# 摘要

This paper examines information leakage in distributed ledgers. We show how the lack of time priority in the period between the publication of a transaction and its validation by miners or designated participants can expose a transaction’s “footprint” to the market, resulting in potential front-running and manipulation. We propose a cryptology-based approach for solving information leakage problems in distributed ledgers that relies on using a “hash” (or mathematical identifier) to secure time-priority followed by a second communication revealing more features of the underlying market transaction. Solving the information leakage problem greatly expands the potential applications of private distributed ledger technology.

这篇文章研究了分布式账本技术中的信息泄露问题。我们演示了在交易的公布到比特币矿机或者特定参与者证实交易有效这段时间中，缺乏时序是怎样揭示出交易走向市场的“脚印”，从而导致潜在的非法预先交易和操作。为了解决分布式账本技术中信息泄露问题，我们提出了一个基于密码学的方法。该方法通过“哈希”（或者其他数学标识符）和紧随其后的可以显示更多潜在市场交易信息的二次通讯信息来确保交易时序。信息泄露问题的解决可以增加个人分布式账本技术的潜在应用。

# 引言

Advocates of the blockchain, the distributed ledger technology that underlies Bitcoin,see an almost limitless future for the innovation. Apart from its role in cryptocurrencies,distributed ledger technologies are being developed to handle stock trades, clear and settle leveraged loans, handle catastrophe reinsurance, keep track of land titles and transactions,track the ownership of intellectual properties, facilitate peer-to-peer marketplaces – the list goes on and on. Much of the appeal of the blockchain lies in its use of a decentralized distributed ledger technology in which an immutable single record emerges of the various transactions encased in the blocks. The ability to trade assets in such a setting, along with the emergence of new “smart contracts” that can automatically trigger additional steps such as recording ownership changes or authorizing payments, can have, in the words of the Bank of England, “far-reaching implications for the financial industry”.

用于比特币中的分布式账本技术——区块链技术的先驱者，见证了它在技术革命中的广泛应用前景。除了在加密货币中的应用，分布式账本技术还广泛应用于股票交易，解决杠杆贷款问题，处理巨灾再保险，跟踪解决土地所有权相关事务，知识产权的所有权鉴定，促进P2P市场发展等等。区块链的吸引力很大程度上来自于其使用分散的分布式账本技术，该技术通过不可变单记录反映区块中各种可变的事务。分布式账本技术处理资产交易的能力，连同可以自动触发额外步骤如记录交易变化的所有者或者授权支付的“智慧合同”的出现，将对金融业产生深远的影响。

While not disputing this rosy outlook, we argue in this paper that this new technology comes with some very old problems. In particular, a fundamental problem facing traders in traditional market settings is how to hide their trades and trading intentions from other traders. Disguising a trade’s “footprint” is necessary to keep others from copying, or even worse, “front-running” your trades, thereby extracting rents that should have been yours. A variety of algorithmic and technological solutions are dedicated to this task in current markets. As we discuss here, the same information leakage can take place in a distributed ledger setting. This problem arises because even though the blocks in the blockchain are time-stamped, there is no actual time priority in the process of getting a transaction validated and onto the distributed ledger. One contribution of our paper is to show how information leakage can arise in the interim period between the publication of such a transaction and its validation by miners or designated participants, exposing participants in a distributed ledger to potential front-running and manipulation.

首先，本文主要探讨伴随这项新技术产生的一些古老的问题，而不是争论其乐观的前景。比如，在传统贸易市场中，交易者面对的一个基本问题就是怎样隐藏他们自己的交易和交易倾向。伪装交易的“足迹”是为了保障交易不被他人复制和不被他人非法预先交易而获取了本属于自己的利益。在目前的市场中，已经有许多技术解决方案应用于解决这个问题。我们要在这里讨论的是，类似的信息泄露问题同样发生在分布式账本技术中，即使区块链有时间戳，这个问题仍然越发频繁地发生，在分布式账本技术中验证一个事务有效是没有真正的时间有序的。我们的文章的贡献之一就是展示了信息泄露是怎样在类似事务的公布和其被矿机或者指定参与者验证这段时间升温的，从而导致这些参与者走向潜在的非法预先交易和操作。

