Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33591

Delimitation of Legal Attributes and Resolution of Dilemmas in the Criminal Protection of Virtual Property

Yongnan Li

Law School, Shanxi University, Taiyuan, China
1239298494@qq.com

Abstract. To build a sound criminal protection framework for virtual property, one must first clarify its legal nature. In this study, virtual property is understood as property that exists in the virtual world, carrying two defining features at once, namely a data form and real property value. From the standpoint of civil-criminal coordination, the real right theory offers a reasonable account of its legal attributes.At present, the criminal protection of virtual property still encounters many practical problems. Judicial decisions tend to be inconsistent. It is hard to conduct asset valuation and evidence preservation. Supervision and law enforcement are not strong enough. Platforms fail to perform effective management. Black and gray markets are growing at a fast pace. These issues are mainly caused by the complexity of case forms. High technical obstacles also slow down judicial processes. Industrial governance is far from enough. Platform supervision is rarely put into practice.To address these challenges, a wide range of measures should be adopted. These measures need to span judicial, regulatory, and theoretical dimensions, along with the coordination between civil and criminal law. More specifically, practical difficulties in the criminal protection of virtual property can be effectively resolved through unified adjudication standards, strengthened platform oversight, promoted theoretical synergy between civil law and criminal law, and improved civil-criminal coordinated protection mechanisms.

Keywords: virtual property, criminal protection, dual attributes of data and property, civil and criminal coordination

1. Introduction

The rapid development of the digital economy has enriched the forms of virtual property, and the frequent occurrence of related criminal offenses has highlighted the increasing importance of the criminal protection of virtual property. Currently, a core divergence has emerged within the academic circle between the data theory and the property theory regarding the legal attributes of virtual property. Although research on criminal protection paths and the application of charges has been carried out, a unified consensus has not yet been reached. In judicial practice, prominent problems such as different judgments in similar cases and the absence of regulatory oversight exist, and the existing protection system struggles to adapt to practical needs. Taking the delimitation of the legal attributes of virtual property as the logical starting point, this paper sorts out the disputes over its attributes and clarifies the proper definition, systematically examines the multi-dimensional

DOI: 10.54254/2753-7048/2026.33591

dilemmas and underlying causes faced by current criminal protection, and finally puts forward targeted resolution paths from the four dimensions of judiciary, regulation, theory, and civil-criminal coordination. It provides ideas for improving the criminal protection system of virtual property and responding to the judicial needs of the digital age.

2. Delimitation of the legal attributes of virtual property

2.1. Theoretical disputes over the attributes of virtual property

2.1.1. The data theory: the essence of virtual property as data

The data theory holds that virtual property is an electromagnetic record existing in cyberspace, which is essentially data. Data is a symbolic record used to describe things, stored in computer systems after digital processing, and presented in the form of characters, graphics, images, audio, video, etc [1]. In terms of legal application, the data theory advocates regulating virtual property under cyber security-related charges, such as the crime of illegally obtaining data from computer information systems and the crime of sabotaging computer information systems. The main reasons supporting the data theory include the following. First, the core legal interest of virtual property is the security of network systems and the order of data management, rather than property rights. Second, data is closely related to virtual property, and acts of infringing on virtual property do not directly act on virtual property itself, but on the data carrying virtual property. Therefore, supporters of the data theory argue that virtual property should be incorporated into the regulatory system of cyber crimes.

From a technical perspective, the data theory conforms to the data essence of virtual property, responds to the protection needs of cyberspace data security, and has certain reference significance. However, this theory equates virtual property with ordinary data, making it difficult to fully protect users' property rights and interests, and has obvious limitations, mainly reflected in the following two aspects. First, it denies the economic value of virtual property. Although virtual property takes data as the carrier, it has transcended the scope of pure data and is a crystallization of users' time, capital investment and market value. Second, the protection it affords is inadequate. The conviction and sentencing of cyber crimes are mostly based on the criteria of technical harm, which are difficult to accurately reflect the actual property losses of the victim, fail to achieve the balance between crime and punishment, and tend to result in excessively lenient sentencing.

