

✓ Blockchain in 1 diagram

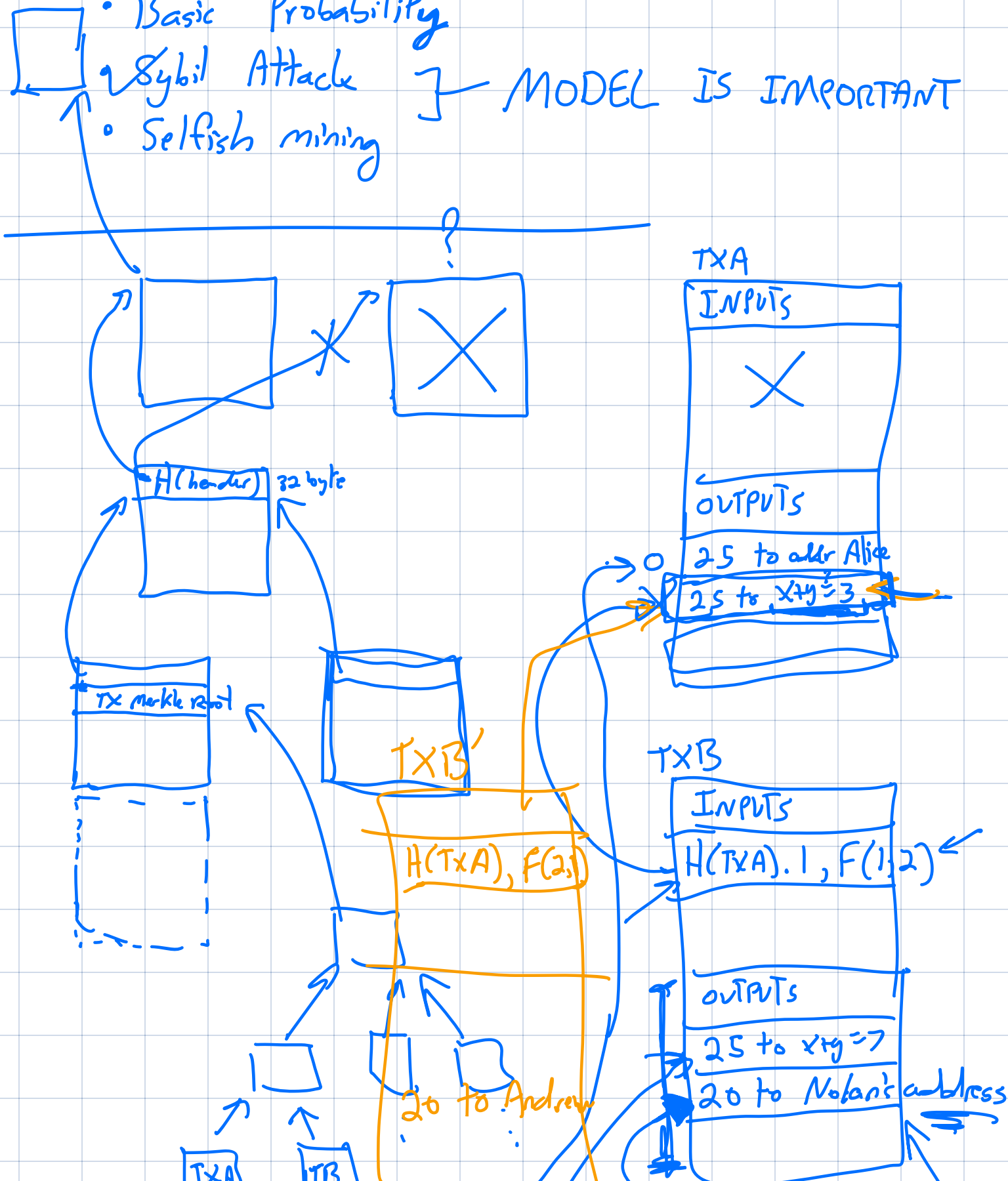
• Doublespend Scenario

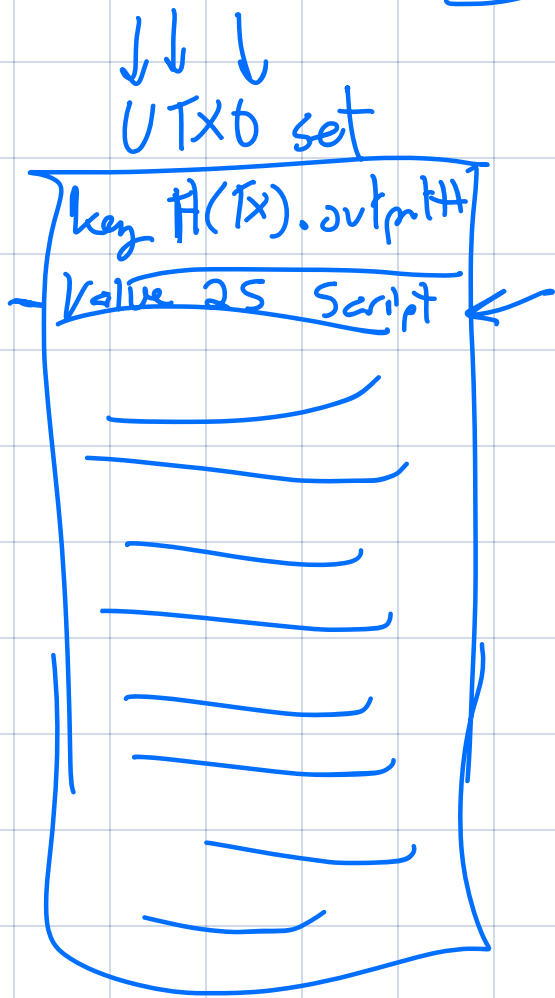
• Basic Probability

• Sybil Attack

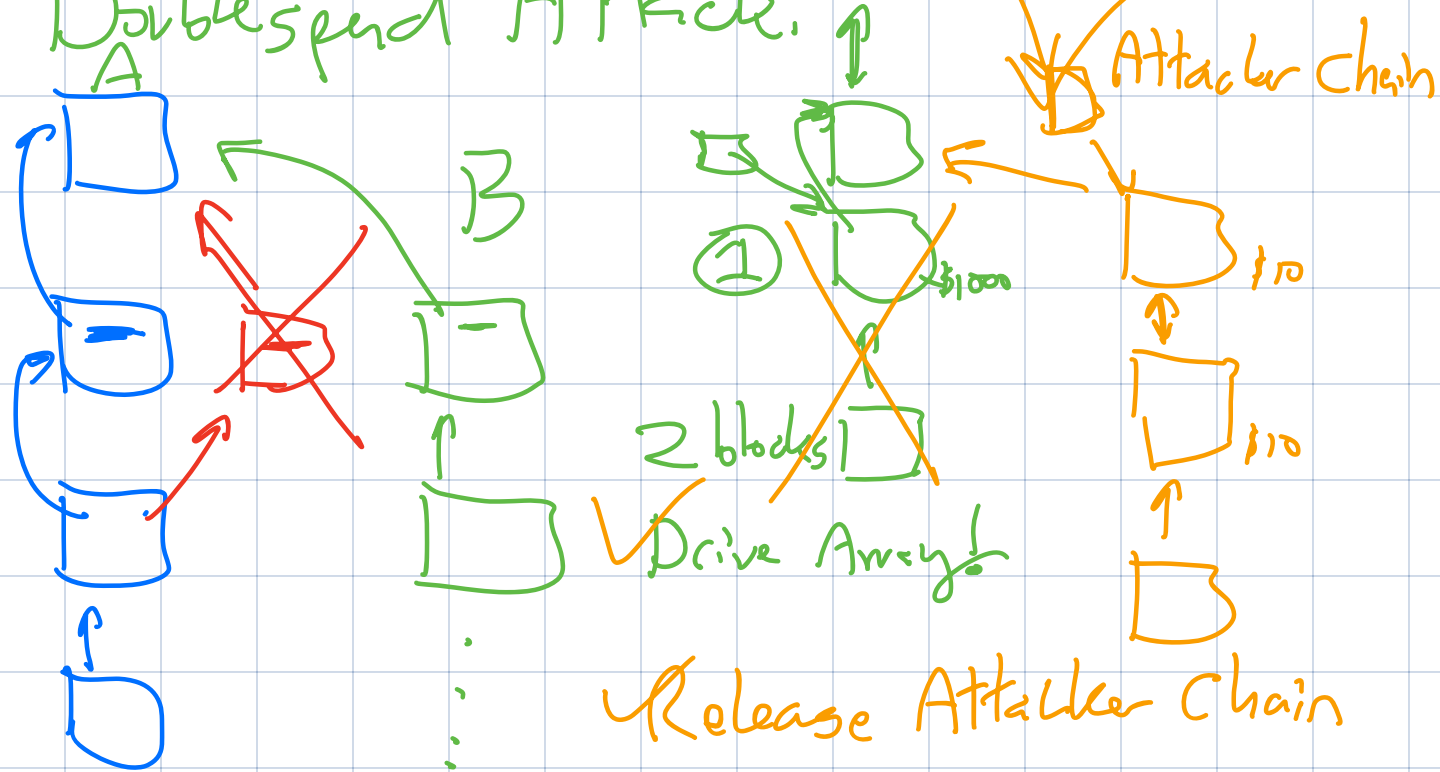
• Selfish mining

} MODEL IS IMPORTANT





DAG



Until pow of B exceeds A, A's the winner!
 D✓

Mining Random #

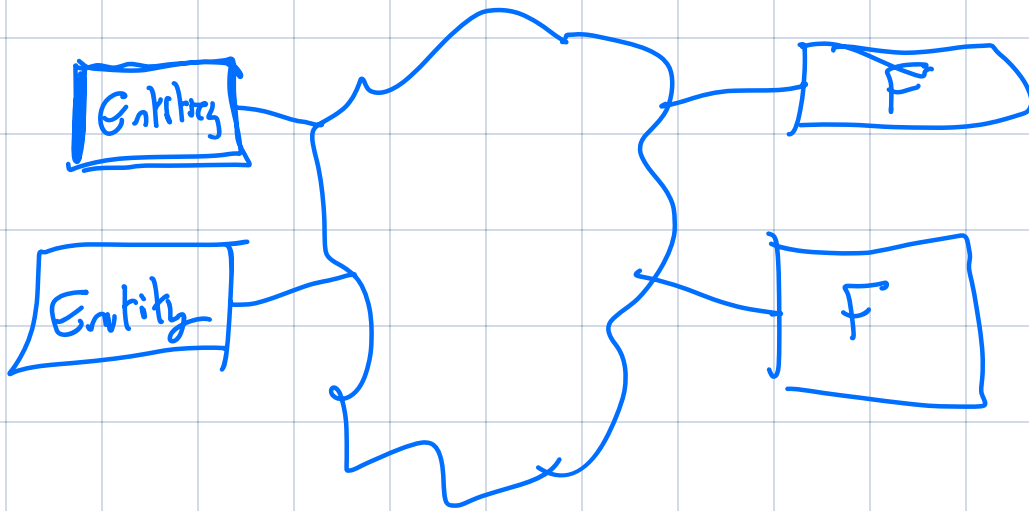
target if $H(H(\text{block contents})) < \text{target}$

block is good! $\downarrow$ pow puzzle

if target $\frac{2^{256} - 1}{2}$

The Sybil Attack

Doucer $\Rightarrow$ Network model



Can we make it so 1 entity $\Rightarrow$ ^{ONLY} 1 identity

Lemma 1: if it takes P processing power to prove an identity then attacker w/ $K \cdot P$ power can prove K identities.

Lemma 2: time Attack on processing power
if validation is grouped in Rounds then
attacker with $K \cdot P$ power can prove $K \cdot R$
identities where R is # Rounds.

Lemma 3: web of trust

Lemma 4: time lead wOT

- all prob is ultimately $\frac{\# \text{Successes}}{\text{total}} \quad \Downarrow \quad \frac{1}{2}$
- if $P(a) = x$, $P(\sim a) = 1 - x$
- if a AND b happens $\rightarrow P(a) \cdot P(b) \frac{1}{4}$
- if a OR b happens $\rightarrow 1 - (1 - P(a))(1 - P(b)) \frac{3}{4}$
- Poisson
 $P(k \text{ successes, } \frac{\text{events}}{\text{interval}}) = \frac{1^k e^{-1}}{k!}$

if you have 20% hash power
what's the likelihood of finding 3 blocks in 10 minutes

$$P(3, 0.20) \rightarrow 0.1\% \checkmark$$