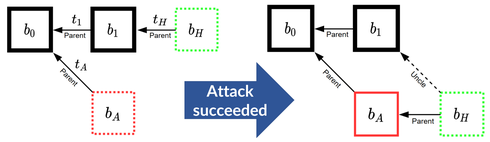
Uncle Maker

(Time)Stamping Out The Competition

Aviv Yaish, Gilad Stern, Aviv Zohar
The Hebrew University of Jerusalem

The Riskless Uncle Maker (RUM) Attack. In certain cases, an attacker can replace the last mainchain block by mining a block with a **false** timestamp.



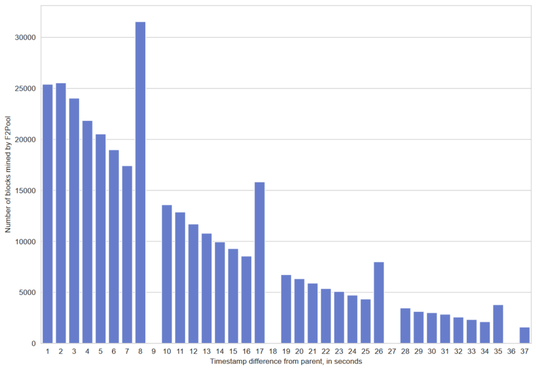
If b_1 has a time difference between 9 and 18 seconds relative to its parent b_0, then an attacker should mine for 9 seconds a block b_A which points to b_0 as its parent, and falsely set its timestamp to be less than 9 seconds relative to b_0's timestamp.

Theorem 1 (informal). The RUM attack is **riskless**: its probability of success is equal to the probability of mining a block honestly.

Theorem 2 (informal). If an attacker uses the RUM attack, its expected **relative share of blocks** will be larger than mining honestly, while the absolute number remains the same.

Theorem 3 (informal). An attacker can increase its expected absolute & relative **rewards** by using RUM (vs mining honestly).

Uncle Making in the Wild. F2Pool (the 2nd largest mining pool in the PoW era) executed the attack for two years, unnoticed!

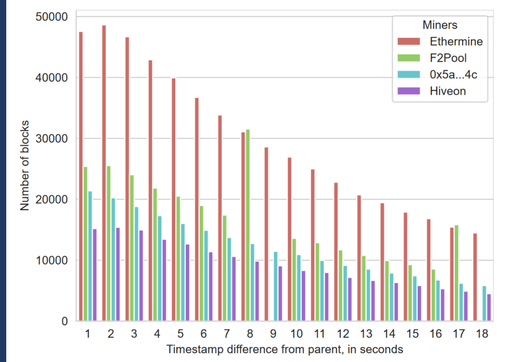


Still Relevant. Ethereum forks hold a combined amount of ~23% of the total hash-rate of the "glory-days" of the PoW era.

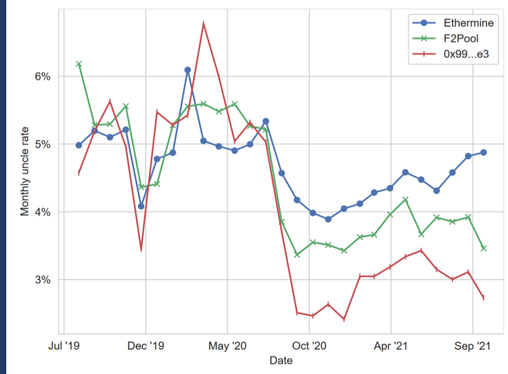
First evidence of an in-the-wild attack on a major cryptocurrency: Ethereum was under attack for **two years.**

First riskless attack which **dominates** mining honestly.

https://ia.cr/2022/1020



F2Pool didn't mine even a **single** block with a timestamp difference which is divisible by 9 relative to its parent block.



By using the attack, F2Pool decreased the number of uncle blocks it mined, thereby increasing profits. 0x99...e3 used a more aggressive & effective version of the attack.

Algorithm 1: Riskless uncle maker attack

```
1  on event initialize:
2      chain ← publicly known blocks ;
3      do: mine honestly on top of the tip of chain ;
4  end
5  on event we mined a block b:
6      do: publish b and append it to chain ;
7      do: mine honestly on top of the tip of chain ;
8  end
9  on event others mined a block b:
10     if t_b ∈ [9, 18) then
11         trigger event: attack against b ;
12     else
13         do: append b to chain ;
14         do: mine honestly on top of the tip of chain ;
15     end
16 end
17 on event attack against b:
18     t_H ← 0 ;
19     while t_H < 9 & no-one mined a new block do
20         mine b_A with t_{b_A} = 8 on top of b.parent ;
21         t_H ← currentTime − b.timestamp ;
22     end
23     if honest miners mined a new block b′ then
24         do: append b to chain ;
25         trigger event: others mined a block b′ ;
26     else if we mined b_A then
27         trigger event: we mined a block b_A ;
28     else
29         do: append b to chain ;
30         do: mine honestly on top of the tip of chain ;
31     end
32 end
```

Acknowledgments. The Ministry of Science & Technology, Israel, the Israel Science Foundation (grants 1504/17 & 1443/21), The Hebrew University of Jerusalem's Federmann Cyber Security Research Center in conjunction with the Israel National Cyber Directorate.