BLACK MARKET MERCHANT MINING METHOD AND SYSTEM, AND STORAGE MEDIUM

TECHNICAL FIELD

[0001] This specification relates to the field of Internet technologies, and in particular, to a black market merchant mining method and system, and a storage medium.

BACKGROUND

[0002] With development of Internet technologies, a user and a merchant can perform a transaction over the internet. The Internet also provides an opportunity for some black markets while providing transaction convenience to the user and the merchant. For example, the black market can register merchants (namely, black market merchants) in batches on a transaction platform, and can use the black market merchants to conduct a commercial activity over the Internet for an illegal profit.

[0003] The transaction platform identifies the black market merchants by using some risk control policies, to avoid bringing an asset loss to the user and the transaction platform by the black market merchants. For example, when the merchant requests to join the transaction platform, the transaction platform can request the merchant to provide detailed reported information, so that the transaction platform can accurately identify the black market merchant based on the reported information. However, experience of the black market against risk control is continuously improved over time. In a merchant joining stage, reported information of the black market merchant is gradually perfected, making it difficult for the transaction platform to effectively identify the black market merchant based on the reported information.

[0004] Content of the background part is merely information learned of by the inventor, and neither means that the information has entered a public domain before an application date of the present disclosure, nor means that the information can become a conventional technology of the present disclosure.

SUMMARY

[0005] This specification provides a black market merchant mining method and system, and a storage medium, to obtain more second black market merchants based on a first black market merchant in a transaction stage of a black market merchant, and implement precision prevention and control on the black market merchant.

[0006] According to a first aspect, this specification provides a black market merchant mining method, including: determining a first black market merchant; determining a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant, where the black market user is a person who performs a transaction test on the first black market merchant; and determining a second black market merchant from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user.

[0007] According to a second aspect, this specification further provides a black market merchant mining system, including at least one storage medium and at least one processor. The at least one storage medium stores at least one instruction set, to perform black market merchant mining. The at least one processor is communicatively connected to the at least one storage medium. When the mining system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set: determining a first black market merchant; determining a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant, where the black market user is a person who performs a transaction test on the first black market merchant; and determining a second black market merchant from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user.

[0008] According to a third aspect, this specification further provides a computer-readable nonvolatile storage medium. The computer-readable nonvolatile storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the black market merchant mining method according to the first aspect is implemented.

[0009] Other functions of the black market merchant mining method and system, and the

storage medium provided in this specification are partially listed in the following descriptions. Creative aspects of the black market merchant mining method and system, and the storage medium provided in this specification can be fully explained by practice or by using the methods, apparatuses, and combinations described in the following detailed examples.

BRIEF DESCRIPTION OF DRAWINGS

[0010] To describe the technical solutions in the embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following descriptions show merely some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0011] FIG. 1 is a schematic diagram of a transaction risk control scenario according to an embodiment of this specification;

[0012] FIG. 2 is a diagram of a hardware structure of a computing system according to an embodiment of this specification;

[0013] FIG. 3 is a flowchart of a black market merchant mining method according to an embodiment of this specification; and

[0014] FIG. 4 is a schematic diagram of historical transaction data according to an embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0015] Specific application scenarios and requirements of this specification are provided in the following descriptions, so that a person skilled in the art can manufacture and use content of this specification. For the person skilled in the art, various local modifications to the disclosed embodiments are clear, and the general principles defined here can be applied to other embodiments and applications without departing from the spirit and scope of this specification. Therefore, this specification is not limited to the shown embodiments, but has a widest scope consistent with that of the claims.

[0016] The terms used here are only intended to describe a particular example embodiment, but do not impose a limitation. For example, unless otherwise specified in the context, the singular

forms "one", "a", and "the" used here can also include a plural form. When used in this specification, the terms "include", "comprise", and/or "have" indicate/indicates existence of an associated integer, step, operation, element, and/or component, but does not exclude existence of one or more other features, integers, steps, operations, elements, components, and/or groups, or another feature, integer, step, operation, element, component, and/or group can be added to the system/method.

[0017] In consideration of the following descriptions, these and other features of this specification, operations and functions of related components of the structure, and economy of combination and manufacturing of components can be significantly improved. With reference to the accompanying drawings, all of these form a part of this specification. However, it should be clearly understood that the accompanying drawings are merely used for the purpose of illustration and description, and are not intended to limit the scope of this specification. It should be further understood that the accompanying drawings are not drawn to scale.

[0018] The flowchart used in this specification illustrates operations implemented by a system in some embodiments of this specification. It should be clearly understood that operations in the flowchart can be implemented out of sequence. On the contrary, operations can be implemented reversely or simultaneously. In addition, one or more other operations can be added to the flowchart. One or more operations can be removed from the flowchart.

[0019] For ease of description, the terms that appear below in this specification are first explained.

[0020] A black market is a group or organization engaged in an illegal activity over the Internet for an illegal profit. The black market has a wide activity range, including a network fraud, a network theft, a network attack, an illegal sale of personal information, manufacturing and spreading of a network virus, etc. A black market activity is usually carried out by a specialized group or organization. In this specification, the black market can register a large quantity of black market merchants in batches on a transaction platform, and use these black market merchants to conduct an illegal commercial activity over the Internet for an illegal profit. The black market merchants not only endanger privacy security and property security of a normal user, but also cause an asset loss to the transaction platform.

[0021] A risk control policy is a series of methods, measures, and practices used to reduce or manage a potential risk. In this specification, the risk control policy can include a series of risk

control rules formulated to cope with a risk transaction, and can further include a risk control model obtained through pre-training.

[0022] A location-based service (LBS) is a technology and application for providing a user with various services related to a current location of the user on a basis that geographic location information of the user is obtained through a mobile communication network or based on a satellite positioning technology. Services that can be provided by the LBS include but are not limited to map navigation, a location search, route planning, information push, a social network, a commercial advertisement, etc. The LBS obtains real-time location information of the user by using a global positioning system (GPS) or through cellular network positioning, Wi-Fi positioning, etc., and then provides the user with personalized services and information with reference to data such as a personal preference and a historical behavior of the user.

[0023] The following describes an application scenario of this specification.

[0024] Embodiments of this specification can be applied to a transaction risk control scenario. For example, some black markets may register merchants in batches on a transaction platform, and use these merchants to conduct an illegal commercial activity for an illegal profit. According to the technical solutions provided in embodiments of this specification, a black market merchant can be mined on the transaction platform. Specifically, a risk control system can determine a first black market merchant, determine a black market user based on historical transaction data associated with the first black market merchant, and mine more other black market merchants (namely, a second black market merchant) based on historical transaction data associated with the black market user. After obtaining the other black market merchants through mining, the risk control system can perform risk prevention and control on the black market merchants.