A second, and perhaps more important, contribution of this paper is to suggest a solution. We propose a cryptology-based approach for solving information leakage problems in distributed ledgers. Our two-part process uses a “hash” (or mathematical identifier) to secure time-priority which is then followed by a second communication revealing more features of the underlying market transaction. Because the initial hash does not reveal details of the trade, the ability to front-run a transaction before it is stored in the distributed ledger is curtailed. This solution essentially removes the ability to manipulate the order of transactions and so restores time priority to the validation process.

其次，这篇文章更加重要的贡献在于我们提出了一个基于密码学的方法来解决分布式账本技术中的信息泄露问题。我们的两步走程序通过“哈希”（或其他数学标识符）来确保时序，紧随该时序的二次交流可以显示出市场交易的更多潜在的信息。因为原始的哈希不会显示交易的细节，所以可以减少在交易存储前进行非法预先交易。这个方案基本上消除了操纵交易顺序和恢复验证程序的时序的可能性。

Solving the information leakage problem in distributed ledgers greatly expands the feasibility of distributed ledger applications. To date, proposed uses of distributed ledgers are focused mainly on clearing and settlement where there is little ability to profit from any information leakage. In market settings, however, where information leakage is important, our analysis shows how distributed ledgers could be used to operate decentralized markets that safeguard participants’ information. As perhaps befits a new technology, we argue that new cryptography-based tools can provide a solution to an old problem in a new setting.

解决分布式账本技术中的信息泄露问题可以极大地增加分布式账本技术的应用。至今为止，分布式账本技术的应用主要集中于解决哪里有信息泄露的可能，然而，在市场中，哪里有信息泄露很重要，我们的分析策略演示了怎样利用分布式账本技术操作分散市场来保护参与者的信息。也许这更适合于一项新的技术，但是我们认为一项新的基于密码学的工具应该是可以解决新环境中的老问题的。

1. Information Leakage in Distributed Ledgers

# 2. 分布式账本技术中的信息泄露

To understand why information leakage can occur, it is useful to first set out the distinction between centralized and decentralized systems, and how their differences affect transactions processing. Centralized systems (for example, exchanges) are straightforward: they have a single party, usually in a single location, processing transactions and assigning timestamps to them. Decentralized systems (for example, the Bitcoin blockchain) are much more complex: there is no single party, and instead it relies on a network of independent parties geographically dispersed executing an algorithm to process transactions. The most relevant part of this process for the focus of our paper is the sequencing of transactions, where each transaction is assigned a timestamp and an order relative to every other transaction. As we will discuss, it is the limitations of this sequencing process that sets the stage for information leakage to occur.

为了理解信息泄露为什么会发生,首先有必要了解集中式系统和分散式系统的区别，以及他们对交易产生对不同影响。集中式系统（例如外币兑换）是明确的：通常有一个单方面的机构，来处理交易进程和分配时间戳。分散式系统（例如比特币）则复杂得多：没有独立多机构，相反它依赖一个由地理位置上分散的且互相独立的机构组成的网络通过一种算法来进行交易。本文关注的最有意义的一点就是交易的时序，在这个时序中每笔交易被打上时间戳以及与其他任意一笔交易的先后顺序。正如我们想提出的，这个交易时序进程的限制导致了信息泄漏的发生。

A. Transaction processing in decentralized systems

## A. 分散系统中的交易进程

Due to transmission delays in a network, it is impossible to reach a global agreement on the actual order that transactions happen in a decentralized system. Such latency issues are an all too familiar problem in the current high frequency market structure characterizing equity trading, but for a number of reasons this problem is far more challenging in a distributed ledger setting. One such reason is that while the number of nodes (or exchanges) in equity trading is fairly small, the nodes in a distributed ledger system can number in the thousands, or even tens of thousands. A second is that these nodes can be distributed globally, making transmission delays an inevitable feature of the system.

