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

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.

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

ABSTRACT

This article adopts a marketing perspective to examine how blockchain technology can facilitate innovation by streamlining the licensing process of intellectual property (IP). It notes that in the traditional world, there can be a 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 authors argue that 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 authors also suggest that the size of the community maintaining the blockchain is a crucial factor in ensuring the validity of the blockchain. They suggest that 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 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
and NBER
yi.qian@sauder.ubc.ca

Ning Nan
University of British Columbia
2053 Main Mall
Vancouver, Brit 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 (van der Waal et al., 2020).

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). The trusted and

timely authorization capabilities of blockchain have also attracted significant attention in the medical industry. Blockchain has also 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 limitation 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 firm who creates the invention and a developer firm who 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 firms 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.

In Section 3.3, we make the more realistic assumption of imperfect consensus in blockchain and incorporate the strategic behaviors of blockchain record keepers and outside security threats. 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 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 application by IPwe (PRNewswire, 2021) in the context of our theoretical predictions. 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 firm 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 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). As intangible assets, IPs are essentially ideas or information that can be duplicated and disseminated at 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 for 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 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 for 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

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 deliver higher social welfare and consumer surplus. Chod et al. (2020) argue that blockchain technology can make monitoring mechanisms more efficient than the 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 signal 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 the corporate governance in many ways. Chod and Lyandres (2021) examine the financing of entrepreneurial ventures with initial coin offering, which is an application of the blockchain technology. Our study 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, 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 for protecting 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 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 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 firm's decision on whether and when to disclose information about an invention and transfer the invention to the developer firm.

3. MODEL

We construct a game theoretical model to formalize the strategic interaction between a research firm (R) and a potential developer firm (D). They are both risk neutral agents. R produces an invention i, which can be of two types: one with high value but high investment cost (i=1) and the other with relatively low value and low investment cost (i=2). A high-value invention is assumed to be distinct from R's other inventions that have been transferred to other developer firms while a low-value invention is relatively similar to R's other inventions. This way, the two types of inventions reflect the non-rival nature of IPs. We denote the value of the invention i by v_i, with $v_1 > v_2$, and denote the investment costs for the invention i as c_i, with $c_1 > c_2$. While R bears the investment cost of an invention, it does not harvest the value of the invention until the invention is transferred to D for commercialization.

As mentioned earlier, the non-exclusive and non-rival nature of IP causes a conflict of interest during the invention transfer process: D would prefer to verify the value of the invention, including ensuring that it is not overly similar to inventions already transferred from R to D's rivals, which

requires R to disclose information about the invention as much as possible; yet the more information is disclosed by R, the less incentive D would have to pay for the invention (Arrow, 1962; Bhattacharya and Guriev, 2006). After all, the invention or IP is essentially non-exclusive information. Once the information is shared, D can immediately gain knowledge about 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 at the pre-protection phase $t = 0$, or at a post-protection phase $t = T$. At $t = 0$, R can choose to disclose or withhold information about the value of the invention. We use $\emptyset = 1$ to denote the case where R discloses information about the invention, and $\emptyset = 0$ to denote the case where R does not disclose information about the invention.

On the one hand, if R discloses information about the invention, it increases the chances for the two firms to reach an agreement at an early stage. If an IP transfer agreement is reached, the game ends. On the other hand, if the agreement is not reached before the grant of IP protection, partial information about the invention would be leaked. Consequently, D can use the leaked information to commercialize the invention with a possibility of success at $\mu \in [0,1]$. If D succeeds, the game ends. If not, D can make an offer at $t = T$ when the IP protection is granted. At that time, the game ends regardless of whether an IP transfer agreement is reached or not. The IP transfer game is depicted in Figure 1. This model setup captures the tension between IP protection and timely transfer of invention, as well as the underlying conflict of interests between R and D. Below, we first analyze the solutions for mitigating this tension in the traditional world and then explore the potential solutions and concerns brought by blockchain technology.

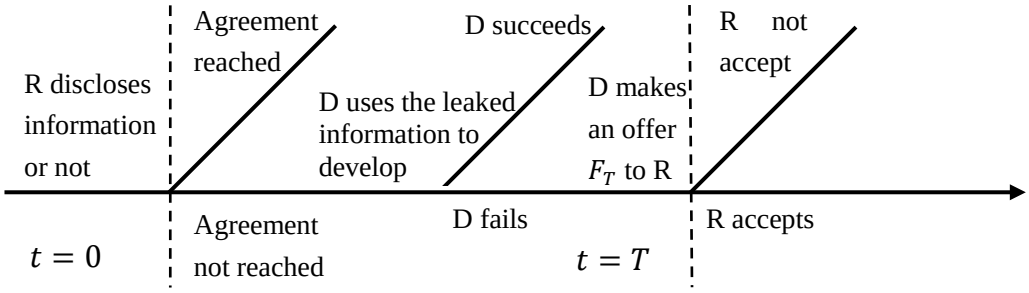

Figure 1. IP Transfer Game Timeline

3.1 Traditional world

Our literature review shows that patents and licensing agreements verified by authoritative institutions are the main solution 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 research firm (R) and developer firm (D) to gain a baseline understanding of tradeoffs in IP transfer, IP protection, and timely development of inventions.

We consider licensing agreements whereby R assigns potential IP to D for a flat fee F. The value of F depends on the bargaining power of the two firms. The bargaining process is modeled based on the widely used form in the literature (Nash 1950; Binmore et al., 1986; Osborne and Rubinstein 1994), $\max_F (\Delta DU)^{\alpha} (\Delta RU)^{1-\alpha}$ where $0 < \alpha < 1$ denotes the bargaining power of D, and ΔDU and ΔRU are the respective gains of D and R when one option is chosen over the other. We use the Cobb-Douglas form to simplify the calculation. The results are robust against other forms of bargaining process.

