The Backbone Model

Introduction to Blockchain Science and Engineering

Aggelos Kiayias

Dionysis Zindros, Christos Nasikas

The Ledger Objective

- First formal definition of the objective of a “robust transaction ledger” was formulated by
  Garay, **K**, Leonardos in [GKL14]
- In the same work, we proved that a suitable abstraction of the bitcoin protocol (the bitcoin backbone) realizes the ledger objective
- … and also can be used to achieve other primitives such as consensus (with some work..)

Defining the ledger objective

Participants maintain a log of transactions. It is divided in two parts, **permanent** and **pending.** We denote LOG, the permanent and $\underline{\text{LOG}}$ the permanent+pending.

Persistence/Consistency: at any time t1<=t2, for participants P1, P2, in respective times, it holds that LOG1 is a prefix of $\underline{\text{LOG2}}$

Liveness: if a transaction *tx* is made available to all participants for a period of time at least *u*, it holds that any honest participant's LOG will contain *tx*.

(liveness assumes “neutral” transactions).

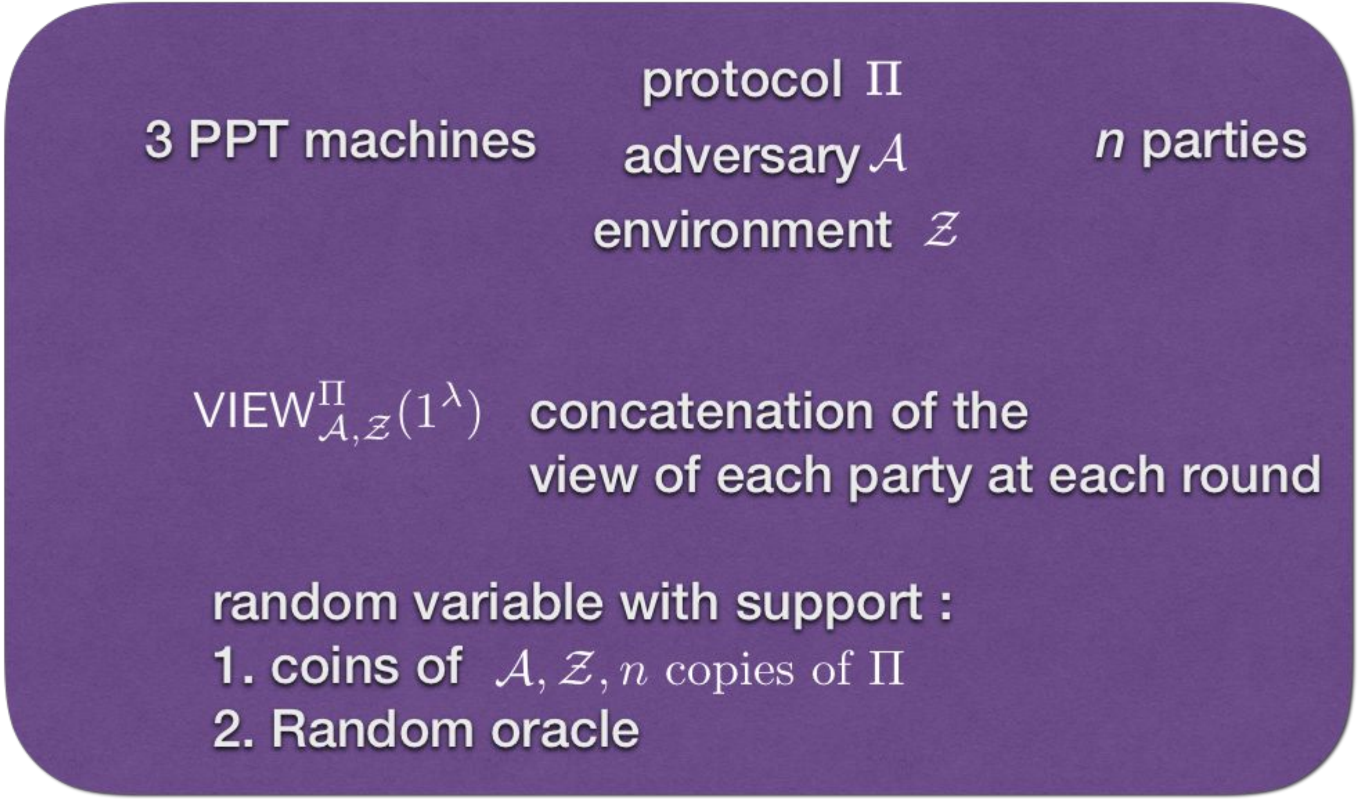
Execution model

- Time is divided in rounds.
- In each round each party is allowed *q* queries to a hash function (RO)
- messages are sent through a “diffusion” mechanism
- The adversary is rushing and may :
    1. spoof messages
    2. inject messages
    3. reorder messages

Participants

- There are n-t honest parties each one producing q queries to the hash function per round.
- The adversary is able to control t parties acting as a malicious mining pool.
    - A “flat” version of the world in terms of hashing power.
    - It is worse for honest parties to be separate (they have to pay the price of being decentralized).