由于网络传输的延迟性，在交易发生的分散系统中不可能达成一个确切时序的共识。这个延迟问题在高频交易市场的公平交易中经常发生，但是这个问题由于一些原因导致其在分布式账本系统中更具挑战性。其中一个原因就是交易节点（比如交易所）的数量在股票交易中非常少，但是在分布式账本系统中的交易点却成千上万。其次，这些交易节点分散在整个系统中，使得交易延迟不可避免。

As a result, the various algorithms employed in a distributed ledger can only attempt to make all parties in the network agree on what (for short time intervals) is essentially an arbitrary ordering of the transactions. In the period between the broadcast of a Bitcoin transaction and its being processed by the network, for example, there are typically no guarantees offered with regards to its order relative to other transactions in the same state or to what timestamp the transaction will eventually be assigned.

因此，目前应用于分布式账本系统中的各种算法仅仅能让网络中各方（在一小段时间内）在什么是交易无序上达成一致。比如，在比特币交易的发布到通过网络传输这段时间中，交易之间的时序没有任何证明，也没有对交易时间戳的分配的证明。

Crucially, the content of any transaction (where we are using transaction in a broader sense to include events such as a trade, a quote, or indication of interest) that will be posted to the distributed ledger will be observable by all or parts of the network in this potentially lengthy period. This visibility allows other participants to act upon the information carried in the transaction before it has been processed and received a guaranteed ordering relative to other transactions. Depending on the algorithm employed, some participants may also be able to alter the relative ordering of transactions, arbitrarily and potentially to their own benefit. And, depending on the extent of these alterations, any changes can range from being undiscoverable to the rest of the network, to being probable but unprovable. Once the transaction has been processed by the network, it will be permanently stored and given a definitive place in the order sequence in the distributed ledger. Only at this point is it possible to offer the guarantee that no new transactions may end up with an earlier time priority than the original transaction.

更重要地，将要在分布式账本系统中发布的交易（我们使用广泛意义上的交易来包含交易、引用、预购等等）内容在这一段潜在的漫长时间内变得对所有或者网络中的部分参与者可见，这就让其他参与者可以在交易得到证明之前根据交易信息进行操作。通过算法，参与者也可以修改交易的相关顺序，从而有意无意地增加自己的收益。根据这个修改的影响范围，任何改变都可以变得对其余网络不可见，可信但无法证明。一旦交易在网络中达成，它将被永久存储，并且在分布式系统中分配一个绝对序号。只有在这个时候才能保证新的交易不会在原交易之前完成。

The lack of time priority in the validation stage applies generally across distributed ledger settings, but its severity depends upon the validation process employed. In particular, public distributed ledgers and private distributed ledgers use different validation methods and, as we discuss below, these methods can affect the information leakage problem.

验证阶段缺少时序通常应用于分布式账本系统中，但是其严重程度取决于验证过程。特别地，公共分布式分类帐和私人分布式分类帐使用不同的验证方法，并且，正如下面我们讨论的，这些方法会导致信息泄露。

B. Transaction processing in Bitcoin and Ethereum

## B. 比特币和以太坊中的交易进程

In a public distributed ledger system like the Bitcoin and Ethereum networks, transactions are processed by “miners” (essentially high powered computers) who write these transactions into blocks, and collect the fees associated with each transaction. There are numerous miners on the network, and which one writes a specific block is random, with the probability of doing so equal to their share of mining power relative to the total. When a transaction is broadcasted, it is forwarded by the network and kept in a transaction pool known as a mempool. When a miner mines a new block, it will consist of transactions from this mempool. The miner can reorder or censor transactions as they see fit, to the point where empty blocks (with no transactions) are perfectly valid. This behavior, combined with infrequent generation of blocks, can result in unpredictable delays between a transaction being broadcast and it being assigned an order relative to other transactions in the distributed ledger. As Figure 1 shows, these delays in Bitcoin have typically been around 10 minutes, but they can be much longer due to there being no theoretical upper bound on how long it can take.

