of early agreements and risks of information leakage if no agreement is reached before IP protection. Ferreira et al. (2023) analyze the interactions between blockchain governance and the market structure of the industries in the blockchain ecosystem. They focus on the 'proof-of-work system', while we consider a broader set of blockchain functionalities. Elegant as these models are, they may not be directly suitable for analyzing nuanced IP-related topics.

While the research to date has emphasized the significant potential of the technical capabilities of blockchain in solving some long-enduring issues, it explicitly or implicitly cautions us against behavioral issues driven by the diverse interests of the parties involved in a blockchain system. Specifically, the distribution of information among a community of record keepers can instigate strategic behaviors such as misreporting or collusion among utility-driven record keepers (Cong and He 2019). Such strategic behaviors in turn can lower the quality of the consensus. Moreover, when insiders of a blockchain system collude to create false records via selfish-mining (Eyal and Sirer 2013) or long-range attack (Deirmentzoglou et al. 2019), the quality of consensus becomes uncertain to parties relying on the authenticity of records for their business such as research and developer firms involved in an IP transfer. The uncertainty in the quality of consensus can impair the promise of blockchain and ultimately harm the incentive of IP generation and transfer. In addition to behavioral issues from inside a blockchain system, the transparency of smart contracts and internet-based blockchain systems can invite security attacks from the outside (Kannengießer et al. 2020). The strategic behaviors of hackers become a new concern.

To date, there lacks a formal examination of the implications of these behavioral issues to IP generation, protection, and transfer. To fill this knowledge gap, we construct a model in which a representative research firm interacts with a representative developer firm. We investigate how the potential benefits and behavioral concerns of a blockchain system influence the research entity's decision on whether and when to disclose information about an invention and transfer the invention to the developer firm. Such a decision process underlies much of the marketing problems in the real world, ranging from musicians' choices of venues and means of distributing their creative works to artists' commercialization strategies and safeguards. The deficiency in formal modeling of blockchain-based IP management in the marketing literature calls for research to fill this void. We can relate our model to the emerging studies on conjectured applications in marketing, such as NFT. NFT stands for "Non-Fungible Token." It is a type of digital asset that represents ownership or proof of authenticity of a unique item or piece of content using blockchain technology. Unlike cryptocurrencies such as Bitcoin or Ethereum, which are fungible (meaning one unit is interchangeable with another), each NFT is

distinct and cannot be exchanged on a one-to-one basis. NFTs have gained popularity in digital art, collectibles, virtual real estate, and even music, allowing creators to sell and collectors to buy unique digital items with verified ownership and scarcity. The blockchain ensures transparency and authenticity, as ownership records are stored publicly and cannot be altered.

Colicev (2023) explores how non-fungible tokens (NFTs) can create value for brands by leveraging scarcity, authenticity, and direct engagement with consumers. The paper highlights NFTs as a tool for enhancing brand loyalty, fostering unique consumer experiences, and unlocking new revenue streams through digital collectibles and branded virtual assets. A recent working paper by Ding and Wang (2023) investigates how emotional similarity between images and accompanying audio impacts sales of NFT products. They find that greater emotional congruence between visual and auditory elements enhances consumer engagement and increases the likelihood of NFT product sales, suggesting a strategic approach to optimizing multimedia content for digital collectibles. Malik, Appel, and Luo (2023) review the current application of blockchain technology in creative industries, emphasizing its potential to enhance transparency, reduce intermediaries, and enable new revenue models such as NFTs. The paper identifies research opportunities in areas like blockchain scalability, regulatory frameworks, and the integration of smart contracts to further innovate within creative sectors. These provide some practical applications and real-world context for our theoretical model.

Joo et. al. (2023) discuss features of distributed ledgers that could help improve brand safety, consumer privacy, and transparency in digital advertising. There is a clear demand in marketing for understanding the usage and limitations of blockchains, as overviewed in Peres et. al. (2023), and our research sheds light on an important role of blockchain in new products and the commercialization and marketing of them thereof. It also lends natural leverage of blockchain in product authenticity and safety, which is one of the key future directions highlighted in Peres et. al. (2023), by securing intellectual property, as well as privacy (Marthews and Tucker, 2023).

Most of the current literature on blockchain in marketing remains speculative and descriptive based on technical facts of blockchains. We provide one of the very first theoretical study based on rigorous game-theory models.

3. MODEL

Blockchain could ease concerns of trust in a marketplace with strangers and facilitate the marketing of intellectual property. For example, aspiring musicians who release their music online could benefit from NFT, a form of blockchain system as reviewed in the previous section, so that they could be more certain of receiving credits and payoffs should more popular musicians choose to sample their work. Visual artists who produce work that could be used by brands or publishers could be more open to publishing their work online using such a system, as it could ensure they are credited and compensated. Be it creative individuals or professional entities engaging in research and development, one would benefit from a tractable framework that could provide guidance to both the research and developer sides of the IP transaction. van der Waal (2020) conceptualizes an R&D blockchain infrastructure in the context of epidemics, and we follow their efforts to formalize the key elements. We develop a game-theoretical model to formalize the strategic interaction between a research/innovative individual or firm (R) and a potential developer firm (D) within the context of intellectual property (IP) transfer. Both agents are risk-neutral. *R* produces inventions, categorized into two types: high-value, high-investment-cost ($i = H$), and low-value, low-investment-cost ($i = L$). High-value inventions are considered unique, not transferred to other developers, while low-value inventions are relatively common. This distinction captures the non-rivalrous nature of intellectual properties. The proportion of high-value invention is p, $0 < p < 1$. Denoting the value of invention i as v_i (with $v_H > v_L$) and the investment cost as c_i (with $c_H > c_L$), R bears the investment cost with no immediate returns until the invention is transferred to D for commercialization. Appendix B tabulates the list of symbols in our model with explanations.

As previously discussed, the non-exclusive and non-rivalrous nature of intellectual property (IP) introduces a fundamental conflict of interest during the invention transfer process. Developer firm D seeks to assess the value of the invention, ensuring its distinctiveness from those previously transferred

by R to D's competitors. This assessment necessitates R's comprehensive disclosure of information about the invention. However, a paradox emerges – the more information R discloses, the weaker D's incentive to compensate for the invention (Arrow, 1962; Bhattacharya and Guriev, 2006). In essence, the invention, or IP, represents non-exclusive information; once shared, D gains immediate knowledge of the invention.

The attainment of IP protection takes T periods. Whether the invention is of high or low value is unknown to D until some information about the invention is disclosed. D can either sign an IP transfer agreement with R in the pre-protection phase $t = 0$, or in the post-protection phase $t = T$. At $t = 0$, R can choose to disclose or withhold information about the value of the invention.

On the one hand, if R discloses information about the invention, it heightens the probability of the two firms reaching an agreement at an early stage, concluding the game upon successful IP transfer. Conversely, failure to reach an agreement before the grant of IP protection results in partial information leakage about the invention. Subsequently, D can utilize the leaked information to potentially commercialize the invention with a success rate $\mu \in [0,1]$. If D succeeds, the game concludes. If not, D has the option to make an offer at $t = T$ when the IP protection is granted, marking the game's end regardless of reaching an IP transfer agreement. Figure 1 illustrates the IP transfer game, capturing the inherent tension between IP protection and timely invention transfer, alongside the underlying conflict of interests between R and D. In the following sections, we analyze traditional solutions to mitigate this tension and explore potential solutions and concerns introduced by blockchain technology.

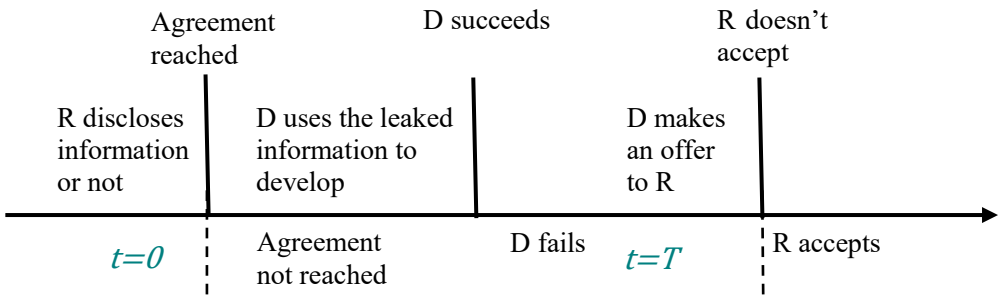


Figure 1. IP Transfer Game Timeline

3.1 Traditional world

Our literature review shows that patents and licensing agreements verified by authoritative institutions are the main solutions to facilitate IP transfer in the traditional world (i.e., the world without blockchain). We analyze the optimal decisions regarding information disclosure and licensing agreements of the researcher (*R*) and developer firm (*D*) to gain a baseline understanding of tradeoffs in IP transfer, IP protection, and timely development of inventions.

We examine licensing agreements where the researcher (*R*) transfers potential intellectual property (IP) to the developer firm (*D*) for a flat fee F, the value of which is contingent on the bargaining power of both entities. The bargaining process is structured using a widely employed form in the literature (Nash 1950; Binmore et al., 1986; Osborne and Rubinstein 1994), $(\Delta DU)^{\alpha}\ (\Delta RU)^{1-\alpha}$ where $0 < \alpha < 1$ represents the bargaining power of D, and ΔDU and ΔRU denote the respective gains of *D* and *R* when one option is chosen over the other. We utilize the Cobb-Douglas form for simplicity in calculations, with robustness maintained across various forms of bargaining processes.

We use superscripts '*d*' and '*w*' to respectively denote the research firm's disclosing and withholding information. If *R* chooses to withhold information at $t = 0$ and the licensing agreement is executed at $t = 0$, then the expected value of the invention is $(pv_H + (1-p)v_L)$. The expected utility of *D* is expressed as: $DU_{0i}^{w} = pv_H + (1-p)v_L - F_{0i}^{w}, i = H, L$. Similarly, the expected utility of *R* is given by*:* $RU_{0i}^{w} = F_{0i}^{w} - c_i, i = H, L$. In the scenario where the licensing agreement is signed at $t = T$, the valuation of a high-value invention is $\delta^T v_H$, and of a low-value invention is $\delta^T v_L$. Correspondingly, the expected utility of *D* becomes: $DU_{Ti}^{w} = \delta^T v_i - F_{Ti}^{w}, i = H, L$. Here, δ^T serves as a discount factor at time *T* to account for the cost of delayed IP transfer. A higher value of δ^T implies a greater preservation of the value of the invention over time. *R*'s corresponding expected utility is formulated as: $RU_{Ti}^{w} = F_{Ti}^{w} - c_i, i = H, L$.

If R opts to *disclose information at* $t = 0$, and the licensing agreement is executed at $t = 0$, then the expected utility of *D* is given by: $DU_{01}^{d} = v_i - F_{0i}^{d}, i = H, L$. Correspondingly, *the expected utility of R is* formulated as*:* $RU_{0i}^{d} = F_{0i}^{d} - c_i, i = H, L$.

In cases where the agreement is not reached at $t = 0$, there is a probability μ that D can successfully commercialize the invention by exploiting the leaked information without licensing. If D fails, with the probability $(1 - \mu)$, D can still make an offer at $t = T$, and the scenario is the same as when R withholds information because whether an invention is of high or low value is common knowledge at $t = T$. It is important to note that in the traditional world, it is challenging for a research firm to prove the disclosure and unauthorized use of IP-related information and obtain compensation promptly. Therefore, we assume that compensation is 0 in the traditional world to simplify the model analysis (the results remain valid when we relax this assumption).

This model setup implies that R with a high-value invention can disclose information to signal the value of its invention in order to get a better licensing fee when signing the agreement at $t = 0$. If R withholds information, another research firm with a low-value invention can potentially pool with R to get a higher licensing fee. Disclosing information, on the other hand, would reveal the low value of this other firm's invention and lower its licensing fee.

To gain a clear view of the interests of R and D, we summarize the licensing fees, utilities of R and D, respectively, corresponding to various decision scenarios in Lemma 1.

Lemma 1. *The licensing fees and utilities of Firms R and D corresponding to various decision scenarios are displayed in Table 1.*

Table 1. Licensing fees and utilities of the developer firm in different cases

	$(w, 0)$	(w, T)	$(d, 0)$	(d, T)
F_H	$(1-\alpha)(pv_H + (1-p)v_L)$	$(1-\alpha)\delta^T v_H$	$(1-\mu)(1-\alpha)v_H$	$(1-\alpha)\delta^T v_H$
F_L	$(1-\alpha)(pv_H + (1-p)v_L)$	$(1-\alpha)\delta^T v_L$	$(1-\alpha)v_L$	$(1-\alpha)\delta^T v_L$
DU_H	$\alpha(pv_H + (1-p)v_L)$	$\alpha\delta^T v_H$	$(\alpha + \mu - \alpha\mu)v_H$	$\alpha\delta^T v_H$
DU_L	$\alpha(pv_H + (1-p)v_L)$	$\alpha\delta^T v_L$	αv_L	$\alpha\delta^T v_L$

Note: $RU_i = F_i - c_i, i = H, L$.

In Table 1, we denote R's choice to disclose or withhold information about the invention as d and w, respectively. T and 0 respectively indicates whether a licensing agreement is reached at $t = T$ or $t = 0$. Four cases result from the combination of the decisions of R and D: $(w, 0)$, (w, T), $(d, 0)$, (d, T).

The first two rows in Table 1 correspond to the licensing fees for research firm *i,* denoted as F_i $(i = H, L)$. DU_i $(i = H, L)$ indicates *D*'s utility from signing an agreement with the research firm i. A comparison of the utilities of *R* and *D* in the various decision scenarios leads to Proposition 1.

Proposition 1[1] *There exist three thresholds:* $\overline{\mu_1} = \frac{(1-p)(v_H - v_L)}{v_H}$, $\overline{\mu_2} = 1 - \delta^T$, *and* $p_{0T} = \frac{\delta^T v_H - v_L}{v_H - v_L}$ *such that:*

(a) When $\mu \geq \overline{\mu_1}$ *and* $p \geq p_{0T}$, R_H *prefers to withhold information and reach an agreement with the developer firm at* $t = 0$ *to pool with* R_L*, and the flat fee is* $F_0 = (1-\alpha)(pv_H + (1-p)v_L)$ *(pooling equilibrium);*

(b) When $\mu \leq min\{\overline{\mu_1}, \overline{\mu_2}\}$, R_h *prefers to disclose information to separate with* R_L*. Both firms sign an IP transfer agreement at* $t = 0$ *(separating equilibrium type I);*

(c) When $\mu \geq \overline{\mu_2}$ *and* $p < p_{0T}$, R_h *prefers to sign an agreement with the developer firm at* $t = T$ *to separate with* R_L*, who signs at* $t = 0$*. The corresponding licensing fees are displayed in Table 1 (separating equilibrium type II).*

Proposition 1 highlights that the research firm's choice to disclose information about the invention is contingent upon a complex interplay of factors, including the developer firm's success rate (μ) in using the disclosed information for invention development, the proportion of research firms with high-value inventions (p) in a market, the value gap between the high- and low-value inventions ($v_H - v_L$), and the discount factor (δ^T). Furthermore, μ also reflects the level of protection afforded to the intellectual properties.