Execution and View



3 PPT machines

protocol Π

adversary $\mathcal{A}$

environment $\mathcal{Z}$

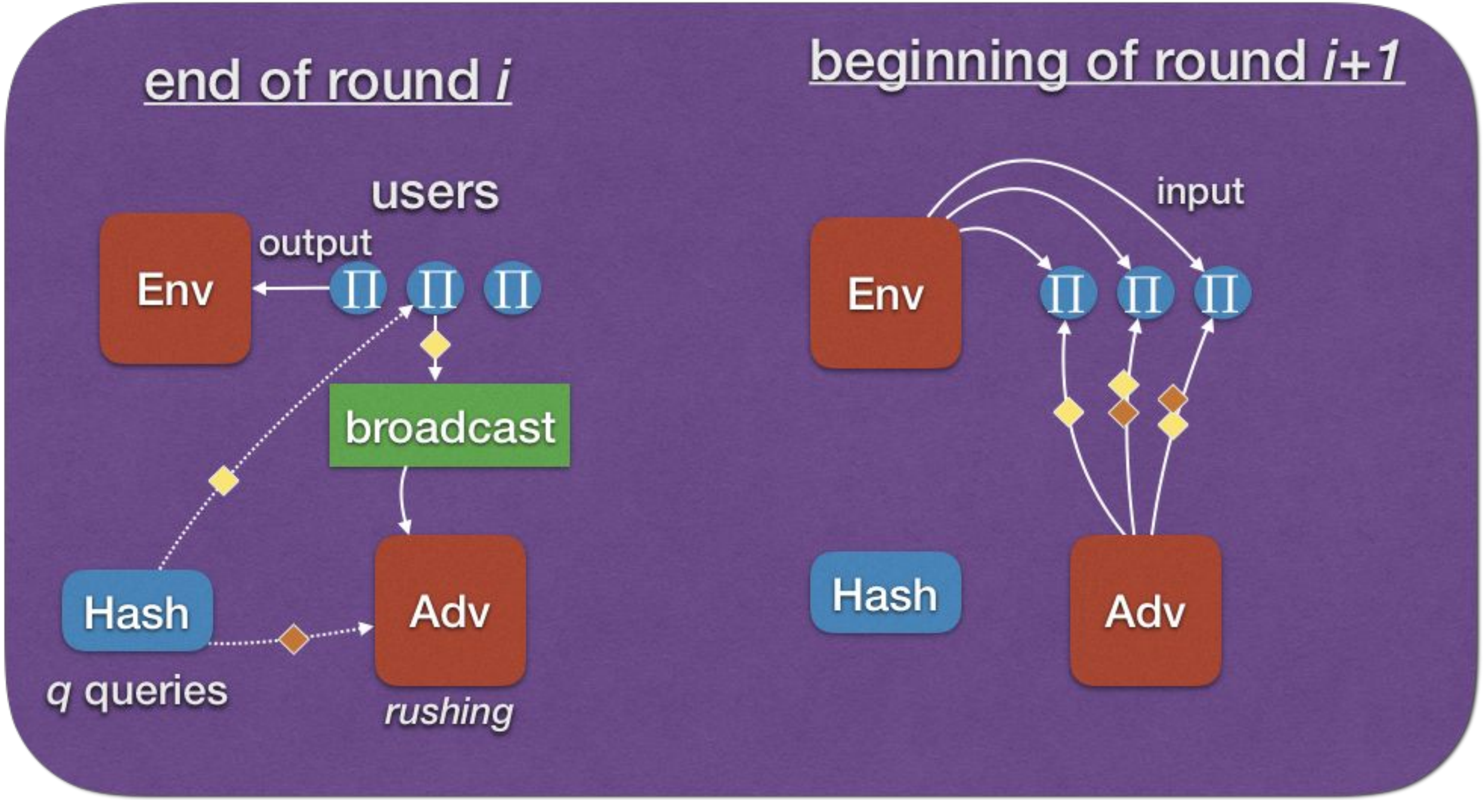
n parties

VIEW$^{\Pi}_{\mathcal{A},\mathcal{Z}}(1^{\lambda})$ concatenation of the view of each party at each round

random variable with support :

1. coins of $\mathcal{A}, \mathcal{Z}, n$ copies of Π
2. Random oracle

Round structure



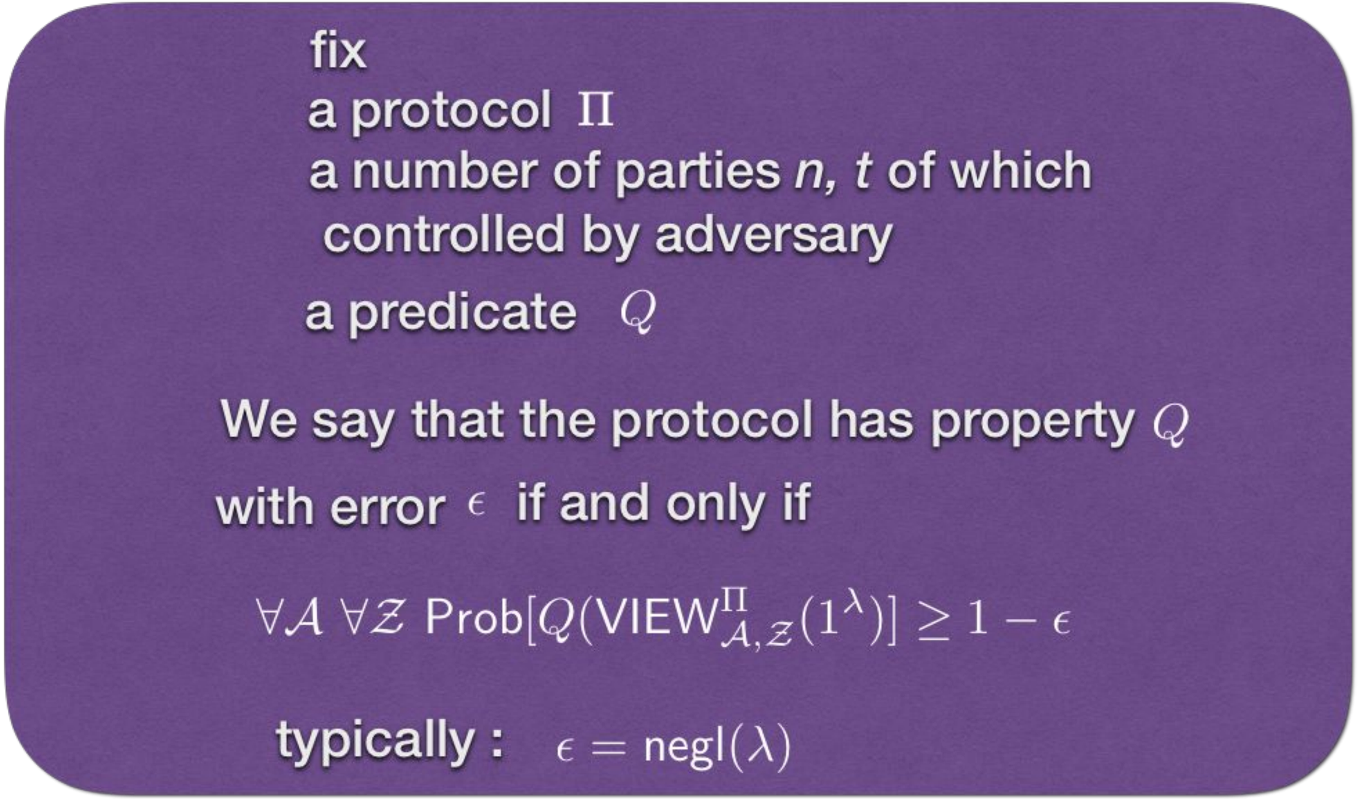
The environment

Represents the processes executed by the player that are external to the protocol being analyzed. (e.g., what is the data structure that organises pending transactions).

We will quantify over all(*) possible environments.

> (*) Suitably excluding certain environments that are unsuitable depending on the property.