在如比特币和以太坊为代表的公共分布式分类账本系统中，交易通过“矿机”（通常是高性能电脑）向对应区块中写入交易信息并收集每笔交易的费用进行。互联网上的矿机数量非常庞大，矿机写入的区是随机的，就有可能 当一个交易发布后，它将通过网络推进并且存储在一个称为交易池的内存池中，矿机写入新的区块中的信息包含来自内存池中的交易。矿机根据配置重新排序或审查交易，在这个时候，空区（没有任何交易的区）也是完全合法的。这种行为，连同区块的少有的分区，会导致在分布式账本技术中，交易的公布到其被确定分配相对于其他交易的顺序之间出现不可预见的延迟。如图1所示，在比特币中这类延迟达到了10分钟，但是由于没有一个理论上的上界所以这种延迟可能会更长。

Most miners are agnostic to the content or source of transactions, and will seek to optimize their own returns by including as many transactions as they can in each block (thus collecting the fees). This category of miner will not have any incentive to manipulate the relative order of transactions, but neither will they have any interest of keeping them in any particular order. Thus, transactions containing conflicting orders may be shuffled around arbitrarily for a time period of multiple minutes.

绝大部分矿机并不知道交易的内容和源头，它们会通过尽可能多地收集每个区块中的交易信息（收集费用）来优化返回内容。这类矿机不会改变交易的相对顺序，也不会让交易保持某种顺序。因此，顺序冲突的交易可能在几分钟之内被重新排序。

Other miners, however, may have motivations beyond simply collecting transaction and block-fees. For example, they can decide to inspect the orders awaiting processing in the mempool, and then put in their own conflicting orders in front of the other orders. The fact that they can blame the resulting sequencing on network delays, which do occur in decentralized systems, makes this a tricky problem to fight. That most miners are anonymous only contributes to the difficulty of knowing whether such data snooping (and front-running) has actually occurred. What is clear is that there should be no expectation of privacy for broadcast data in a public distributed ledger.

然而，其他矿机可能对简单收集交易和区块费用感兴趣。比如，它们可以监控时序，等待内存池中的进程，然后把它们自己冲突的序列提交到其他交易序列的前面。它们可以将结果序列归咎于网络延迟，这个情况确实在分散系统中存在，使得这个问题变得十分棘手。大多数的矿机是匿名的，这使得它们很难知道这种数据监听和前线运行是否正常。不过清楚的是，公共分布式分类账中不应有隐私的广播数据。

C. Transaction processing in leader driven decentralized systems

C. 领导人推动分散系统的交易进程

In contrast to the public distributed ledgers described above, there can also be private distributed ledger systems. In such systems (examples include Symbiont Assembly or Axoni), an elected leader is responsible for processing transactions. These leader-driven systems don’t necessarily operate on blocks, but the transactions are written to a distributed ledger. Relative to Bitcoin, the delay between a transaction broadcast and it being written to the ledger is much shorter, often on the order of seconds for a global system. That’s still more than enough time for other participants on the network to broadcast their own transactions with conflicting orders in them.

相比在公共分配帐上面的描述，还可以有私人分布式总账系统。在这样的系统中（如共生体装配或axoni），选出的领导人负责处理交易。这些领导者驱动的系统不一定在块上运行，但事务被写入分布式的分类帐。相对于比特币，一个事务广播和它被写入到分类帐之间的延迟要短得多，在一个全球性的系统中，这个延迟往往只有秒级。对于在网络上的其他参与者，这个时间对于广播他们自己的交易到冲突的订单中仍然足够。

Like Bitcoin miners, the leader has a great degree of freedom in how to order transactions relative to each other. Indeed, the problem is exacerbated by the fact that the leader in this kind of system knows ahead of time that it is the one responsible for writing transactions to the ledger, and can plan accordingly. By the rules of such systems, only when a transaction is outright censored or delayed for a long period of time (several seconds) does a leader-election algorithm kick in and change the system over to a different leader. As in Bitcoin, any leader has no obligation to order transactions in the order it received them, and network delays can make the perceived order different for different observers, making it difficult to prove suspected willful reordering.