[0025] According to the technical solutions provided in this specification, the black market merchant can be mined based on historical transaction data between a user and a merchant. In other words, according to the technical solutions provided in this specification, the black market merchant is identified in a merchant transaction stage instead of a merchant joining stage. In this way, even if reported information provided by the black market merchant is relatively complete, the technical solutions provided in this specification can still be used to accurately identify the black market merchant based on transaction data of the merchant, to implement precise prevention and control on the black market merchant. Further, according to the technical solutions provided in this specification, when the first black market merchant is determined, more other black market

merchants can be mined in a timely manner based on the historical transaction data related to the first black market merchant, so that more black market merchants can be identified in a more timely manner, to help improve timeliness of risk prevention and control.

[0026] FIG. 1 is a schematic diagram of a transaction risk control scenario according to an embodiment of this specification. As shown in FIG. 1, the scenario 100 can include a user 110, a merchant 120, and a transaction platform 130.

[0027] The user 110 can be a person who buys a product or a service on the transaction platform 130. The user 110 can also be referred to as a consumer.

[0028] The merchant 120 can be a merchant joining the transaction platform 130. The merchant 120 can conduct a commercial activity on the transaction platform 130, for example, provide the user 110 with the product or the service.

[0029] The transaction platform 130 can be a system or platform that provides the user 110 and the merchant 120 with a transaction service. The transaction platform 130 can be considered as a bridge between the user 110 and the merchant 120, and can provide the user 110 and the merchant 120 with a transaction environment. For example, the transaction platform 130 can be an electronic commerce platform, a financial transaction platform, an acquiring platform, etc. In some embodiments, the transaction platform 130 can further provide a payment service between the user 110 and the merchant 120. In some embodiments, the transaction platform 130 can further cooperate with a third-party payment platform, to provide the payment service between the user 110 and the merchant 120 on the third-party payment platform.

[0030] The user 110 and the merchant 120 can complete a transaction on the transaction platform 130. For example, the transaction platform 130 can include a client and a server. The client can display an interaction page to the user 110, and the product or the service provided by the merchant 120 can be displayed on the interaction page. The user 110 can select a target product or a target service on the interaction page and place an order, and the user 110 can further pay for the transaction on the interaction page. The server can interact with the client in response to an operation performed by the user on the interaction page, to provide the client with a necessary background service, for example, the transaction service and the payment service. After the user 110 completes payment, the merchant 120 can obtain an amount corresponding to the transaction.

[0031] The transaction platform 130 can further store transaction data corresponding to each transaction. Still as shown in FIG. 1, the scenario 100 can further include a database 150. The

database 150 is configured to store historical transaction data generated on the transaction platform 130. For example, the database 150 can store transaction data corresponding to a plurality of historical transactions. Transaction data corresponding to each historical transaction can include but is not limited to a user identifier, a merchant identifier, a transaction time, a transaction amount, a payment place, a payment account, and a collection account, It should be noted that the historical transaction data in the database 150 can be stored in a plurality of manners. A storage manner of the historical transaction data is not limited in this specification. To display the historical transaction data intuitively, a graph structure is used to represent the historical transaction data in FIG. 1. For example, in the database 150, one circle can represent one user, one rectangular box can represent one merchant, and an edge connected between the circle and the rectangular box can represent a transaction between the user and the merchant.

[0032] In a transaction scenario, to ensure transaction security, the transaction platform 130 further needs to perform risk control on a transaction between the user 110 and the merchant 120. For example, as shown in FIG. 1, the scenario 100 can further include a risk control system 140. The risk control system 140 can be a system that provides the transaction platform 130 with a risk control service. The risk control system 140 can provide the transaction platform 130 with some risk control policies. The risk control policies are used to prevent occurrence of risk events such as fraud, money laundering, and malicious operations, to improve transaction security.

[0033] In some embodiments, the risk control system 140 can be independently developed by a transaction service provider and integrated within the transaction platform 130, and serve as a service module of the transaction platform 130. In some embodiments, the risk control system 140 can alternatively be used as an external system of the transaction platform 130, and is provided by an external risk control service provider. When the transaction platform 130 needs to use the risk control service, a risk control interface provided by the risk control system 140 can be invoked to use the risk control service provided by the risk control system 140.

[0034] A black market merchant mining method provided in this specification can be performed by the risk control system 140. The risk control system 140 can store data or instructions of the black market merchant mining method described in this specification, and can execute or be configured to execute the data or the instructions. In some embodiments, the risk control system 140 can include a hardware device with a data information processing function and a necessary program required for driving the hardware device to work.

[0035] For example, with reference to FIG. 1, the risk control system 140 can obtain the historical transaction data from the database 150. After determining a first black market merchant, the risk control system 140 can determine a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant; and further, determine more other black market merchants (namely, a second black market merchant) from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user. Further, after obtaining more other black market merchants through mining, the risk control system 140 can update a risk control policy corresponding to these black market merchants, and provide an updated risk control policy for the transaction platform 130. Therefore, the transaction platform 130 can perform prevention and control on a transaction risk of the black market merchant in a timely and effective manner based on the updated risk control policy.

[0036] FIG. 2 is a diagram of a hardware structure of a computing system 200 according to an embodiment of this specification. The computing system 200 can serve as the risk control system 140 in FIG. 1. The computing system 200 can perform a black market merchant mining method described in this specification.

[0037] As shown in FIG. 2, the computing system 200 can include at least one storage medium 230 and at least one processor 220. In some embodiments, the computing system 200 can further include a communication port 250, an internal communication bus 210, and an I/O component 240.

[0038] The internal communication bus 210 can be connected to different system components. For example, the storage medium 230, the processor 220, the communication port 250, and the I/O component 240 can be connected through the internal communication bus 210.

[0039] The I/O component 240 supports an input/output between the computing system 200 and another component.

[0040] The communication port 250 is used for data communication between the computing system 200 and the outside. For example, the communication port 250 can be used for data communication between the computing system 200 and a network. The communication port 250 can be a wired communication port, or can be a wireless communication port.

[0041] The storage medium 230 can include a data storage apparatus. The data storage apparatus can be a non-transitory storage medium, or can be a transitory storage medium. For example, the data storage apparatus can include one or more of a disk 232, a read-only storage

medium (ROM) 234, or a random access storage medium (RAM) 236. The storage medium 230 further includes at least one instruction set stored in the data storage apparatus. The instruction set can be computer program code. The computer program code can include a program, a routine, an object, a component, a data structure, a process, a module, etc. for performing the black market merchant mining method provided in this specification.