Property of a protocol



fix

a protocol Π

a number of parties *n, t* of which controlled by adversary

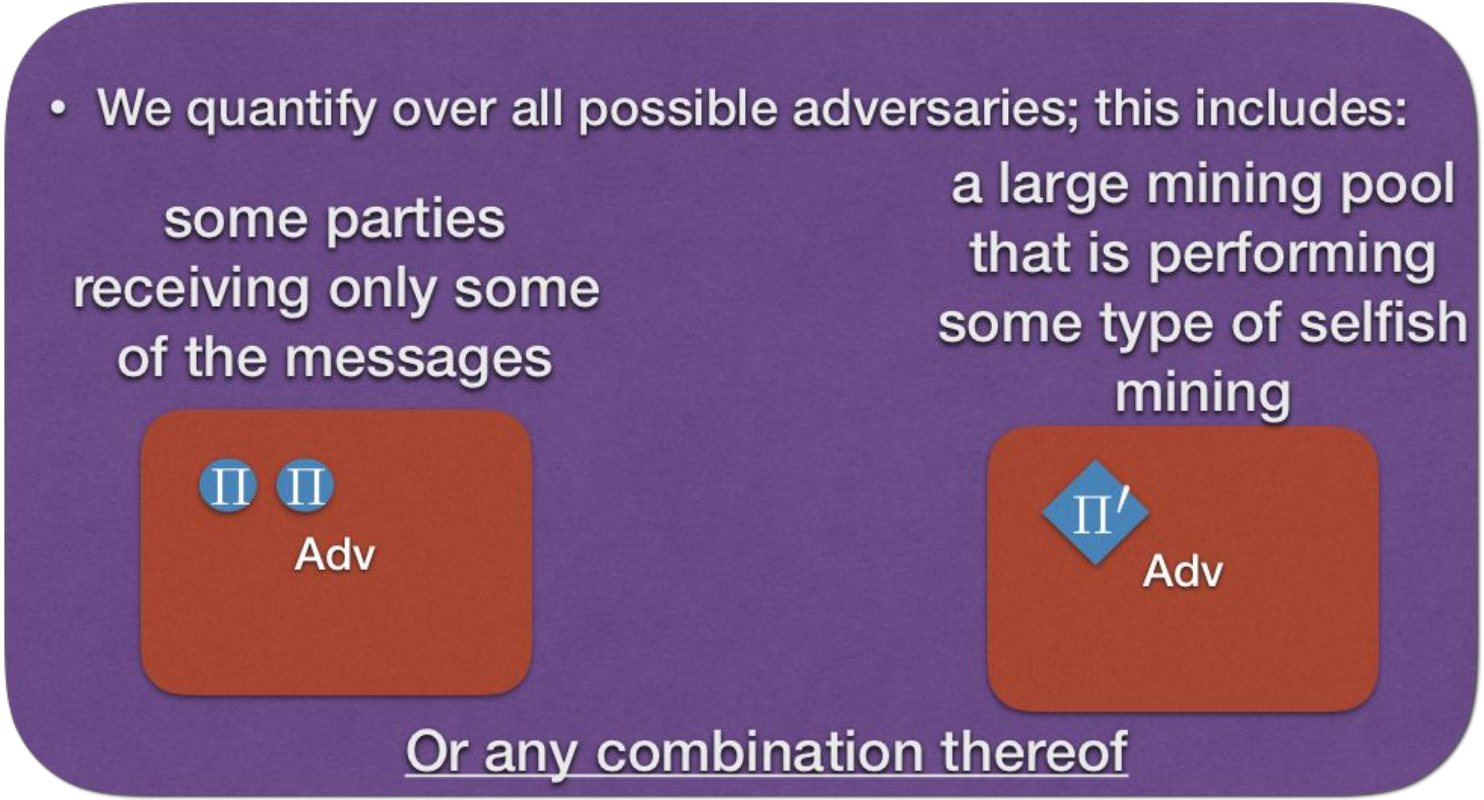
a predicate Q

We say that the protocol has property Q with error ϵ if and only if

$$\forall \mathcal{A}\ \forall \mathcal{Z}\ \mathsf{Prob}[Q(\mathsf{VIEW}^{\Pi}_{\mathcal{A},\mathcal{Z}}(1^{\lambda}))] \geq 1 - \epsilon$$

typically : $\epsilon = \mathsf{negl}(\lambda)$

Generality of the model



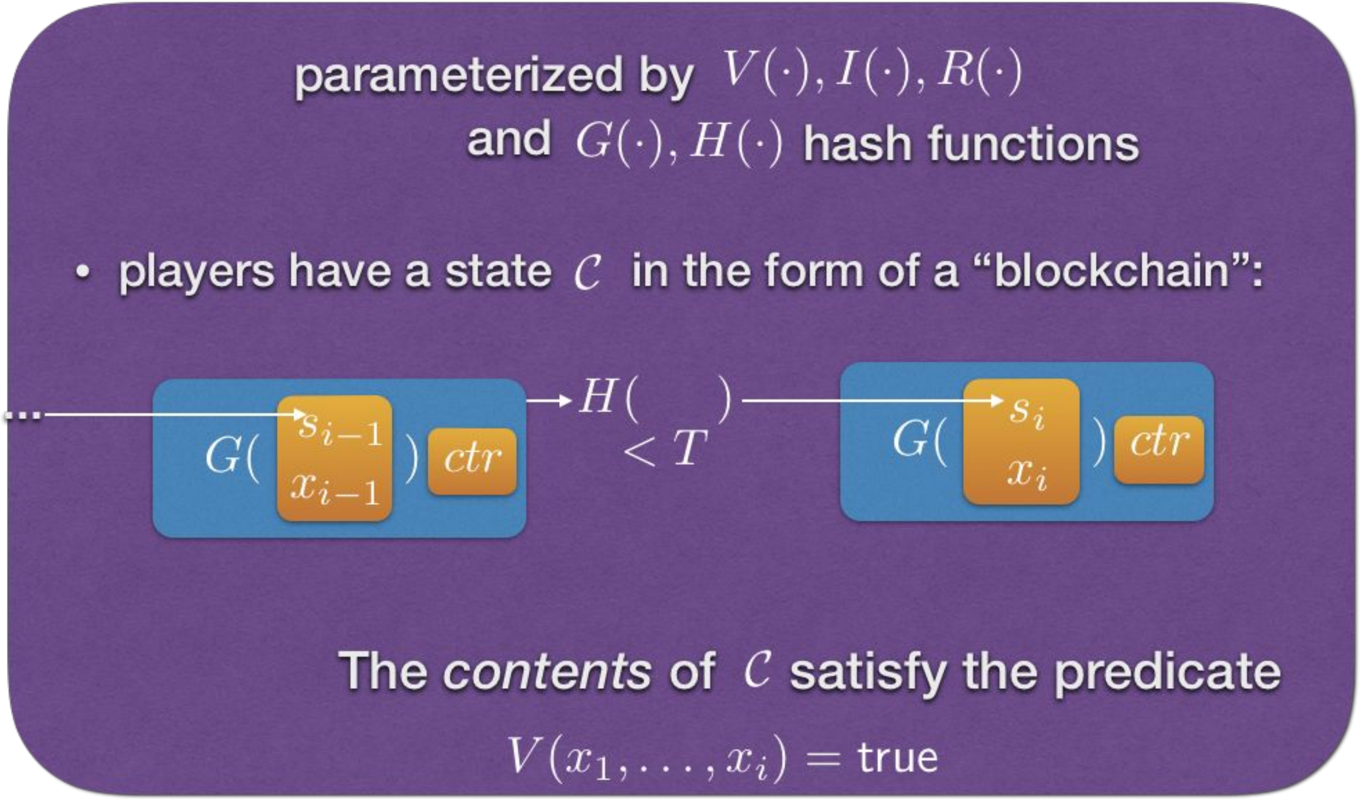
- We quantify over all possible adversaries; this includes:

some parties receiving only some of the messages

a large mining pool that is performing some type of selfish mining

Or any combination thereof

The bitcoin backbone, I



parameterized by $V(\cdot), I(\cdot), R(\cdot)$ and $G(\cdot), H(\cdot)$ hash functions