If the degree of IP protection is sufficiently high, it is easy for the research firm to prove its ownership of the invention and obtain compensation from *D*. Correspondingly, the developer firm is less likely to use the disclosed information to develop and commercialize the invention. However, in reality, it is usually difficult for a research firm to prove its ownership of an invention and to receive protection before a patent is granted. This is because information disclosure from the research to the

[1] Please see the proofs of Propositions 1 to 5, and Corollaries 1 and 2 in Appendix A.

developer firm is often untraceable, or the record of information disclosure is not verifiable (Anton and Yao 2004). This creates significant challenges in the intellectual property (IP) and innovation transfer processes across various industries due to several practical limitations: the lack of robust record-keeping mechanisms (Gupta and Kumar, 2020), the complexity of trade secrets (Hall et al., 2014), and the potential costs and unpredictable outcomes of lawsuits (Rimmer, 2019). These factors can discourage research firms from pursuing legal actions.

These predictions align with empirical evidence from a study of 1,612 licensing agreements, indicating that industries placing greater importance on IP rights exhibit a higher frequency of licensing, as a percentage of all alliances, particularly for "prospective" (to-be-developed) technologies (Anand and Khanna 2000). In sectors with traditionally weak IP protection (i.e., a high μ), firms tend to opt for non-licensing alliances like joint ventures (Oxley 1999), venture capital funding (Gans, et. al. 2000), and other alliance forms (Arora, et. al. 2001, Hall and Ziedonis 2001).

The proportion of firms with high-value inventions among all research firms (p) indicates the degree of trust that a developer firm can have for research firms in the market. Arrow (1974, c.1, p.23) emphasized trust as "an important lubricant of a social system," as it is impossible to fully contract upon all possible states of nature. If the "trust" is sufficiently high (i.e., a high proportion of research firms provide high-value inventions), it is unnecessary for the research firm to disclose information to reach an agreement at $t = 0$. Both the research and the developer firms have more incentives to sign before the patent is granted. While if the "trust" level is low, the research firm with a high-value invention needs to disclose as much information as possible to signal the superior value of its invention, increasing the risk of leaking information without reaching an agreement, thus discouraging the research firm from disclosing information.

The incentive for R_H to separate from R_L grows as the value gap between high- and low-value inventions ($v_H - v_L$) increases and the cost of waiting to license later decreases (i.e., the discount factor δ^T $increases$). A larger value gap means that a high-value invention is worth a much higher transfer fee than a low-value invention, and the potential loss for R_H is greater in a pooling equilibrium. Similarly, when the discount factor is bigger, the cost of waiting to license at $t = T$ is lower. This

motivates R_H to sign the agreement at $t = T$ to separate from R_L. However, the discount factor is highly correlated with the length of the period T, with a longer T leading to a smaller discount factor. Therefore, a prolonged period for obtaining patents elevates the research firm's incentive to sign an IP transfer agreement at the beginning of the period ($t = 0$).

The research firm with a low-value invention (R_L) may benefit from the pooling equilibrium by signing an agreement at $t = 0$ with its invention being perceived at a higher value. R_L, however, always loses from the discount factor at $t = T$. In addition, the value of the invention is verified at $t = T$. Therefore, the optimal strategy for R_L is to sign an agreement at $t = 0$.

Corollary 1. *The developer firm always benefits when a research firm discloses information about the invention at* $t = 0$.

Corollary 1 conveys the intuition that the research firm *R*'s decision to withhold information about the invention puts developer firm *D* on the disadvantageous side of the information asymmetry due to the non-rival nature of IP. This is because *D* cannot distinguish the value of the invention. However, when *R* discloses information about the invention, *D* has a choice to decline the agreement with *R* and commercialize the invention on its own. This puts *D* on the advantageous side of the information asymmetry due to the non-exclusive nature of IP.

In summary, IP protection and transfer in the traditional world does not have a universal and Pareto-optimal solution for the two main parties, namely the research and developer firms. There is a strong tendency for research firms with high-value inventions to delay IP transfer and withhold information about the invention. Only under certain rare conditions such as a high degree of trust in the market, IP transfer delay can be mitigated without impairing the research firm's interest.

3.2 World with Blockchain

Blockchain technology, as highlighted by Cong and He (2019), relies on decentralized consensus for validating records, presenting a promising avenue for streamlining intellectual property (IP) transfer while safeguarding IP rights. However, the engagement of a community of record-keepers in the blockchain ecosystem introduces a novel challenge: the intricate relationship between decentralized

consensus and information distribution (Cong and He, 2019). The dissemination of information to a network of inherently distrustful record keepers poses the risk of system manipulation by these participants. Without meticulous oversight, a blockchain-based solution for IP protection and transfer may inadvertently trade old challenges for new ones. For example, in the Non-Fungible Token (NFT) market, the absence of IP record censorship has given rise to unprecedented issues such as content piracy and infringement (Forbes, 2022a; Fortune, 2021). Furthermore, instances of insider misconduct, exemplified by the alleged insider trading involving a former manager at OpenSea, a prominent NFT marketplace, have heightened concerns among stakeholders (The National Law Review, 2022). It is imperative to discern the conditions under which both the new tension introduced by blockchain and the pre-existing tension related to IP protection can be effectively mitigated.

Building on the theoretical framework proposed by Cong and He (2019), our analysis centers on a blockchain protocol that interacts with *K* homogenous potential keepers to validate records associated with specific transactions or activities. These activities may include scenarios such as the disclosure of information about a new invention by a research firm, the retrieval of disclosed information by a developer firm, or the facilitation of payment transfers. To model the occurrence of a transaction or activity, we introduce a binary variable $\tilde{\omega}$ (where $\tilde{\omega} \in \{0,1\}$), which takes the value 1 if the transaction or activity occurs and 0 otherwise. The decentralized consensus outcome within the blockchain is represented by $\tilde{z}$, which is similarly binary ($\tilde{z} \in \{0,1\}$), with 1 indicating a state of perfect consensus. To evaluate the reliability of this consensus in the context of contracting, we measure its quality as $-Var(\tilde{\omega} - \tilde{z})$, where a lower variance indicates a higher degree of alignment between the true state of the activity and the consensus outcome.

When engaged, each keeper $k \in K \equiv \{1,2,\cdots,K\}$ submits an individual report, $\tilde{y}_k$, where $\tilde{y}_k$ takes values in $\{0,1\}$. The set of all reports, denoted as $y \equiv \{\tilde{y}_k\}_{k\in K}$, encapsulates the collective input provided by keepers. For illustrative purpose, we focus on a scenario in which the decentralized consensus on a transaction or activity, denoted as $\tilde{z}(y)$, is computed as:

$$\tilde{z}(y) = \begin{cases} 1 & with\ probability\ \sum_k w_k \tilde{y}_k \\ 0 & otherwise. \end{cases}$$

where $\omega_k \geq 0$ represents the weight assigned to the k-th keeper's input, ensuring that $\sum_{k=1}^{K} w_k = 1$, and $w_k \to 0$ as $K \to \infty$, reflecting a diminishing influence of any single participant in the consensus process. This framework provides a foundation for analyzing the reliability and robustness of decentralized consensus mechanisms in contractual settings, with implications for both economic efficiency and legal enforceability.

Each risk-neutral keeper strategically submits a report, denoted as y_k, with the objective of maximizing their normalized utility function $U(y_k; y)$,

$$U(y_k; y) = b_k \cdot \lfloor \tilde{z}(y) - \tilde{\omega} \rfloor - h_k \lfloor y_k - \tilde{\omega} \rfloor \qquad (1)$$

where b_k and h_k are positive, bounded above zero for all k. b_k represents the benefit accrued to record keeper k when an untruthful consensus is reached, while h_k denotes the cost associated with misreporting. Recognized as a significant source of information quality threats (Gartner 2020), users or insiders within a blockchain system may intentionally exploit imperfect consensus to enhance their individual utility. Notably, the 51% attack or majority attack stands out as a well-documented insider threat, wherein certain insiders control more than 51% of blockchain nodes, thereby gaining the ability to disrupt transactions and manipulate records. An illustrative example occurred in August 2021 when Crypto Bitcoin SV, then ranked as the 44th largest cryptocurrency globally, fell victim to a 51% attack, resulting in approximately a 4% decline in the value of Bitcoin SV within 24 hours of the attack (Bloomberg, 2021). It is crucial for firms to carefully weigh the benefits and costs associated with misreporting when contemplating such actions.

We denote the imperfect consensus derived from the finite set of keepers as a probability φ, representing the accuracy in recording IP-related actions, such as the disclosure of IP-related information. Building on the previous analysis, the probability φ is defined as the sum of the weights of the truthful record keepers, $\varphi = \sum_{k \in \mathbf{K}^*} w_k \leq 1$, where $\mathbf{K}^* = \{k \in \mathbf{K}: b_k w_k < h_k\}$ is the subset of truthful record keepers.

Lemma 2. *The consensus quality* $\varphi = -I_{k \leq \frac{b}{h}}$, *exhibiting improvement with the expansion of K.*

For more general b_k and h_k satisfying conditions specified in Equation (1), the consensus becomes perfect, i.e., $\varphi = 1$ as $K \to \infty$. The impact of the perfect consensus on the research firm's IP transfer decisions provides an idealized scenario of using blockchain for IP protection and transfer.

A smart contract encoded in the blockchain system can automatically verify the information disclosure and information retrieval records in the blockchain system and transfer compensation payment C from the developer firm to the research firm in the case that the developer firm uses the disclosed information to commercialize the invention. We assume the penalty for IP infringement is severe enough to deter the developer firm from unauthorized use of IP-related information. i.e., $C > v_H$. On the other hand, the cost of participating in the blockchain is c_0, and that c_0 is low enough to ensure the participation of the firms when the consensus in the blockchain is truthful.

A blockchain system can benefit R_H by preventing the disclosed information from being misused by the developer firm. It therefore incentivizes R_H to disclose information at $t = 0$ to separate from firms with low-value inventions. The expected utility of R_H when it discloses information is:

$$RU_{kH}^{db} = \begin{cases} \mu\varphi C + (1-\mu)F_{TH}^{db} - c_H - c_0 & if\ an\ agreement\ is\ not\ reached\ at\ t = 0 \\ F_{0H}^{db} - c_H - c_0 & if\ an\ agreement\ is\ reached\ at\ t = 0 \end{cases}$$

$$\text{s.t. } F_{0H}^{db} - c_0 \geq max\{F_{TH}^{w}, F_{0H}^{w}\}$$

where the superscripts 'd' and 'b' respectively represent R_H disclosing and withholding information within the blockchain system. $t = 0, T$ and the difference in the IP transfer fees is the incentive compatibility condition (ICC) for R_H in that R_H's expected utility from disclosing information to separate from firms with low-value inventions (R_L) should be higher than its expected utility from withholding information to pool with R_L.

The expected utility for the developer firm (D) is:

$$DU_{kH}^{b} = \begin{cases} \mu(v_H - \varphi C) + (1-\mu)\left(\delta^T v_H - F_{TH}^{b}\right) & if\ an\ agreement\ is\ not\ reached\ at\ t = 0 \\ v_H - F_{0H}^{b} & if\ an\ agreement\ is\ reached\ at\ t = 0 \end{cases}$$

$$\text{s.t. } \mu(v_H - \varphi C) + (1-\mu)\left(\delta^T v_H - F_{TH}^{b}\right) \leq v_H - F_{0H}^{b}$$

where $t = 0, T$, and the difference in the IP transfer fees is the ICC for D not to misuse the disclosed information of R_h.

Solving the utility maximization problem, we obtain that $F_{0H}^{b} = (1-\alpha)((1-\mu+\alpha\delta^{T}\mu)v_H + C\mu\varphi)$, and $\varphi \geq max\left\{\frac{[(1-\delta^{T}\alpha)\mu-(1-\delta^{T})]v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C}, \frac{pv_H+(1-p)v_L-(1-\mu+\alpha\delta^{T}\mu)v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C}\right\} = \tilde{\varphi}$.

To have some insights, we first consider the case when $K \to \infty$, where the consensus is perfect.

Proposition 2 (Perfect consensus). *When $K \to \infty$, the research firm with a high-value invention would disclose information to signal the value of its invention in order to reach an agreement at $t = 0$.*

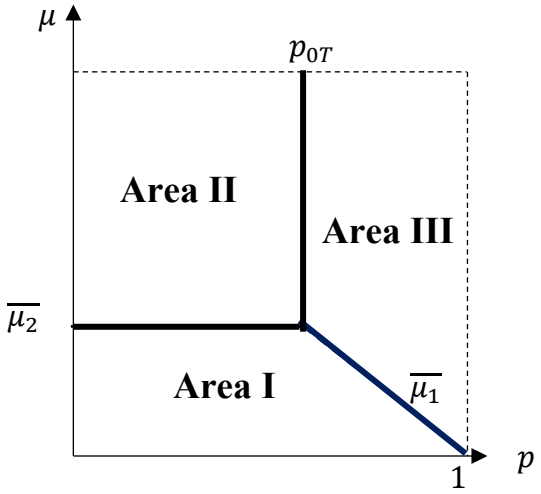
Recall that the research firm with a low-value invention always prefers to sign an agreement at $t = 0$. Hence, with the mediation of a blockchain system, the two-party IP-transfer game becomes monitored by a system of multiple parties abiding by consensus, and all the agreements would be signed at $t = 0$. For high-value inventions, the flat fee is $F_{0H}^{b} = (1-\alpha)v_H$; while for low-value inventions, the flat fee is $F_{0L}^{b} = (1-\alpha)v_L$. The mediation of a blockchain system enables the actions related to an IP to be traced as time-stamped records. Consequently, the research firm with a high-value invention has more incentive to disclose information about their new invention to signal its true value, as the invention ownership and information disclosure are recorded in the blockchain. Meanwhile, knowing the penalty for infringing the research firm's IP, the developer firm is more likely to sign an agreement with the research firm when it makes a credible commitment. Therefore, the research firm can now disclose information about the invention to signal its true value without concern about the leakage of information.

Proposition 2 gives us the theoretical insights into the growing trend for IP-intensive industries to invest in blockchain applications (PRNewswire, 2021). Essentially, a blockchain system with perfect consensus diminishes the dilemma of research firms regarding information disclosure. It also prevents the developer firm from attempting to commercialize an invention using the disclosed information. The two-party game between the research firm and developer firm therefore has a Pareto optimal solution: rapid IP transfer without the risk of IP infringement.