[0042] The at least one processor 220 is configured to execute the at least one instruction set. The processor 220 can be in a form of one or more processors. In some embodiments, the processor 220 can include one or more hardware processors, for example, a microcontroller, a microprocessor, a reduced instruction set computer (RISC), an application-specific integrated circuit (ASIC), an application-specific instruction set processor (ASIP), a central processing unit (CPU), a graphics processing unit (GPU), a physical processing unit (PPU), a microcontroller unit, a digital signal processor (DSP), a field programmable gate array (FPGA), an advanced RISC machine (ARM), a programmable logic device (PLD), any circuit or processor that can perform one or more functions, or any combination thereof.

[0043] To merely describe a problem, only one processor 220 is shown in the computing system 200 in the accompanying drawings. However, it should be noted that, the computing system 200 provided in this specification can further include a plurality of processors. Therefore, the operations and/or method steps disclosed in this specification can be performed by one processor, or can be jointly performed by a plurality of processors. For example, if the processor 220 in the computing system 200 described in this specification performs step A and step B, it should be understood as that step A and step B can be jointly or separately performed by two different processors 220 (for example, a first processor performs step A, and a second processor performs step B, or a first processor and a second processor jointly perform step A and step B).

[0044] FIG. 3 is a flowchart of a black market merchant mining method P300 according to an embodiment of this specification. As described above, a computing system 200 can perform the black market merchant mining method P300 in this specification. Specifically, a processor 220 in the computing system 200 can read an instruction set stored in a local storage medium of the computing system 200, and then perform the black market merchant mining method P300 in this specification based on a stipulation of the instruction set.

[0045] As shown in FIG. 3, the black market merchant mining method P300 can include the following steps.

[0046] S320: Determine a first black market merchant.

[0047] According to the black market merchant mining method P300 provided in this specification, more other black market merchants can be mined based on a known black market merchant when the black market merchant is known. For ease of description, in this specification, the known black market merchant is referred to as the first black market merchant (or an initial black market merchant), and another black market merchant mined based on the first black market merchant is referred to as a second black market merchant. Specifically, in S320, a risk control system 140 can first determine the first black market merchant. Then, the risk control system 140 performs subsequent S340 and S360, so that the second black market merchant is mined based on the first black market merchant.

[0048] It should be noted that in actual applications, the risk control system 140 can determine one or more first black market merchants in S320. When there are a plurality of first black market merchant, the risk control system 140 can separately perform subsequent S340 and S360 for each first black market merchant, in other words, separately execute a process of mining the second black market merchant for each first black market merchant.

[0049] The risk control system 140 can determine the first black market merchant in a plurality of manners. The following provides example descriptions by using several possible implementations as examples.

[0050] In some embodiments, the risk control system 140 can receive customer complaint information for a target transaction. In response to the customer complaint information, the risk control system 140 determines that a target merchant associated with the target transaction is the first black market merchant.

[0051] The customer complaint information can be complaint information of a customer (namely, a user). For example, when the user encounters a problem such as a fraud in a process of executing the target transaction with a merchant, and considers that the merchant may be a risk merchant, the user can send customer complaint information to a transaction platform 130. The customer complaint information can include related information of the target transaction, a complaint reason, etc. After receiving the customer complaint information, the transaction platform 130 can forward the customer complaint information to the risk control system 140. After receiving the customer complaint information, the risk control system 140 determines that the target merchant associated with the target transaction is the first black market merchant. Because

the customer complaint information is risk information directly fed back by a participant (namely, the user) of the target transaction, and has relatively high reliability, the risk control system 140 determines the first black market merchant based on the customer complaint information, so that accuracy of the determined first black market merchant can be ensured.

[0052] In some embodiments, after receiving the customer complaint information, the risk control system 140 can further identify, based on the customer complaint information and other multi-dimensional information, whether the target merchant associated with the target transaction is a black market merchant. The multi-dimensional information includes at least one of the following: merchant information of the target merchant, historical transaction data associated with the target merchant, and historical customer complaint information associated with the target merchant. The risk control system 140 determines a risk level of the target merchant based on the multi-dimensional information. If the risk level is higher than or equal to a preset level, the risk control system 140 determines the target merchant as the first black market merchant.

[0053] The multi-dimensional information can include but is not limited to: transaction information of the target transaction, transaction information of a historical transaction, service conduction information of the target merchant, etc. For example, when the customer complaint information represents that the target merchant has a fraud behavior, the risk control system 140 can view whether same or similar customer complaint information exists in a historical transaction associated with the target merchant. If yes, the risk control system 140 can determine that the target merchant associated with the target transaction is the first black market merchant. For another example, when the customer complaint information represents that the target merchant has a fraud behavior, the risk control system 140 can determine, based on the transaction information of the target transaction and the service conduction information of the target merchant, whether the target merchant is a black market merchant. For example, if a transaction product involved in the transaction information of the target transaction is a book, and the service conduction information of the target merchant does not involve book-type service conduction content, the risk control system 140 can determine that a merchant associated with the target transaction is the first black market merchant.

[0054] In the above-mentioned solution, after receiving the customer complaint information, the risk control system 140 comprehensively determines, based on the customer complaint information and other more-dimensional information, whether to use, as the first black market

merchant, the target merchant associated with the target transaction, to further improve accuracy of the determined first black market merchant.

[0055] In some embodiments, the risk control system can further determine the first black market merchant based on reported information of the merchant. For example, the risk control system can inspect, in a preset period, a merchant that joins the transaction platform. In an inspection process, the risk control system verifies authenticity of each merchant based on reported information of the merchant (that is, verifies authenticity of a merchant body). If reported information of a specific merchant is incomplete or includes false information, the risk control system can determine that the merchant is the first black market merchant. The reported information is basic information and a proof material that need to be provided before the merchant joins the transaction platform. The reported information can include basic information, legal person information, service conduction information, a bank account, etc. of the merchant.

[0056] In some embodiments, the risk control system can determine the first black market merchant based on a merchant blacklist. For example, the risk control system can use a specific merchant in the merchant blacklist as the first black market merchant. The merchant blacklist includes a merchant who is listed in a barred transaction list or a restricted transaction list due to violation of a specific rule, a fraud behavior, or another bad behavior. A common reason for being added to the merchant blacklist can include but is not limited to one or more of the following: a fraud behavior, a violation operation, violation of a platform rule, frequent customer complaints, suspected involvement in money laundering, or another financial violation behavior.

