Selfish-mine is one of several strategies that have been developed to subvert the Bitcoin protocol [4]. According to [32], Bitcoin mining is not incentivecompatible[1] and this can lead to the emergence of mining pools that follow the selfish-mine strategy to gain advantage and earn revenue in excess of their fair share. Key to the operation of the selfish-mine strategy is the selective and opportunistic revelation of blocks discovered or mined by members of the pool.

Selfish-mine là một trong một số chiến lược đã được phát triển để lật đổ giao thức Bitcoin [4]. Theo [32], khai thác Bitcoin không khuyến khích[1] và điều này có thể dẫn đến sự xuất hiện của các nhóm khai thác theo chiến lược khai thác ích kỷ để giành lợi thế và kiếm doanh thu vượt quá chia sẻ công bằng của họ. Chìa khóa cho hoạt động của chiến lược mỏ ích kỷ là sự mặc khải có chọn lọc và cơ hội của các khối được phát hiện hoặc khai thác bởi các thành viên của nhóm.

This causes the honest nodes to waste their resources mining blocks that are destined not to be in the main chain. The main chain is the branch of the blockchain consisting a chain of blocks (linked by pointers to the previous block) with the largest sum of work done in expectation, beginning at the genesis block.

Điều này làm cho các nút trung thực lãng phí các khối khai thác tài nguyên của chúng mà không được nằm trong chuỗi chính. Chuỗi chính là nhánh của blockchain bao gồm một chuỗi các khối (được liên kết bởi các con trỏ với khối trước đó) với tổng công việc lớn nhất được thực hiện trong kỳ vọng, bắt đầu từ khối genesis.

To specify the selfish-mine strategy, we assume that the miners are divided into two groups [32], the honest nodes following the Bitcoin rules and a minority of dishonest nodes following the selfish-mine strategy[2]. We refer to the fraction of the total computing power commanded by the selfish pool as alpha (α). The detailed operation of the selfish-mine strategy is shown in Algorithm 1 and the state transition diagram in Figure 5.4.

Để chỉ định chiến lược khai thác ích kỷ, chúng tôi giả định rằng các công cụ khai thác được chia thành hai nhóm [32], các nút trung thực theo quy tắc Bitcoin và một số ít các nút không trung thực theo chiến lược khai thác ích kỷ[2]. Chúng tôi đề cập đến một phần của tổng sức mạnh tính toán được chỉ huy bởi nhóm ích kỷ là alpha (α). Hoạt động chi tiết của chiến lược mỏ ích kỷ được thể hiện trong Thuật toán 1 và sơ đồ chuyển trạng thái trong Hình 5.4.

Initially, the selfish pool has not discovered any blocks, so the dishonest nodes in the pool mine on the last public block received (block with the serial number np). The serial number of a block is synonymous with its position (depth) in the blockchain. This is shown in lines 2 to 5 of Algorithm 1 and step (0) in the state machine (SM).

Ban đầu, pool ích kỷ không phát hiện ra bất kỳ khối nào, vì vậy các nút không trung thực trong mỏ pool trên khối công khai cuối cùng nhận được (khối có số sê-ri np). Số sê-ri của một khối đồng nghĩa với vị trí (độ sâu) của nó trong chuỗi khối. Điều này được thể hiện trong các dòng 2 đến 5 của Thuật toán 1 và bước (0) trong máy trạng thái (SM).

However, when a dishonest node mines a block (SM step (1)), the block is only announced to other dishonest nodes in the selfish pool. At this stage, the honest nodes continue to mine on the older public block np while the dishonest nodes mine on the newer secret block with serial number ns = np + 1. We refer to the segment of the blockchain at the dishonest nodes comprising of the secret block(s) ns as the secret extension.

Tuy nhiên, khi một nút không trung thực khai thác một khối (bước SM (1)), khối đó chỉ được thông báo cho các nút không trung thực khác trong nhóm ích kỷ. Ở giai đoạn này, các nút trung thực tiếp tục khai thác trên khối công khai cũ hơn np trong khi các nút không trung thực khai thác trên khối bí mật mới hơn với số sê-ri ns = np + 1. Chúng tôi đề cập đến phân đoạn của chuỗi khối tại các nút không trung thực bao gồm khối bí mật (s) ns là phần mở rộng bí mật.