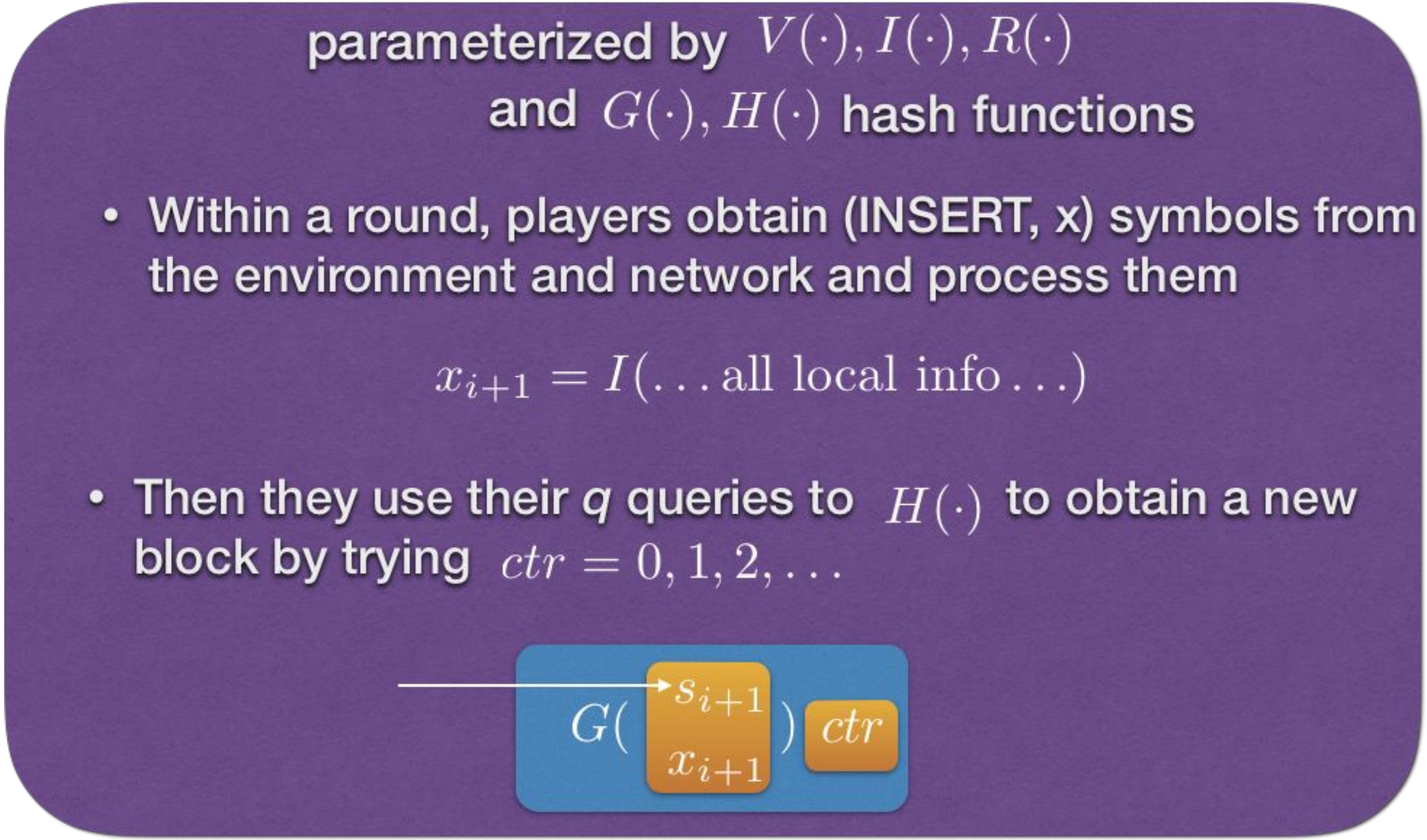
- players have a state $\mathcal{C}$ in the form of a "blockchain":

...
$G($ s_{i-1} x_{i-1} $)$ ctr
$H($ $)$
$< T$
$G($ s_i x_i $)$ ctr

The *contents* of $\mathcal{C}$ satisfy the predicate

$$V(x_1, \ldots, x_i) = \text{true}$$

The Bitcoin Backbone, II



parameterized by $V(\cdot), I(\cdot), R(\cdot)$

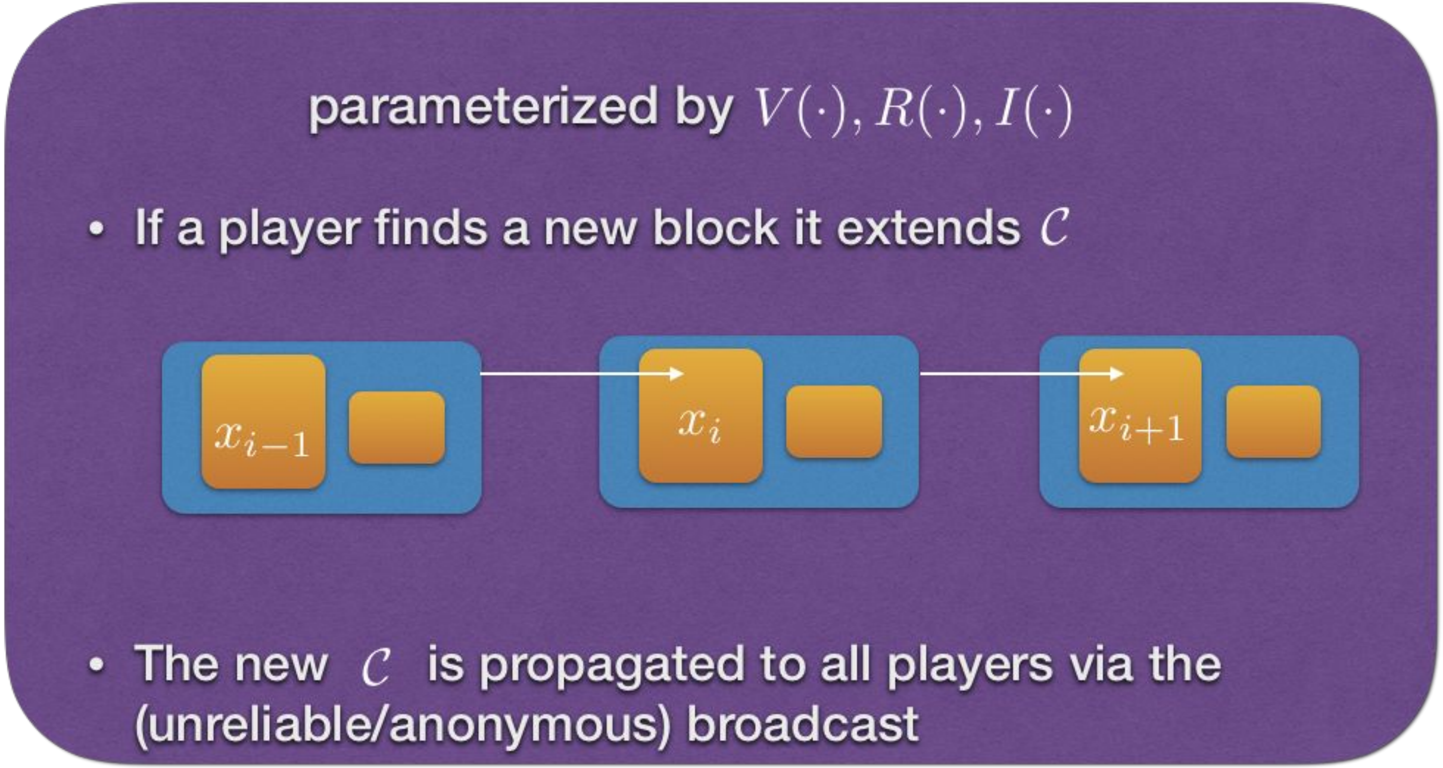
and $G(\cdot), H(\cdot)$ hash functions

- Within a round, players obtain (INSERT, x) symbols from the environment and network and process them

$$x_{i+1} = I(\ldots \text{all local info} \ldots)$$

- Then they use their *q* queries to $H(\cdot)$ to obtain a new block by trying $ctr = 0, 1, 2, \ldots$