像比特币矿机一样,领导者在彼此如何订单交易有很大的自由度。事实上,这加剧了这样一个事实，即这种系统的领导者提前知道，它是一个负责写交易的分类帐，并可以据此计划。通过这种系统的规则,只有当一个交易是彻底审查或延迟了很长一段时间（几秒钟）领导者选取算法才开始生效并改变系统的领导者。与比特币一样，任何领导者都没有义务按照其收到的订单来进行交易，而网络延迟会使不同的观察者的认知顺序不同，因此很难证明是有意的重新排序。

D. Distributed systems and time

分布式系统和时间

The issues outlined above are due to two features of these systems: 1) they are decentralized, meaning no central authority can force miners or leaders respectively to process transactions in a particular order, and 2) they are distributed, meaning that the nodes making up the system are distributed geographically, and due to network delays may receive transactions in a different order. Systems that are distributed, but have a central authority managing them, can achieve much better performance. But even this category of systems will be unable to preserve correct ordering globally for transactions happening near each other in time. For example, Google’s “TrueTime” system can guarantee relative ordering of events that happen at least 7 milliseconds (ms) apart globally but for events happening closer in time, the actual ordering cannot be guaranteed. This lack of time priority sets the stage for information leakage and potential front-running in distributed ledgers.

上述问题是由于这些系统的两个特点:1)他们是分散的,这意味着没有中央权威可以迫使矿机或领导人分别在一个特定的顺序来处理交易,2)他们是分布式的,这意味着节点组成系统分布在地理上,由于网络延迟可能会收到不同的交易顺序。虽然是分布式的系统,但有一个中央集权管理,可以实现更好的性能。但即使是这类系统，也无法在全球范围内及时地为彼此发生的交易保持正确的排序。例如,谷歌的“视时”系统可以保证在全球范围最少7毫秒事件发生的相对顺序，但对于发生时间更加接近的事件,则无法保证顺序。这种缺乏时间优先顺序给分布式账簿系统中信息泄漏和潜在的非法预先交易提供了平台。

1. A Proposed Solution

# 3.一个建议的解决方案

The basic problem to be solved is straightforward: remove the ability of miners or leaders to profit from trading on the information in your transaction. Once your transaction has been written to the distributed ledger, the problem is largely ameliorated, but it is in the preceding processing stage that information leakage can occur. So a natural starting point for a solution is to consider changes to how this initial processing takes place, with the aim of establishing strict time priority for transactions.

需要解决的这个基本问题很简单:删除矿机或领导者从交易中的信息交易的获得利润的能力。一旦您的事务已写入到分布式分类帐，问题在很大程度上可以得到改善，但在前面的阶段，仍然会发生信息泄漏。因此，解决方案的一个自然出发点是考虑如何改变初始化过程，目的是为事务建立严格的时间优先级。

Our proposal as applied to a financial market involves two steps. First, the details of an order are run through a cryptographic hash function (discussed in detail below), producing an identifier mathematically linked to the order, but not exposing any details of the order itself,other than the fact that some trade is desired.Broadcasting that hash value and waiting for it to be processed by the system will reserve an order’s time priority. Once the priority has been secured, the order itself is broadcast. At this stage, the information leakage is not of any concern as all involved markets will recognize the relationship between the order and its corresponding hash value, thus executing them at the reserved time priority. We now turn to specifying this process in more detail at a heuristic level, with more explanation given in the Appendix.