If R withholds information at $t = 0$, and the licensing agreement is signed at $t = 0$, then the expected value of the invention is $(pv_1 + (1-p)v_2)$, and the expected utility of D is: $DU_{0i}^h = pv_1 + (1-p)v_2 - F_0^h, i = 1,2$. The expected utility of R is: $RU_{0i}^h = F_0^h - c_i, i = 1,2$. When the licensing

agreement is signed at $t = T$, the valuation of a high-value invention is $\delta^T v_1$ and of a low-value invention is $\delta^T v_2$. Correspondingly, the expected utility of D is: $DU_{Ti}^h = \delta^T v_i - F_{Ti}^h$, $i = 1,2$. Here, δ^T is a discount factor at time T to account for the cost of delayed IP transfer. A higher value of δ^T means that a greater proportion of the value of the innovation in question is preserved over time. R's corresponding expected utility is: $RU_{Ti}^h = F_{Ti}^h - c_i$, $i = 1,2$

If R discloses information at $t = 0$, and the licensing agreement is signed at $t = 0$, then the expected valuation of a high-value invention is v_1 and of a low-value invention is v_2, the expected utility of D is: $DU_{01}^d = v_i - F_{0i}^d$, $i = 1,2$. The expected utility of R is: $RU_{0i}^d = F_{0i}^d - c_i$, $i = 1,2$. When 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 case is the same as when R withholds information because whether an invention is of high- or low-value is common knowledge at $t = T$.

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 in the various decision scenarios in Table 1. The licensing fees indicate the utilities of R. Meanwhile, D's utilities in the same decision scenarios are displayed in Table 2.

Table 1. Licensing fees in different cases

	$(\boldsymbol{H},\boldsymbol{0})$	$(\boldsymbol{H},\boldsymbol{T})$	$(\boldsymbol{D},\boldsymbol{0})$	$(\boldsymbol{D},\boldsymbol{T})$
$\boldsymbol{F_1}$	$(1-\alpha)(pv_1+(1-p)v_2)$	$(1-\alpha)\delta^T v_1$	$(1-\mu)(1-\alpha)v_1$	$(1-\alpha)\delta^T v_1$
$\boldsymbol{F_2}$	$(1-\alpha)(pv_1+(1-p)v_2)$	$(1-\alpha)\delta^T v_2$	$(1-\alpha)v_2$	$(1-\alpha)\delta^T v_2$

Table 2. Utilities of the developer firm in different cases

	$(\boldsymbol{H},\boldsymbol{0})$	$(\boldsymbol{H},\boldsymbol{T})$	$(\boldsymbol{D},\boldsymbol{0})$	$(\boldsymbol{D},\boldsymbol{T})$
$\boldsymbol{DU_1}$	$\alpha(pv_1+(1-p)v_2)$	$\alpha\delta^T v_1$	$(\alpha+\mu+\alpha\mu)v_1$	$\alpha\delta^T v_1$
$\boldsymbol{DU_2}$	$\alpha(pv_1+(1-p)v_2)$	$\alpha\delta^T v_2$	αv_2	$\alpha\delta^T v_2$

In these tables, we denote R's choice to disclose or withhold information about the invention with D and H, respectively. T and 0 respectively indicates whether a licensing agreement is reached at $t = T$ or $t = 0$. Four cases resulting from the combination of the decisions of R and D: $(H,0)$, (H,T), $(D,0)$, (D,T). The two rows in Table 1 correspond to the licensing fees for research firm *i*, denoted as F_i $(i = 1,2)$. DU_i $(i = 1,2)$ in Table 2 indicates D's utility from signing an agreement with research firm i. Here, *i*=1 refers to the research firm with a high-value invention, consistent with the notation in the basic model setup. A comparison of the utilities of R and D in the various decision scenarios leads to Lemma 1.

Lemma 1[1].

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

(2) The research firm with a low-value invention always prefers to withhold information and sign an IP transfer agreement at $t = 0$.

(3) The research firm with a high-value invention prefers to disclose information and reach an agreement at $t = 0$ when $\mu \leq min\{\overline{\mu_1}, \overline{\mu_2}\}$, with $\overline{\mu_1} = \frac{(1-p)(v_1-v_2)}{v_1}$, $\overline{\mu_2} = 1-\delta^T$; Otherwise,

[1] Please see the proofs of Lemma 1, Propositions 1 to 8, and Corollary 1 in Appendix A.

it prefers to withhold information and sign the agreement at $t = 0$ when $\overline{\mu_1} \leq \mu \leq \overline{\mu_2}$, or withhold information and sign the agreement at $t = T$ when $\overline{\mu_2} \leq \mu \leq \overline{\mu_1}$.

Lemma 1 conveys the intuition that the research firm R's decision to withhold information about the invention puts the 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. 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, its value of the invention is verified at $t = T$. Therefore, the optimal strategy for R_L is to sign an agreement at $t = 0$.

As for the research firm with a high-value invention (R_h), the decision on information disclosure and IP transfer depends on the benefit and cost of disclosing information about the invention. Information disclosure helps R_h to separate from R_L. This in turn increases its chance to obtain a better licensing fee when signing an IP transfer agreement at $t = 0$. However, the leaked information about the invention may reduce the incentive of the developer firm to sign the agreement since the developer firm can use the information to commercialize the invention. If the developer firm has a high probability of success, it would be less interested in signing the agreement when it obtains the disclosed information. This reduces R_h's incentive to disclose information at $t = 0$.