[0057] S340: Determine a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant, where the black market user is a person who performs a transaction test on the first black market merchant.

[0058] As mentioned above, a black market usually registers a merchant (namely, the black market merchant) on the transaction platform, to use the merchant to conduct an illegal commercial activity for a profit. In actual applications, after registering the black market merchant on the transaction platform, the black market enables some "test persons" to first try to conduct a transaction with the black market merchant, to ensure that the black market merchant can normally conduct a transaction activity, and a transaction is not blocked by the transaction platform. The black market user helps the black market merchant conduct a transaction test, to ensure that another

normal user can successfully make a transaction with the black market merchant. In this specification, the "test person" is referred to as a black market user, and a transaction between the black market user and the black market merchant is referred to as a test transaction. For distinguishing, in this specification, a user other than the black market user is referred to as a normal user, and a transaction between the normal user and the black market merchant is referred to as a normal transaction.

[0059] After determining the first black market merchant, the risk control system can obtain, from a database, the historical transaction data associated with the first black market merchant. Further, the risk control system determines the black market user from the user set with the transaction relationship with the first black market merchant based on the historical transaction data associated with the first black market merchant. "With the transaction relationship" can mean that a transaction has occurred. For example, if a user X and a merchant Y have a transaction relationship, it indicates that the user X and the merchant Y have made a transaction. For example, the risk control system can determine, based on the historical transaction data associated with the first black market merchant, that the user set with the transaction relationship with the first black market merchant is {user 1, user 2, user 3, user 4, user 5}, and the risk control system can determine the black market user from the user set.

[0060] The test transaction usually occurs after the black market merchant is registered and before the normal transaction occurs. In other words, the test transaction is usually several transactions executed first after the black market merchant is registered. Therefore, in some embodiments, the risk control system can determine, based on the above-mentioned features, transaction data of N historical transactions from the historical transaction data associated with the first black market merchant. The N historical transactions are N transactions occurring first after the first black market merchant is registered, and N is an integer greater than or equal to 1. Further, the risk control system can determine, based on the transaction data of the N historical transactions, the black market user from a user associated with the N historical transactions.

[0061] For example, if N=1, the risk control system can determine that a user associated with the 1st transaction that occurs after the first black market merchant is registered is the black market user. For another example, if N=2, the risk control system can determine the 1st transaction and the 2nd transaction that occur after the first black market merchant is registered. If a user associated with the 1st transaction is a user 1, and a user associated with the 2nd transaction is a user 2, the risk

control system can determine a black market user from the user 1 and the user 2. For example, the risk control system uses both the user 1 and the user 2 as black market users, or uses one of the user 1 and the user 2 as a black market user.

[0062] In the above-mentioned solution, the risk control system finds the N historical transactions occurring first after the first black market merchant is registered, and then determines a black market user from the user associated with the N historical transactions. Such a black market user identification manner is based on a feature "the transaction test occurs after the black market merchant is registered and before a service is normally conducted". Therefore, the black market user can be accurately identified.

[0063] Further, when performing the transaction test on the first black market merchant, the black market user mainly tests a transaction path of the first black market merchant. A transaction amount of the test transaction initiated by the black market user is usually relatively small, to reduce test costs. That is, the transaction amount of the test transaction is less than a preset amount. A value of the preset amount is not limited in this specification, and can be set based on an actual application scenario.

[0064] Therefore, in some embodiments, the risk control system can further consider the feature "the transaction amount of the test transaction is relatively small" when identifying the black market user. For example, after determining the N historical transactions occurring first after the first black market merchant is registered, the risk control system can determine, from the N historical transactions based on the transaction data of the N historical transactions, a first transaction that satisfies a first condition. The first condition includes: the transaction amount is less than or equal to the preset amount. Further, the risk control system determines that a user associated with the first transaction is a black market user.

[0065] In the above-mentioned solution, the risk control system identifies the black market user not only based on the feature "the transaction test occurs after the black market merchant is registered and before a service is normally conducted", but also based on the feature "the transaction amount of the test transaction is relatively small", to improve accuracy of the identified black market user.

[0066] In actual applications, it is found that the black market usually registers a large quantity of black market merchants in batches in a plurality of different areas. When the black market merchants are offline transaction merchants, because the black market merchants are distributed

in different areas, the black market user usually does not perform a transaction test in the areas in which the black market merchants are located; instead, performs a remote transaction test on the black market merchants through a specific technical means. In this way, test costs can be reduced. Based on this, the test transaction initiated by the black market user usually has the following feature: a payment location of the test transaction is not in the same geographical area as a merchant location of the black market merchant.

[0067] It should be noted that a division manner of the geographical area is not limited in this specification. "The payment location of the test transaction is not in the same geographical area as the merchant location of the black market merchant" can be understood as that the payment location is obviously different from the merchant location of the black market merchant. For example, the payment location is in a country A, and the merchant location of the black market merchant is in a country B. For another example, the payment location and the merchant location of the black market merchant are located in the same country, but correspond to different areas.

[0068] Therefore, in some embodiments, the risk control system can further consider the feature "the payment location of the test transaction is not in the same geographical area as the merchant location of the black market merchant" when identifying the black market user. For example, after determining the N historical transactions occurring first after the first black market merchant is registered, the risk control system can determine, from the N historical transactions based on the transaction data of the N historical transactions, the first transaction that satisfies the first condition. The first condition includes: the transaction amount is less than or equal to a preset transaction amount, and the payment location is not in the same geographical area as the merchant location of the black market merchant. Further, the risk control system determines that the user associated with the first transaction is a black market user.

[0069] For example, the risk control system determines a transaction amount and a payment location from transaction data of each of the N historical transactions for the historical transaction, and determines, based on the transaction amount and the payment location, whether the historical transaction satisfies the first condition. When the first condition is satisfied, the risk control system determines the historical transaction as the first transaction. It should be noted that the risk control system can determine one or more first transactions. This is not limited in this specification. When there are a plurality of first transactions, the risk control system can use a user associated with the plurality of first transactions as a black market user. That is, the risk control system can determine

one or more black market users.

[0070] In some embodiments, when determining a payment location of a historical transaction, the risk control system can determine the payment location based on an IP address field in transaction information of the historical transaction, or can determine the payment location based on an LBS-related field in transaction information of the historical transaction, or can determine the payment location based on both an IP address field and an LBS-related field in transaction information of the historical transaction. The IP address field and the LBS-related field in the transaction information represent location information of a terminal device used when a user initiates a transaction. Therefore, a payment location of the transaction is determined based on the IP address field and/or the LBS-related field in the transaction information, to ensure accuracy of the payment location.