我们应用到金融市场的建议包含两个步骤。首先，一个订单的详细信息会通过加密哈希函数（后文详述），产生一个基于顺序的数学标识符，但不暴露除了特定需求的交易信息之外的其他任何细节。广播哈希值并等待系统处理，将保留订单的时间优先级。一旦优先权得到保障，订单本身就会被广播。在这个阶段，我们不用担心信息泄露，因为所有相关市场都清楚订单和相应的哈希值之间的关系，从而可以按照保留的时序处理它们。现在我们将在一个启发式的层次上更详细地指定这个过程，并在附录中给出更多的解释。

A. Cryptographic hashes - the transaction’s fingerprint

A.密码散列——交易的指纹

A cryptographic hash function is a mathematical algorithm that performs a one-way transformation on a message consisting of arbitrary data, producing a (cryptographic) hash value. One-way means that reversing the algorithm and learning anything about the original data is infeasible. On the same note, any small change in the original data will result in an extensive change in the corresponding hash value, making it look uncorrelated with the first hash value. This property also makes it infeasible to find two different messages that produce the same hash value.

加密散列函数是一种数学算法，它对任意数据组成的消息进行单向变换，产生一个（加密）哈希值。单向意味着逆向算法和获取原始数据都是不可行的。同样的，原始数据中的任何微小变化都会导致相应散列值的广泛变化，使得它与第一个哈希值不相关。这个特性还使得寻找两个产生相同哈希值的不同消息是不可行的。

Cryptographic hashes are the mathematical equivalent of fingerprints. Just as a fingerprint is a unique identifier of a person, a hash is a unique identifier of some data, such as a text document, image, or offer to buy a stock. One common use-case of hashing is a situation where someone wants you to be able to verify that your copy of a document is an exact replication of their copy. Once you have been given the hash, the document can be sent over an unreliable or untrusted channel, and this allows you to verify that you received the correct and unchanged document. The analogy would be using the fingerprint of a person to identify them; you may know nothing else about the person, and the fingerprint doesn’t let you deduce any information about them, but once the person shows up, you can verify that he or she is the one you expected.

加密哈希是指纹的数学等价。正如一个指纹是一个人的唯一标识符，散列是一些数据的唯一标识符，如文本文档，图像，或提供购买股票。一个常见的散列的情况是，有人希望你能够验证你的文件副本是他们的副本的精确复制。一旦你得到了散列，该文件可以发送在一个不可靠的或不可信的渠道，这使您能够验证你收到了正确和不变的文件。这个比喻将使用一个人的指纹来识别他们，你可能不知道其他人，指纹不会让你推断出任何关于他们的信息，但一旦该人出现，你可以验证他或她是你所期望见到的人。

In this paper, we use the hash of a financial order to lock in a time priority for that order.The user will craft the order they want to execute, keep it confidential but publish the hash. No one receiving the hash will be able to deduce any information about the order, but when, at a later time, the full order is published, it is trivial for anyone to verify that this is the order used to generate the hash. Any modification to the order after publication of the hash, by the creator or others, will be plainly visible. This removes the incentive to re-order transactions completely - the hashes are devoid of meaningful information, removing the incentive to delay orders, and more importantly, the ability to act on any information in other participants’orders.

在本文中，我们使用一个金融订单的散列锁定该订单的时间优先级。用户将执行他们想要执行的订单，保持订单机密，但发布其散列值。接收到哈希的人不能够推断出关于订单的任何信息，但是，在稍后的时间，完整的顺序被公布，任何人都可以轻松地通过哈希值验证交易时序。在哈希公布后，任何由创作者或其他人修改过的订单，将很容易区别。这完全杜绝了重新修改时序的动机——散列值是缺乏实际意义的信息, 它可以杜绝延迟交易时序的行为,更重要的是,能够在其他参与者的交易时序上产生作用。

B. Broadcasting the details of the transaction

B.广播交易的细节

The second stage of the process involves sending in the details of the transaction. This occurs once the hash has been processed and assigned an index and timestamp. With time priority established, information leakage is not a problem because all market participants will recognize the relationship between the transaction and its corresponding hash value, thus executing them at its reserved time priority. Figure 2 sets out graphically how this general process will work.