Second, R_h has to balance between the loss from the pooling equilibrium when signing at $t = 0$ and that from the discount factor at $t = T$. With an increase in the proportion of high-value inventions

p, the loss from the pooling equilibrium decreases as D's expected quality of the invention is higher. This in turn enhances R_h's incentive to reach an agreement at $t = 0$. The threshold value of p for R_h to be indifferent between pooling and separating from R_L increases with the discount factor δ^T. Recall that higher δ^T means less loss from signing at $t = T$. This increases the likelihood for R_h to sign an IP transfer agreement at $t = T$ to separate from R_L. Meanwhile, the threshold value of p increases or decreases respectively with v_1 or v_2 due to the corresponding change in the value gap $(v_1 - v_2)$ and the subsequent loss of signing an agreement at $t = 0$.

We can divide the equilibria into two types according to the range of p: pooling equilibrium and separating equilibrium. Figure 2 illustrates the types of equilibria and the research firm decisions and agreement outcomes associated with them (shown as Areas I, II, and III).

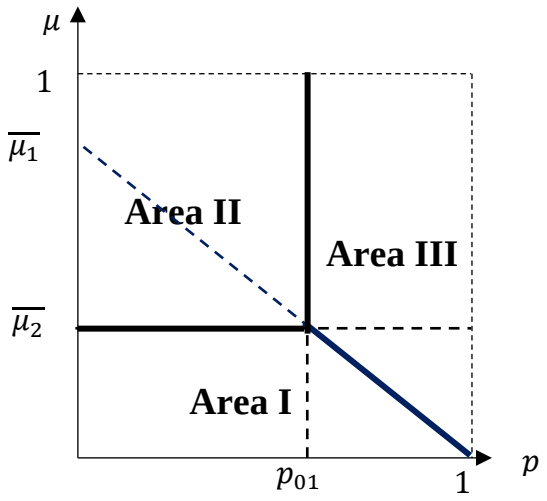

Figure 2. Equilibria in the traditional world

Area I, **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 $t = 0$.

The above analysis leads to the following predictions:

Proposition 1 (pooling equilibrium).

When $\overline{\mu_1} \leq \mu \leq \overline{\mu_2}$, R_h prefers to withhold information and sign an agreement with the developer firm at $t = 0$ to pool with R_L, and the flat fee is $F_0 = (1-\alpha)(pv_1 + (1-p)v_2)$.

Proposition 2 (separating equilibrium).

(1) When $\mu \leq min\{\overline{\mu_1}, \overline{\mu_2}\}$, R_h prefers to disclose information to separate with R_L and sign an IP transfer agreement at $t = 0$;

(2) When $\overline{\mu_2} \leq \mu \leq \overline{\mu_1}$, R_h prefers to sign an agreement with the developer firm at $t = T$ to separate with R_L. The corresponding licensing fees are displayed in Table 1.

Propositions 1 and 2 together indicate that the research firm's decision to disclose information about the invention is determined by a combination of factors, including the probability of success (μ) for the developer firm to use the disclosed information to develop and commercialize the invention, the proportion of research firms with high-value inventions (p) in a market, the value gap between the high- and low-value inventions ($v_1 - v_2$), and the discount factor (δ^T). Additionally, μ also reflects the level of protection for the IPs.

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 developer firm is either untraceable, or the record of information disclosure is not verifiable (Anton and Yao 2004). Moreover, the potential costs and unpredictable outcomes of a lawsuit can discourage research firms from taking legal actions.

These predictions are consistent with empirical findings based on a study of 1,612 licensing agreements that licensing, as a percentage of all alliances, is much more frequent in industries where IP rights are important than other industries, especially with respect to "prospective" (to-be-developed) technologies (Anand and Khanna 2000). In sectors where IP protection is traditionally weak (i.e., a high μ), firms are more likely to engage in non-licensing alliances such as 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 incentive 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 ($v_1 - v_2$) increases and the discount factor (δ^T), as well as the cost of waiting to license later decreases (i.e., the discount factor δ^T incresases). 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 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 ($t = 0$).

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 perfect consensus in blockchain

Blockchain technology utilizes decentralized consensus to validate records (Cong and He 2019) , which has the potential to facilitate fast IP transfer while safeguarding IP rights . However, the reliance of a community of record keepers in blockchain also creates a new tension between decentralized consensus and information distribution (Cong and He, 2019). The distribution of information to a community of mutually-distrusting record keepers poses the risks of record keepers manipulating the system. If not managed properly, a blockchain-based IP protection and transfer solution can replace the old problem with a new one. For example, in the Non-Fungible Token (NFT) market, inadequate censorship of IP ownership has resulted in numerous instances of content piracy. There have also been instances of misconduct by community managers, such as the alleged insider trading by a former product manager at OpenSea, a leading NFT marketplace (The National Law Review, 2022; Fortune, 2021). We have to find the conditions when blockchain-induced new tension and the IP protection-transfer tension are both remedied.

Our modeling of strategic behaviors of record keepers in a blockchain system is based on the work of Cong and He (2019). We consider a blockchain protocol that contacts K homogenous potential keepers to verify records of a transaction or an activity such as the disclosure of information about a new invention by a research firm, the retrieval of the disclosed information by a developer firm, or the transfer of payments. The transaction or activity, denoted as $\tilde{\omega}$, $\tilde{\omega} \in \{0,1\}$ takes the value of one if the transaction or activity occurs and zero otherwise. We denote the decentralized consensus on $\tilde{\omega}$ in blockchain by $\tilde{z}$, which takes a value in $\{0,1\}$, with 1 meaning perfect consensus. We model the quality of the consensus of contracting by $-Var(\tilde{\omega} - \tilde{z})$.