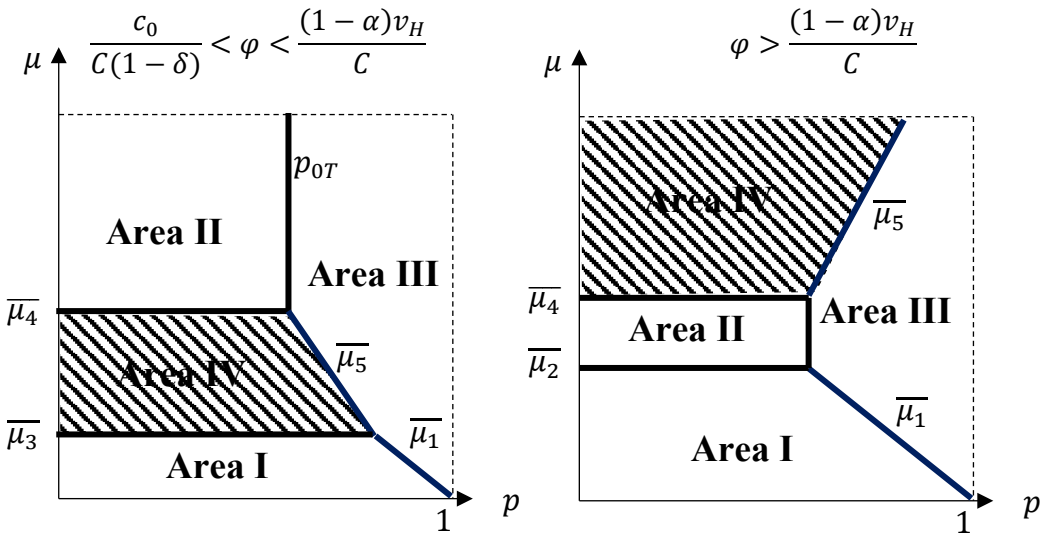
In reality, the number of record keepers of a blockchain system is finite. Consequently, the quality of consensus in blockchain is likely to be compromised in real-world applications. The relaxation of the perfect consensus assumption requires us to rethink the benefits of blockchain for IP transfer, the

decisions of the research or developer firms, and the impact of behavioral factors within and outside the blockchain system.

Proposition 3 (Imperfect consensus). *There exist two quality thresholds of consensus in a blockchain,* $\hat{\varphi} = \frac{c_0}{C(1-\delta)}$ *and* $\tilde{\varphi} = \frac{(1-\alpha)v_H}{C}$. *When the quality of consensus is below* $\hat{\varphi}$*, no research firm will join the blockchain; In the medium quality of consensus range* $\hat{\varphi} < \varphi < \tilde{\varphi}$*, all research firms will join the blockchain if the success rate of the developer firm in commercializing the IP is moderate; When the quality of consensus is above* $\tilde{\varphi}$*, all research firms will join the blockchain if the success rate of the developer firm in commercializing the IP is high. As shown in Figure 2.*



Panel a. In the traditional world



Panel b. With Blockchain

Figure 2. Equilibria under Different Conditions

Area I & Area IV. **separating equilibrium**: R_h discloses information, both firms sign an agreement at time $t = 0$;

Area II. separating equilibrium: R_L signs at $t = 0$, while R_h signs at $t = T$;

Area III. **pooling equilibrium**: R_h withholds information, both firms sign an agreement at $t = 0$.

Proposition 3 indicates that when the quality of consensus of the blockchain is low, the developer firm lacks the incentive to participate in the blockchain. The quality of the consensus determines the authenticity of the records in blockchain. A low-quality consensus ($\varphi < \tilde{\varphi}$) implies potential misreporting of information within the blockchain, including IP ownership and transfer actions, reducing the research firm's ability to seek compensation in cases of developer firm misuse of disclosed information. Consequently, this diminishes the research firm's motivation to disclose information prior to patent approval.

In cases where the consensus quality is moderate, the developer firm would opt to join the blockchain when the success rate of utilizing leaked information for commercialization is also moderate. The rationale behind this decision is that with a very low success rate, the benefits of blockchain adoption are minimal, and the additional costs are unwarranted. However, with a high success rate, the consensus quality of the blockchain may not sufficiently offset potential losses from information leakage, leading the research firm to prefer information concealment. Conversely, with a high consensus quality, the research firm would choose blockchain adoption as long as the success rate of utilizing leaked information for commercialization remains high.

3.2 Unobservable Quality of Consensus

From a firm's perspective, the quality of decentralized consensus in blockchain can be unobservable. Record keepers, especially those trying to game the system, can exploit vulnerabilities in blockchain nodes to hide their misreporting behaviors (Deirmentzoglou et al. 2019; Eyal and Sirer 2013). Accordingly, we consider that neither the developer firm D nor the research firm/entity R_h can

observe φ, the quality of decentralized consensus of the blockchain system. Instead, they only have an estimation of it, which is defined as $E(\varphi) = \varphi + \epsilon$. $E(\varphi)$ is formed either from a firm's own inspection or from word-of-mouth. ϵ measures the discrepancy between the estimated and the actual qualities of the consensus.

When the firms overestimate the quality of the blockchain records, the expected utility of R_h from disclosing information is:

$$RU_{jH}^{u} = \begin{cases} \mu(\varphi+\epsilon)C + (1-\mu)F_{TH}^{u} - c_H - c_0 & if\ an\ agreement\ is\ not\ reached\ at\ t=0 \\ F_{0H}^{u} - c_H - c_0 & if\ an\ agreement\ is\ reached\ at\ t=0 \end{cases}$$

$$\text{s.t. } F_{0H}^{u} - c_0 \geq max\{F_{TH}^{w}, F_o^{w}\}$$

where $j = 0, T$, and the difference in the IP transfer fees is the ICC of R_h in that R_h's expected utility from disclosing information should be higher than the expected utility from withholding information. The expected utility for D is:

$$DU_{jH}^{u} = \begin{cases} \mu(v_H - (\varphi+\epsilon)C) + (1-\mu)(\delta^T v_H - F_{TH}^{u})\ if\ an\ agreement\ is\ reached\ at\ t=0 \\ v_H - F_{0H}^{u} \quad if\ an\ agreement\ is\ not\ reached\ at\ t=0 \end{cases}$$

$$\text{s.t. } \mu(v_H - \varphi C) + (1-\mu)\left(\delta^T v_H - F_{TH}^{h}\right) \leq v_H - F_{0H}^{u}$$

where $j = 0, T$, and the difference in the IP transfer fees is the ICC for D not to misuse the disclosed information about the high-value invention.

From solving the utility maximization problem, we obtain that $F_{0H}^{u} = (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_H + C\mu(\varphi+\epsilon))$, R_h's expected utility from signing an IP transfer agreement at $t = 0$ is:

$$RU_{0H}^{u} = (1-\alpha)\left((1-\mu+\alpha\delta^T\mu)v_H + C\mu(\varphi+\epsilon)\right) - c_H - c_0.$$

R_h's expected utility from signing at $t = T$ is:

$$RU_{TH}^{u} = \mu(\varphi+\epsilon)C + (1-\mu)(1-\alpha)\delta^T v_H - c_H - c_0.$$

where $\varphi \geq max\left\{\frac{[(1-\delta^T\alpha)\mu-(1-\delta^T)]v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} - \varepsilon, \frac{pv_H+(1-p)v_L-(1-\mu+\alpha\delta^T\mu)v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} - \epsilon\right\} = \varphi^U$. Therefore, we obtain the following proposition:

Proposition 4: *When $RU_{0H}^{u} > max\{RU_{TH}^{u}, RU_{0H}^{w}, RU_{TH}^{w}\}$, i.e. $\varphi \geq \varphi^U$, the research firm with a high-value invention prefers to disclose information and reach the IP transfer agreement at $t = 0$;*

otherwise, the research firm with high-value invention prefers to withhold information, and the equilibrium is the same as that in the traditional world.

Further insights into firm decisions are gained through the following analysis of the cases where R_h overestimates or underestimates the quality of decentralized consensus.

R_h overestimate: $E(\varphi) > \varphi$, i.e. $\epsilon > 0$

If R_h's estimation of the quality of decentralized consensus is less than the threshold φ^U for disclosing information and signing agreement at t=0 ($\varphi < E(\varphi) < \varphi^U$, i.e., $0 < \epsilon < \tilde{\varphi} - \varphi$), R_h would withhold information, and the equilibrium is the same as that in the traditional world. An over-estimation of the quality of blockchain does not affect the equilibrium.

In the case that R_h's estimation of the quality of consensus exceeds the threshold yet the threshold is greater than the actual quality of consensus ($\varphi < \varphi^U < E(\varphi)$, i.e., $\epsilon > \tilde{\varphi} - \varphi > 0$), R_h would disclose information and sign the agreement at $t = 0$ with its overestimation of the quality of the consensus, i.e., the separating equilibrium is sustainable. However, if R_h knew the actual quality of the consensus, it should withhold information and defer the signing of the agreement, i.e., the equilibrium is the same as that in the traditional world. The overestimation of the quality of consensus therefore changes R_h's IP transfer decisions as well as the equilibrium. R_h may suffer utility loss due to the overestimation. Moreover, R_h may change its long-term invention production strategy.

If R_h's estimation of the quality of consensus is greater than the threshold yet the threshold is less than the actual quality of consensus ($\varphi^U < \varphi < E(\varphi)$, i.e., $\epsilon > 0 > \tilde{\varphi} - \varphi$), R_h prefers to disclose information and signs the agreement at $t = 0$, i.e., the separating equilibrium is sustainable. The overestimation of the quality of the consensus does not affect the equilibrium.

R_h underestimates: $E(\varphi) < \varphi$, i.e. $\epsilon < 0$

If R_h's underestimated quality of consensus is less than the threshold for disclosing information and signing agreement at t=0 ($E(\varphi) < \varphi < \varphi^U$, i.e., $\epsilon < 0 < \tilde{\varphi} - \varphi$), R_h would withhold information, and the equilibrium is the same as that in the traditional world. The underestimation of the quality of consensus does not affect the equilibrium.

If the threshold is between R_h's estimated and actual quality of consensus ($E(\varphi) < \varphi^U < \varphi$, i.e., $\epsilon < \tilde{\varphi} - \varphi < 0$), R_h prefers to withhold information according to the estimated quality of the consensus. However, the actual quality of the consensus would warrant R_h's information disclosure and early IP transfer decision, i.e., the equilibrium is the same as that in the traditional world under the estimated quality, while the separating equilibrium is sustainable under the actual quality of the consensus. The underestimation of the quality of the blockchain consensus therefore hurts the utility of both R_h and D.

If R_h's underestimated quality of consensus is greater than the threshold ($\varphi^U < E(\varphi) < \varphi$, i.e., $\tilde{\varphi} - \varphi < \epsilon < 0$), R_h prefers to disclose information to separate with low-value inventions and sign the agreement at $t = 0$ under both estimated and actual qualities of the consensus. The underestimation of the quality of the consensus has no impact on the equilibrium.

Insights from the above analysis can be summarized as follows:

Proposition 5. *When the discrepancy between the estimated and actual quality of the consensus in blockchain ϵ satisfies $\epsilon > \tilde{\varphi} - \varphi > 0$, the research firm with a high-value invention will switch from withholding to disclosing information in order to separate from the research firm with a low-value invention and sign the IP transfer agreement at $t = 0$; while if, $\epsilon < \tilde{\varphi} - \varphi < 0$, the research firm with a high-value invention will switch from disclosing to withholding information; otherwise, neither overestimation nor underestimation has any effect on the equilibrium.*

The intuition behind Proposition 5 is as follows: The quality of the consensus φ, is crucial in determining the authenticity and reliability of records within the blockchain. When the consensus quality falls below the threshold $\tilde{\varphi}$, it implies a higher likelihood of misreporting and inaccuracies in the blockchain records, including those related to IP ownership and transfer actions. This diminished trust in the blockchain's integrity undermines the research firm's confidence in using it as a secure platform for IP transactions.

The quality of the decentralized consensus in blockchain indicates the possibility that R_h can successfully obtain compensation when the developer firm infringes its IP rights. When R_h overestimates the quality of the consensus ($E(\varphi) > \tilde{\varphi}$), it would have more incentive to disclose information and separate with low-value inventions. However, the developer firm may prefer to use the

disclosed information to develop and commercialize the invention if the possibility of being caught is lower than R_h's estimated possibility. Thus, overestimation hurts the utility of R_h. Meanwhile, if R_h underestimates the quality of the consensus in blockchain ($E(\varphi) < \tilde{\varphi}$), it may be deterred to disclose information to separate with low-value inventions. This hurts the utility of R_h as well. In summary, both overestimation and underestimation of blockchain consensus quality can harm the interests of R_h. Only when the quality of the decentralized consensus is either sufficiently high ($\tilde{\varphi} < E(\varphi) < \varphi$) or low ($E(\varphi) < \varphi < \tilde{\varphi}$), the harmful effect of overestimation or underestimation is negligible.

A low-quality consensus ($\varphi<\tilde{\varphi}$) poses several risks:

1. **Misuse of Disclosed Information**: Research firms cannot rely on the blockchain to accurately verify and protect their disclosed information. This increases the risk that developer firms may misuse this information without proper compensation or legal recourse.
2. **Loss of Compensation**: In cases of misuse, the research firm's ability to seek compensation is significantly hindered. The blockchain's role in ensuring accountability and traceability is compromised, making it an unreliable platform for high-value transactions.
3. **Cost of Participation**: The costs associated with participating in the blockchain, including transaction fees and the effort required to maintain secure records, become unjustifiable if the blockchain cannot guarantee the authenticity and security of these records.

Users or insiders of a blockchain system have been recognized as a main source of information quality threats (Gartner 2020). Some record keepers can deliberately exploit imperfect consensus to increase their individual utility. One well-known insider threat is the 51% attack or majority attack, where certain insiders control more than 51% of the blockchain nodes, thereby enabling them to disrupt transactions and manipulate records. In August 2021, Crypto Bitcoin SV, ranked as the 44th largest cryptocurrency globally at that time, reported falling victim to a 51% attack, leading to a decline of approximately 4% in the value of Bitcoin SV within 24 hours of the attack (Bloomberg, 2021). However, such actions require careful consideration of firm decisions, weighing the benefits and costs of misreporting.

In Section 3.1, we have shown that in each period, a risk-neutral record keeper submits a report of y_k to maximize his normalized utility $U(y_k; y)$ (refer back to Equation 1). This model setup indicates that the quality of an individual keeper's report is dependent on the benefit from misreporting, the cost of misreporting, and the weight of the keeper's validating notes in the formation of decentralized consensus. If the number of record keepers K is infinite, then $w_k \to 0$ when $K \to \infty$. However, when K is finite, we can divide the keepers into two subsets, one including keepers who report truthfully (we denote this subset as "*H*", who report as $\tilde{y}_H^* = \tilde{\omega}$), the other containing the keepers who misreport (we denote them as "C", who report as $\tilde{y}_C^* = 1 - \tilde{\omega}$). If the keepers attempt to cheat and change the consensus, a large proportion of them need to collude to create their own branch of a blockchain and make this branch chosen as the main branch by the fork resolution rule applied to the distributed ledger (Kannengießer et al. 2020). Selfish-mining (Eyal and Sirer 2013) and long-range attack (Deirmentzoglou et al. 2019) are examples of this type of collusion among record keepers. A commonly used threshold for the proportion of record keepers to successfully collude is 50% of all record keepers (Eyal and Sirer 2013). Accordingly, a successful majority attack of misreporting requires the proportion of honest keepers to be less than 50% ($w < 50\%$) . Therefore, the consensus is $\tilde{z}(y) = \begin{cases} \tilde{\omega}, & if\ w \geq 50\% \\ 1 - \tilde{\omega}, & if\ w < 50\% \end{cases}$, where w is the proportion of the keepers who report truthfully.