过程的第二阶段包括发送交易的详细信息。一旦哈希被处理并分配索引和时间戳，那么该过程就会发生。随着时间优先级的确定，所有的市场参与者将识别交易和相应的哈希值之间的关系，从而执行它们在其保留的时间优先级，所以信息泄漏不再是问题。图2以图形方式显示这个一般过程是如何工作的。

An important feature of this process is that it entails a general delay in the execution of orders. To see why, consider a setting in which participants can set out offers to buy or sell an object. If a market receives a hash, then the sender has to be given time to broadcast their actual offer before any other offers can be executed. This is most easily handled with a timeout; after a hash has been written to the ledger, the sender has a certain time interval to broadcast their offer, or their time priority is forfeited. To allow for normal delays, this timeout would be on the order of seconds in a private distributed ledger (or potentially minutes for a public distributed ledger like Bitcoin).

这个过程的一个重要特征是，它需要在执行交易时增加一个通用延迟。为了了解原因，我们设置一个参与者可以购买或出售对象的场景。如果一个市场收到一个散列，那么发送者在给定时间广播他们的实际报价之前，任何其他报价都可以执行。这个通过超时可以很容易解决；散列已写入分类帐后，发送者有一定的时间广播他们的报价，或他们的时间优先级被回收。为了允许正常的延迟，这个超时在私人的分布式分类帐中应是秒级的（或在公共的分布式分类帐中为分钟级，如比特币）。

1. A Market-based Example

# 4.一个以基于市场的例子

To clarify both the problem and how our proposed solution would work, we illustrate its operation with a simple example based on trading a financial asset (denoted AXAX). Suppose we consider a trading platform that is running on top of a blockchain or distributed ledger. The underlying ledger is decentralized and the platform utilizes on-ledger, decentralized matching of offers (an example of this is currently found in the Counterparty protocol). In this trading platform, Alice wants to buy 100 AXAX at maximum price of $90. She checks the order book and sees the following orders: -Sell 90 AXAX at $89 -Sell 10 AXAX at $90 -Sell 100 AXAX at $91

为了解决问题和展示我们提出的解决方案是如何工作的，我们用一个基于交易的金融资产（AXAX表示）的简单例子来说明它怎么工作的。我们假设一个运行在区块链或分布式总账最顶层的交易平台，下层的分类帐是分散的，平台利用分类帐，分散匹配的报价（例如，这是目前发现在交易对手协议）。在这个交易平台，爱丽丝希望在最高90美元的价格购买100 AXAX。她检查了订购单并看到了以下订单 -以89美元售出90 AXAX -以80美元售出10 AXAX -以91美元售出100 AXAX

These three orders were created by Bob, a malicious trader who owns a mining pool.He watches the AXAX mempool to intercept matching orders. Alice, of course, doesn’t know that and she puts in a market order for 100 AXAX. When Alice’s order arrives in the mempool,Bob creates an order to cancel the 2 first orders on the book and places them in the Block before the Alice order. When the market executes Alice’s order, only the last Bob order is still open so Alice executes at a price of 91, and not at the blended price of 89.10 that she expected,giving her a worse execution of $1900.

这三个订单是由一个恶意的拥有采矿池的交易者鲍伯创造的。他看到AXAX池拦截匹配订单。爱丽丝，当然，不知道这些，她下了一个100AXAX的市场订购单。当爱丽丝的命令抵达采矿池，鲍伯创建一个取消2个订单中的块的命令放在爱丽丝之前的订单。当市场执行爱丽丝的命令，只有最后鲍勃命令仍然是开放的，所以爱丽丝执行的价格为91，而不是89.10的混合价格预期，给她一个更糟糕的$1900的执行结果。

With the proposed solution, Alice would first craft a valid offer (she wants to buy 100 AXAX at 90), run a cryptographic hash algorithm, and publish this encrypted offer to the ledger.Alongside the hidden information in the hash, some visible (termed “in clear”) information such as the market place name and the asset name will be published. This information will be used to determine on what queue the offer should be added. Once the hash has been retained by the ledger, a place in the queue is definitely attributed to the Alice offer. Now Alice has the guarantee that Bob will not be able to insert a cancellation order in the queue before her offer.She then publishes to the ledger the offer in clear (not hashed and so with details visible to everyone). Once the offer details are retained by the ledger, the matching engine will execute the order at 89.1 as expected by Alice. The transaction is posted to the ledger based on the time priority established by the publication of the hash.