Upon contact, each keeper $k \in \mathbf{K} \equiv \{1,2,\cdots,K\}$ submits a report, $\tilde{y}_k$, which takes values in $\{0,1\}$, yielding a collection of reports, y, which is denoted as $y \equiv \{\tilde{y}_k\}_{k\in\mathbf{K}}$. For the purpose of illustration, we examine the case where the decentralized consensus on a transaction or activity, denoted as $\tilde{z}(y)$, is calculated as:

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

where $\omega_k \geq 0$ is the weight of the validating note, $\sum_{k=1}^{K} w_k = 1$, and $w_k \to 0$ as $K \to \infty$.

Each risk-neutral keeper submits a report y_k to maximize their normalized utility $U(y_k; y)$,

$$\max_{y_k \in \{0,1\}} U(y_k; y) = b_k \cdot \lfloor \tilde{z}(y) - \tilde{\omega} \rfloor - h_k \lfloor y_k - \tilde{\omega} \rfloor \qquad (1)$$

where b_k and h_k are positive, uniformly bounded above zero for all k. b_k denotes the record keeper k's benefit when an untruthful consensus is reached, while h_k denotes the cost of misreporting.

Each contacted keeper chooses y_k to optimize U, which gives

$$\tilde{y}_k^* = \begin{cases} \tilde{\omega} & if\ b_k w_k < h_k \\ 1 - \tilde{\omega} & otherwise. \end{cases}$$

where $K^* \equiv \{k \in \mathbf{K}: b_k w_k < h_k\}$ is the subset of keepers who report truthfully. The resulting quality of the decentralized consensus is then: $-Var(\tilde{\omega} - \tilde{z}) = -(1 - \sum_{k\in\mathbf{K}^*} w_k)^2$.

The effectiveness of blockchain-based solutions depends on how much the size of the contact pool K improves the quality of consensus by diminishing each record keeper's incentive to manipulate records. To illustrate this, we can consider the case of homogenous symmetric keepers with $b_k = b > 0$, $h_k = h > 0$ and $w_k = 1/K$. The consensus quality is simply $-\mathrm{I}_{k \leq \frac{b}{h}}$, which improves as K increases.

For more general b_k and h_k satisfying conditions specified in Equation (1), the consensus becomes perfect, i.e., $\tilde{z} = \tilde{\omega}$ 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.

With the mediation of a blockchain system, actions related to an IP can 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. If the developer firm uses the disclosed information to commercialize the invention, 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 from the developer firm to the research firm. We assume that the compensation is greater than v_1. In other words, the penalty of IP infringement is severe enough to deter the developer firm from unauthorized use of IP-related information.

In the traditional world, it is difficult for a research firm to prove the disclosure and unauthorized use of IP-related information and obtain compensation right away. Therefore, we assume that the compensation is 0 in the traditional world to simplify the model analysis (the results still hold when we relax this assumption). 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 now can disclose information about the invention to signal its true value

without concerning about the leakage of information. We assume that 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.

Proposition 3. With perfect consensus in a blockchain system, 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 according to Lemma 1 part (b), 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 to consensus, and all the agreements would be signed at $t = 0$. For high-value inventions, the flat fee is $F_{01}^b = (1 - \alpha)v_1$; while for low-value inventions, the flat fee is $F_{02}^b = (1 - \alpha)v_2$.

Proposition 3 gives us the theoretical insight 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.

3.3 World with imperfect consensus in blockchain

In reality, the number of record keepers of a blockchain system is finite. Therefore, the decentralized consensus obtained by the community of record keepers is subject to the utility-driven behaviors of individual keepers. In other words, 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 benefit 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.

3.3.1 The benefit of blockchain with imperfect consensus

We assume that the imperfect consensus resulting from the finite set of keepers has a probability φ to correctly record IP-related actions such as the disclosure of IP-related information. In this case, we define the probability φ 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

In Proposition 2, we have shown that the research firm with a high-value invention (R_h) prefers to sign an agreement with the developer firm at $t = T$ in most cases. 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:

$$RU_{j1}^{im} = \begin{cases} \mu\varphi C + (1-\mu)F_{T1}^{im} - c_1 - c_0 & if\ an\ agreement\ is\ not\ reached\ at\ t = 0 \\ F_{01}^{im} - c_1 - c_0 & if\ an\ agreement\ is\ reached\ at\ t = 0 \end{cases}$$

$$\text{s.t. } F_{01}^{im} - c_0 \geq max\{F_{T1}^{h}, F_0^{h}\}$$

where $j = 0, T$, 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:

$$DU_{j1}^{im} = \begin{cases} \mu(v_1 - \varphi C) + (1-\mu)\left(\delta^T v_1 - F_{T1}^{im}\right) & if\ an\ agreement\ is\ not\ reached\ at\ t = 0 \\ v_1 - F_{01}^{im} & if\ an\ agreement\ is\ reached\ at\ t = 0 \end{cases}$$

$$\text{s.t. } \mu(v_1 - \varphi C) + (1-\mu)\left(\delta^T v_1 - F_{T1}^{im}\right) \leq v_1 - F_{01}^{im}$$

where $j = 0, T$, 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 $F_{01}^{im} = (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_1 + C\mu\varphi)$, and $\varphi \geq max\left\{\frac{[(1-\delta^T\alpha)\mu-(1-\delta^T)]v_1}{\mu C} + \frac{c_0}{(1-\alpha)\mu C}, \frac{pv_1+(1-p)v_2-(1-\mu+\alpha\delta^T\mu)v_1}{\mu C} + \frac{c_0}{(1-\alpha)\mu C}\right\} = \tilde{\varphi}$. Hence, we obtain the following proposition:

Proposition 4. A blockchain system facilitates the signing of an IP transfer agreement at $t = 0$ when the quality of decentralized consensus is not too low ($\varphi \geq \tilde{\varphi}$), otherwise it decreases the incentive of the research firm with a high-value invention to disclose information.