To connect the above setup with firm decisions, we consider the reputation of a blockchain system as a collective-level consequence of individual keeper behaviors. Blockchain reputation is indicated by w, the proportion of the keepers who report truthfully. The reputation in turn influences firms' choice between a blockchain-based IP transfer solution and the IP protection in the traditional world.

To explicate the impact of blockchain reputation, we extend the game into infinite periods. The record keepers are categorized into three types: honest (who always report truthfully), dishonest (who always misreport), and strategic (who report truthfully or not according to the benefits they can obtain). Their respective proportions are τ, β and γ, and $\tau + \beta + \gamma = 1$. Recall that $\tilde{\varphi}$ denotes the threshold level of the quality of consensus for firms to benefit from a blockchain system. We assume that $\tau <$

$\tilde{\varphi} < \tau + \gamma$ to ensure that research firms with a high-value invention will participate when all the strategic keepers report truthfully, and exit when all the strategic keepers misreport.

Proposition 6. *When the reputation of a blockchain system falls to $\varphi < \tilde{\varphi}$, all research firms will exit the blockchain system.*

Consider the case when $\varphi > \tilde{\varphi}$ in the t^{th} period. The utility of an individual keeper who never misreports is: $\frac{c_0}{K} + \delta\left(\frac{c_0}{K}\right) + \delta^2\left(\frac{c_0}{K}\right) + \cdots = \frac{c_0}{(1-\delta)K}$. While if the keepers misreport and successfully change the consensus, the research firm will update its belief about the reputation of the blockchain system. Thus, research firms with a high-value invention will exit in the next period. Meanwhile, when the developer firm expects that the research firm with a high-value invention to exit, they will only pay a low licensing fee $(1-\tau)v_2 - c_0$ to the remaining low-value inventions. However, when firms with a low-value invention choose to license through the traditional channel, they can get at least $(1-\tau)v_2 > (1-\tau)v_2 - c_0$. Therefore, research firms with a low-value invention will also exit the blockchain. Thus, for the keepers who misreport at the t^{th} period, they may gain extra in that period, but lose all the potential gains in future periods. They need to balance between gaining from one-time misreporting and gaining from continuous transaction payoffs from honestly reporting, i.e. $h_k\lfloor y_k - \tilde{\omega}\rfloor = \frac{c_0\delta^t}{K(1-\delta)} + F(w,K)$, where $F(w,K)$ contains other costs such as the consumption of electricity, equipment purchases, and maintenance costs. If the benefit of misreporting exceeds the cost, then the strategic keepers will choose to misreport, and the blockchain reputation (the proportion of honest keepers) will become $\tilde{\varphi} = \tau$, and research firms of both types will exit the blockchain system.

4. Security threats outside a blockchain system

The section above highlights the impact of the size of the record keeper community on the quality of consensus in blockchain. This size is not only based on the participation/withdrawal decision of individual keepers, but also subject to the manipulation of external parties such as hackers. Data from Check Point Research (CPR) shows that global attacks on blockchain networks increased by 38% in 2022 compared to the same period the previous year (News Desk, 2022; Check Point Research, 2023).

Furthermore, blockchain analytics firm Chainalysis reported that hackers stole $3.8 billion in cryptocurrency from platforms worldwide in 2022, up from $3.3 billion during the same period in 2021 (Korn, 2022; CNBC 2022). Hackers can take advantage of vulnerabilities in smart contracts or nodes in a blockchain and tamper with the authenticity of IP-related records (Henry et al. 2018; Li et al. 2017; Pun et al. 2021). Such security attacks can cause disutility to both research and developer firms. We now include security threats imposed by hackers into the process of consensus formation modeled in Section 3.2. The analysis in this section aims to deepen our understanding of the relationship between externally manipulated record keeper community size and blockchain-based IP licensing process.

To gain insights into the impact of outside security attacks, we illustrate with a common method for a hacker to attack blockchain, the so-called *Eclipse attack* (Kannengießer et al. 2020). In an Eclipse attack, hackers try to isolate selected nodes in a blockchain system and prevent them from obtaining a true picture of activities in the system. This allows the hacker's nodes to manipulate the current ledger state and falsely report IP ownership, information disclosure, and other IP-related activities. This will decrease the quality of the consensus and dissuade the firms from joining the blockchain system.

The problem for the hacker is to find out the optimal number of keepers (nodes) to isolate. We denote the unit cost (such as equipment rentals, electricity consumption, etc.) of isolating selected nodes (i.e., blocking some keepers from a true view of the ledger) as c_a, and the number of keepers the hacker isolates as M ($0 < M < K$). Without the hacker attack, the quality of consensus ($\varphi(K)$) is correlated with the number of keepers in the blockchain system (K). When the hacker isolates M of the keepers, the quality of consensus becomes $\varphi(K-M)$. As $\varphi(K)$ increases with K, the quality of consensus decreases when the hacker blocks some of the keepers, and the hacker may gain utility from the increase of misreporting rate $\big(\varphi(K)-\varphi(K-M)\big)$. We assume that the per-keeper value of the blockchain is v_a, so the potential gain of the hacker from the attack is: $Kv_a \cdot \big[\big(1-\varphi(K-M)\big)-\big(1-\varphi(K)\big)\big]$. That is, the utility function of the hacker is: $Kv_a \cdot \big[\big(1-\varphi(K-M)\big)-\big(1-\varphi(K)\big)\big] - M \cdot c_a$. To solve the utility maximization problem, we obtain the first order condition:

$$K \cdot \varphi'(K-M)v_a - c_a = 0 \qquad (2)$$

where $\varphi(K) = \sum_{k\in\mathbf{K}^*} w_k \leq 1$ and $\mathbf{K}^* = \{k \in \mathbf{K}: b_k w_k < h_k\}$.

For firms hoping to join the blockchain system, the decrease in the quality of consensus from $\varphi(K)$ to $\varphi(K-M)$ can dissuade them from joining. Figure 4 illustrates the changes with respect to K. In the top panel of Figure 4, $\varphi'(K)$ is the probability density function of $\varphi(K)$, which shows the marginal increase of the quality of consensus (correct reporting rate). For arbitrary $K' \in K$, $\varphi(K')$ denotes the correct reporting rate when the number of keepers in the blockchain is K', which is illustrated as the area (A+B+D). More specifically, when the hacker isolates M of the keepers, the correct reporting rate drops to $\varphi(K'-M)$, which is illustrated as the area (D). Therefore, the increase of misreporting rate is $\big(\varphi(K')-\varphi(K'-M)\big)$, as the area (A+B) illustrates. Since the hacker's revenue gain from each keeper when misreporting is v_a, the total revenue the hacker can obtain is $K'v_a[\varphi(K')-\varphi(K'-M)]$.

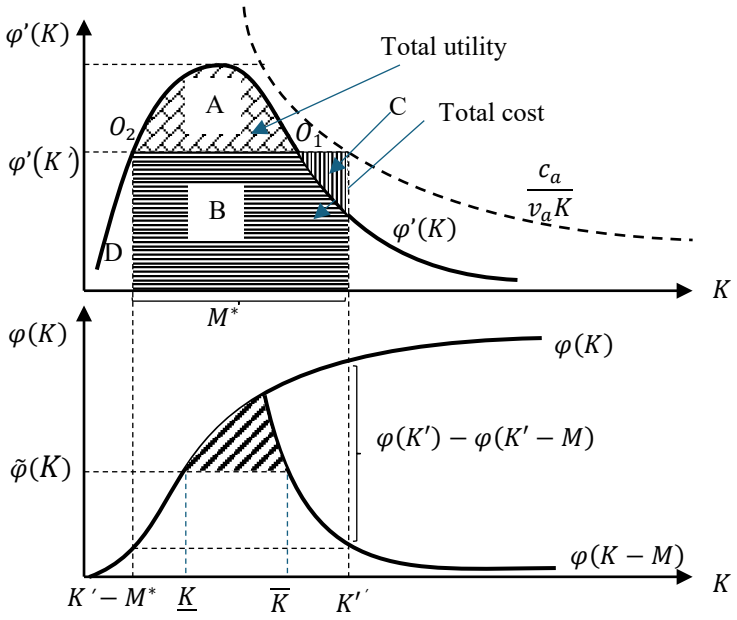


Figure 3. Optimal size of the blockchain platform

Notes: We use the normal distribution of $\varphi(K)$ to draw this figure; *the analysis is robust to both unimodal and multimodal distributions.*

The dotted line in the top panel of Figure 4 represents the standardized marginal cost of attacking to increase the misreport rate, and $\frac{M\,c_a}{K'\,v_a}$ denotes the standardized cost of isolating M of the keepers, as the area (B+C) demonstrates, and the total cost the hacker has to pay is $M\,c_a$. When the total revenue of attacking exceeds the total cost (i.e., when Area A is greater than Area C), the hacker has enough incentive to launch the attack. Otherwise, the attack will not take place. If K is so small that the marginal

revenue never exceeds the marginal cost for the hacker to isolate any number of keepers, then the hacker has no incentive to attack the blockchain system. We focus on the interesting situation where the attack is not so costly that it may take place when the potential value of the blockchain system is large enough (K is sufficiently large).

For the hacker, the optimal number of keepers to isolate (M^*) is the difference between o_1 and o_2. o_2 lies at the point where the marginal revenue of isolating a keeper equals the marginal cost of doing so, as Equation (2) shows. If the marginal revenue exceeds the marginal cost, the hacker has sufficient incentive to increase the number of keepers to isolate; otherwise, the hacker prefers to decrease the number of keepers to isolate.

In the bottom panel, for an arbitrary K', $\varphi(K)$ increases with K. When the hacker isolated M^* of the keepers, the number of keepers in the blockchain becomes $(K' - M^*)$, and the quality of consensus drops from $\varphi(K')$ to $\varphi(K' - M^*)$. This indicates that $\varphi(K' - M^*)$ decreases with K when K surpasses a certain value, as illustrated in the Figure. Back to Section 3.2, we have learned that firms prefer to join the blockchain system only when $\varphi(K) \geq \tilde{\varphi}(K)$. Therefore, the firms have an incentive to join the blockchain only when $\varphi(K) \geq \tilde{\varphi}(K)$ and $\varphi(K' - M^*) \geq \tilde{\varphi}(K)$, indicating that there exist both a lower bound and an upper bound of the size of the blockchain (the number of keepers). Thus, we can obtain the following proposition:

Proposition 7. *There exist both a lower bound and an upper bound for the optimal size of the blockchain keeper community, denoted as* $\underline{K}$ *and* $\overline{K}$*, only when* $\underline{K} \leq K \leq \overline{K}$*, the developer firm would pay for a high-value invention and the research firm would disclose information about the invention before the grant of the patent to maximize their profits.*

When the size of the blockchain increases, the quality of the consensus increases. Meanwhile, the incentive for hackers to attack the blockchain and tamper with IP-related records also increases, resulting in a decrease in the quality of the consensus. Therefore, the blockchain system faces a tradeoff between the expansion of the size and risk of hacking. When the size of the blockchain community (K) is too small ($K < \underline{K}$), the quality of consensus is so low that firms have no incentive to join the blockchain system. On the other hand, when $K \geq \overline{K}$, the decline in consensus quality due to hacking

outweighs the increase in consensus quality from community expansion, making firms reluctant to join the blockchain. Only when K is moderate ($\underline{K} \leq K \leq \overline{K}$), the increase in consensus quality due to the keeper-community expansion is greater than the decrease in consensus quality due to the risk of hacking, making it beneficial for firms to join the blockchain system. Then the blockchain system achieves an equilibrium, as outlined in the final theoretical prediction below.

Corollary 2. When the size of the blockchain is moderate, $\underline{K} \leq K \leq \overline{K}$, with a sufficiently high quality of consensus $\varphi(K) \geq \tilde{\varphi}(K)$ and $\varphi(K - M) \geq \tilde{\varphi}(K)$, and a low risk of security attack, the blockchain system achieves an equilibrium.

5. Repeated Game with Blockchain

The model analysis above is situated in a one-time IP transaction. In reality, a blockchain application can be used in a series of IP transactions. The analysis in this section seeks to gain insights into this realistic scenario by considering a repeated game with blockchain.

If researcher R with high-value invention discloses information and the developer firm does not use the leaked information for commercialization, the research firm's utility is: $F_H(d,0) + \delta F_H(d,0) + \delta^2 F_H(d,0) + \cdots = \frac{F_H(d,0)}{1-\delta} = \frac{(1-\alpha)}{1-\delta} v_H$. The developer firm's profit is $\frac{\alpha}{1-\delta} v_H$. If the developer firm uses the leaked information to commercialize, they would converge to the traditional model.

If the developer firm D deviates from the equilibrium, they can secure a profit of $\mu v_H + (1-\mu)\alpha\delta^T v_H$ at this stage but would obtain a profit as we describe in the benchmark scenario. The developer firm's profit would be $\mu v_H + (1-\mu)\alpha\delta^T v_H + \frac{\delta}{1-\delta}\pi_D$ if it chooses to cooperate rather than mimic the technology. The developer firm's decision to cooperate instead of mimicking the technology occurs when $\frac{\alpha}{1-\delta} v_H > \mu v_H + (1-\mu)\alpha\delta^T v_H + \frac{\delta}{1-\delta}\pi_D$. This condition can be further simplified as $\delta > \frac{(\mu+(1-\mu)\alpha\delta^T)v_H - \alpha v_H}{(\mu+(1-\mu)\alpha\delta^T)v_H - \pi_D}$.

The correlation shows that δ^T increases with π_D. This implies that as the non-cooperative game's profit for the developer firm D rises, their motivation to cooperate with the research entity R diminishes. This is a straightforward observation. Hence, we can gauge the incentive for D to cooperate by

contrasting its profits with and without blockchain. This outcome is summarized in the following proposition.

Proposition 8. *The blockchain incentivizes the developer firm to utilize leaked information for commercialization rather than licensing when* $\overline{\mu_3} < \mu < \overline{\mu_2}$*, and disincentivizes this behavior when* $\overline{\mu_2} < \mu < \overline{\mu_4}$.

Proposition 8 suggests that blockchain can influence D's decision to collaborate with R by leveraging the information disclosed by the latter for commercialization. Since R has an incentive to adopt blockchain only under specific circumstances, as illustrated in Proposition 3, the impact of blockchain only affects D's incentive in these regions. Interestingly, we find that the blockchain would incentivize D not to cooperate when the success rate of using the leaked information to develop is relatively low. In such instances, R would disclose its information regardless of blockchain adoption. However, embracing blockchain could elevate the licensing fee, resulting in reduced profits for the developer firm and increased incentive to deviate from cooperation. On the contrary, with a relatively high success rate, blockchain would encourage D to collaborate. In this scenario, R would finalize the agreement at time T without blockchain, but opt for blockchain at time 0, thereby enhancing D's profits and fostering cooperation.