[0071] In the above-mentioned solution, the risk control system identifies the black market user based on all of the following three features of the test transaction: "the transaction test occurs after the black market merchant is registered and before a service is normally conducted", "the transaction amount of the test transaction is relatively small", and "the payment location of the test transaction is not in the same geographical area as the merchant location of the black market merchant". Therefore, accuracy of the identified black market user can be further improved.

[0072] The following provides example descriptions of a black market user identification process with reference to FIG. 4.

[0073] FIG. 4 is a schematic diagram of historical transaction data according to an embodiment of this specification. In FIG. 4, a circle represents a user, a rectangular box represents a merchant, and an edge between the circle and the rectangular box represents a transaction between the user and the merchant. It can be learned that the historical transaction data shown in FIG. 4 can reflect transaction relationships between a plurality of users and a plurality of merchants.

[0074] As shown in FIG. 4, it is assumed that the risk control system receives customer complaint information for the target transaction, and the target transaction is a transaction between a user 5 and a merchant A. In this case, the risk control system can determine, based on the customer complaint information or based on the customer complaint information and other more-dimensional information, that the merchant A is the first black market merchant.

[0075] Still as shown in FIG. 4, the first black market merchant (merchant A) has a total of five historical transactions, and users associated with the five historical transactions are a user 1,

a user 2, a user 3, a user 4, and a user 5. The risk control system can determine the black market user from the five users based on historical transaction data associated with the first black market merchant (merchant A).

[0076] Specifically, the risk control system can find, in the five historical transactions based on the historical transaction data associated with the first black market merchant (merchant A), a transaction that satisfies the following condition, and use the transaction as a test transaction:

[0077] Condition X1: The transaction is in the first N transactions occurring first after the first black market merchant (merchant A) is registered.

[0078] Condition X2: The transaction amount is less than or equal to the preset amount.

[0079] Condition X3: The payment location is not in the same geographical area as the merchant location of the first black market merchant (merchant A).

[0080] It should be noted that the risk control system can selectively use some or all of the three conditions with reference to a specific application scenario. For example, when the first black market merchant is an online merchant, the risk control system can use the condition X1 and the condition X2. When the first black market merchant is an offline merchant, the risk control system can use the condition X1, the condition X2, and the condition X3. When a quantity of historical transactions of the first black market merchant is relatively small, the risk control system can use the condition X1 or the condition X2.

[0081] Further, after finding the test transaction, the risk control system can determine that a user associated with the test transaction is a black market user. For example, as shown in FIG. 4, it is assumed that the risk control system determines, based on the above-mentioned conditions in a historical transaction associated with the first black market merchant (merchant A), that a transaction between the user 1 and the first black market merchant (merchant A) is a test transaction. In this case, the risk control system can use the user 1 as a black market user.

[0082] S360: Determine a second black market merchant from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user.

[0083] The second black market merchant is another black market merchant mined based on the first black market merchant. It should be noted that in actual applications, the risk control system 140 can determine one or more second black market merchants in S360.

[0084] As mentioned above, the black market usually registers a plurality of black market

merchants in batches on the transaction platform for collection. The black market performs a transaction test on the black market merchants, to ensure that the black market merchants can normally conduct transactions, and the transactions are not blocked by the transaction platform. To reduce test costs, the black market performs a transaction test on the plurality of black market merchants by using the same "test person". In other words, these black market merchants all make transactions with the "test person". When the risk control system has found the black market user (namely, the "test person") in S340, a merchant who has made a historical transaction with the black market user is very likely to be a black market merchant. Therefore, the risk control system 140 can determine the second black market merchant from the merchant set with the transaction relationship with the black market user based on the historical transaction data associated with the black market user. For example, in the merchant set with the transaction relationship with the black market user, a merchant other than the first black market merchant is determined as a second black market merchant. In this method, more comprehensive second black market merchants can be mined based on the black market user.

[0085] As mentioned above, the test transaction is usually several transactions executed first after the black market merchant is registered. Therefore, in some embodiments, the risk control system can determine, based on the above-mentioned features, the merchant set with the transaction relationship with the black market user based on the historical transaction data associated with the black market user; and find, in the merchant set based on historical transaction data associated with each merchant in the merchant set, a merchant that satisfies a second condition. The second condition includes: N transactions occurring first after registration include a second transaction made with the black market user, and N is an integer greater than or equal to 1. Further, the risk control system can use, as the second black market merchant, the merchant that satisfies the second condition.

[0086] In the above-mentioned solution, the risk control system finds the merchant set with the transaction relationship with the black market user, and determines whether each merchant in the merchant set satisfies a condition "a transaction with the black market user is in the N transactions occurring first after the merchant is registered". If a specific merchant satisfies the second condition, the risk control system determines that the merchant is a second black market merchant. Such a second black market merchant identification manner is based on the feature "the transaction test occurs after the black market merchant is registered and before a service is

normally conducted". Therefore, the second black market merchant can be accurately identified.

[0087] As mentioned above, when the black market user performs a transaction test on the second black market merchant, a transaction amount of the test transaction initiated by the black market user is usually relatively small, to reduce test costs. That is, the transaction amount of the test transaction is less than the preset amount. Therefore, in some embodiments, the risk control system can further consider the feature "the transaction amount of the test transaction is relatively small" when identifying the second black market merchant. In other words, the second condition used when the risk control system identifies the second black market merchant can further include: a transaction amount of the second transaction is less than or equal to the preset amount. For example, after determining the merchant set with the transaction relationship with the black market user, the risk control system determines whether each merchant in the merchant set satisfies the following two conditions: "the transaction with the black market user is in the N transactions occurring first after the merchant is registered" and "the transaction amount with the black market user is less than or equal to the preset amount". If a specific merchant satisfies the above-mentioned two conditions, the merchant is determined as a second black market merchant.

[0088] In the above-mentioned solution, the risk control system identifies the second black market merchant not only based on the feature "the transaction test occurs after the black market merchant is registered and before a service is normally conducted", but also based on the feature "the transaction amount of the test transaction is relatively small", to improve accuracy of the identified second black market merchant.