2.1.2. The property theory: virtual property as a right object with economic value

The property theory holds that virtual property possesses the core characteristics of "property" in the criminal law sense, constitutes a right object with economic value, and should therefore be included in the protection scope of property crimes. The essential attribute of property lies in its value, which means it can satisfy people's material or spiritual needs and be measured by monetary value, including use value and exchange value [2]. The main reasons supporting the property theory are as follows. One is that the core legal interest of virtual property is the user's property right, rather than mere network order. Infringement upon virtual property is essentially a violation of others' property interests, which is homogeneous to the legal interest infringement caused by traditional property crimes. Beyond that, virtual property already possesses the essential attributes of property under criminal law. It holds both use value and exchange value. For this reason, it ought to be brought within the protective scope of property crimes. Doing so also aligns with the criminal law logic that

DOI: 10.54254/2753-7048/2026.33591

defines property. It equally respects the basic principle of equal protection for equivalent legal interests.

From the standpoint of legal interest protection, the property theory accurately captures the economic value of virtual property. It effectively remedies a flaw in the data theory, which overlooks the property rights of users. In doing so, it provides a theoretical path for the criminal protection of virtual property that fits well with social understanding. This gives it considerable practical significance.Nevertheless, this theory is not without limitations. Two key points need to be taken seriously. The property theory overlooks the data nature of virtual property. It treats virtual property as independent from its data carrier. It also ignores a basic feature that virtual property is based on electronic data. Meanwhile, this theory leaves a protection gap. Some infringements against virtual property are carried out by damaging computer systems or altering data. The theory fails to fully explain the dual violation of legal interests. It cannot cover the damage caused to both the order of network data management and system security. A further point needs to be made. Virtual property already carries the essential attributes of property under criminal law. It possesses both use value and exchange value and should therefore be brought within the protective scope of property crimes. Including it in that scope also aligns with how criminal law defines property. It further respects the basic principle of equal protection for equivalent legal interests.

2.2. Proper delimitation of the legal attributes of virtual property

2.2.1. Dual attributes: the integration of data form and property value

The theoretical divergence between the data theory and the property theory is essentially a one-sided interpretation of the single legal attribute of virtual property. Neither of them can fully grasp the essential characteristics of virtual property, and the root cause of their limitations lies in the separation of the data attribute and economic value of virtual property. In fact, the legal attribute of virtual property is not an either-or choice, but a dual attribute integrating data form and property value. This attribute is jointly determined by the existence mode and social function of virtual property, and also constitutes the core theoretical basis for its criminal law protection.

In terms of data attribute, virtual property cannot exist independently of cyberspace. It takes electromagnetic records as the carrier and data as the manifestation form, and is a collection of digital symbols that can be identified, operated and transmitted in computer information systems. This data form serves as the physical basis of virtual property, and is also the fundamental feature that distinguishes it from traditional tangible property, which determines that virtual property necessarily possesses the legal attribute of data. Its existence and circulation are always restricted by the technical rules of network systems, and are thus closely related to legal interests such as network data security and system management order. Regarding economic value, virtual property is not pure technical data, but condenses users' investment of labor, material and financial capital. It forms objective exchange value through market transactions, and can meet users' demands for spiritual entertainment, social interaction and other practical uses, with clear use value. This property value is the core motivation for virtual property to be recognized by the public and become the object of legal protection, and also endows it with the essential attribute of "property" in the criminal law sense.

Data form and property value are not mutually exclusive, but organically unified in virtual property itself. Data form is the premise for the existence and realization of property value, while property value is the realistic basis for data form to possess legal protection significance. The two jointly constitute the inseparable dual legal attributes of virtual property. This attribute characteristic

DOI: 10.54254/2753-7048/2026.33591

also determines that the criminal law protection of virtual property can neither ignore the technical characteristics of its data carrier nor deny the essential connotation of its property value, and it is necessary to construct a protection system that takes into account multiple legal interests on the basis of these dual attributes.

2.2.2. Delimitation of the attributes of virtual property from the perspective of civil and criminal coordination

The delimitation of virtual property's attributes is both a prerequisite for resolving its criminal protection dilemmas and the foundation for achieving coordinated civil-criminal protection. Given the foregoing dual-attribute definition of virtual property and the theoretical divergence between the data theory and the property theory at the criminal law level, a clear determination of its right attributes at the civil law level becomes the key to bridging civil-criminal coordination and breaking the theoretical impasse. Currently, three core theories dominate the civil law discourse on the right attributes of virtual property. Drawing on their research logic, the author endorses the real right theory. A detailed introduction and evaluation from a civil-criminal perspective follows.