6. DISCUSSIONS AND CONCLUSION

Blockchain has captivated many people's imagination in recent years. Management researchers have investigated investor reactions to a firm's disclosure of a potential foray into Blockchain technology (Cheng et al. 2019), the benefit of blockchain in improving supply chain transparency (Chod et al. 2020), and a blockchain-based decentralized clearing process (Csóka and Herings 2018). Meanwhile, researchers have paid increasing attention to the caveats of blockchain (e.g., Cong and He 2019; Yeoh 2017). Our study adds to this emerging line of work and shows a few benefits and challenges of blockchain in the domain of IP protection and transfer.

Building on a bargaining model (Nash 1950), we analyze the applications and implications of blockchain in IP transactions. A set of theoretical predictions derived from our model emphasize the

complex interplay among the well-known tension between IP protection and transfer, and the emerging impact of blockchain keeper or hacker behaviors. A key insight from our theoretical propositions is that new types of uncertainties can result from new parties involved in blockchain-based decentralized consensus. Research or developer firms' perception and assessment of these uncertainties in turn drive their IP transfer decisions. Meanwhile, the widely-cited benefits of blockchain such as immutability and disintermediation are subject to utility-driven behaviors of firms, record keepers, and outside hackers. The insights from our model analysis are integrated into a conceptual framework in Figure 4.

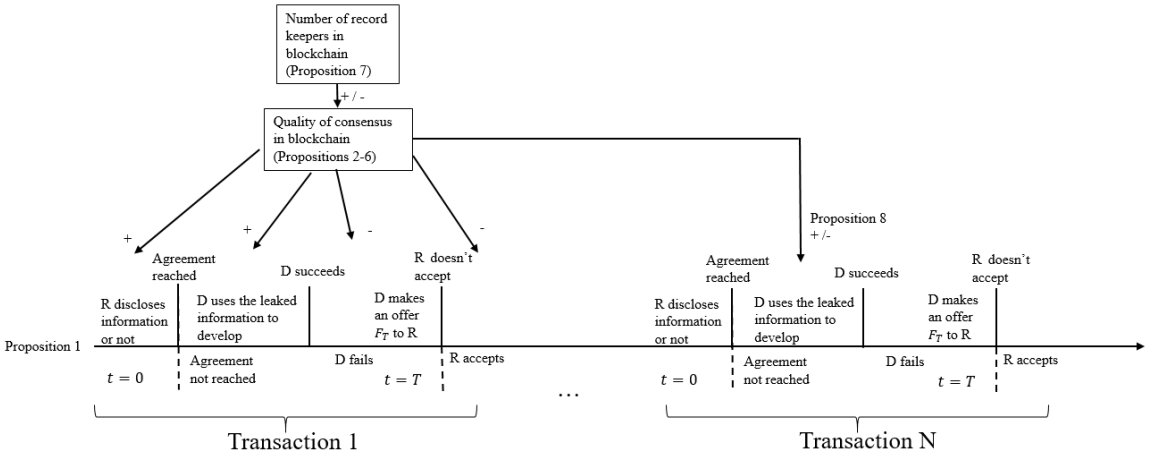


Figure 4: A conceptual framework based on our model analysis

As illustrated in Figure 4, by comparing Propositions 1, 2 and 3, we gain a basic understanding of how a blockchain system brings the potential to revert the IP transfer decisions of research firms. These propositions help to explain the increasing interests in blockchain of IP-intensive industries, such as pharmaceutical, automotive, luxury and consumer goods industries (Clark 2018; Nature, 2020; van der Waal et al., 2020). Essentially, an idealized application of blockchain can bring a Pareto optimal solution to IP transfer from research to developer firms.

History is witnessing the brave implementation of our theoretical proposals. On April 20, 2021, the company IPwe "announced plans to begin representing patents as non-fungible tokens (NFTs) or digital assets by working with IBM to create the infrastructure for representing patents as NFTs and storing the records on a blockchain network" (PRNewswire, 2021). The news releases an optimistic view about the potential of blockchain to ease IP transfer and commercialization. Investors and innovators are looking forward to this new form of liquidity to their IP asset class. In a most recent

technology update, it is reported that among gainers, IBM rose 3.8% after disclosing plans to work with privately held IPwe to transform its patented technology and other digital assets into non-fungible tokens (NFT) secured by the IBM blockchain network (MT Newswires, 2021). In addition, blockchain adoption is experiencing remarkable growth in multiple industries, encompassing finance, manufacturing, and entertainment sectors. Prominent finance corporate Visa and manufacturing leader Dell, for example, are at the forefront of utilizing blockchain to improve patent and digital rights management (Forbes, 2020; Mahony et al., 2023). Entertainment giants such as Marvel, Disney, and Warner Bros. pioneer the authorizing and selling of digital content as NFTs on blockchains to resolve the long-standing online streaming piracy issues (Forbes, 2022b; PRNewswire, 2023b; Zacks Equity Research, 2023). Bonhams, head of digital art, said that "Through NFTs, we are able to crystalize unique performances, and own and collect what would otherwise be intangible." (Sherwood, 2021). Leveraging blockchain technology, these firms could safely control content access, meticulously track content rights, and efficiently ensure royalty collection.

Notably, consistent with our theoretical predictions, emerging markets with relatively lower levels of traditional IP protection exhibit a propensity for more proactive exploration of blockchain technologies. In African and Latin American markets, such as Nigeria, Colombia, and El Salvador, governments have taken the lead in establishing national blockchain-based platforms for IP transfer and entity information identification (AIBC, 2022). Particularly, the Nigeria national IP rights wallet project, launched in 2022, stands as one of the largest crypto initiatives globally. This ambitious project aims to facilitate the international commercialization of various forms of IP rights, including trademarks, patents, and streaming, through blockchain-enabled agreements (PRNewswire, 2022).

Nevertheless, for firms considering blockchain-based IP protection and transfer, our study provides a balanced view of the pros and cons of using blockchain. We emphasize the concerns about the quality of decentralized consensus and causes of false records and misreporting, once we consider the strategic behaviors of blockchain record keepers. Imperfect consensus may lead to infringement risks in new forms, as seen in cases such as Hermès v. Rothschild and Nike v. StockX, where contentious NFT IP records resulted in copyright lawsuits (Ferrill & Shaw, 2023; Peltz, 2023). Propositions 2 and 3 reveal

three key contingencies in IP transfer decisions, namely the quality of decentralized consensus, the value of the invention, and the degree of patent protection. These propositions taken together suggest that blockchain is not a plug-and-play solution; instead, firms require knowledge about blockchain technology and blockchain user behaviors in order to optimize their IP protection and transfer decisions. Propositions 4, 5, and 6 reveal three key contingencies in IP transfer decisions, namely the quality of decentralized consensus, the value of the invention, and the firm ability to accurately assess the quality of the consensus. These propositions taken together suggest that blockchain is not a plug-and-play solution; instead, firms require the knowledge about blockchain technology and blockchain user behaviors in order to optimize their IP protection and transfer decisions.

Last but not least, Proposition 7 shows that the quality of decentralized consensus is not fully determined by factors within a blockchain community. Outside hackers can exploit technical vulnerabilities in a blockchain system to harm both research and developer firms' interests. In 2022, losses due to crypto hacking surged to $3.8 billion, notably surpassing the $3.3 billion recorded in 2021 (CNBC, 2023). For firms considering the utilization of blockchain for managing IP transfers, a thorough evaluation of cyberattack risks is imperative. While casual intuition about blockchain advocates the benefit of large blockchain communities, our model analysis shows potential concerns about the size of the community.

Propositions 4 to 8 lead to the insights that a realistic application of blockchain is likely to generate a multi-party game among firms, blockchain record keepers, and hackers. Finding optimal solutions in such a game requires a holistic understanding of the economics of IP, the technology capabilities of blockchain, and the utility-driven behaviors involved in a blockchain system. To this end, our theoretical model takes an initial step towards this holistic understanding. Our model bridges the IP literature and the emerging research about blockchain and crypto economics. It helps to define a new parameter space of blockchain-based IP protection and transfer solutions.

Our model setup and analysis are subject to several limitations and thereby invite future work. The theoretical nature of our study keeps the insights abstract. Future research can conduct empirical tests to evaluate the external validity of our propositions. While acknowledging the importance of IP laws,

we abstract away their interplay with blockchain to ensure the parsimony of our model. Future research can expand the scope of our model to consider the substitution or complementarity between centralized and decentralized approaches of IP protection.

Regarding the technology design of blockchain, our model abstracts away two key considerations for real-world applications: the scalability of a blockchain application and the blockchain data origin integrity. Both issues require on-chain or off-chain solutions, whose costs can influence the decisions of the firms and record keepers. For example, a common solution to the scalability issue is to divide a blockchain network into smaller networks, namely shards, and to manage the shards in parallel (Chen et al., 2023). However, the increased difficulty in reaching a consensus across different shards can deter research firms from using the blockchain. This calls for future research to extend our Proposition 3 regarding the effect of an imperfect consensus on research firm participation in blockchain. Regarding data origin integrity, common solutions require intermediaries, such as an online marketplace owner, to manage the data creation and verification (Alizila, 2020; Burstall and Clark, 2017; World Economic Forum, 2020). The strategic behaviors of the intermediaries can complicate the decisions of research and developer firms. Future research can examine the generalizability of our propositions to intellectual properties embodied in physical materials such as a handbag design.

Blockchain represents the continuous trend to use emerging technologies to enable innovation. Amidst hypes and misunderstandings, our study attempts to take a balanced view of the promise and caveats of using blockchain for IP protection. We hope the theoretical model developed in this paper can provide a foundation for future research to explore other aspects of blockchain. Practically, a firm could perform a targeted analysis of its readiness to use blockchain-based solutions. IP-related blockchain systems could also learn from this research to operate with both caution and confidence. Given the concerns about blockchain revealed by our analysis, it is unlikely for blockchain to replace institution-based IP protection in the near future. Instead, blockchain can alleviate the bottleneck effect of the centralized approach of IP protection on information dissemination. Blockchain systems have the potential to serve as a complementary solution to speed up knowledge sharing in collaborative innovation projects such as vaccine development.

REFERENCE

[1] AIBC, Blockchain technology: The future of Africa's digital economy. https://aibc.world/news/blockchain-technology-the-future-of-africas-digital-economy/, 2022 (accessed 27 September 2022).

[2] Alizila. 2020. Alibaba ipr report demonstrates brand-protection leadership. https://www.alizila.com/alibaba-ipr-report-demonstrates-brand-protection-leadership

[3] H. Alsabah, A. Capponi, 2020. Pitfalls of Bitcoin's Proof-of-Work: R&D arms race and mining centralization, SSRN 3273982. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273982

[4] D. Amiram, E. Lyandres, D. Rabetti, 2020. Competition and Product Quality: Fake Trading on Crypto Exchanges, SSRN 3745617. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745617

[5] J. Abadi, M. Brunnermeier, 2018. Blockchain economics, in National Bureau of Economic Research, SSRN 25407. https://www.nber.org/papers/w25407

[6] B.N. Anand, T. Khanna, The Structure of Licensing Contracts, The Journal of Industrial Economics, 48(1) (2000) 103-135. https://onlinelibrary.wiley.com/doi/abs/10.1111/1467-6451.00114

[7] J.J. Anton, D.A. Yao, Little Patents and Big Secrets: Managing Intellectual Property, The RAND Journal of Economics, 35(1) (2004) 1-22. http://www.jstor.org/stable/1593727

[8] A. Arora, A. Fosfuri, A. Gambardella, Markets for Technology and their Implications for Corporate Strategy, Industrial and Corporate Change, 10(2) (2001) 419-451. https://doi.org/10.1093/icc/10.2.419

[9] K. Arrow, Economic welfare and the allocation of resources for invention, in: The rate and direction of inventive activity: Economic and social factors, Princeton University Press, 1962, pp. 609-626.

[10] K.J. Arrow, The limits of organization, WW Norton & Company, 1974.

[11] Bao, W., Hudders, L., Yu, S., & Beuckels, E. (2024). Virtual luxury in the metaverse: NFT-enabled value recreation in luxury brands. *International Journal of Research in Marketing*.

[12] M. Bartoletti, L. Pompianu, An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns, in, (Springer International Publishing, Cham, 2017), pp. 494-509.BB

[13] D. Batista, H. Kim, V.L. Lemieux, H. Stancic, C. Unnithan, Blockchains and Provenance: How a Technical System for Tracing Origins, Ownership and Authenticity Can Transform Social Trust, in: V.L. Lemieux, C. Feng Eds. Building Decentralized Trust: Multidisciplinary Perspectives on the Design of Blockchains and Distributed Ledgers, (Springer International Publishing, Cham, 2021), pp. 111-128.

[14] B.D.Baysinger, R.D. Kosnik, T.A. Turk, Effects of Board and Ownership Structure on Corporate R&D Strategy, Academy of Management Journal, 34(1) (1991) 205-214. https://journals.aom.org/doi/abs/10.5465/256308S. Bechtold, F. Höffler, An Economic Analysis of Trade-Secret Protection in Buyer-Seller Relationships, The Journal of Law, Economics, and Organization, 27(1) (2009) 137-158. https://doi.org/10.1093/jleo/ewp020

[15] S. Bhattacharya, S. Guriev, Patents vs. Trade Secrets: Knowledge Licensing and Spillover, Journal of the European Economic Association, 4(6) (2006) 1112-1147. https://doi.org/10.1162/JEEA.2006.4.6.1112

[16] K. Binmore, A. Rubinstein, A. Wolinsky, The Nash Bargaining Solution in Economic Modelling, The RAND Journal of Economics, 17(2) (1986) 176-188. http://www.jstor.org/stable/2555382

[17] M. Boldrin, D. Levine, The case against intellectual property, The American Economic Review, 92(2) (2002) 209-212. 10.1257/000282802320189267

[18] Bloomberg, Crypto Coin Bitcoin SV Appears to Have Faced a '51% Attack.' https://www.bloomberg.com/news/articles/2021-08-04/crypto-coin-bitcoin-sv-appears-to-have-suffered-a-51-attack, 2021 (accessed 4 August 2021).