[0089] As mentioned above, the test transaction initiated by the black market user usually has the following feature: the payment location of the test transaction is not in the same geographical area as the merchant location of the black market merchant. Therefore, in some embodiments, the risk control system can further consider the feature "the payment location of the test transaction is not in the same geographical area as the merchant location of the black market merchant" when identifying the second black market merchant. In other words, the second condition used when the risk control system identifies the second black market merchant can further include: the payment location is not in the same geographical area as the merchant location of the black market merchant. For example, after determining the merchant set with the transaction relationship with the black market user, the risk control system determines whether each merchant in the merchant set satisfies the following three conditions: "the transaction with the black market user is in the N transactions

occurring first after the merchant is registered", "the transaction amount with the black market user is less than or equal to the preset transaction amount", and "a payment location of the transaction with the black market user is not in the same geographical area as the merchant location of the black market merchant". If a specific merchant satisfies the above-mentioned three conditions, the merchant is determined as a second black market merchant.

[0090] It should be noted that for a manner of determining the payment location of the transaction, references can be made to the above-mentioned related descriptions. Details are omitted here for simplicity.

[0091] In the above-mentioned solution, the risk control system identifies the second black market merchant based on all of the following three features of the test transaction: "the transaction test occurs after the black market merchant is registered and before a service is normally conducted", "the transaction amount of the test transaction is relatively small", and "the payment location of the test transaction is not in the same geographical area as the merchant location of the black market merchant". Therefore, accuracy of the identified second black market merchant can be further improved.

[0092] In some embodiments, after determining the merchant set with the transaction relationship with the black market user, the risk control system can further rule out a merchant in a whitelist from the merchant set. The whitelist can be a merchant list including a merchant without a risk. Further, the risk control system determines whether each remaining merchant in the merchant set satisfies the second condition, and determines that a merchant that satisfies the second condition is a second black market merchant.

[0093] In the above-mentioned solution, in addition to identifying the second black market merchant based on the second condition, the risk control system first rules out the merchant in the whitelist from the merchant set with the transaction relationship with the black market user. In this way, the merchant in the whitelist can be prevented from being identified as a second black market merchant, to reduce a probability of wrong determining, and further improve accuracy of the identified second black market merchant.

[0094] It should be noted that, the risk control system can determine one or more second black market merchants based on one black market user. This is not limited in this specification.

[0095] The following provides example descriptions of a second black market merchant identification process with reference to FIG. 4.

[0096] As shown in FIG. 4, it is assumed that the risk control system determines that the user 1 is a black market user in S340. The user 1 has a total of four historical transactions, and merchants associated with the four historical transactions are a merchant A, a merchant B, a merchant C, and a merchant D. Because the risk control system has determined that the merchant A is a first black market merchant, the risk control system can determine the second black market merchant from the other three merchants (the merchant B, the merchant C, and the merchant D) other than the merchant A.

[0097] Specifically, the risk control system can determine, from the three merchants (the merchant B, the merchant C, and the merchant D) based on historical transaction data associated with the user 1, a merchant that satisfies the following conditions:

[0098] Condition Y1: A transaction with the user 1 is in the first N transactions occurring first after the merchant is registered.

[0099] Condition Y2: A transaction amount of the transaction with the user 1 is less than or equal to the preset amount.

[0100] Condition Y3: A payment location of the transaction with the user 1 is not in the same geographical area as the merchant location.

[0101] The merchant D is taken as an example. The risk control system can determine whether the merchant D satisfies the condition Y1, that is, determine whether a transaction (namely, the second transaction) between the user 1 and the merchant D is in the first N transactions occurring first after the merchant D is registered. If yes, the risk control system can continue to determine whether the merchant D satisfies the condition Y2, that is, determine whether a transaction amount of the transaction (namely, the second transaction) between the user 1 and the merchant D is less than or equal to the preset amount. If yes, the risk control system can continue to determine whether the merchant D satisfies the condition Y3, that is, determine whether a payment location of the transaction (namely, the second transaction) between the user 1 and the merchant D is not in the same geographical area as the merchant location of the merchant D. If yes, the risk control system determines that the merchant D is a merchant that satisfies the above-mentioned conditions, and determines that the merchant D is the second black market merchant.

[0102] It should be noted that the risk control system can selectively use some or all of the three conditions with reference to a specific application scenario. For example, when the merchant D is an online merchant, the risk control system can use the condition Y1 and the condition Y2.

When the merchant D is an offline merchant, the risk control system can use the condition Y1, the condition Y2, and the condition Y3. When a quantity of historical transactions of the merchant D is relatively small, the risk control system can use the condition Y1 or the condition Y2.

[0103] Similar to a manner of determining the merchant D, the risk control system determines, in the same manner, whether the merchant C and the merchant B are second black market merchants. Details are omitted here for simplicity. FIG. 4 shows an example in which the identified second black market merchant includes the merchant D.

[0104] How the risk control system obtains the second black market merchant based on the known first black market merchant through mining is described above. A person skilled in the art can understand that the black market merchant mining method provided in this specification can be cyclically performed. For example, after the risk control system identifies the second black market merchant in S320 to S360 described above, the second black market merchant can be used as the first black market merchant in S320, and a black market merchant mining process described in S320 to S360 is repeatedly performed, to obtain more black market merchants through mining. It can be learned that according to the black market merchant mining method provided in this specification, all other possible black market merchants can be mined as much as possible based on one black market merchant, to help control the other black market merchants in a timely manner, and avoid, in a timely manner, a transaction risk brought by the other black market merchants.

[0105] In some embodiments, after obtaining the first black market merchant and the second black market merchant through mining, the risk control system can adjust a risk control policy of the first black market merchant and the second black market merchant. Risk control strength of an adjusted risk control policy is higher than risk control strength of the risk control policy existing before adjustment.

[0106] In this specification, the risk control policy can be a risk control rule that is formulated by the risk control system for different merchants to perform risk management on the merchants. Different merchants can correspond to different risk control policies. The risk control policy can include but is not limited to a merchant limit policy or a merchant transaction frequency control policy. For example, after obtaining the first black market merchant and the second black market merchant through mining, the risk control system can reduce a limit of the first black market merchant and the second black market merchant, so that the first black market merchant and the second black market merchant cannot make a large transaction or cannot make any transaction.

For another example, the risk control system can limit a transaction frequency of the first black market merchant and the second black market merchant, so that the first black market merchant and the second black market merchant cannot make a high-frequency transaction or cannot make any transaction.