Theorem 1. Blockchain expedites IP transfer only when the quality of the decentralized consensus among blockchain record keepers is not too low ($\varphi \geq \tilde{\varphi}$).

The quality of the consensus determines the authenticity of the records in blockchain. A low-quality consensus ($\varphi < \tilde{\varphi}$) means that blockchain may misreport information disclosure, IP ownership, and other IP transfer actions, and thereby lower the possibility for the research firm to seek compensation when the developer firm misuses disclosed information. This in turn lowers the research firm's incentive to disclose information before the patent is granted. When the quality of the consensus is good ($\varphi \geq \tilde{\varphi}$), the blockchain system provides enough IP protection. If the developer firm misuses the disclosed information, the research firm can use records in blockchain to prove its IP ownership and ask for compensation. In this case, the developer firm is likely to receive the penalty, which motivates the developer firm to sign the license agreement instead. Without the concern about IP infringement, R_h prefers to disclose information about its high-value invention to separate from R_L in order to reach an agreement at $t = 0$.

3.3.2 Firm decisions under imperfect 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 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. And 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:

$$RU_{j1}^{u} = \begin{cases} \mu(\varphi+\epsilon)C + (1-\mu)F_{T1}^{u} - c_1 - c_0 & if\ an\ agreement\ is\ not\ reached\ at\ t=0 \\ F_{01}^{u} - c_1 - c_0 & if\ an\ agreement\ is\ reached\ at\ t=0 \end{cases}$$

$$\text{s.t. } F_{01}^{u} - c_0 \geq max\{F_{T1}^{h}, F_{o}^{h}\}$$

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:

$$DU_{j1}^{u} = \begin{cases} \mu(v_1 - (\varphi+\epsilon)C) + (1-\mu)(\delta^T v_1 - F_{T1}^{u})\ if\ an\ agreement\ is\ reached\ at\ t=0 \\ v_1 - F_{01}^{u} & if\ an\ agreement\ is\ not\ reached\ at\ t=0 \end{cases}$$

$$\text{s.t. } \mu(v_1 - \varphi C) + (1-\mu)\left(\delta^T v_1 - F_{T1}^{h}\right) \leq v_1 - F_{01}^{u}$$

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 $F_{01}^{u} = (1-\alpha)((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon))$, R_h's expected utility from signing an IP transfer agreement at $t = 0$ is:

$$RU_{01}^{u} = (1-\alpha)\left((1-\mu+\alpha\delta^T\mu)v_1 + C\mu(\varphi+\epsilon)\right) - c_1 - c_0$$

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

$$RU_{T1}^{u} = \mu(\varphi+\epsilon)C + (1-\mu)(1-\alpha)\delta^T v_i - c_1 - c_0$$

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

Therefore, we obtain the following proposition:

Proposition 5: When $RU_{01}^u > \max\{RU_{T1}^u, RU_{01}^h, RU_{T1}^h\}$, 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 underestimate: $E(\varphi) < \varphi$, 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 6. 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 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.

3.3.3 Record keeper behaviors under imperfect consensus

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. However, they have to consider firm decisions when weighing the benefit and cost of misreporting.

In Section 3.2, 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 7. 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.

3.3.4 Security threats outside a blockchain system

In addition to issues arising inside a blockchain keeper community, the quality of consensus in a blockchain system is subject to security attacks from the outside. Data from Check Point Research (CPR) shows that global attacks on blockchain networks increased by 28% in the third quarter of 2022 compared to the same period the previous year (Report, 2022). Furthermore, blockchain analytics firm Chainalysis reported that hackers stole $1.9 billion in cryptocurrency from platforms worldwide between January and July 2022, up from $1.2 billion during the same period in 2021 (Korn, 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.

In Sections 3.2 and 3.3.1, we have shown that with perfect or good quality of consensus in blockchain, the research firm with a high-value invention can disclose information about the invention to separate from a firm with a low-value invention before obtaining the patent, and all the agreements will be signed at $t = 0$. In addition, research firms with low-value inventions will not join the blockchain. We now include security threats imposed by hackers into the process of consensus formation modeled in Section 3.3.1.

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:$\max_M Kv_a \cdot \big[\big(1-\varphi(K-M)\big)-\big(1-\varphi(K)\big)\big]-M\cdot c_a$. 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 $\varphi(K)=\sum_{k\in\mathbf{K}^*} w_k \le 1$ 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 3 illustrates the changes with respect to K. In the top panel of Figure 3, $\varphi'(K)$ 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 $K'v_a[\varphi(K')-\varphi(K'-M)]$.