The Bitcoin Backbone, III

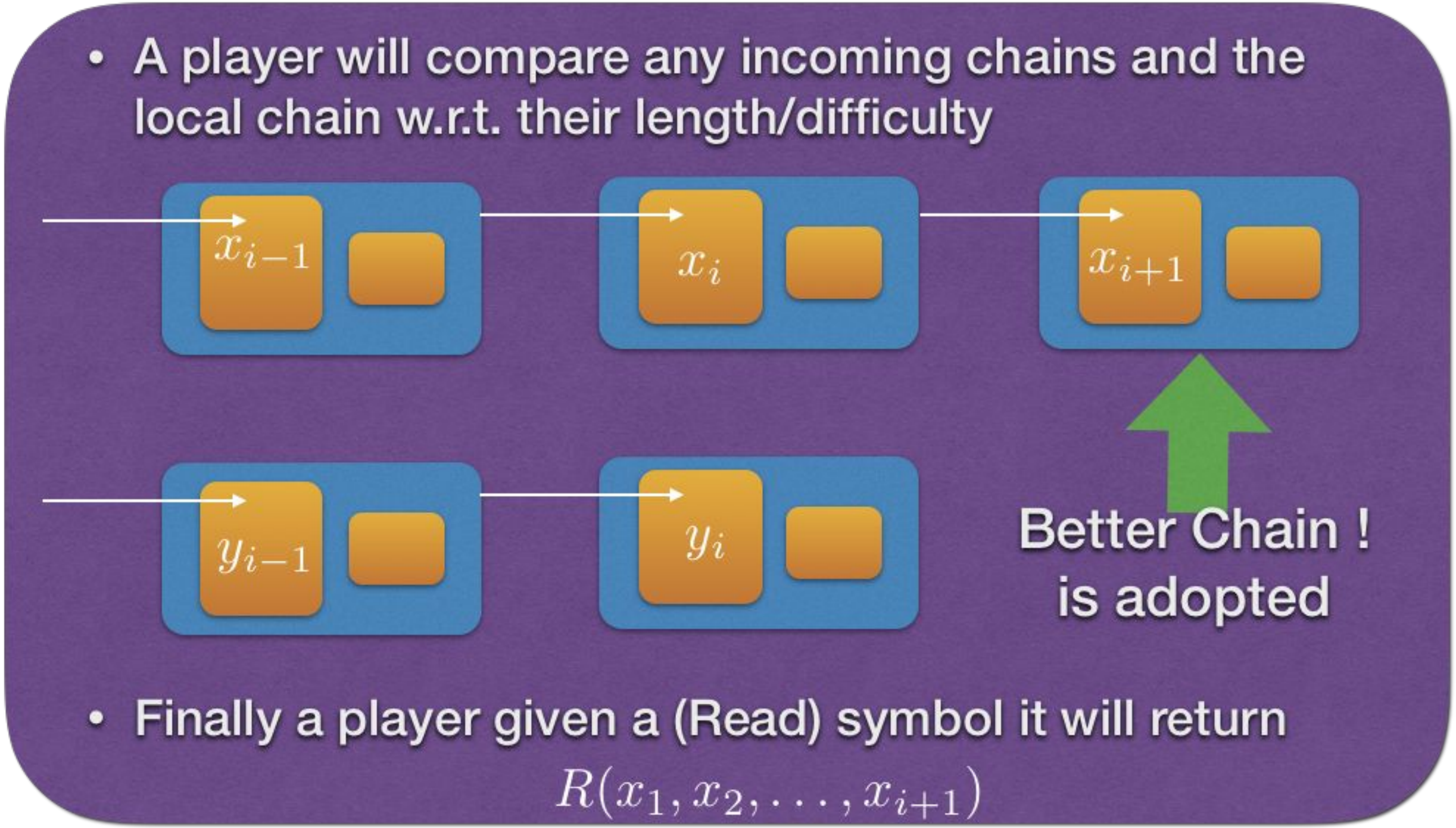


parameterized by $V(\cdot), R(\cdot), I(\cdot)$

- If a player finds a new block it extends $\mathcal{C}$

- The new $\mathcal{C}$ is propagated to all players via the (unreliable/anonymous) broadcast

The Bitcoin Backbone, IV



- A player will compare any incoming chains and the local chain w.r.t. their length/difficulty

x_{i-1} x_i x_{i+1}

y_{i-1} y_i

Better Chain ! is adopted

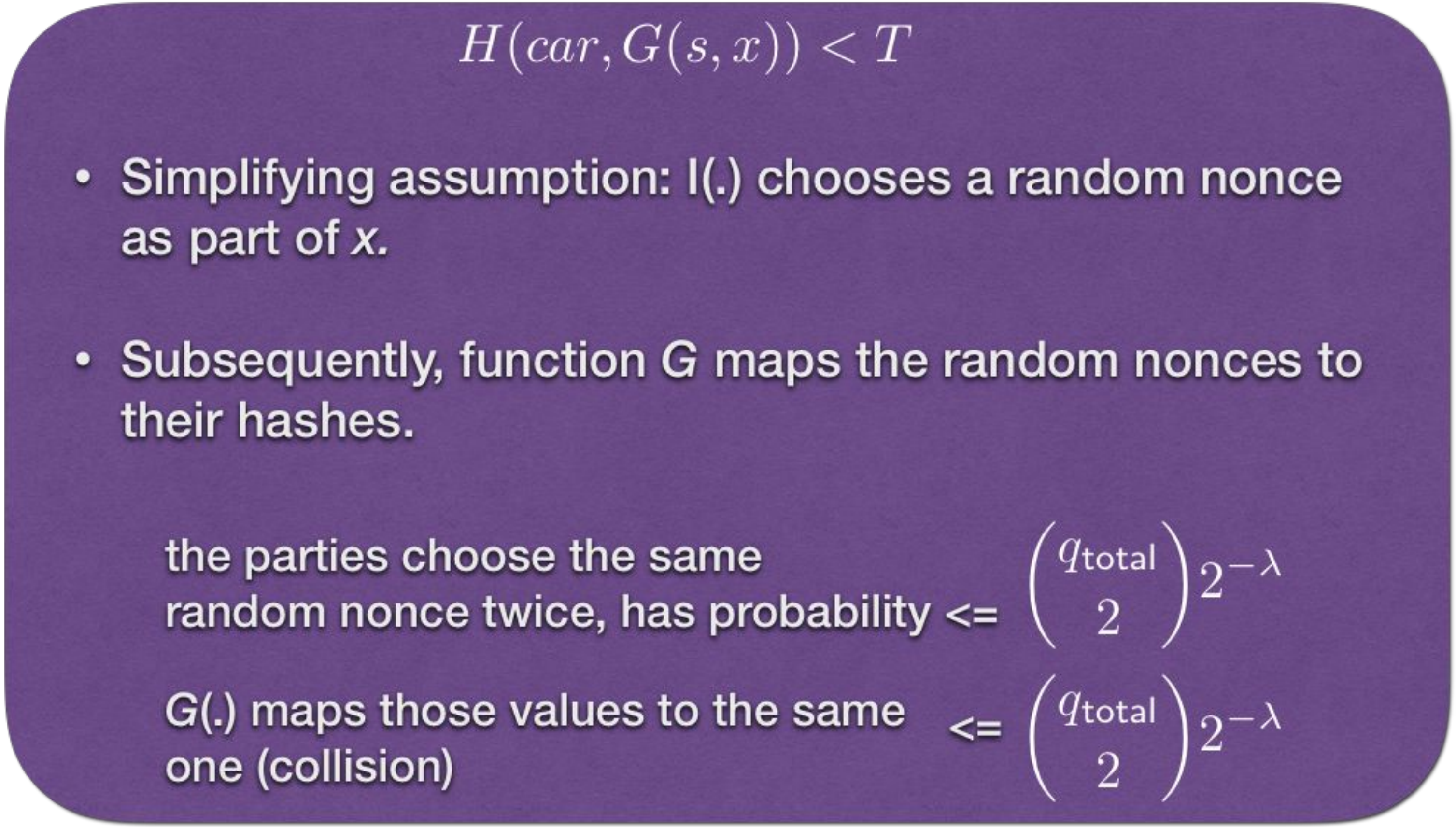
- Finally a player given a (Read) symbol it will return