采用我们提出的解决方案，爱丽丝首先将草拟一份有效的订单（她想以90的价格购买 100 AXAX），运行一个加密哈希算法，并向总账发布此加密订单。除了隐藏信息的哈希，一些可见的（称为“in clear”）信息如市场名称和资产名称将被公布，此信息将用于确定订单被添加到队列的那个位置。一旦散列被分类帐记录，队列中的某个地方肯定是属于爱丽丝订单，现在爱爱丽丝就可以保证鲍勃无法插入队列中取消之前的订单。然后她向分类账提供明确的订单（不是散列,而是包含明细且对所有人可见的订单）。一旦报价明细由总账保留，匹配引擎将按照爱丽丝的预期价格89.1执行订单。根据发布哈希表所建立的时间优先级，将交易过帐到分类帐上。

Two features of this process are worth noting. First, with this protocol, no information leakage occurs because the initial hash revealed no relevant information that could be exploited by Bob before the offer’s place in the queue is guaranteed. Second, once the initial hash has been broadcast the market must delay for a short period while the actual order is sent to the market. If Alice does not publish the order in clear before the end of this short interval, the hash will be removed from the queue and she will lose any fee paid to publish the hash.

这个过程中有两个特点值得注意。首先，由于这个协议，在订单在市场中顺序被确定之前，初始散列不会显示任何可以被鲍勃利用的交易相关的信息，所以没有信息泄漏发生。其次，一旦初始哈希被广播，交易市场必须延迟一小段时间等待实际订单发送。如果爱丽丝在这一小段时间结束之前不发布命令，则该散列将从队列中移除，并且将失去发布哈希的所有费用。

1. Conclusions

# 5.总结

The distributed ledger may be the technology that brings us a completely new form of market, one where order matching itself is handled not by a centralized entity but in a decentralized manner not controlled by any one organization. Before such a market structure can evolve, however, it will have to resolve some basic problems inherent in decentralized trading. As we have discussed in this paper, one such problem is its susceptibility to information leakage and front-running. This problem arises from the lack of time priority in the process of writing transactions to the distributed ledger, opening the door to the manipulation of trade order and the insertion of trades based on information in others’ orders.

分布式分类帐是一种技术，它给我们带来了一种全新的市场形式，即订单匹配本身不是由一个集中的实体处理，而是以一种不受任何一个组织控制的分散方式处理。然而，在这样的市场结构演变之前，它必须解决分散交易中固有的一些基本问题。正如我们在本文中讨论的，这样的问题之一是它对信息泄漏和非法预先交易的敏感性。这个问题归咎于向交易的分布式分类帐写入信息缺乏时间优先级，使得他人可以根据别人的订单插入自己的订单到预定的交易序列。

We have shown one way to solve the problem of information leakage by using a cryptographic hash function to reserve a transaction’s time priority, and then once this is established following with a second message giving the order’s details. In effect, we are using an order’s “fingerprint” to hide its “footprint” in the distributed ledger. We believe this is an innovative approach to dealing with information leakage in a distributed ledger setting. Our paper shows how a cryptology-based trading mechanism may play a role in facilitating trading in distributed ledger markets.

我们展示了一种解决信息泄漏的方法，通过使用加密哈希函数保留交易的时间优先级，一旦这个优先级确立后，再给出了交易的细节。实际上，我们使用订单的“指纹”来隐藏它在分布式分类帐中的“足迹”。我们相信这是一个可以解决分布式账本技术中信息泄露的具有创新性的方法。我们的文章显示了在分布式账本技术市场中，一个基于密码学的交易机制是怎样促进交易进行的。