[19] R. Burstall, B. Clark, Blockchain, IP and the fashion industry, Managing Intell. Prop, 266(2017) 9.
[20] C. Catalini, J.S. Gans, Some simple economics of the blockchain, *Communications of the ACM*, *63*(7)(2020) 80-90.
[21] Check Point Research, Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/, 2023 (accessed 5 January 2023).
[22] Chen, W., Zheng, Z., Huang, H., SpringerLink (Online service), & Springer Nature - Springer Computer Science eBooks 2023 English International. (2023). In Chen W., Zheng Z. and Huang H.(Eds.), Blockchain scalability (1st 2023.;1; ed.). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-1059-5
[23] CNBC, Crypto investors lost nearly $4 billion to hackers in 2022. https://www.cnbc.com/2023/02/04/crypto-investors-lost-nearly-4-billion-dollars-to-hackers-in-2022.html, 2023 (accessed 4 April 2023).
[24] M A.V. Chaban, How can technology inject trust and reliability in vaccine distribution? Blockchain and cloud offer government and healthcare leaders new visibility into a historic vaccine rollout. https://www.ibm.com/blogs/industries/vaccination-management-ibm-blockchain-covid-19-vaccines/ 2021 (accessed 21 January 2021).
[25] S.F. Cheng, G.D. Franco, H. Jiang, P. Lin, Riding the Blockchain Mania: Public Firms' Speculative 8-K Disclosures, Management Science, 65(12) (2019) 5901-5913. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2019.3357
[26] J. Chod, E. Lyandres, A Theory of ICOs: Diversification, Agency, and Information Asymmetry, Management Science, 67(10) (2021) 5969-5989. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2020.3754
[27] J. Chod, N. Trichakis, G. Tsoukalas, H. Aspegren, M. Weber, On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption, Management Science, 66(10) (2020) 4378-4396. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2019.3434
[28] CNBC, Crypto investors lost nearly $4 billion to hackers in 2022. https://www.cnbc.com/2023/02/04/crypto-investors-lost-nearly-4-billion-dollars-to-hackers-in-2022.html, 2023 (accessed 4 April 2023).
[29] Colicev, A. (2023). How can non-fungible tokens bring value to brands. *International Journal of Research in Marketing*, *40*(1), 30-37.
[30] L.W. Cong, Z. He, Blockchain Disruption and Smart Contracts, The Review of Financial Studies, 32(5) (2019) 1754-1797. https://doi.org/10.1093/rfs/hhz007
[31] L.W. Cong, Y. Xiao, Categories and Functions of Crypto-tokens, In: *The Palgrave Handbook of FinTech and Blockchain*. Palgrave Macmillan, Cham, 2021, pp. 267-284.
[32] L.W. Cong, X. Li, K. Tang, Y. Yang, 2020. Crypto Wash Trading, National Bureau of Economic Research, #30783, https://www.nber.org/papers/w30783.
[33] P. Csóka, P.J.-J. Herings, Decentralized Clearing in Financial Networks, Management Science, 64(10) (2018) 4681-4699. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2017.2847
[34] E. Deirmentzoglou, G. Papakyriakopoulos, C. Patsakis, A Survey on Long-Range Attacks for Proof of Stake Protocols, IEEE Access, 7(2019) 28712-28725.
[35] Ding, M. A., & Wang, X. S. (2023). The Effect of Image-Audio Emotional Similarity on NFT Product Sales. *Xin (Shane), The Effect of Image-Audio Emotional Similarity on NFT Product Sales (June 26, 2023)*.
[36] News Desk, A rise in cyberattacks reported in third quarter of 2022. https://techxmedia.com/a-rise-in-cyberattacks-reported-in-third-quarter-of-2022/, 2022 (accessed 11 November 2022).
[37] Eyal, E.G. Sirer, Majority is not enough, Communications of the ACM, 61(7) (2018) 95-102.
[38] D. Ferreira, J. Li, R. Nikolowa (2023). Corporate capture of blockchain governance. *The Review of Financial Studies*, *36*(4), 1364-1407.

[39] Ferrill, E. D., & Shaw, S. Digital IP's New Frontier. Best Lawyers. https://www.bestlawyers.com/article/explosive-growth-of-nfts-and-blockchain-technology/5284, 2023 (accessed 18 June 2023).
[40] Forbes, OpenSea NFT Marketplace Review, https://www.forbes.com/advisor/investing/cryptocurrency/opensea-nft-marketplace/, 2022a (accessed 6 December 2022).
[41] Forbes, Entertainment Industry Pushes to Shift Intellectual Property to Web3. https://www.forbes.com/sites/joshwilson/2022/04/20/entertainment-industry-pushes-to-shift-intellectual-property-to-web3/, 2022b (accessed 20 April 2022).
[42] Forbes, Visa Applies for Digital Dollar Blockchain Patent. https://www.forbes.com/sites/jasonbrett/2020/05/14/visa-submits-patent-application-for-digital-dollar-using-blockchain/, 2020 (accessed 14 May 2020).
[43] Forbes, Spotify has acquired blockchain startup mediachain. https://www.forbes.com/sites/hughmcintyre/2017/04/27/spotify-has-acquired-blockchain-startup-mediachain/?sh=78185b8e69ee, 2017 (accessed 27 April 2017).
[44] Forbes, The entire concept of intellectual property Is proof that free markets aren't perfect. https://www.forbes.com/sites/timworstall/2015/01/25/the-entire-concept-of-intellectual-property-is-proof-that-free-markets-arent-perfect/?sh=f00e3c64e0a2, 2015 (accessed 25 Jan, 2015).
[45] Fortune, Commentary: How copyright violations can crash your NFT party. https://fortune.com/2021/08/04/nfts-copyright-violations-penalties-non-fungible-tokens-collectibles-nfttorney-jonathan-schmalfeld/, 2021 (accessed 4 August 2021).
[46] J.S. Gans, D.H. Hsu, S. Stern, When does start-up innovation spur the gale of creative destruction? in, (National bureau of economic research Cambridge, Mass., USA, 2000).
[47] J.S. Gans, D.H. Hsu, S. Stern, The Impact of Uncertain Intellectual Property Rights on the Market for Ideas: Evidence from Patent Grant Delays, Management Science, 54(5) (2008) 982-997. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1070.0814
[48] Gartner, With blockchain, it's garbage in – garbage forever. https://blogs.gartner.com/avivah-litan/2020/10/23/with-blockchain-its-garbage-in-garbage-forever/, 2020 (accessed 23 October 2020).
[49] M. Gittelman, B. Kogut, Does Good Science Lead to Valuable Knowledge? Biotechnology Firms and the Evolutionary Logic of Citation Patterns, Management Science, 49(4) (2003) 366-382. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.49.4.366.14420
[50] Gupta, R., & Kumar, A. (2020). Challenges in Information Disclosure in the Indian Pharmaceutical Industry. *Journal of Intellectual Property Rights*, 25(3), 231-245.
[51] Hall, B. H., Helmers, C., Rogers, M., & Sena, V. (2014). The Choice Between Formal and Informal Intellectual Property: A Review. Journal of Economic Literature, 52(2), 375-423.
[52] B.H. Hall, R.H. Ziedonis, The Patent Paradox Revisited: An Empirical Study of Patenting in the U.S. Semiconductor Industry, 1979-1995, The RAND Journal of Economics, 32(1) (2001) 101-128. http://www.jstor.org/stable/2696400
[53] R. Henry, A. Herzberg, A. Kate, Blockchain Access Privacy: Challenges and Directions, IEEE Security & Privacy, 16(4) (2018) 38-45.
[54] N. Jia, K.G. Huang, C.M. Zhang, Public Governance, Corporate Governance, and Firm Innovation: An Examination of State-Owned Enterprises, Academy of Management Journal, 62(1) (2019) 220-247. https://journals.aom.org/doi/abs/10.5465/amj.2016.0543
[55] N. Kannengießer, S. Lins, T. Dehling, A. Sunyaev, Trade-offs between Distributed Ledger Technology Characteristics, ACM Computing Surveys, 53(2) (2020) 1-37.
[56] J. Korn, Report: $1.9 billion stolen in crypto hacks so far this year. https://www.cnn.com/2022/08/16/tech/crypto-hack-rise-2022/index.html, 2022 (accessed 16 August, 2022).
[57] Joo, M., Kim, S. H., Ghose, A., & Wilbur, K. C. (2023). Designing Distributed Ledger technologies, like Blockchain, for advertising markets. *International Journal of Research in Marketing*, *40*(1), 12-21.

[58] A. Lehar, C.A. Parlour, Miner collusion and the bitcoin protocol, Available at SSRN 3559894, (2020).
[59] Z. Li, J. Kang, D. Ye, Q. Deng, Y. Zhang, Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 14(8) (2017) 3690-3700..
[60] LVMH, LVMH partners with other major luxury companies on Aura, the first global luxury blockchain. https://www.lvmh.com/news-documents/news/lvmh-partners-with-other-major-luxury-companies-on-aura-the-first-global-luxury-blockchain/, 2021 (accessed 20 April 2021).
[61] Mahony, I., Colandreo, B., & Schneider, J. Blockchain and intellectual property: A case study. In Blockchain & Cryptocurrency Regulation 2023, USA, (2023). https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/03-blockchain-and-intellectual-property-a-case-study
[62] Malik, N., Appel, G., & Luo, L. (2023). Blockchain technology for creative industries: Current state and research opportunities. *International Journal of Research in Marketing*, *40*(1), 38-48.
[63] Marthews, A., & Tucker, C. (2023). What blockchain can and can't do: Applications to marketing and privacy. *International Journal of Research in Marketing*, *40*(1), 49-53.
[64] D.C. Mowery, The relationship between intrafirm and contractual forms of industrial research in American manufacturing, 1900–1940, Explorations in Economic History, 20(4) (1983) 351-374. https://www.sciencedirect.com/science/article/pii/0014498383900244
[65] MT Newswires, Technology Sector Update for 04/20/2021: XRX, VLDR, CRWD, IBM. https://www.nasdaq.com/articles/technology-sector-update-for-04-20-2021%3A-xrxvldrcrwdibm-2021-04-20, 2021 (accessed 29 April 2021).
[66] J.F. Nash, The Bargaining Problem, Econometrica, 18(2) (1950) 155-162. http://www.jstor.org/stable/1907266
[67] National Law Review, The NFT collection: the rise of NFTs – copyright strikes back? (Part 3). https://www.natlawreview.com/article/nft-collection-rise-nfts-copyright-strikes-back-part-3, 2022 (accessed 7 July 2022).
[68] Nature, Coronavirus: everyone wins when patents are pooled [editorial], Nature, 581 (2020) 240.
[69] M. J. Osborne, A. Rubinstein, A Course in Game Theory, MIT Press,1994.
[70] J.E. Oxley, Institutional environment and the mechanisms of governance: the impact of intellectual property protection on the structure of inter-firm alliances, Journal of Economic Behavior & Organization, 38(3) (1999) 283-309. https://www.sciencedirect.com/science/article/pii/S0167268199000116
[71] Peltz, M., A Landmark Decision for Trademarks and NFTs. Falcon Rappaport & Berkman LLP. https://frblaw.com/hermes-v-rothschild-a-landmark-decision-for-trademarks-and-nfts/, 2023 (accessed 10 February 2023).
[72] Peres, R., Schreier, M., Schweidel, D. A., & Sorescu, A. (2023). Blockchain meets marketing: Opportunities, threats, and avenues for future research. *International Journal of Research in Marketing*.
[73] D. Popp, T. Juhl, D. K. Johnson, Time in purgatory: Examining the grant lag for US patent applications. Topics in Economic Analysis & Policy, 4(1)(2004) 1-45.
[74] PRNewswire, The Flash Web3 Movie Experience. https://www.prnewswire.com/news-releases/the-flash-web3-movie-experience-301877298.html, 2023 (accessed 14 July 2023).
[75] PRNewswire, Nigeria to Launch Major Crypto Initiative, IP Exchange Marketplace and Wallet, on Algorand in Partnership with Developing Africa Group and Koibanx. https://www.prnewswire.com/news-releases/nigeria-to-launch-major-crypto-initiative-ip-exchange-marketplace-and-wallet-on-algorand-in-partnership-with-developing-africa-group-and-koibanx-301553306.html, 2022 (accessed 23 May 2022).

[76] PRNewswire, IPwe and IBM seek to transform corporate patents with next generation NFTs using IBM blockchain, IBM News Room, https://newsroom.ibm.com/2021-04-20-IPwe-and-IBM-Seek-to-Transform-Corporate-Patents-With-Next-Generation-NFTs-Using-IBM-Blockchain, 2021 (accessed 28 April 2021).
[77] H. Pun, J.M. Swaminathan, P. Hou, Blockchain Adoption for Combating Deceptive Counterfeits, Production and Operations Management, 30(4) (2021) 864-882. https://onlinelibrary.wiley.com/doi/abs/10.1111/poms.13348
[78] J. Redman, World's largest online art gallery deviantart collaborates with opensea to detect potential NFT infringement – blockchain bitcoin news. https://news.bitcoin.com/worlds-largest-online-art-gallery-deviantart-collaborates-with-opensea-to-detect-potential-nft-infringement/, 2021 (accssed 20 August 2021)
[79] Rimmer, M. (2019). *Intellectual Property and Climate Change: Inventing Clean Technologies*. Edward Elgar Publishing. ISBN: 9781785368366.
[80] P. Romer, When Should We Use Intellectual Property Rights? American Economic Review, 92(2) (2002) 213-216. https://www.aeaweb.org/articles?id=10.1257/000282802320189276
[81] Shavell, S., & Van Ypersele, T. (2001). Rewards versus intellectual property rights. *The Journal of Law and Economics*, *44*(2), 525-547.
[82] Sherwood, H. Royal Ballet dancer to auction world's first ballet NFTs. *Guardian*, Nov. 29, 2021. https://www.theguardian.com/stage/2021/nov/29/royal-ballet-dancer-natalia-osipova-to-auction-worlds-first-ballet-nfts Accessed May 28, 2024.
[83] J. Schmalfeld, Commentary: How copyright violations can crash your NFT party. Fortune. https://fortune.com/2021/08/04/nfts-copyright-violations-penalties-non-fungible-tokens-collectibles-nfttorney-jonathan-schmalfeld/, 2021 (accessed 4 August 2021).
[84] D. Shores, Breaking Down Moderna's COVID-19 Patent Pledge: Why Did They Do It? https://ipwatchdog.com/2020/11/11/breaking-modernas-covid-19-patent-pledge/id=127224/ 2020 (accessed 11 November 2020).
[85] SiliconANGLE. Tech Mahindra adopts IBM Blockchain to power digital rights management for entertainment. https://siliconangle.com/2020/07/08/tech-mahindra-adopts-ibm-blockchain-power-digital-rights-management-entertainment/, 2020 (accessed 8 July 2020)
[86] Sonoco Products, Sonoco ThermoSafe Creating Industrywide PharmaPortalTM Platform Using IBM Blockchain Technology to Help Deliver Improved Transparency and Traceability across the Temperature Controlled Pharmaceutical Supply Chain, GlobeNewswire News Room, https://www.globenewswire.com/news-release/2020/07/30/2070160/26553/en/Sonoco-ThermoSafe-Creating-Industrywide-PharmaPortal-Platform-Using-IBM-Blockchain-Technology-To-Help-Deliver-Improved-Transparency-and-Traceability-Across-the-Temperature-Controll.html, 2020 (accessed 30 July 2020).
[87] D. Tapscott, A. Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world, Penguin, 2016.
[88] D.J. Teece, Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy, Research Policy, 15(6) (1986) 285-305. https://www.sciencedirect.com/science/article/pii/0048733386900272
[89] The Washington Post, What it means for the U.S. to back waivers on coronavirus vaccine patents. https://www.washingtonpost.com/world/2021/05/06/coronavirus-vaccine-patent-waiver-biden-wto/, 2021 (accessed 6 May 2021).
[90] Tirole, J. (1996). A theory of collective reputations (with applications to the persistence of corruption and to firm quality). *The Review of Economic Studies*, *63*(1), 1-22.
[91] R. Trehan, D. Bansal, S. J. Nair, Using blockchain to accelerate efficient clinical trials during a pandemic. Infosys. https://www.infosys.com/blockchain/documents/accelerate-efficient-clinical-trials-pandemic.pdf, 2020 (last accessed 9 July 2021).
[92] M.B. van der Waal, C. dos S. Ribeiro, M. Ma, G.B. Haringhuizen, E. Claassen, L.H.M. van de Burgwal, Blockchain-facilitated sharing to advance outbreak R&D, Science, 368(6492) (2020) 719-721. https://www.science.org/doi/abs/10.1126/science.aba1355