[0107] In some embodiments, after obtaining the first black market merchant and the second black market merchant through mining, the risk control system can further evaluate a risk level of the first black market merchant and the second black market merchant, and further adjust the risk control policy of the first black market merchant and the second black market merchant based on a risk level evaluation result. For example, the risk control system can determine a risk level of the first black market merchant based on the historical transaction data, reported information, etc. of the first black market merchant, and adjust a risk control policy of the first black market merchant based on the risk level of the first black market merchant. The risk control system can determine a risk level of the second black market merchant based on historical transaction data, reported information, etc. of the second black market merchant, and further adjust a risk control policy of the second black market merchant based on the risk level of the second black market merchant. For specific content of the risk control policy and an adjustment manner of the risk control policy, references can be made to the above-mentioned related descriptions. Details are omitted here for simplicity.

[0108] Further, the risk control system transfers the adjusted risk control policy to the transaction platform. The transaction platform controls, based on the adjusted risk control policy, a transaction of the first black market merchant and the second black market merchant, so that the transaction platform can perform prevention and control on a risk transaction of the first black market merchant and the second black market merchant in a timely manner, to improve transaction security on the transaction platform.

[0109] In conclusion, in the black market merchant mining method provided in this specification, after determining the first black market merchant, the risk control system can determine the black market user (namely, a person who performs a transaction test on the first black market merchant) from the user set with the transaction relationship with the first black market merchant based on the historical transaction data associated with the first black market merchant; and further, determine the second black market merchant from the merchant set with the transaction relationship with the black market user based on the historical transaction data

associated with the black market user. It can be learned that according to the above-mentioned solution, the black market merchant can be mined based on historical transaction data between the user and the merchant. Even if reported information provided by the black market merchant is relatively complete, the above-mentioned solution can still be used to accurately identify the black market merchant in a transaction stage of the black market merchant, to implement precise prevention and control on the black market merchant. Further, according to the above-mentioned solution, when the first black market merchant is determined, more other black market merchants can be mined in a timely manner based on the historical transaction data related to the first black market merchant, so that more other black market merchants can be identified in a more timely manner, to help improve timeliness of risk prevention and control.

[0110] Another aspect of this specification provides a computer-readable non-transitory storage medium. The computer-readable non-transitory storage medium stores at least one instruction set, to perform black market merchant mining. When the at least one instruction set is executed by a processor, the at least one instruction set instructs the processor to implement steps of the black market merchant mining method P300 described in this specification. In some possible implementations, aspects of this specification can further be implemented in a form of a program product, including program code. When the program product runs on a computing system 200, the program code is used to enable the computing system 200 to perform steps of the black market merchant mining method P300 described in this specification. The program product used to implement the above-mentioned method can be a portable compact disk read-only memory (CD-ROM) including program code, and can run on the computing system 200. However, the program product in this specification is not limited thereto. In this specification, a readable storage medium can be any tangible medium that includes or stores a program, and the program can be used by or in combination with an instruction execution system. The program product can be any combination of one or more readable media. The readable medium can be a readable signal medium or a readable storage medium. The readable storage medium can be, for example, an electrical system, apparatus, or device, a magnetic system, apparatus, or device, an optical system, apparatus, or device, an electromagnetic system, apparatus, or device, an infrared system, apparatus, or device, or a semiconductor system, apparatus, or device, or any combination thereof. More specific examples of the readable storage medium include: an electrical connection including one or more conducting wires, a portable disk, a hard disk, a random access memory (RAM), a read-only

memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage component, a magnetic storage component, or any proper combination thereof. The computer-readable storage medium can include a data signal propagated in a baseband or as part of a carrier, and carries readable program code. The propagated data signal can be in a plurality of forms, and includes but is not limited to an electromagnetic signal, an optical signal, or any proper combination thereof. The readable storage medium can further be any readable medium other than the readable storage medium, and the readable medium can be used to send, propagate, or transmit a program used by or in combination with an instruction execution system, apparatus, or component. The program code included in the readable storage medium can be transmitted in any proper medium, including but not limited to a wireless medium, a wired medium, optical cable, an RF medium, or any proper combination thereof. Program code for performing an operation of this specification can be written in any combination of one or more program design languages. The program design language includes an object-oriented program design language, for example, Java or C++, and further includes a conventional procedural program design language, for example, "C" language, or a similar program design language. The program code can be completely executed on the computing system 200, partially executed on the computing system 200, executed as an independent software package, partially executed on the computing system 200 and partially executed on a remote computing device, or completely executed on a remote computing device.

[0111] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multitasking and parallel processing are possible or may be advantageous.

[0112] In conclusion, after reading the detailed disclosure, a person skilled in the art can understand that the detailed disclosure can be presented only in an example manner, and can impose no limitation. Although it is not explicitly stated here, a person skilled in the art can understand that the requirements of this specification include various proper changes, improvements, and modifications to the embodiments. These changes, improvements, and modifications are intended to be presented in this specification, and fall within the spirit and scope

of the example embodiments of this specification.

[0113] In addition, some terms in this specification are used to describe the embodiments of this specification. For example, "one embodiment", "an embodiment", and/or "some embodiments" mean that particular features, structures, or characteristics described with reference to the embodiments can be included in at least one embodiment of this specification. Therefore, it can be emphasized and understood that two or more of "an embodiment", "one embodiment", or "alternative embodiments" referred in parts of this specification do not necessarily indicate the same embodiment. In addition, particular features, structures, or characteristics can be properly combined in one or more embodiments of this specification.

[0114] It should be understood that in the above-mentioned descriptions of the embodiments of this specification, to help understand a feature, for the purpose of simplifying this specification, various features are combined in a single embodiment, accompanying drawing, or description thereof in this specification. However, this does not mean that the combination of these features is necessary. It is entirely possible for a person skilled in the art to mark some devices and understand the devices as separate embodiments when reading this specification. In other words, the embodiments in this specification can also be understood as an integration of a plurality of secondary embodiments. Content of each secondary embodiment is also true when features are less than all features in one of the above-mentioned disclosed embodiments.

[0115] Each patent, patent application, publication of a patent application, and other materials, for example, articles, books, instructions, publications, documents, and products, that are cited in this specification and that are other than any document that is inconsistent or conflict with this document or that imposes limiting impact on the widest scope of the claims can be incorporated herein by reference and used for all purposes now or later associated with this document. In addition, the term in this document shall prevail when there is any inconsistency or conflict between the description, definition and/or use of a related term in any material and the description, definition and/or use of a related term in this document.

[0116] Finally, it should be understood that the principles of the implementation solutions of this specification are described in the implementation solutions of the application disclosed in this specification. Other modified embodiments also fall within the scope of this specification. Therefore, the embodiments disclosed in this specification are merely examples and not limitations. A person skilled in the art can use an alternative configuration according to the embodiments of

this specification to implement the application in this specification. Therefore, the embodiments of this specification are not limited to the embodiments accurately described in the application.