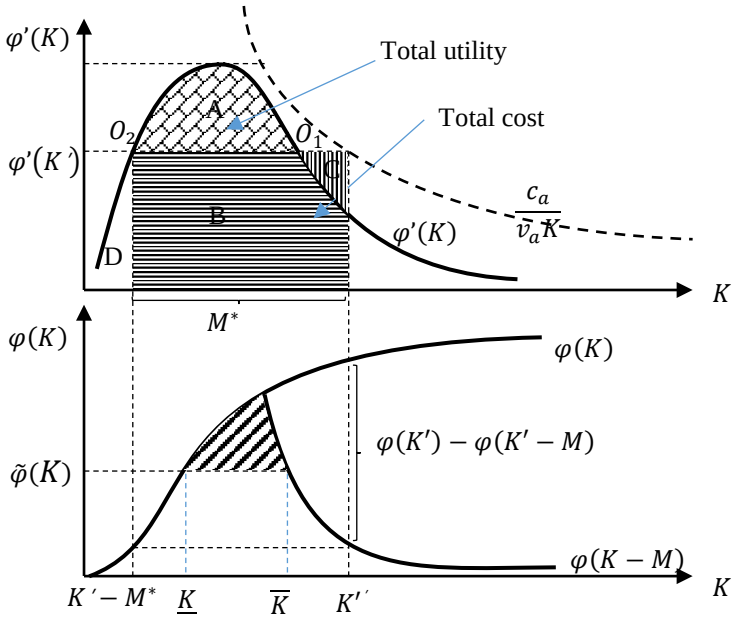

Figure 3. Optimal size of the blockchain platform

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 3 represents the standardized marginal cost of attacking to increase the misreport rate, and $\frac{M\, c_a}{K\prime\, v_a}$ 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 the area A is greater than the 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 in 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, while 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 3.3.1, we have learned that firms prefer to join the blockchain system only when $\varphi(K) \geq \tilde{\varphi}(K)$. Therefore, the firms have 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 8. 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 of the hackers to attack the blockchain and tamper with IP-related records also increases, resulting in the decrease of 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 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 1. When the size of the blockchain is moderate, $\underline{K} \leq K \leq \overline{K}$, with a sufficient 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.

4. 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.

Specifically, by comparing Propositions 1, 2, and 3, we gain a basic understanding about 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 secured by the IBM blockchain network (MT Newswires, 2021).

Nevertheless, for firms considering the 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. 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, Propositions 7 and 8 show 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. 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.

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 targeted analysis of their 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] 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

[2] 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

[3] Ashmore, D, OpenSea NFT Marketplace Review – Forbes Advisor, https://www.forbes.com/advisor/investing/cryptocurrency/opensea-nft-marketplace/, 2022 (accessed 6 December 2022).

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

[5] 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

[6] 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

[7] 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

[8] 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.

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

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

[11] 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.
[12] 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/10.5465/256308
[13] S. 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
[14] 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
[15] 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
[16] M. Boldrin, D. Levine, The case against intellectual property, The American Economic Review, 92(2) (2002) 209-212. 10.1257/000282802320189267
[17] R. Burstall, B. Clark, Blockchain, IP and the fashion industry, Managing Intell. Prop., 266(2017) 9.
[18] C. Catalini, J.S. Gans, Some simple economics of the blockchain, *Communications of the ACM*, *63*(7)(2020) 80-90.
[19] 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).
[20] 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
[21] 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
[22] 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
[23] 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
[24] 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.
[25] 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.
[26] 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

[27] E. Deirmentzoglou, G. Papakyriakopoulos, C. Patsakis, A Survey on Long-Range Attacks for Proof of Stake Protocols, IEEE Access, 7(2019) 28712-28725.
[28] 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).
[29] I. Eyal, E.G. Sirer, Majority is not enough, Communications of the ACM, 61(7) (2018) 95-102.
[30] D. Ferreira, J. Li, R. Nikolowa. Corporate capture of blockchain governance. European Corporate Governance Institute (ECGI)-Finance, Available at SSRN 3324228,
[31] 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 Jan 25, 2015).
[32] 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).
[33] 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
[34] 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).
[35] 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
[36] 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
[37] R. Henry, A. Herzberg, A. Kate, Blockchain Access Privacy: Challenges and Directions, IEEE Security & Privacy, 16(4) (2018) 38-45.
[38] 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
[39] N. Kannengießer, S. Lins, T. Dehling, A. Sunyaev, Trade-offs between Distributed Ledger Technology Characteristics, ACM Computing Surveys, 53(2) (2020) 1-37.
[40] 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 August 16, 2022).
[41] S.J. Kumar, G. Rigg, K.L. Green, 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 July 7, 2022).
[42] A. Lehar, C.A. Parlour, Miner collusion and the bitcoin protocol, Available at SSRN 3559894, (2020).
[43] 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..
[44] 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).

[45] H. McIntyre, 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).
[46] 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
[47] 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).
[48] J.F. Nash, The Bargaining Problem, Econometrica, 18(2) (1950) 155-162. http://www.jstor.org/stable/1907266
[49] Nature, Coronavirus: everyone wins when patents are pooled [editorial], Nature, 581 (2020) 240.
[50] M. J. Osborne, A. Rubinstein, A Course in Game Theory, MIT Press,1994.
[51] 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
[52] 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.
[53] PRNewswire, IPwe and IBM seek to transform corporate patents with next generation NFTs using IBM blockchain, IBM News Room, 2021 (accessed 28 April 2021)， https://newsroom.ibm.com/2021-04-20-IPwe-and-IBM-Seek-to-Transform-Corporate-Patents-With-Next-Generation-NFTs-Using-IBM-Blockchain
[54] 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
[55] 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)
[56] 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
[57]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).
[58] 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).
[59] 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, 2020 (accessed July 30 2020)
[60] D. Tapscott, A. Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world, Penguin, 2016.

[61] 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
[62] 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).
[63] 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).
[64] 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
[65] 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
[66] O.E. Williamson, Comparative Economic Organization: The Analysis of Discrete Structural Alternatives, Administrative Science Quarterly, 36(2) (1991) 269-296. http://www.jstor.org/stable/2393356
[67] 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).
[68] 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 May 25 2021).
[69] 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.
[70] D. Yaga, P. Mell, N. Roby, K. Scarfone, 2019, Blockchain technology overview. arXiv:1906.11078. https://arxiv.org/abs/1906.11078
[71] 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
[72] D. Yermack, Corporate governance and blockchains*, Review of Finance, 21(1) (2017) 7-31. https://doi.org/10.1093/rof/rfw074
[73] 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
[74] 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 Proof of Lemma 1, and Propositions 1 and 2