$$R(x_1, x_2, \ldots, x_{i+1})$$

Requirements for functions

- Input Validity. Function I(.) produces inputs acceptable according to V(.)
- Input Entropy. Function I(.) on the same input, will not produce the same output with overwhelming probability.

Input Entropy



$$H(car, G(s,x)) < T$$

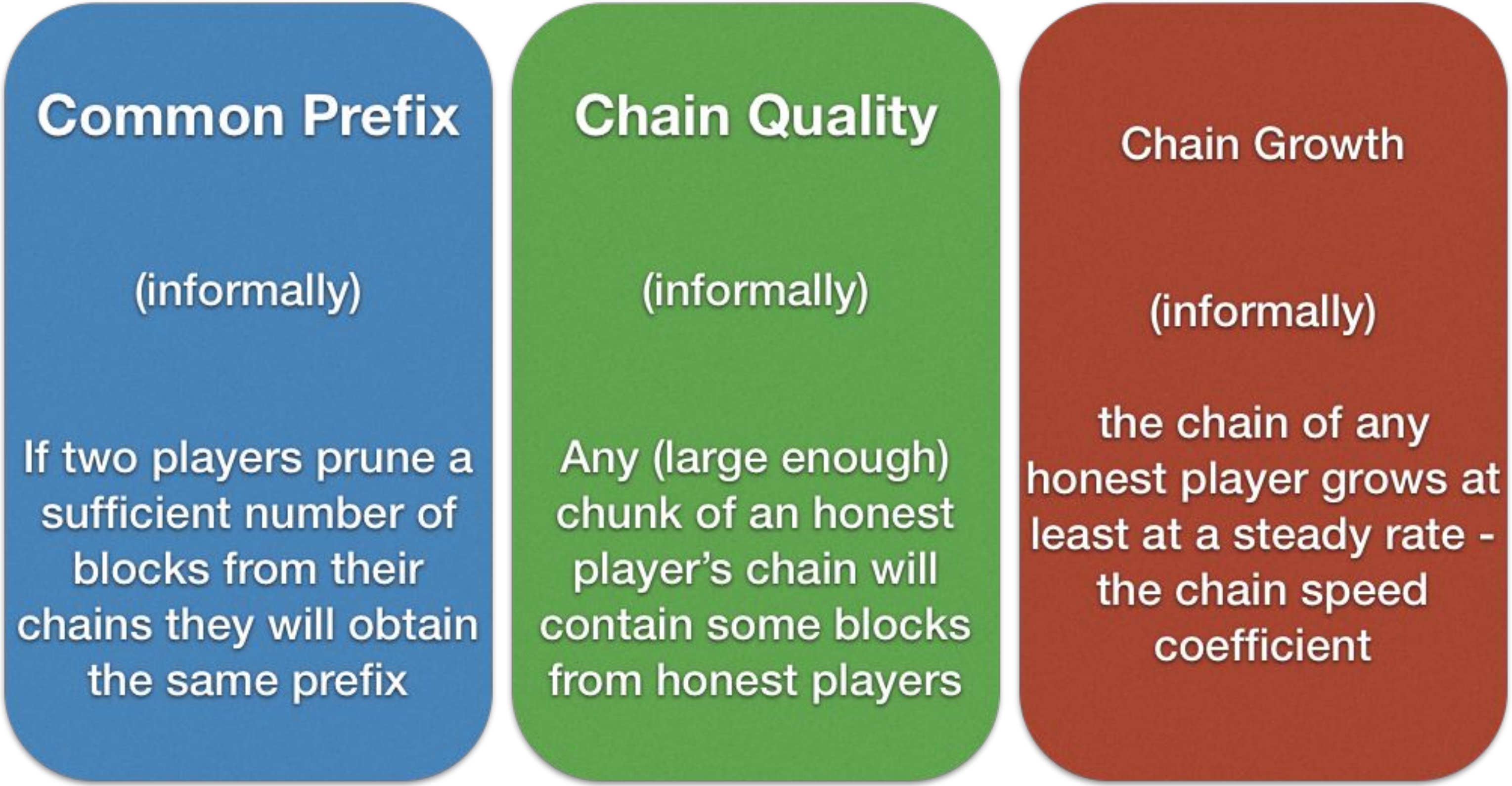
- Simplifying assumption: I(.) chooses a random nonce as part of *x.*

- Subsequently, function *G* maps the random nonces to their hashes.

the parties choose the same random nonce twice, has probability <= $\binom{q_{\text{total}}}{2} 2^{-\lambda}$

G(.) maps those values to the same one (collision) <= $\binom{q_{\text{total}}}{2} 2^{-\lambda}$

Basic Properties



Common Prefix

(informally)

If two players prune a sufficient number of blocks from their chains they will obtain the same prefix

Chain Quality

(informally)

Any (large enough) chunk of an honest player's chain will contain some blocks from honest players

Chain Growth

(informally)

the chain of any honest player grows at least at a steady rate - the chain speed coefficient

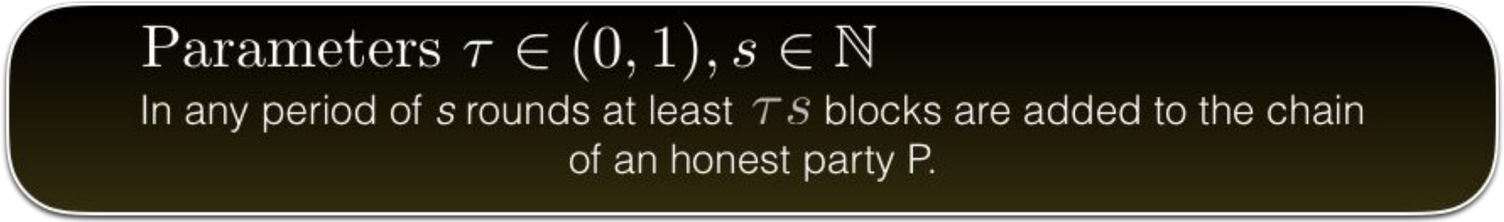
Common Prefix

(strong common prefix / consistency)

$$\forall r_1, r_2, (r_1 \le r_2), P_1, P_2, \text{ with } \mathcal{C}_1, \mathcal{C}_2 : \; \mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2$$

- The property holds true in a probabilistic sense with an error that decays exponentially in *k*