[93] W. Wen, M. Ceccagnoli, C. Forman, Opening Up Intellectual Property Strategy: Implications for Open Source Software Entry by Start-up Firms, Management Science, 62(9) (2016) 2668-2691. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2015.2247
[94] Williamson, Comparative Economic Organization: The Analysis of Discrete Structural Alternatives, Administrative Science Quarterly, 36(2) (1991) 269-296. http://www.jstor.org/stable/2393356
[95] World Economic Forum, The future of financial infrastructure. http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf, 2017 (accessed 28 April 2017).
[96] World Economic Forum, 2020. Redesigning Trust: Blockchain Deployment Toolkit. Online material retrieved from https://widgets.weforum.org/blockchain-toolkit/data-integrity
[97] WTO, Waiver from certain provisions of the trips agreement for the prevention, containment and treatment of Covid-19. Document Symbol IP/C/W/672, 2021 (accessed 25 May 2021).
[98] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of blockchain-based systems for architecture design, in: 2017 IEEE International Conference on Software Architecture (ICSA), (2017), pp. 243-252.
[99] D. Yaga, P. Mell, N. Roby, K. Scarfone, 2019, Blockchain technology overview. arXiv:1906.11078. https://arxiv.org/abs/1906.11078
[100] Yang, F., Shi, Y., Wu, Q., Li, F., Zhou, W., Hu, Z., ... & Zhang, Y. (2019, May). The survey on intellectual property based on blockchain technology. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)* (pp. 743-748). IEEE.
[101] P. Yeoh, Regulatory issues in blockchain technology, Journal of Financial Regulation and Compliance, 25(2) (2017) 196-208. https://doi.org/10.1108/JFRC-08-2016-0068
[102] D. Yermack, Corporate governance and blockchains*, Review of Finance, 21(1) (2017) 7-31. https://doi.org/10.1093/rof/rfw074
[103] F. Yiannas, A new era of food transparency powered by blockchain, Innovations: Technology, Governance, Globalization, 12(1-2) (2018) 46-56. https://doi.org/10.1162/inov_a_00266
[104] Zacks Equity Research, Warner Bros. Discovery (WBD) Embraces Blockchain in The Flash. https://www.nasdaq.com/articles/warner-bros.-discovery-wbd-embraces-blockchain-in-the-flash, 2023 (accessed 17 July 2023).
[105] L. Zhang, Intellectual Property Strategy and the Long Tail: Evidence from the Recorded Music Industry, Management Science, 64(1) (2018) 24-42. https://pubsonline.informs.org/doi/abs/10.1287/mnsc.2016.2562

Appendix A: Mathematical Proofs

A.1 Proofs of Proposition 1 and Corollary 1

Given the strategy sets of the research R and the developer D firms, there are three possible cases of IP transfer. Our proof is organized into the three cases below.

Case 1: If an IP transfer agreement is reached at $t = T$, the developer firm can distinguish between the inventions with a high- or low-value whether the research firms disclose information at $t = 0$ or not. Correspondingly, the utility of the research firm i is: $RU_{Ti}^{w} = F_{Ti}^{w} - c_i$, the utility for the developer firm is: $DU_{Ti}^{w} = \delta^T v_i - F_{Ti}^{w}$. If the agreement is not reached, then the expected utility for the research firm is $RU_{Tin}^{w} = -c_i$, and that for the developer firm is $DU_{Tin}^{w} = 0$. Then the two firms will bargain on the licensing fee, $\max_{F_{Ti}^{w}} \left((\delta^T v_i - F_{Ti}^{w} - 0)^{\alpha}\left(F_{Ti}^{w} - c_i - (0 - c_i)\right)^{1-\alpha}\right)$. To solve the problem, we take the logarithm of the objective function and obtain: $\max_{F_{Ti}^{w}}[\alpha \cdot Log(\delta^T v_i - F_{Ti}^{w}) + (1-\alpha) Log F_{Ti}^{w}]$. The first order condition is: $\frac{-\alpha}{\delta^T v_i - F_{Ti}^{h}} + \frac{1-\alpha}{F_{Ti}^{h}} = 0$, and the second order condition is: $\frac{-\alpha}{\left(\delta^T v_i - F_{Ti}^{h}\right)^2} - \frac{1-\alpha}{\left(F_{Ti}^{h}\right)^2} < 0$. Solving the problem, we obtain: $F_{Ti}^{w} = (1-\alpha)\delta^T v_i$.

Case 2: The research firm i ($i = 1,2$) withholds information, and the agreement is reached at $t = 0$. In this case, the developer firm cannot distinguish between the high- and low-value inventions. The utility of the research firm i is: $RU_{0i}^{w} = F_0^{w} - c_i$. The utility for the developer firm is: $DU_{0i}^{w} = pv_H + (1-p)v_L - F_0^{w}$. If the agreement is not reached at $t = 0$, then the expected utility of the research firm is $RU_{Ti}^{w} = \begin{cases} F_{Ti}^{w} - c_i, if\ the\ agreement\ is\ reached\ at\ t = T \\ -c_i, \qquad \text{no agreement is reached} \end{cases}$

The utility of the developer firm is $DU_{Ti}^{w} = \begin{cases} \delta^T v_i - F_{Ti}^{w}, if\ the\ agreement\ is\ reached\ at\ t = T \\ 0 \qquad \text{no agreement is reached} \end{cases}$.

In Case 1, we demonstrate that the optimal licensing fee when the firms prefer to reach an agreement. Therefore, the two firms will bargain on signing at $t = 0$ over $t = T$, $\max_{F_0^h} \left(\left(pv_H + (1-p)v_L - F_0^{w} - (\delta^T v_i - F_{Ti}^{w})\right)^{\alpha}\left(F_0^{w} - c_i - (F_{Ti}^{w} - c_i)\right)^{1-\alpha}\right)$, plugging the optimal $F_{Ti}^{w} = (1-\alpha)\delta^T v_i$ into the function and solving the problem, we obtain: $F_0^{w} = (1-\alpha)(pv_H + (1-p)v_L)$.

Case 3: The research firm i ($i = 1,2$) discloses information, and the agreement is signed at $t = 0$. When research firm i discloses information, the developer firm can distinguish between the high- and low-value inventions at $t = 0$. However, the developer firm may choose to use the disclosed information to commercialize the invention without licensing. If the agreement is reached at $t = 0$, then the research firm i will get F_{0i}^d. If the agreement is not reached, then there is a possibility of μ that the developer firm can succeed. If the developer firm fails, it still can make an offer to the research firm at $t = T$. Therefore, the expected utility of the research firm i by signing the agreement at $t = 0$ is: $RU_{0i}^d = F_{0i}^d - c_i$, and that of the developer firm is: $DU_{0i}^d = v_i - F_{0i}^d$. Then the two firms will bargain on the licensing fee, which is, $\max_{F_{0i}^d}\left(\left(v_i - F_{0i}^d - \left(\mu v_H + (1-\mu)\left(\delta^T v_i - F_{Ti}^d\right)\right)\right)^{\alpha}\left(F_{0i}^d - c_i - \left((1-\mu)F_{Ti}^d - c_i\right)\right)^{1-\alpha}\right)$. Solving the problem, we obtain that: $F_{0i}^d = (1-\alpha)(1-\mu)v_i$.

Here, we can compare the cases when research firm with a high-value invention withholding information and disclosing information. We denote $DU_H(d,0) = DU_{0H}^d$, $DU_H(w,0) = DU_{0H}^w$, $DU_L(d,0) = DU_{0L}^d$, $DU_L(w,0) = DU_{0L}^w$, $F_H(d,0) = F_{0H}^d$, $F_H(w,0) = F_{0H}^w$, $F_H(d,T) = F_{TH}^d$ $F_H(w,T) = F_{TH}^h$, $F_L(d,0) = F_{0L}^d$, $F_L(w,0) = F_{0L}^w$, $F_L(d,T) = F_{TL}^d$, $F_L(w,T) = F_{TL}^w$.

(a) We can then obtain the following:

$DU_H(d,0) - DU_H(w,0) = (\alpha + \mu + \alpha\mu)v_1 - \alpha(pv_1 + (1-p)v_2) \geq \alpha v_1 + \mu v_1 - \alpha v_1 \geq 0,$

$DU_L(d,0) - DU_L(w,0) = 0, DU_H(d,T) - DU_H(w,T) = 0, DU_L(d,T) - DU_L(w,T) = 0.$

Therefore, the developer firm is always better off when the research firm discloses information about the invention.

(b) For the research firm with a low-value invention, $F_L(w,0) - F_L(w,T) = (1-\alpha)(pv_H + (1-p)v_L) - (1-\alpha)\delta^T v_L \geq (1-\alpha)v_L - (1-\alpha)\delta^T v_L \geq (1-\alpha)(1-\delta^T)v_L \geq 0$, $F_L(d,0) - F_L(d,T) = (1-\alpha)v_L - (1-\alpha)\delta^T v_L \geq (1-\alpha)(1-\delta^T)v_L \geq 0,$

Therefore, for R_L, the optimal strategy is always licensing at $t = 0$.

(c) For the research firm with a high-value invention (R_h), it prefers to disclose information and sign at $t = 0$ if and only if $\begin{cases} F_H(d,0) \geq F_H(w,0) \\ F_H(d,0) \geq F_H(w,T) \end{cases}$, which implies that

$$\begin{cases} F_H(d,0) - F_H(w,0) = (1-\mu)(1-\alpha)v_H - (1-\alpha)(pv_H + (1-p)v_L) \geq 0 \\ F_H(d,0) - F_H(w,T) = (1-\mu)(1-\alpha)v_H - (1-\alpha)\delta^T v_H \geq 0 \end{cases} \Rightarrow$$

$\begin{cases} 0 \leq \mu \leq \frac{(1-p)(v_H - v_L)}{v_H} \\ 0 \leq \mu \leq 1 - \delta^T \end{cases}$, that is, $0 \leq \mu \leq min\left\{\frac{(1-p)(v_H - v_L)}{v_H}, 1-\delta^T\right\}$, then the separating equilibrium is sustainable.

For R_h, if $\begin{cases} F_H(d,0) \leq F_1(w,0) \\ F_H(d,0) \geq F_1(w,T) \end{cases}$, it prefers to withhold information, and pool with R_L, which implies that $\begin{cases} F_H(d,0) - F_H(w,0) = (1-\mu)(1-\alpha)v_H - (1-\alpha)(pv_H + (1-p)v_L) \leq 0 \\ F_H(d,0) - F_H(w,T) = (1-\mu)(1-\alpha)v_H - (1-\alpha)\delta^T v_H \geq 0 \end{cases} \Rightarrow$

$\begin{cases} \frac{(1-p)(v_H - v_L)}{v_H} \leq \mu \leq 1 \\ 0 \leq \mu \leq 1 - \delta^T \end{cases}$, that is, $\frac{(1-p)(v_H - v_L)}{v_H} \leq \mu \leq 1 - \delta^T$, then the pooling equilibrium is sustainable.

For R_h, if $\begin{cases} F_H(d,0) \geq F_H(w,0) \\ F_H(d,0) \leq F_H(w,T) \end{cases}$, then it prefers to withhold information and sign the agreement with D at $t = T$, which implies that $\begin{cases} F_H(d,0) - F_H(w,0) = (1-\mu)(1-\alpha)v_H - (1-\alpha)(pv_H + (1-p)v_L) \geq 0 \\ F_H(d,0) - F_H(w,T) = (1-\mu)(1-\alpha)v_H - (1-\alpha)\delta^T v_H \leq 0 \end{cases} \Rightarrow$

$\begin{cases} 0 \leq \mu \leq \frac{(1-p)(v_H - v_L)}{v_H} \\ 1 - \delta^T \leq \mu \leq 1 \end{cases}$, that is, $1 - \delta^T \leq \mu \leq \frac{(1-p)(v_H - v_L)}{v_H}$, then the separating equilibrium is sustainable.

A.2 Proof of Proposition 2

With perfect consensus in the blockchain, if the developer firm D uses the information disclosed by the research firm to commercialize the invention, such action can be traced and exposed by blockchain records. This deters D from infringing on the disclosed information, which in turn alleviates the concern of the research firm to disclose information. Thus, the utility for R_H to disclose information and sign an agreement at $t = 0$ is: $RU_{0H}^b = F_{0H}^b - c_H$, and the utility for D is: $DU_{0H}^b = v_H - F_{0H}^b$. If the agreement does not reach at $t = 0$, then the expected utility for the research firm is $RU_{TH}^b = (1-\alpha)\delta^T v_H - c_H$, and that for the developer firm is $DU_{Ti}^b = \alpha\delta^T v_i$. Then the research firm and the developer firm bargain on the licensing fee, $\max_{F_{Ti}^b}\left(\left(v_H - F_{0H}^b - \alpha\delta^T v_H\right)^{\alpha}\left(F_{0H}^b - c_H - c_0 - \left((1-\alpha)\delta^T v_H - c_H - c_0\right)\right)^{1-\alpha}\right)$.

Solving the problem, we obtain: $F_{0H}^b = (1-\alpha)v_H$, $RU_{0H}^b = (1-\alpha)v_H - c_H - c_0$. Since we know that if R_H withholds information, the utility it can achieve is: $RU_{0H}^w = (1-\alpha)(pv_H + (1-p)v_L) - c_H$. And, $RU_{0H}^b - RU_{0H}^w = (1-\alpha)(1-p)(v_H - v_L) - c_0$. Since $c_0 < (1-\alpha)(1-p)(v_H - v_L)$, we get $RU_{0H}^b \geq RU_{TH}^b$. Therefore, with perfect consensus, R_H prefers to disclose information at $t = 0$.