The real right theory holds that anything legally transferable, manageable, and possessing certain economic value can be recognized as a legal thing [3]. Virtual property fully satisfies these criteria; therefore, it constitutes a thing and may be governed by the provisions of property law. The creditor's right theory, by contrast, views virtual property as essentially a creditor's right, a certificate of the service contract between game operators and players [4]. What players obtain by paying fees is merely the game service, not ownership of the virtual property itself, which remains with the operator. The intellectual property theory takes a different view. It treats virtual property as a creative intellectual achievement. Since its existence depends on the operator's development and design, this line of thinking suggests protection through copyright under intellectual property law [5]. From a comprehensive perspective, the real right theory stands out as the most reasonable choice. Virtual property shows clear specificity and independence at the civil law level. It can be fixed in a certain time and space through account and password. It is also traded as an independent item in daily social life. It can therefore serve as a valid object of real rights. This theory also fits well with the logic of criminal law. It matches the theory of physical manageability. As an intangible asset, virtual property can be controlled and disposed of by its holders. This is consistent with China's criminal law and judicial interpretations. These rules recognize that property can include intangible items. The real right theory thus effectively connects civil protection and criminal protection. By contrast, the creditor's right theory has obvious flaws. It cannot tell virtual property itself apart from service contract relations. It also ignores the different values that virtual property holds for different users [6].The intellectual property theory is opposed by most scholars, as items such as equipment and currency in virtual property are neither expressions of thoughts and emotions nor original, and thus do not constitute creative intellectual achievements. In summary, the real right theory conforms to the dual attributes of virtual property, connects civil and criminal law theories with judicial practice, and represents a reasonable delimitation of virtual property's attributes from the perspective of civil-criminal coordination.

DOI: 10.54254/2753-7048/2026.33591

3. Examination of the dilemmas in the criminal protection of virtual property

3.1. Multi-dimensional dilemmas in the criminal protection of virtual property

3.1.1. Judicial confusion: divergences in adjudication and imbalance in the application of charges

In Chinese criminal law academia, only a very few scholars advocate the innocence doctrine [7], yet the mainstream view currently affirms criminal punishment for the act of stealing virtual property. Judicial practice, however, remains deeply divided on the application of specific charges, with inconsistent rulings in analogous cases and frequent charge alterations between higher and lower courts being prevalent. The applicable boundaries of theft, fraud, illegal acquisition of computer information system data, and infringement of citizens' personal information have long been blurred. There even emerge situations where the charges brought by the prosecution directly conflict with the court's final judgments, gravely undermining the uniformity of criminal law application and the authority of judicial adjudication. Consider property infringement cases involving the theft of virtual currencies such as USDT. Some courts explicitly recognize the economic value and property attributes of virtual currency, classify it as criminal-law "property", and ultimately impose conviction and sentencing for theft [8]. Other courts, by contrast, focus on the perpetrator's act of fabricating facts and concealing the truth, hold that such conduct satisfies the constitutive elements of fraud, and thus enter a conviction for fraud [9]. For the same act of virtual property infringement, entirely different conviction outcomes ensue merely due to divergent judicial perceptions of the nature of the conduct and the attributes of virtual property. More notably, subversive charge alterations occur in some cases during the appellate process: a first-instance court may characterize the relevant conduct as the crime of concealing or disguising criminal proceeds, while the second-instance court, upon trial, directly quashes the original judgment and reclassifies the conviction as the crime of infringing citizens' personal information [10]. Such charge alterations not only result in different determinations of the crime's nature but also directly impact sentencing outcomes, severely eroding the stability of judicial adjudication.