Chain Growth

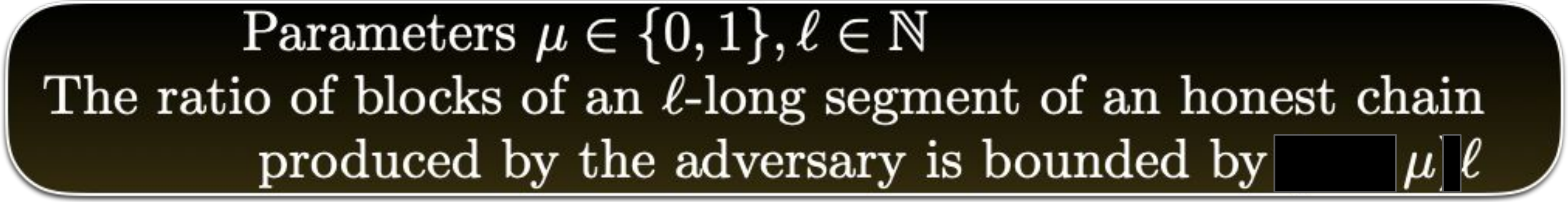


Parameters $\tau \in (0,1), s \in \mathbb{N}$

In any period of *s* rounds at least τs blocks are added to the chain of an honest party P.

- The property holds true in a probabilistic sense with an error probability that exponentially decays in *s*

Chain Quality



Parameters $\mu \in \{0, 1\}, \ell \in \mathbb{N}$

The ratio of blocks of an ℓ-long segment of an honest chain produced by the adversary is bounded by [redacted] μ [redacted] ℓ

- The probability holds true probabilistically with an error that exponentially decays in ℓ

Proof Strategy

1. Define the notion of *typical execution.*
2. Argue that typical executions have with overwhelming probability.
3. Prove CG, CP, CQ
4. Derive persistence and liveness.

Honest parties - Successful Rounds

probability
at least one honest
party finds a POW
in a round

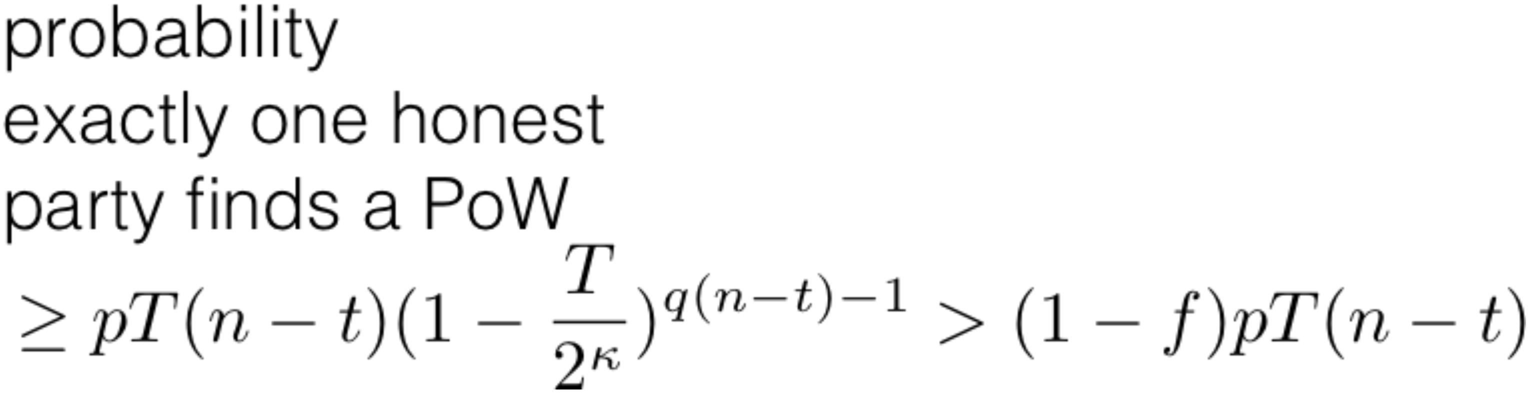
$$f = 1 - (1 - \frac{T}{2^\kappa})^{q(n-t)}$$

$$p = q/2^\kappa$$

Observe

$$f = pT(n-t) - (\frac{T}{2^\kappa})^2(\ldots) \approx pT(n-t)$$

Uniquely successful rounds - honest parties



probability
exactly one honest
party finds a PoW

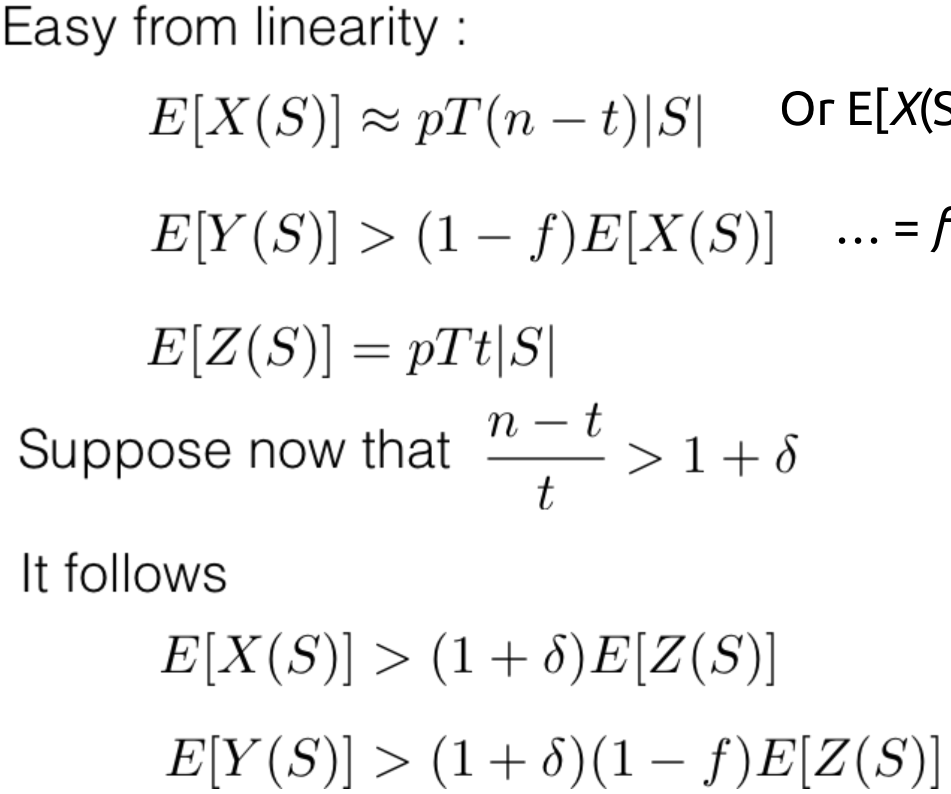
$$\geq pT(n-t)(1-\frac{T}{2^{\kappa}})^{q(n-t)-1} > (1-f)pT(n-t)$$

(think: as S1, …, S*n-t*, the event that the respective honest party uniquely finds a PoW.)
They are mutually exclusive events. For S*i*, it holds that one of the queries of *i* is successful (1-(1-*T*/2^κ)^*q*)==*pT*, while the rest fail.

Notations

- Let S a set of consecutive rounds.
- $X(S)$ = number of *successful rounds.*
- $Y(S)$ = number of *uniquely successful rounds*.
- $Z(S)$ = total number of PoWs computed during S.