A.3 Proof of Proposition 3

Under imperfect consensus, if the research firm discloses information, the expected utility of signing an agreement at $t = 0$ is: $RU_{0H}^b = F_{0H}^b - c_H$, and the utility for the developer firm is: $DU_{0H}^b = v_H - F_{0H}^b$. If the agreement is not reached at $t = 0$, the expected utility for the research firm is $RU_{TH}^b = \mu\varphi C + (1-\mu)F_{TH}^b - c_H - c_0$, and that for the developer firm is $DU_{TH}^b = \mu(v_H - \varphi C) + (1-\mu)\left(\delta^T v_H - F_{TH}^b\right)$. Then the research firm and the developer firm bargain on the licensing fee, $\max_{F_{0H}^b}\left(\left(v_H - F_{0H}^b - \left(\mu(v_H - \varphi C) + (1-\mu)\left(\delta^T v_H - F_{TH}^b\right)\right)\right)^{\alpha}\left(F_{0H}^b - c_H - c_0 - \left(\mu\varphi C + (1-\mu)F_{TH}^b - c_H - c_0\right)\right)^{1-\alpha}\right)$. Solving the problem, we obtain that: $F_{0H}^b = (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_H + C\mu\varphi)$, $RU_{0H}^b = (1-\alpha)\left((1-\mu+\alpha\delta^T\mu)v_H + C\mu\varphi\right) - c_H$, $DU_{0H}^b = v_H - (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_H + C\mu\varphi)$,

The research firm prefers to disclose information if and only if $\begin{cases} RU_{0H}^b \geq RU_{0H}^w \\ RU_{0H}^b \geq RU_{TH}^w \end{cases}$, implying that

$$\begin{cases} (1-\alpha)\left((1-\mu+\alpha\delta^T\mu)v_H + C\mu\varphi\right) - c_H - c_0 \geq (1-\alpha)(pv_H + (1-p)v_L) - c_H \\ (1-\alpha)\left((1-\mu+\alpha\delta^T\mu)v_H + C\mu\varphi\right) - c_H - c_0 \geq (1-\alpha)\delta^T v_H - c_H \end{cases} \Rightarrow$$

$$\begin{cases} \varphi \geq \frac{pv_H + (1-p)v_L - (1-\mu+\alpha\delta^T\mu)v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} \\ \varphi \geq \frac{[(1-\delta^T\alpha)\mu - (1-\delta^T)]v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} \end{cases}, \text{ that is,}$$

$$\varphi \geq max\left\{\frac{[(1-\delta^T\alpha)\mu - (1-\delta^T)]v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C}, \frac{pv_H + (1-p)v_L - (1-\mu+\alpha\delta^T\mu)v_H}{\mu C} + \frac{c_0}{(1-\alpha)\mu C}\right\}.$$

A.4 Proof of Proposition 4

When research and developer firms cannot observe the quality of the consensus in blockchain, and the research firm discloses information, the expected utility of the research firm when signing at $t = 0$ is: $RU_{01}^{u} = F_{01}^{u} - c_1 - c_0$, the utility for the developer firm is: $DU_{01}^{u} = v_1 - F_{01}^{u}$. If the agreement is not reached at $t = 0$, then the expected utility for the research firm is $RU_{T1}^{u} = \mu E(\varphi)C + (1-\mu)F_{T1}^{u} - c_1 - c_0$, and that for the developer firm is $DU_{T1}^{u} = \mu(v_1 - E(\varphi)C) + (1-\mu)(\delta^T v_1 - F_{T1}^{u})$. Then the research firm and the developer firm bargain on the licensing fee, $\max_{F_{T1}^{u}} \Big(\big(v_1 - F_{01}^{u} - \big(\mu(v_1 - E(\varphi)C) + (1-\mu)(\delta^T v_1 - F_{T1}^{u}) \big) \big)^{\alpha} \big(F_{01}^{u} - c_1 - c_0 - (E(\varphi)C + (1-\mu)F_{T1}^{u} - c_1 - c_0) \big)^{1-\alpha} \Big)$.

Solving the problem, we obtain that: $F_{01}^{u} = (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon))$, $RU_{01}^{u} = (1-\alpha)\big((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon)\big) - c_1 - c_0$, $DU_{01}^{u} = v_1 - (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon))$,

The research firm with a high-value invention prefers to disclose information if and only if

$\begin{cases} RU_{01}^{u} \geq RU_{01}^{h} \\ RU_{01}^{u} \geq RU_{T1}^{h} \end{cases}$, implying that

$$\begin{cases} (1-\alpha)\big((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon)\big) - c_1 - c_0 \geq (1-\alpha)(pv_1 + (1-p)v_2) - c_1 \\ (1-\alpha)\big((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon)\big) - c_1 - c_0 \geq (1-\alpha)\delta^T v_1 - c_1 \end{cases} \Rightarrow$$

$$\begin{cases} \varphi \geq \frac{pv_1 + (1-p)v_2 - (1-\mu+\alpha\delta^T\mu)v_1}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} - \epsilon \\ \varphi \geq \frac{[(1-\delta^T\alpha)\mu - (1-\delta^T)]v_1}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} - \epsilon \end{cases}$$, that is,

$$\varphi \geq max\left\{ \frac{[(1-\delta^T\alpha)\mu - (1-\delta^T)]v_1}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} - \epsilon, \frac{pv_1 + (1-p)v_2 - (1-\mu+\alpha\delta^T\mu)v_1}{\mu C} + \frac{c_0}{(1-\alpha)\mu C} - \epsilon \right\} = \varphi^U.$$

A.5 Proof of Proposition 5

From Proposition 3, we obtain that the research firm with a high-value invention (R_H) prefers to disclose information iff $\varphi \geq \tilde{\varphi}$,

1) if $\varphi \geq \tilde{\varphi}$, then R_H prefers to disclose information under the actual quality of consensus. If $\epsilon \geq 0$, then $\varphi + \epsilon \geq \tilde{\varphi}$, R_H still prefers to disclose information. The over-estimation of the quality of the consensus has no effect on R_H's decision; if $\epsilon < 0$, and $\varphi + \epsilon < \tilde{\varphi}$, that is, $\epsilon < \tilde{\varphi} - \varphi < 0$, then R_H will switch from disclosing information to withholding information.

2) If $\varphi < \tilde{\varphi}$, then R_H prefers to withhold information under the actual quality of consensus. If $\epsilon \leq 0$, then $\varphi + \epsilon < \tilde{\varphi}$, R_H still prefers to withhold information. The under-estimation of the quality of the consensus has no effect on R_H's decision; if $\epsilon > 0$, when $\varphi + \epsilon > \tilde{\varphi}$, that is, $\epsilon > \tilde{\varphi} - \varphi > 0$, then R_H will switch from withholding information to disclosing information.

A.6 Proof of Proposition 6

When the quality of the consensus in blockchain falls to $\varphi < \tilde{\varphi}$, the reputation of the blockchain falls to $\varphi = \tau$. If firms rely on blockchain for IP transfers, they can only get a licensing fee of $(1-\tau)v_L - c_0$. For the research firms with high-value inventions, they will exit the blockchain because the quality of the consensus is lower than the threshold for a profitable experience with the blockchain system.

For the research firms with low-value inventions, they will also exit the blockchain because their gain from the traditional method of IP transfer is at least $(1-\tau)v_L > (1-\tau)v_L - c_0$.

Therefore, research firms with either a high-value or a low-value invention will exit the blockchain if the quality of the consensus falls to $\varphi < \tilde{\varphi}$.

A.7 Proof of Proposition 7 and Corollary 2

The utility function of the hacker is:

$$\max_M Kv_a \cdot \left[\left(1-\varphi(K-M)\right) - \left(1-\varphi(K)\right)\right] - M \cdot c_a.$$

Solving the utility maximization problem, we obtain the first order condition:

$$K \cdot \varphi'(K-M)v_a - c_a = 0$$

where $\varphi(K) = \sum_{k\in\mathbf{K}^*} w_k \leq 1$ and $\mathbf{K}^* = \{k \in \mathbf{K}: b_k w_k < h_k\}$.

Assumption: $\frac{b_k}{h_k}$ *follows a unimodal distribution* $F(k)$.

This assumption indicates the existence of a threshold $\widehat{K}$ such that $F''(k) > 0$ when $K < \widehat{K}$ and $F''(x) \leq 0$ otherwise. It can be generalized to many distributions such as a normal distribution, Poisson distribution, etc. We use $f(x)$ to denote the probability density function of $F(x)$.

Given $\frac{1}{w_k} > \frac{b_k}{h_k}$, we can obtain $\varphi(K) = F(K)$, $f(K) = F'^{(K)}$. Consequently, $K \cdot \varphi'(K-M) = K \cdot F'(K-M)$, and $\varphi'(K-M) = f(K-M)$. We denote the threshold that the hacker has sufficient incentive to attack the blockchain system as K^*.

As $F(x)$ follows a unimodal distribution assumption, $F'(K-M)$ is maximized at $F'\left(\widehat{K} - M\right)$, and $\varphi'(K-M)$ is maximized at $\varphi'\left(\widehat{K} - M\right)$. This in turn means that:

When $K^* < \frac{c_a}{v_a f(\widehat{K}-M)}$, $KF'\left(\widehat{K} - M\right)v_a - c_a < 0$ always holds. Therefore, $M^* = 0$, and $\varphi(K-M^*)$ increases with K when $K > K^*$; the hacker has sufficient incentive to attack the blockchain system.

When $K^* > \frac{c_a}{v_a F'(\widehat{K}-M)}$, the optimal M is obtained when $F'(K-M^*) = \frac{c_a}{v_a K}$. The left-hand side of the equation represents the marginal revenue the hacker can get from attacking, while the right-hand side denotes the standardized marginal cost of the attack. It is obvious that $M^* > 0$ and $\varphi(K-M^*)$ is decreasing with K. From Section 4, we obtain that there exists a threshold of $\underline{K}$ such that when $\varphi \geq \varphi\left(\widetilde{K}\right) = \tilde{\varphi}(K)$ the firms have an incentive to join the blockchain system. With hacker's attack, the consensus of the blockchain changes from $\varphi(K)$ to $\varphi(K-M)$, implying that $\begin{cases} \varphi(K) \geq \varphi\left(\widetilde{K}\right) \\ \varphi(K-M) \geq \varphi\left(\widetilde{K}\right) \end{cases} \Longrightarrow$

$\begin{cases} K \geq \widetilde{K} \\ K - M \leq \widetilde{K} \end{cases} \Longrightarrow \widetilde{K} \leq K \leq \widetilde{K} + M.$

Rewriting $\widetilde{K} = \underline{K}$, and $\widetilde{K} + M = \overline{K}$, we can conclude that there exists a range of the size of the blockchain ($\widetilde{K} \leq K \leq \widetilde{K} + M$) such that both research firms and developer firms have incentives to join the blockchain and to license the invention at $t = 0$; that is, the separating equilibrium is sustainable.

A.8 Proof of Proposition 8

If the developer firm never "mimics" (using the leaked information to develop for commercialization), the profit is $\frac{1}{1-\delta}\alpha\, v_H$. If it chooses to mimic, its profit becomes $\mu v_H + (1-\mu)\alpha\delta^T v_H$ at this period; Otherwise, the profit will become Π for the future period, which makes the total profit become $\mu v_H + (1-\mu)\alpha\delta^T v_H + \frac{\delta}{1-\delta}\Pi$ $((\alpha + \mu - \alpha\mu)v_H - C\varphi\mu)$, it can be easily found that the developer firm has

no incentive to mimic when $\frac{1}{1-\delta}\alpha\, v_H > \mu v_H + (1-\mu)\alpha\delta^T v_H + \frac{\delta}{1-\delta}\Pi$, which is equivalent to requiring $\alpha > (1-\delta)(\mu v_1 + (1-\mu)\alpha\delta^T) + \delta\Pi$, leading to $\delta > \frac{\mu+(1-\mu)\alpha\delta^T-\alpha}{\mu+(1-\mu)\alpha\delta^T-\Pi}$.

Note that in the equation, the numerator is the profit difference of the current period between not mimicking and mimicking, and the denominator is the profit difference of the mimicking between the current period and the future period. An increase in the future period profit would enhance the developer firm's incentive to mimic.

Consider the scenario with blockchain, if the research firm and the developer firm reach an agreement at $t = T$, then

$$\frac{\alpha}{1-\delta}v_H > \mu v_H + (1-\mu)\alpha\delta^T v_H + \frac{\delta}{1-\delta}\alpha\delta^T v_H$$

$$\delta^T > \frac{\mu + (1-\mu)\alpha\delta^T - \alpha}{\mu + (1-\mu)\alpha\delta^T - (\alpha+\mu-\alpha\mu) + \frac{C\varphi\mu}{v_H}}$$

Consider the case when $\varphi > \tilde{\varphi}$ in the t^{th} period. The utility of an individual keeper who never misreports is: $\frac{c_0}{K} + \delta\left(\frac{c_0}{K}\right) + \delta^2\left(\frac{c_0}{K}\right) + \cdots = \frac{c_0}{(1-\delta)K}$. While if the keepers misreport and successfully change the consensus, the research firm will update its belief about the consensus quality of the blockchain system. Thus, research firms with a high-value invention will exit in the next period. Meanwhile, when the developer firm expects that the research firm with a high-value invention to exit, they will only pay a low licensing fee $(1-\tau)v_L - c_0$ to the remaining low-value inventions. However, when firms with a low-value invention choose to license through the traditional channel, they can get at least $(1-\tau)v_L > (1-\tau)v_L - c_0$. Therefore, research firms with a low-value invention will also exit the blockchain. Thus, for the keepers who misreport at the t^{th} period, they may gain extra in that period, but lose all the potential gains in future periods. They need to balance between gaining from one-time misreporting and gaining from continuous transaction payoffs from honestly reporting, i.e. $h_k\lfloor y_k - \tilde{\omega}\rfloor = \frac{c_0\delta^T}{K(1-\delta)} + F(w,K)$, where $F(w,K)$ contains other costs such as the consumption of electricity, equipment purchases, and maintenance costs. If the benefit of misreporting exceeds the cost,

then the strategic keepers will choose to misreport, and the blockchain reputation (the proportion of honest keepers) will become $\tilde{\varphi} = \tau$. Research firms of both types will exit the blockchain system.

Appendix B. Table of Symbols

R	Research firm/entity
R_H / R_L	Research firm/entity with high-value / low-value invention
D	Developer firm
^{d} / ^{w}	R discloses / withholds information
v_H/v_L	The value of high-value / low-value invention
c_H/c_L	The cost of high-value / low-value invention
p	The proportion of high-value invention
$t = 0$ / T	The agreement is reached at time $t = 0$ / $t = T$
F	The flat licensing fee
F_H / F_L	The flat licensing fee for high-value / low-value invention
α	The bargaining power of developer firm
δ	Discount factor
δ^T	Discount factor for time $t = T$
μ	The success rate of commercialization using the leaked information
DU	The expected utility of developer firm
RU	The expected utility of research firm/entity
c_0	The cost of participating the blockchain
φ	The quality of consensus / consensus quality
C	Compensation payment of infringement
^{b}	With blockchain
K	The size (number of keepers) of blockchain
M	The number of keepers the hackers isolated
v_a	Per-keeper value of the blockchain
c_a	Unit cost of isolating selected nodes of the blockchain
M^*	The optimal number of keepers to isolate