Significant divergences also appear in judicial characterization. Take the stealing of QQ accounts for subsequent fraud as an example. Some courts treat the account theft merely as a means of fraud and convict the whole course of conduct as a single count of fraud [11]. Others take a different path. They independently evaluate the act of illegally obtaining network data behind the account theft and characterize it as the crime of illegal acquisition of computer information system data [12]. Such disarray reveals inconsistent adjudicative standards and arbitrary charge determination. It poses a serious challenge to the traditional criminal law charge system. At the same time, it exposes the theoretical lag and weak explanatory power of traditional criminal law theory when facing new types of property crimes in the digital era.The digital economy is developing rapidly. Virtual property crimes keep evolving and their conduct patterns grow ever more complex. Against this backdrop, the current logic of criminal law application and the governance model for cybercrimes can barely meet practical needs. Systematic reflection and upgrading are urgently required. Clear judicial identification rules and unified standards for conviction and sentencing must be established. Only in this way can a criminal judicial protection system for virtual property be built, one that truly aligns with the developmental laws of the digital economy.

DOI: 10.54254/2753-7048/2026.33591

3.1.2. Identification difficulties: problems of value evaluation and evidence fixation

Another dilemma in the criminal protection of virtual property lies in judicial authentication. Clear standards for value evaluation are missing. Evidence preservation also brings great troubles to judicial practice. The conviction and sentencing of property crimes mainly depend on the amount of illegal gains. The value of virtual property must be calculated precisely. It directly affects the identification of crimes and the judgment of penalties. Some scholars hold that the value of virtual property changes sharply with users' personal needs. Its value is highly unstable in different periods [13]. It may even lose all value once users lose interest. Such features make virtual property hard to evaluate. The difficulty in evaluation directly affects conviction and sentencing in criminal cases.

Besides, virtual property is intangible and its value composition is diverse. Judicial organs cannot set up a single unified evaluation rule. No clear guidance is provided for different kinds of virtual property. Market transactions are not fully open and prices change frequently. These factors weaken the reliability of current evaluation methods. No objective and unified standard can be used to confirm the crime amount. The accuracy of criminal judgment is thus reduced. Beyond the difficulty of value assessment, evidence collection and review also stand in the way of judicial authentication. In fact, they make value evaluation even harder. Virtual property is stored on online servers as electronic data. Records of its existence and transfer all take the form of digital information. Such data can be easily altered or deleted. It is unstable and can be copied over and over again. Once an infringement occurs, offenders may swiftly remove or modify relevant data through technical means. If judicial organs fail to collect the evidence in time, it will simply be lost. Adding to this difficulty, virtual property transactions are often conducted across multiple platforms and tend to be hidden. Different internet service providers hold the relevant data. The length of data storage and the rules for data management vary from platform to platform. Some platforms do not even have a complete system to keep transaction records. As a result, evidence collection by judicial organs is further constrained. Consequently, judicial organs can hardly get complete evidence to judge the value of virtual property. Lacking sufficient and reliable evidence, value evaluation cannot be supported by solid facts. Judicial organs cannot confirm the real value of virtual property when the infringement takes place. They can only make decisions based on statements from victims and confessions from defendants. The objectivity and reliability of value judgment are greatly weakened.A vicious circle is thus formed. Difficulties in evidence preservation leave no solid support for value evaluation. Unreliable value evaluation further leads to inaccurate judicial authentication. This dilemma has become an urgent problem in the criminal protection of virtual property and needs to be solved as soon as possible.

3.2. The sources of the difficulties in virtual property protection

3.2.1. Varied case forms and the strong technical barriers faced by courts

A central reason behind the struggle to protect virtual property under criminal law is the sheer complexity it takes in practice. This complexity shows itself in two main ways. First, virtual property covers many types, which throws identification standards into confusion. Second, related crimes have grown more hidden and more reliant on technology. Judicial authorities are forced to meet a higher and higher technical bar. The two trends feed each other and make criminal protection even harder. Virtual property is not like traditional property. It rests on network data and comes in many forms. Identity accounts, game equipment, and virtual currencies all count as examples. Across these types, attributes and value differ a great deal. Gaps like these stand right in the way of