As long as the selfish pool has not learned3 of any competing public block (block at the same depth of the blockchain as ns), the pool assumes a lead of one block and continues to mine on the secret block ns hoping to achieve a lead of two of more blocks. This is presented in lines 8 to 14 of Algorithm 1. However, since the pool is in the minority, the honest nodes will catch up.

Chừng nào nhóm ích kỷ chưa học được 3 khối bất kỳ cạnh tranh công khai nào (khối ở cùng độ sâu của blockchain như ns), nhóm này giả định dẫn đầu một khối và tiếp tục khai thác khối bí mật ns để đạt được vị trí dẫn đầu hai khối nữa. Điều này được trình bày trong các dòng 8 đến 14 của Thuật toán 1. Tuy nhiên, do nhóm này chiếm thiểu số, các nút trung thực sẽ bắt kịp.

When an honest node mines a block, it immediately broadcasts it to all the nodes in the network. When the block is received by the pool 4, the pool computes the lead and a course of action is selected based on the value of the lead. The lead refers to how long the secret branch is compared to the public branch of the blockchain. The secret branch comprises the secret extension and the parent public branch (the chain of blocks beginning at the predecessor to the first secret block all the way to the genesis block). This is presented in lines 17 to 36 of Algorithm 1. If the last public block known to the selfish pool has serial number np and latest secret block ns, then:

lead = ns −np (5.1)

Khi một nút trung thực khai thác một khối, nó ngay lập tức phát nó tới tất cả các nút trong mạng. Khi khối được nhận bởi nhóm 4, nhóm sẽ tính toán khách hàng tiềm năng và một quá trình hành động được chọn dựa trên giá trị của khách hàng tiềm năng. Dẫn đầu đề cập đến thời gian chi nhánh bí mật được so sánh với chi nhánh công khai của blockchain. Nhánh bí mật bao gồm phần mở rộng bí mật và nhánh công khai mẹ (chuỗi khối bắt đầu từ tiền thân đến khối bí mật đầu tiên cho đến khối genesis). Điều này được trình bày trong các dòng từ 17 đến 36 của Thuật toán 1. Nếu khối công khai cuối cùng được biết đến với nhóm ích kỷ có số sê-ri np và khối bí mật mới nhất ns, thì:

lead = ns −np (5.1)

If lead < 0, it means that the secret branch has fallen behind the public branch. The selfish pool could continue mining on the last block ns of the secret extension, but the probability of catching up with the majority of honest nodes is negligible, so the selfish pool abandons the secret extension and starts mining on the last known public block np.

Nếu lead <0, điều đó có nghĩa là nhánh bí mật đã tụt lại phía sau nhánh công cộng. Nhóm ích kỷ có thể tiếp tục khai thác trên khối ns cuối cùng của tiện ích mở rộng bí mật, nhưng xác suất bắt kịp phần lớn các nút trung thực là không đáng kể, vì vậy nhóm ích kỷ từ bỏ tiện ích mở rộng bí mật và bắt đầu khai thác trên khối công khai cuối cùng được biết đến.

If lead = 0, it means that the secret branch and the public branch are of equal length. The selfish pool immediately publishes (making a secret block public by broadcasting it to all the honest nodes) the only secret block in the extension causing the blockchain to fork (after a transmission delay) at all the honest nodes and a race to begin as to which branch will form the main chain. This is presented in lines 24 to 28 of Algorithm 1 and step (8) of the SM. Depending on the network topology and propagation delays, one of the two competing blocks arrives first at an honest node in the network. Since the honest nodes follow the Bitcoin protocol rules, they will mine on the block they first received whether it is a public block or a published block.