CLAIMS

What is claimed is:

1. A black market merchant mining method, comprising:

determining a first black market merchant;

determining a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant, wherein the black market user is a person who performs a transaction test on the first black market merchant; and

determining a second black market merchant from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user.

2. The method according to claim 1, wherein the determining a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant comprises:

determining transaction data of N historical transactions from the historical transaction data associated with the first black market merchant, wherein the N historical transactions are N transactions occurring first after the first black market merchant is registered, and N is an integer greater than or equal to 1; and

determining, based on the transaction data of the N historical transactions, the black market user from a user associated with the N historical transactions.

3. The method according to claim 2, wherein the determining, based on the transaction data of the N historical transactions, the black market user from a user associated with the N historical transactions comprises:

determining, from the N historical transactions based on the transaction data of the N historical transactions, a first transaction that satisfies a first condition, wherein the first condition comprises: a transaction amount is less than or equal to a preset amount; and

determining that a user associated with the first transaction is the black market user.

4. The method according to claim 3, wherein the first black market merchant is an offline transaction merchant, and the first condition further comprises: a payment location is not in a same geographical area as a merchant location of the first black market merchant.

5. The method according to claim 1, wherein the determining a second black market merchant from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user comprises:

determining the merchant set with the transaction relationship with the black market user based on the historical transaction data associated with the black market user;

finding, in the merchant set based on historical transaction data associated with each merchant in the merchant set, a merchant that satisfies a second condition, wherein the second condition comprises: N transactions occurring first after registration comprise a second transaction made with the black market user, and N is an integer greater than or equal to 1; and

using, as the second black market merchant, the merchant that satisfies the second condition.

6. The method according to claim 5, wherein the second condition further comprises: a transaction amount of the second transaction is less than or equal to a preset amount.

7. The method according to claim 6, wherein the second condition further comprises: the second black market merchant is an offline transaction merchant, and a payment location of the second transaction is not in a same geographical area as a merchant location of the second black market merchant.

8. The method according to claim 1, wherein the determining a first black market merchant comprises:

in response to receiving customer complaint information for a target transaction, determining that a target merchant associated with the target transaction is the first black market merchant, wherein the customer complaint information is used to indicate that the target merchant is a risk merchant.

9. The method according to claim 8, wherein the determining that a target merchant associated with the target transaction is the first black market merchant comprises:

obtaining multi-dimensional information associated with the target merchant, wherein the multi-dimensional information comprises at least one of the following: merchant information of the target merchant, historical transaction data associated with the target merchant, and historical customer complaint information associated with the target merchant;

determining a risk level of the target merchant based on the multi-dimensional information; and

determining the target merchant as the first black market merchant when the risk level is

higher than or equal to a preset level.

10. The method according to claim 1, wherein the method further comprises:

adjusting a risk control policy of the first black market merchant and the second black market merchant, wherein risk control strength of an adjusted risk control policy is higher than risk control strength of the risk control policy existing before adjustment.

11. A black market merchant mining system, comprising:

at least one storage medium, storing at least one instruction set, to perform black market merchant mining; and

at least one processor, communicatively connected to the at least one storage medium, wherein when the mining system runs, the at least one processor reads the at least one instruction set, and performs the following operations based on an indication of the at least one instruction set:

determining a first black market merchant;

determining a black market user from a user set with a transaction relationship with the first black market merchant based on historical transaction data associated with the first black market merchant, wherein the black market user is a person who performs a transaction test on the first black market merchant; and

determining a second black market merchant from a merchant set with a transaction relationship with the black market user based on historical transaction data associated with the black market user.

12. The system according to claim 11, wherein to determine the black market user from the user set with the transaction relationship with the first black market merchant, the at least one processor performs the following operations:

determining transaction data of N historical transactions from the historical transaction data associated with the first black market merchant, wherein the N historical transactions are N transactions occurring first after the first black market merchant is registered, and N is an integer greater than or equal to 1; and

determining, based on the transaction data of the N historical transactions, the black market user from a user associated with the N historical transactions.

13. The system according to claim 12, wherein to determine the black market user from the user associated with the N historical transactions, the at least one processor performs the following operations:

determining, from the N historical transactions based on the transaction data of the N historical transactions, a first transaction that satisfies a first condition, wherein the first condition comprises: a transaction amount is less than or equal to a preset amount; and

determining that a user associated with the first transaction is the black market user.

14. The system according to claim 13, wherein the first black market merchant is an offline transaction merchant, and the first condition further comprises: a payment location is not in a same geographical area as a merchant location of the first black market merchant.

15. The system according to claim 11, wherein to determine the second black market merchant from the merchant set with the transaction relationship with the black market user, the at least one processor performs the following operations:

determining the merchant set with the transaction relationship with the black market user based on the historical transaction data associated with the black market user;

finding, in the merchant set based on historical transaction data associated with each merchant in the merchant set, a merchant that satisfies a second condition, wherein the second condition comprises: N transactions occurring first after registration comprise a second transaction made with the black market user, and N is an integer greater than or equal to 1; and

using, as the second black market merchant, the merchant that satisfies the second condition.

16. The system according to claim 15, wherein the second condition further comprises: a transaction amount of the second transaction is less than or equal to a preset amount.

17. The system according to claim 16, wherein the second condition further comprises: the second black market merchant is an offline transaction merchant, and a payment location of the second transaction is not in a same geographical area as a merchant location of the second black market merchant.

18. The system according to claim 11, wherein to determine the first black market merchant, the at least one processor performs the following operation:

in response to receiving customer complaint information for a target transaction, determining that a target merchant associated with the target transaction is the first black market merchant, wherein the customer complaint information is used to indicate that the target merchant is a risk merchant.

19. The system according to claim 18, wherein to determine that the target merchant associated with the target transaction is the first black market merchant, the at least one processor

performs the following operations:

obtaining multi-dimensional information associated with the target merchant, wherein the multi-dimensional information comprises at least one of the following: merchant information of the target merchant, historical transaction data associated with the target merchant, and historical customer complaint information associated with the target merchant;

determining a risk level of the target merchant based on the multi-dimensional information; and

determining the target merchant as the first black market merchant when the risk level is higher than or equal to a preset level.

20. A computer-readable nonvolatile storage medium, wherein the computer-readable nonvolatile storage medium stores at least one instruction set, and when the at least one instruction set is executed by at least one processor, the black market merchant mining method according to any one of claims 1 to 10 is implemented.