DOI: 10.54254/2753-7048/2026.33591

uniform identification standards. Judicial rulings start to diverge and the application of charges loses its balance. Equipment and currency types carry a double nature. They bear the stamp of data and the stamp of property at the same time. Their worth flows partly from the technical investment of developers and partly from the time and money users put in. Faced with such cases, judicial organs struggle to choose cleanly between charges tied to data and charges tied to property. The picture grows even dimmer with identity-type virtual items. The line between a user's right to use and a platform's right to manage is tough to trace. Nor can one draw a sharp boundary between property value and personal information rights. Worse still, methods of fixing value shift sharply from one type to another. Forcing a single reckoning across all types can only end in unfair sentencing. The strain between typological variety and a rigid criminal norm throws into stark relief how practical complexity blocks the path of criminal protection. At the same time, the hidden and technical shape of virtual property crimes keeps pushing judicial barriers upward. Fixing evidence and pinning down facts grow ever more difficult. These crimes run on network technology. Methods stay hidden and take many shifting forms. Trojan programs, computer viruses, and other technical tools are often used to slip past platform oversight and judicial probes. Behavioral traces and operation logs sit in electronic form. That form can be swiftly tampered with or erased through technical means. Detection and fixation hence meet stiff resistance. Numbers tell a striking story. Online thieves may grab over two hundred thousand dollars in one strike, yet the arrest rate lingers at two percent. Traditional robbers walk away with a bit over three thousand dollars on average, while the arrest rate jumps past eighty percent. The gap lays bare just how hidden such crimes are and how hard they prove to investigate [14]. Encryption, anonymous shells, and cross-platform transfers let wrongdoers bury criminal traces. Judicial agencies find it hard to secure key evidence like transaction records and operation logs with speed and fullness. Even when scraps of electronic data land in their hands, legality and validity stay tough to guarantee. A tight knot follows. Evidence fixation falters. Valuation lacks a firm footing. Judicial determinations drift further off the mark.

3.2.2. Missing platform oversight and weak industry regulation

Another key reason for the difficulty in criminally protecting virtual property is the lack of a sound regulatory system. This problem shows up in three ways. Platform supervision stays largely on paper. External oversight remains weak. Industry regulation lacks coordination. These three problems overlap and feed into each other. Platform supervision fails to work in practice. Black and gray industries spread unchecked. Together they have become a major barrier to the criminal protection of virtual property.

The absence of real internal platform supervision sits at the heart of this regulatory failure. It also serves as the direct trigger for illegal acts involving virtual property. Platforms are the main place where virtual property is stored, circulated, and traded. The strength of their internal supervision directly shapes the first line of defense for protecting virtual property. Yet in reality, most platforms merely go through the motions. The rights and obligations between network operators and users are poorly defined. Operators stress their own technical management powers but pay little attention to their duty to safeguard users' virtual property. Users, for their part, do not clearly understand the scope of their rights or how to seek redress. This imbalance leaves internal supervision without a clear focus. The gap is especially visible in game virtual property trading. Game operators, citing user service agreements, claim ownership over game accounts, items, and in game currency. They ban users from trading on third party platforms and label such activity as unfair competition. Third party trading platforms take the opposite stance. They point to Article 127 of the Civil Code and argue that game related virtual property is protected by law. Users, they say, have the lawful right to

DOI: 10.54254/2753-7048/2026.33591

dispose of and trade such property, and operators have no authority to restrict this [15]. At the same time, industry regulation remains fragmented. There are no unified industry norms or self discipline mechanisms. No single industry association or self regulatory body exists. Each platform acts on its own in a disorderly fashion. No effective information sharing or coordinated supervision mechanism is in place. Wrongdoers can thus commit crimes across multiple platforms with ease. Industry sanctions are also too weak to deter misconduct. The virtual property sector lacks motivation for self restraint. This deepens the regulatory vacuum and strips the criminal protection of virtual property of a solid industrial base.

4. Ways out of the trouble in criminal protection of virtual property

4.1. Judicial unification: standardizing adjudication standards and the application of charges

In judicial practice of virtual property criminal protection, similar cases frequently lead to inconsistent judgments, undermining judicial credibility and severely weakening the law's protective effect on virtual property. Issuing guiding cases on virtual property crimes is the most direct and effective solution to this problem. With the digital economy's development, virtual property types have kept diversifying-from online game items, virtual currencies to social media accounts and virtual points-with increasingly varied forms. Corresponding criminal acts have also grown more complex, including the evolution of traditional theft and fraud and new crime models emerging from information technology. Abstract legal provisions can hardly cover all complex scenarios, leaving judicial personnel often facing ambiguous identification standards and divergent adjudication approaches in case handling. As typical samples refined from judicial practice, guiding cases can convert abstract legal provisions into concrete, citable adjudication models, providing clear guidance for judicial organs at all levels in handling similar cases and effectively reducing arbitrariness in judicial determination. Given the current judicial practice of virtual property crimes, the issuance of guiding cases should be targeted, focusing precisely on core contentious points in practice and covering different types of virtual property and criminal conduct. The Supreme People's Court and the Supreme People's Procuratorate may issue relevant cases in a targeted manner, offering clear adjudication references for lower courts in hearing virtual property-related cases and ensuring reasonable case determination and lawful adjudication.