Nếu lead = 0, điều đó có nghĩa là nhánh bí mật và nhánh công cộng có độ dài bằng nhau. Nhóm ích kỷ ngay lập tức xuất bản (công khai khối bí mật bằng cách phát nó tới tất cả các nút trung thực), khối bí mật duy nhất trong tiện ích mở rộng khiến blockchain rẽ nhánh (sau khi trì hoãn truyền) tại tất cả các nút trung thực và cuộc đua bắt đầu nhánh nào sẽ tạo thành chuỗi chính. Điều này được trình bày trong các dòng 24 đến 28 của Thuật toán 1 và bước (8) của SM. Tùy thuộc vào cấu trúc liên kết mạng và độ trễ lan truyền, một trong hai khối cạnh tranh sẽ đến đầu tiên tại một nút trung thực trong mạng. Vì các nút trung thực tuân theo các quy tắc giao thức Bitcoin, chúng sẽ khai thác trên khối mà chúng nhận được lần đầu tiên cho dù đó là khối công khai hay khối được xuất bản.

Consequently, some honest nodes will begin mining on the recently published block hence extending the formerly secret branch. We refer to the fraction of honest nodes that mine on the published block as γ, which is the measure of how often a published block arrives first at an honest node when there is a race. An analysis of the effect of block propagation delays on γ using a three node network configuration is presented in Appendix B. Further discussion on γ can be found in [34, 35]. At the same time, nodes in the selfish pool continue mining on the published block. Eventually, a new block is mined that extends either the public branch or the formerly secret branch. There are three possible outcomes.

Do đó, một số nút trung thực sẽ bắt đầu khai thác trên khối được xuất bản gần đây do đó mở rộng nhánh bí mật trước đây. Chúng tôi đề cập đến tỷ lệ các nút trung thực khai thác trên khối được xuất bản là, đây là thước đo tần suất một khối được xuất bản đến trước tại một nút trung thực khi có một cuộc đua. Một phân tích về ảnh hưởng của độ trễ lan truyền khối đối với sử dụng cấu hình mạng ba nút được trình bày trong Phụ lục B. Có thể tìm thấy thảo luận thêm về trong [34, 35]. Đồng thời, các nút trong nhóm ích kỷ tiếp tục khai thác trên khối được xuất bản. Cuối cùng, một khối mới được khai thác mở rộng chi nhánh công cộng hoặc chi nhánh bí mật trước đây. Có ba kết quả có thể xảy ra.

1. The selfish pool mines a successor block to the published block ns. This is shown in Figure 5.1b and step (9) of the SM. In this case, the pool wins the race and receives the reward for both blocks. Both the honest and dishonest nodes begin to mine on the winning block.

Selfish pool khai thác một khối kế tiếp cho khối ns được xuất bản. Điều này được thể hiện trong Hình 5.1b và bước (9) của SM. Trong trường hợp này, pool thắng cuộc đua và nhận phần thưởng cho cả hai khối. Cả hai nút trung thực và không trung thực bắt đầu khai thác trên khối chiến thắng.

1. An honest node mines a successor block to the published block ns. This is shown in Figure 5.1c and step (10) of the SM. In this case, the pool still wins the race but is only credited for one block, the predecessor to the winning block. Both the honest and dishonest nodes begin to mine on the winning block.

Một nút trung thực khai thác một khối kế tiếp đến khối ns đã xuất bản. Điều này được thể hiện trong Hình 5.1c và bước (10) của SM. Trong trường hợp này, pool vẫn chiến thắng cuộc đua nhưng chỉ được ghi có cho một khối, tiền thân của khối chiến thắng. Cả hai nút trung thực và không trung thực bắt đầu khai thác trên khối chiến thắng.

1. An honest node mines a successor block to the competing public block np. This is shown in Figure 5.1d and step (10) of the SM. In this case, the pool loses the race and the revenue for block ns while the honest nodes are credited for both public blocks. The pool abandons the secret extension and both the honest and dishonest nodes begin to mine on the winning block.

Một nút trung thực khai thác một khối kế tiếp cho khối công khai cạnh tranh np. Điều này được thể hiện trong Hình 5.1d và bước (10) của SM. Trong trường hợp này, nhóm sẽ mất cuộc đua và doanh thu cho khối ns trong khi các nút trung thực được ghi có cho cả các khối công khai. Nhóm bỏ qua phần mở rộng bí mật và cả các nút trung thực và không trung thực bắt đầu khai thác trên khối chiến thắng.