Given the strategy sets of the research firm and the developer firm, 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: $RU_{Ti}^{h} = F_{Ti}^{h} - c_i$, the utility for the developer firm is: $DU_{Ti}^{h} = \delta^T v_i - F_{Ti}^{h}$. If the agreement is not reached, then the expected utility for the research firm is $RU_{Tin}^{h} = -c_i$, and that for the developer firm is $DU_{Tin}^{h} = 0$. Then the two firms will bargain on the licensing fee, $\max_{F_{Ti}^{h}} \left(\left(\delta^T v_i - F_{Ti}^{h} - 0 \right)^{\alpha} \left(F_{Ti}^{h} - c_i - (0 - c_i) \right)^{1-\alpha} \right)$. To solve the problem, we take the logarithm of the objective function and obtain: $\max_{F_{Ti}^{h}} \left[\alpha \cdot Log\left(\delta^T v_i - F_{Ti}^{h} \right) + (1-\alpha) Log F_{Ti}^{h} \right]$. 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: $F_{Ti}^{h} = (1-\alpha)\delta^T v_i$.

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: $RU_{0i}^{h} = F_0^{h} - c_i$. The utility for the developer firm is: $DU_{0i}^{h} = pv_1 + (1-p)v_2 - F_0^{h}$. If the agreement is not reached at $t = 0$, then the expected utility of the research firm is $RU_{Ti}^{h} = \begin{cases} F_{Ti}^{h} - c_i, if\ the\ agreement\ is\ reached\ at\ t = T \\ -c_i, \quad \text{no agreement is reached} \end{cases}$

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

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 $t = T$, $\max_{F_0^{h}} \left(\left(pv_1 + (1-p)v_2 - F_0^{h} - \left(\delta^T v_i - F_{Ti}^{h} \right) \right)^{\alpha} \left(F_0^{h} - c_i - \left(F_{Ti}^{h} - c_i \right) \right)^{1-\alpha} \right)$, plugging the optimal $F_{Ti}^{h} = (1-\alpha)\delta^T v_i$ into the function and solving the problem, we obtain: $F_0^{h} = (1-\alpha)(pv_1 + (1-p)v_2)$.

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, $\max_{F_{0i}^{d}} \left(\left(v_i - F_{0i}^{d} - \left(\mu v_1 + (1-\mu)\left(\delta^T v_i - F_{Ti}^{d} \right) \right) \right)^{\alpha} \left(F_{0i}^{d} - c_i - \left((1-\mu) F_{Ti}^{d} - c_i \right) \right)^{1-\alpha} \right)$.

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 $DU_1(D,0) = DU_{01}^{d}$, $DU_1(H,0) = DU_{01}^{h}$,

$DU_2(D,0) = DU_{02}^d$, $DU_2(H,0) = DU_{02}^h$, $F_1(D,0) = F_{01}^d$, $F_1(H,0) = F_0^h$, $F_1(D,T) = F_{T1}^d$ $F_1(H,T) = F_{T1}^h$, $F_2(D,0) = F_{02}^d$, $F_2(H,0) = F_0^h$, $F_2(D,T) = F_{T2}^d$ $F_2(H,T) = F_{T2}^h$.

(a) We can then obtain that $DU_1(D,0) - DU_1(H,0) = (\alpha + \mu + \alpha\mu)v_1 - \alpha(pv_1 + (1-p)v_2) \geq \alpha v_1 + \mu v_1 - \alpha v_1 \geq 0$, $DU_2(D,0) - DU_3(H,0) = 0, DU_1(D,T) - DU_1(H,T) = 0, DU_2(D,T) - DU_2(H,T) = 0.$

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 (R_l), $F_2(H,0) - F_2(H,T) = (1-\alpha)(pv_1 + (1-p)v_2) - (1-\alpha)\delta^T v_2 \geq (1-\alpha)v_2 - (1-\alpha)\delta^T v_2 \geq (1-\alpha)(1-\delta^T)v_2 \geq 0,$

$F_2(D,0) - F_2(D,T) = (1-\alpha)v_2 - (1-\alpha)\delta^T v_2 \geq (1-\alpha)(1-\delta^T)v_2 \geq 0,$

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 $\begin{cases} F_1(D,0) \geq F_1(H,0) \\ F_1(D,0) \geq F_1(H,T) \end{cases}$, which implies that

$$\begin{cases} F_1(D,0) - F_1(H,0) = (1-\mu)(1-\alpha)v_1 - (1-\alpha)(pv_1 + (1-p)v_2) \geq 0 \\ F_1(D,0) - F_1(H,T) = (1-\mu)(1-\alpha)v_1 - (1-\alpha)\delta^T v_1 \geq 0 \end{cases} \Rightarrow$$

$\begin{cases} 0 \leq \mu \leq \frac{(1-p)(v_1-v_2)}{v_1} \\ 0 \leq \mu \leq 1-\delta^T \end{cases}$, that is, $0 \leq \mu \leq min\left\{\frac{(1-p)(v_1-v_2)}{v_1}, 1-\delta^T\right\}$, then the separating equilibrium is sustainable.

For R_h, if $\begin{cases} F_1(D,0) \leq F_1(H,0) \\ F_1(D,0) \geq F_1(H,T) \end{cases}$, it prefers to withhold information, and pool with R_L, which implies that

$$\begin{cases} F_1(D,0) - F_1(H,0) = (1-\mu)(1-\alpha)v_1 - (1-\alpha)(pv_1 + (1-p)v_2) \leq 0 \\ F_1(D,0) - F_1(H,T) = (1-\mu)(1-\alpha)v_1 - (1-\alpha)\delta^T v_1 \geq 0 \end{cases} \Rightarrow$$

$\begin{cases} \frac{(1-p)(v_1-v_2)}{v_1} \leq \mu \leq 1 \\ 0 \leq \mu \leq 1-\delta^T \end{cases}$, that is, $\frac{(1-p)(v_1-v_2)}{v_1} \leq \mu \leq 1-\delta^T$, then the pooling equilibrium is sustainable.