Based on the act characteristics and infringed legal interests, virtual property crimes can be classified into different types, with the charge application logic clarified for each type. For perpetrators who illegally occupy virtual property via traditional means such as theft and fraud, such acts only infringe the victim's property interests without endangering data security, and it is suggested to regulate them under the property crime framework, calculating losses by category according to the victim's possessory loss. When perpetrators obtain virtual property through non-technical means, as such acts do not involve data security interests and only infringe property rights, they shall be convicted and punished for property crimes like theft and fraud. Loss calculation follows the principle of prioritizing actual losses: if the victim does not completely lose possession, losses are calculated based on the perpetrator's illegal gains; if the victim completely loses possession, losses are calculated based on the virtual property's valuation or market transaction price. For perpetrators who illegally obtain virtual property through information technology, thus infringing both property and data security interests, it is suggested to apply the principle of imaginative joinder of offenses. Where a perpetrator obtains virtual property through technical means, such conduct constitutes the crime of illegally obtaining computer information system data and may be convicted once it meets the "serious circumstances" threshold. If the victim does not

DOI: 10.54254/2753-7048/2026.33591

completely lose possession, only this crime shall apply; if the victim completely loses possession, the amount meets the "relatively large" threshold and both crimes are constituted, conviction and sentencing shall follow the rule of punishing the more serious offense [16].

4.2. Strengthening supervision: compacting platform responsibilities and industry governance

Strengthening virtual property supervision is, in essence, about locking in the primary duties of third-party platforms and pushing industry governance toward a systematic, tiered model. That step holds the key to untangling the supervision problem in criminal protection and building a solid safety line for virtual property. Third-party platforms store, circulate, and trade virtual property. They stand as the first line of defense. How thoroughly they carry out their supervisory work directly shapes the real impact of criminal protection. At present, some platforms that deal in virtual property lean heavily on claims of technical neutrality and a mere information-intermediary role. They use these claims as a shield to dodge the supervisory duties they should rightly shoulder. Illegal and harmful acts on their platforms are often met with a blind eye. This posture not only opens the door for wrongdoing involving virtual property but also throws up steep obstacles when judicial organs try to investigate cases. Criminal law, in response, should spell out the supervisory responsibilities and the burden of proof that fall on third-party platforms. Legal pressure must be brought to bear so that platforms are forced to step up and genuinely protect the lawful rights and interests of users. Platforms need to carry out their information preservation duties with real discipline. Data tied to users' virtual property must be kept in good order, with an eye to what judicial practice demands and to the differing traits of various kinds of virtual property. Retention periods should be set in a sensible way. Evidence must not be allowed to vanish, but operational costs must not be pushed to an unreasonable level either. Sound security protection mechanisms deserve equal attention. Regular safety testing and risk screening should be put in place to stop virtual property from being taken, tampered with, or transferred without authorization. If a platform, through deliberate action or gross neglect, fails to meet these duties and heavy property loss lands on users, criminal liability must follow in line with the law. Platforms are also bound by a strict duty to keep information confidential. Any leak of sensitive user data must be blocked without compromise. Criminal law should fix clear liability for such leaks to make deterrence bite. The evidential burden on platforms should be spelled out just as plainly. Platforms must be required to work closely with judicial authorities during case investigations and provide the relevant evidence in good faith. Those that refuse to cooperate, or that hide or destroy evidence, should be answerable before the law.