If lead = 1, it means the secret branch is one block longer than the public branch. To ensure that the secret blocks end up being part of the main chain, the pool publishes both secret blocks in the secret extension as shown in Figure 5.2b. Both blocks reach the honest nodes and the honest nodes abandon mining on the block they were mining on. This is presented in lines 29 to 32 of Algorithm 1 and step (7) of the SM.

Nếu lead = 1, điều đó có nghĩa là nhánh bí mật dài hơn một khối so với nhánh công khai. Để đảm bảo rằng các khối bí mật cuối cùng là một phần của chuỗi chính, nhóm sẽ xuất bản cả hai khối bí mật trong phần mở rộng bí mật như trong Hình 5.2b. Cả hai khối đều đạt đến các nút trung thực và các nút trung thực từ bỏ khai thác trên khối mà chúng đang khai thác. Điều này được trình bày trong các dòng 29 đến 32 của Thuật toán 1 và bước (7) của SM.

If lead > 1, the pool has a comfortable lead over the honest nodes. The pool publishes the first unpublished block in the extension as shown in Figure 5.3b. This is presented in lines 29 to 32 of Algorithm 1 and step (5) of the SM. Step (4) of the SM represents the case where the pool mines a block when lead > 1.

Nếu lead > 1, nhóm có một khách hàng tiềm năng thoải mái trên các nút trung thực. Nhóm này xuất bản khối chưa được công bố đầu tiên trong phần mở rộng như trong Hình 5.3b. Điều này được trình bày trong các dòng 29 đến 32 của Thuật toán 1 và bước (5) của SM. Bước (4) của SM đại diện cho trường hợp bể khai thác một khối khi dẫn > 1.

Ref:

[1]In mechanism design, a process is incentive-compatible (IC) if the honest revelation by participants of any private information requested by the mechanism results in the participants faring best [74]. Any system in which participants can benefit from dishonest behavior lacks the property of IC.

[1]Trong thiết kế cơ chế, một quy trình tương thích khuyến khích (IC) nếu sự tiết lộ trung thực của người tham gia về bất kỳ thông tin cá nhân nào được yêu cầu bởi cơ chế dẫn đến kết quả tốt nhất cho người tham gia [74]. Bất kỳ hệ thống nào trong đó người tham gia có thể hưởng lợi từ hành vi không trung thực đều thiếu tài sản của IC.

[2]There is no incentive to stop multiple selsh pools from emerging as can be seen in the real Bitcoin network which shows the presence of multiple mining pools [23]. We later show that the presence of multiple pools following the selfish-mine strategy causes the strategy to be less profitable.

[2] Không có động cơ nào ngăn chặn nhiều nhóm sel sh xuất hiện như có thể thấy trong mạng Bitcoin thực sự cho thấy sự hiện diện của nhiều nhóm khai thác [23]. Sau này chúng tôi cho thấy rằng sự hiện diện của nhiều nhóm theo chiến lược khai thác ích kỷ khiến chiến lược này có ít lợi nhuận hơn.

[3]In a network model characterized by block propagation delays such as investigated in this thesis, a competing block may have been discovered but delayed in reaching the selfish pool.

[3] Trong một mô hình mạng được đặc trưng bởi sự chậm trễ lan truyền khối như điều tra trong luận án này, một khối cạnh tranh có thể đã được phát hiện nhưng bị trì hoãn trong việc đạt đến sự ích kỷ

hồ bơi.

[4]The selfish-mine algorithm may be executed only at a single controller (gatekeeper) or by every dishonest node. In this sense, the term pool is used to refer generally to both cases, centralized and distributed execution of the selfish-mine strategy.

[4] Thuật toán selfish-mine chỉ có thể được thực thi tại một bộ điều khiển duy nhất (gatekeeper) hoặc bởi mọi nút không trung thực. Theo nghĩa này, thuật ngữ nhóm được sử dụng để chỉ chung cho cả hai trường hợp, thực hiện tập trung và phân phối của chiến lược ích kỷ.