For R_h, if $\begin{matrix} F_1(D,0) \geq F_1(H,0) \\ F_1(D,0) \leq F_1(H,T) \end{matrix}$, then it prefers to withhold information and sign the agreement with D at $t = T$, which implies that

$$\begin{cases} F_1(D,0) - F_1(H,0) = (1-\mu)(1-\alpha)v_1 - (1-\alpha)(pv_1 + (1-p)v_2) \geq 0 \\ F_1(D,0) - F_1(H,T) = (1-\mu)(1-\alpha)v_1 - (1-\alpha)\delta^T v_1 \leq 0 \end{cases} \Rightarrow$$

$\begin{cases} 0 \leq \mu \leq \frac{(1-p)(v_1-v_2)}{v_1} \\ 1-\delta^T \leq \mu \leq 1 \end{cases}$, that is, $1-\delta^T \leq \mu \leq \frac{(1-p)(v_1-v_2)}{v_1}$, then the separating equilibrium is sustainable.

A.2 Proof of Proposition 3

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: $RU_{01}^b = F_{01}^b - c_1$, and the utility for D is: $DU_{01}^b = v_1 - F_{01}^b$. If the agreement does not reach at $t = 0$, then the expected utility for the research firm is $RU_{T1}^b = (1-\alpha)\delta^T v_1 - c_1$,

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, $\max_{F_{Ti}^{b}}\left(\left(v_1 - F_{01}^{b} - \alpha\delta^{T}v_1\right)^{\alpha}\left(F_{01}^{b} - c_1 - c_0 - \left((1-\alpha)\delta^{T}v_1 - c_1 - c_0\right)\right)^{1-\alpha}\right)$. Solving the problem, we obtain: $F_{01}^{b} = (1-\alpha)v_1$, $RU_{01}^{b} = (1-\alpha)v_1 - c_1 - c_0$. Since we know that if R_H withholds information, the utility it can achieve is: $RU_{01}^{h} = (1-\alpha)(pv_1 + (1-p)v_2) - c_1$. And, $RU_{01}^{b} - RU_{01}^{h} = (1-\alpha)(1-p)(v_1 - v_2) - c_0$. Since $c_0 < (1-\alpha)(1-p)(v_1 - v_2)$, we get $RU_{01}^{b} \geq RU_{T1}^{b}$. Therefore, with perfect consensus, R_H prefers to disclose information at $t = 0$.

A.3 Proof of Proposition 4 and Theorem 1

Under imperfect consensus, if the research firm discloses information, the expected utility of signing an agreement at $t = 0$ is: $RU_{01}^{im} = F_{01}^{im} - c_1$, and the utility for the developer firm is: $DU_{01}^{im} = v_1 - F_{01}^{im}$. If the agreement is not reached at $t = 0$, the expected utility for the research firm is $RU_{T1}^{im} = \mu\varphi C + (1-\mu)F_{T1}^{im} - c_1 - c_0$, and that for the developer firm is $DU_{Ti}^{im} = \mu(v_1 - \varphi C) + (1-\mu)\left(\delta^{T}v_1 - F_{T1}^{im}\right)$. Then the research firm and the developer firm bargain on the licensing fee, $\max_{F_{01}^{im}}\left(\left(v_1 - F_{01}^{im} - \left(\mu(v_1 - \varphi C) + (1-\mu)\left(\delta^{T}v_1 - F_{T1}^{im}\right)\right)\right)^{\alpha}\left(F_{01}^{im} - c_1 - c_0 - \left(\varphi C + (1-\mu)F_{T1}^{im} - c_1 - c_0\right)\right)^{1-\alpha}\right)$. Solving the problem, we obtain that: $F_{01}^{im} = (1-\alpha)((1-\mu+\alpha\delta^{T}\mu)v_1 + C\mu\varphi)$, $RU_{01}^{im} = (1-\alpha)\left((1-\mu+\alpha\delta^{T}\mu)v_1 + C\mu\varphi\right) - c_1$, $DU_{01}^{im} = v_1 - (1-\alpha)((1-\mu+\alpha\delta^{T}\mu)v_1 + C\mu\varphi)$,

The research firm prefers to disclose information if and only if $\begin{cases} RU_{01}^{im} \geq RU_{01}^{h} \\ RU_{01}^{im} \geq RU_{T1}^{h} \end{cases}$, implying that

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

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

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

A. 4 Proof of Proposition 5

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, $\max_{F_{T1}^{u}}\left(\left(v_1 - F_{01}^{u} - \left(\mu(v_1 - E(\varphi)C) + (1-\mu)(\delta^{T}v_1 - F_{T1}^{u})\right)\right)^{\alpha}\left(F_{01}^{u} - c_1 - c_0 - (E(\varphi)C + (1-\mu)F_{T1}^{u} - c_1 - c_0)\right)^{1-\alpha}\right)$.

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

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

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

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

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

A.5 Proof of Proposition 6

From Proposition 5, 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 7

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 $(1-\tau)v_2 - c_0$. 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 $(1-\tau)v_2 > (1-\tau)v_2 - c_0$.

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 8 and Corollary 1

The utility function of the hacker is:

$$\max_{M} Kv_a \cdot \big[\big(1-\varphi(K-M)\big) - \big(1-\varphi(K)\big)\big] - M \cdot c_a$$

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 3.3.1, 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 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 $\begin{cases} \varphi(K) \geq \varphi\left(\widetilde{K}\right) \\ \varphi(K-M) \geq \varphi\left(\widetilde{K}\right) \end{cases} \Rightarrow$

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

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.