4.3. Theoretical bridging: linking property protection and data protection

Promoting a deep merger of property protection and data protection is vital. Refining the theoretical system of virtual property will help resolve the difficulties in judicial application. This effort calls for a more sustained theoretical exchange between civil law and criminal law. A protection model must be built that balances the value of virtual property with the order of the network. Theoretical cohesion must be locked into place. At present, actual practice leans heavily on civil lawsuits and remedial steps taken by platforms themselves to govern infringements on virtual property. Both avenues, however, yield only thin results. Their limits not only fail to curb the frequent outbreak of infringements, they may even make matters worse. The root of the trouble is closely tied to an unclear definition, at the civil law level, of the right attributes and protection rules of virtual property. A clear theoretical guide is equally missing at the criminal law level. Civil law, serving as the prior law, remains vague. Such vagueness clouds the boundaries of criminal law intervention. It

DOI: 10.54254/2753-7048/2026.33591

leads, in judicial practice, to splits over attribute identification, the application of charges, and the reckoning of losses. The standardization of protection is eroded as a result.What is needed is to tear down the discipline wall between civil law and criminal law and to deepen their theoretical exchange and the harmonization of their rules. At the civil law level, rules should be pinned down concerning the ownership and value assessment of virtual property as a fresh category of property right. These rules would furnish criminal law protection with ex ante support. Criminal law theory must take the initiative to fall into line with civil law. It should balance the legal interests of property and data and put together a protection frame suited to the digital age. At the same time, theoretical agreement should be pushed forward through back-and-forth among scholars and targeted seminars. The theoretical edifice can thereby be refined. Moreover, the dual nature of virtual property means that criminal law protection cannot lean to one side. A protection model that accommodates both property value and network order ought to be established. Priorities of protection should be marked off according to the features of different kinds of virtual property. Such a model must be woven closely into judicial practice and regulatory measures. It should be lodged in guiding cases and adjudicative rules. It should also supply the theoretical footing for platform oversight and crackdowns on black and gray markets. Fixing the dilemma in criminal protection of virtual property cannot happen without theoretical cohesion. Only by fusing theories of property and data protection, and by tackling theoretical lag, can the criminal protection system grow sharper and more efficient, and better answer the needs of a developing digital economy.

4.4. Smoother links: strengthening how civil and criminal law work together for protection

To improve the civil-criminal collaborative protection mechanism for virtual property, it is necessary to clarify the relationship between the preceding law and criminal law protection rules and to build a legal consensus on the definition of virtual property rights. As the preceding law for virtual property protection, civil law provides the foundation and basis for criminal law intervention through its rules on the ownership and circulation of virtual property rights as well as provisions on tort liability. Criminal law, as a backstop legal safeguard, primarily serves to remedy the deficiencies of the preceding law and to regulate acts that seriously infringe virtual property and meet the threshold for criminal punishment. It must neither overstep by intervening in civil disputes nor be absent by tolerating criminal offenses. A sharp disconnect marks the civil and criminal protection of virtual property today. Civil law defines the right attributes vaguely and leaves protection rules scattered and disorderly. Criminal law, in turn, finds the prior law unclear. The boundary for criminal intervention blurs. Judicial confusion and uneven charge application follow. Users' lawful rights are poorly sheltered. The criminal protection system for virtual property remains constrained. To align the protective rules of the two legal domains, virtual property must be recognized as a new type of property right. Its attributes, ownership, circulation, and tort liability rules need clear definition. Relevant laws and regulations should be reviewed and conflicts removed. A systematic and unified prior-law protection system can then take shape. At the same time, the connection point between criminal law and the prior law should be clarified. The principle of modesty must be upheld. The scope of intervention should be narrowed. Linking rules for value assessment and infringement determination must be improved. A joint mechanism should be built to tighten the coordination between civil and criminal judgments. Forging a legal consensus on virtual property rights is the very foundation for a stronger civil-criminal protection mechanism. Based on the dual attributes of virtual property, legislative, judicial, and theoretical circles should be brought into closer alignment. Right attributes and ownership boundaries must be clarified. The exercise of rights and transaction practices need to be regulated. At the legislative level, provisions should be refined and grey areas

DOI: 10.54254/2753-7048/2026.33591

removed. At the judicial level, the consensus should be embedded in adjudicative practice to unify identification standards. At the theoretical level, research should deepen to meet practical demands. Through such multi-level efforts, the rifts between civil and criminal protection can be closed. A solid legal footing for criminal protection of virtual property can be laid. The protection system can become more orderly and sound.

5. Conclusion

The dual nature of virtual property settles one point straight away. Its criminal protection cannot lean solely toward property value, nor can it fixate only on network order. A balance must be struck between the two. The troubles seen today are plain enough. Judicial rulings pull in different directions. Identification stays a knotty task. Supervision lacks real bite. All these spring from a handful of stubborn sources. The definition of its attributes remains murky. Theoretical threads have not been pulled tight. The supervision machinery is still patchy and half-built. This paper tackles the problem from the ground up. It first marks out the dual legal attributes of virtual property. It then digs into the roots of the current dilemmas. After that, it sets out paths toward a way out. Working from a civil-criminal coordination perspective, the paper sharpens the logic of protection. It also puts forward a practical scheme. The scheme aims to settle judicial splits. It seeks to lift the efficiency of supervision. It also looks to shore up the wider protection system. The value of the paper is as much theoretical as it is practical. It can lend a measure of order to criminal judicial practice over virtual property. It can help keep related unlawful and harmful conduct in check. It can safeguard the lawful rights and interests of users too. Over the longer stretch, it can nudge the digital economy toward healthier development. Future work must stay alert to the shifting shapes of virtual property. The civil-criminal theoretical dialogue needs steady deepening. Supervisory and judicial rules call for careful, step-by-step refinement. The protection mechanism itself must be kept under constant repair. That is how criminal protection for virtual property and the governance of a digital society can move forward in step.

References

[1] Wang, S., & Sa, S. X. (2014). Introduction to database systems (5th ed.). Beijing: Higher Education Press.
[2] Lin, X. X., & Zhang, D. M. (2005). On the legal attributes of the right to virtual property in online games. China Legal Science, (2), 189-192.
[3] Yang, L. X., & Wang, Z. H. (2004). On the real right attribute of network virtual property and its basic rules. Journal of National Prosecutors College, 12(6), 3-13.
[4] Wang, Z. (2008). The dichotomy of virtual property from the perspective of property law and its legal rules. Journal of Fujian Normal University (Philosophy and Social Sciences Edition), (5), 30-35.
[5] Lin, X. X. (2009). On the nature of the right to virtual property. China Legal Science, (1), 88-98.
[6] Qian, M. X., & Zhang, F. (2008). An analysis of the civil law issues of network virtual property. Journal of Fujian Normal University (Philosophy and Social Sciences Edition), (5), 6-12.
[7] Hou, G. Y. (2008). On the inappropriateness of the criminal protection of network virtual property. Journal of Chinese People's Public Security University (Social Science Edition), 24(3), 33-40.
[8] The Intermediate People's Court of Jiaozuo City, Henan Province. (2025). Criminal ruling (2025) Yu 08 Xing Zhong No.21.
[9] The Intermediate People's Court of Xinzhou City, Shanxi Province. (2024). Criminal ruling (2024) Jin 09 Xing Zhong No.37.
[10] The Intermediate People's Court of Changzhou City, Jiangsu Province. (2017). Criminal judgment (2017) Su 04 Xing Zhong No.160.
[11] The Intermediate People's Court of Urumqi City, Xinjiang Uygur Autonomous Region. (2016). Criminal ruling (2016) Xin 01 Xing Zhong No.213.

DOI: 10.54254/2753-7048/2026.33591

[12] The Intermediate People's Court of Hechi City, Guangxi Zhuang Autonomous Region. (2021). Criminal ruling (2021) Gui 12 Xing Zhong No.199.
[13] Cai, X. X. (2019). Research on the legal attributes and criminal protection paths of virtual property. Journal of Southeast University (Philosophy and Social Science Edition), 21(S1), 15-20.
[14] Liu, S. F. (2006). Research on cyber criminal law under technical check and balance. Beijing: Peking University Press.
[15] Compilation Group of Reference Cases for the Special Topic of Network Virtual Property. (2024). Interpretation of reference cases for the special topic of network virtual property. Construction and Application of the People's Court Case Database, (6), 92-104.
[16] Chen, X. Y. (2022). Research on the criminal protection path of virtual property from the perspective of the unity of the legal order. Social Science Trends, (5), 42-49.