Expectations



Easy from linearity :

$$E[X(S)] \approx pT(n-t)|S|$$

Or E[X(S)] = f |S|

$$E[Y(S)] > (1-f)E[X(S)]$$

… = f (1-f) |S|

$$E[Z(S)] = pTt|S|$$

Suppose now that $\frac{n-t}{t} > 1+\delta$

It follows

$$E[X(S)] > (1+\delta)E[Z(S)]$$

$$E[Y(S)] > (1+\delta)(1-f)E[Z(S)]$$

Typical Executions, I

- Let κ be the security parameter.

- A polynomial in κ execution is typical with parameter if for any set of rounds $S, |S| = \Omega(\kappa)$

$$X(S) > (1-\epsilon)E[X(S)]$$
$$Y(S) > (1-\epsilon)E[Y(S)]$$
$$Z(S) < (1+\epsilon)E[Z(S)]$$

  - No collisions, or predictions take place against *H*(.)

Typical Executions, II

Theorem. Typical executions happen almost always

Proof

Case 1. Suppose that

$$\begin{aligned} \exists S : X(S) &\leq (1-\epsilon)E[X(S)] \\ \vee Y(S) &\leq (1-\epsilon)E[Y(S)] \\ \vee Z(S) &\geq (1+\epsilon)E[Z(S)] \end{aligned}$$

X,Y,Z the binomial distribution so we can show with overwhelming probability in κ via a Chernoff bound.

Case 2. There is a collision or prediction for the hash function.

Follows from RO assumption + input entropy assumption.

- Chernoff bounds

X is a binomial distribution $\mu = E[X]$

$$\Pr[X \leq (1-\delta)\mu] \leq e^{-\delta^2 \mu/2}$$

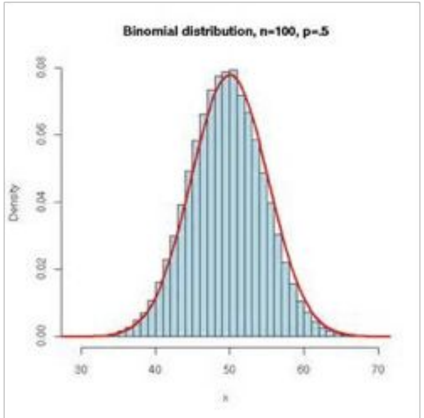
$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\delta^2 \mu/3}$$

E.g., sequence of *n* independent Bernoulli Trials

$$X = \sum_{i=1}^{n} X_i$$

$$X_i \in \{0,1\}, \Pr[X_i = 1] = p$$

$$\mu = np$$



Proving Chain Quality, I

- Consider a chain $\mathcal{C}$ of an honest party and ℓ consecutive blocks from that chain.

- The chain quality coefficient is $\mu = \dfrac{1}{\lambda}$ where $\dfrac{n-t}{t} > \lambda(1+\delta)$

Proof (by contradiction)

Consider a sequence of blocks $B_u \ldots B_v$ in the chain of an honest party with $\ell = v - u + 1$

Proving Chain Quality, II

- Define an expanded sequence of blocks

$$B_{u'} \ldots B_{v'} \qquad L = v' - u' + 1 \geq \ell$$

So that

(or is genesis)

(1) $B_{u'}$ was produced by an honest party at round r_1

(2) $B_{v'}$ was accepted by an honest party at round r_2

(such extension is well defined) $\quad S = \{r_1, \ldots, r_2\}$

$x =$ number of blocks produced by honest parties

For the sake of contradiction: $\quad x < (1 - \mu)\ell$

Proving Chain Quality, III

- **Lemma #1**. Because of typicality all the *L* blocks are computed within $S = \{r_1, \ldots, r_2\}$

- **Lemma #2**. Because of the choice of *S*, we have that $L \geq X(S)$ (otherwise no honest party would accept $B_{v'}$)

- Using the above and $x < (1 - \mu)\ell$ we have :

$$Z(S) \geq L - x \geq \mu L \geq \mu X(S)$$

Proving Chain Quality, IV

- It follows that $Z(S) \geq \mu X(S)$ and $|S| = \Omega(\kappa)$

By typicality: $X(S) > (1-\epsilon)E[X(S)]$

$$Z(S) < (1+\epsilon)E[Z(S)]$$

recall:

$$E[X(S)] \approx pT(n-t)|S|$$

$$E[Y(S)] > (1-f)E[X(S)]$$

$$E[Z(S)] = pTt|S|$$

$$\frac{n-t}{t} > \lambda(1+\delta)$$

$$\lambda(1+\epsilon)pTt|S| > (1-\epsilon)pT(n-t)|S|$$

$$\iff \frac{n-t}{t} < \lambda\frac{1+\epsilon}{1-\epsilon}$$

from which we obtain a contradiction as long as

$$1+\delta > \frac{1+\epsilon}{1-\epsilon}$$

which is implied by: $\delta > 2\epsilon$

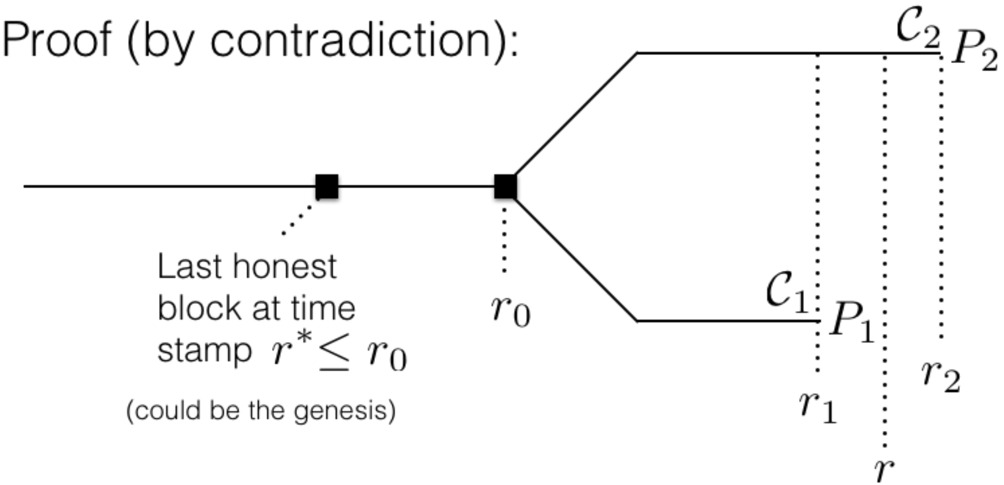
QED

Proving Common Prefix, I

Recall:

$\forall r_1, r_2, (r_1 \leq r_2), P_1, P_2,$ with $\mathcal{C}_1, \mathcal{C}_2 : \mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2$

Proof (by contradiction):



Last honest block at time stamp $r^* \leq r_0$

(could be the genesis)

first round >= r_1 where an honest party has a chain $\mathcal{C}_2'$ with $\mathcal{C}_1^{\lceil k} \not\preceq \mathcal{C}_2'$

$k = \Omega(\kappa)$

Proving Common Prefix, II

At round $r-1$

All honest parties have a chain $\mathcal{C}_i^{r-1}$ with $\mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_i^{r-1}$

At the end of round $r-1$ chain $\mathcal{C}_2'$ is transmitted for which we know that

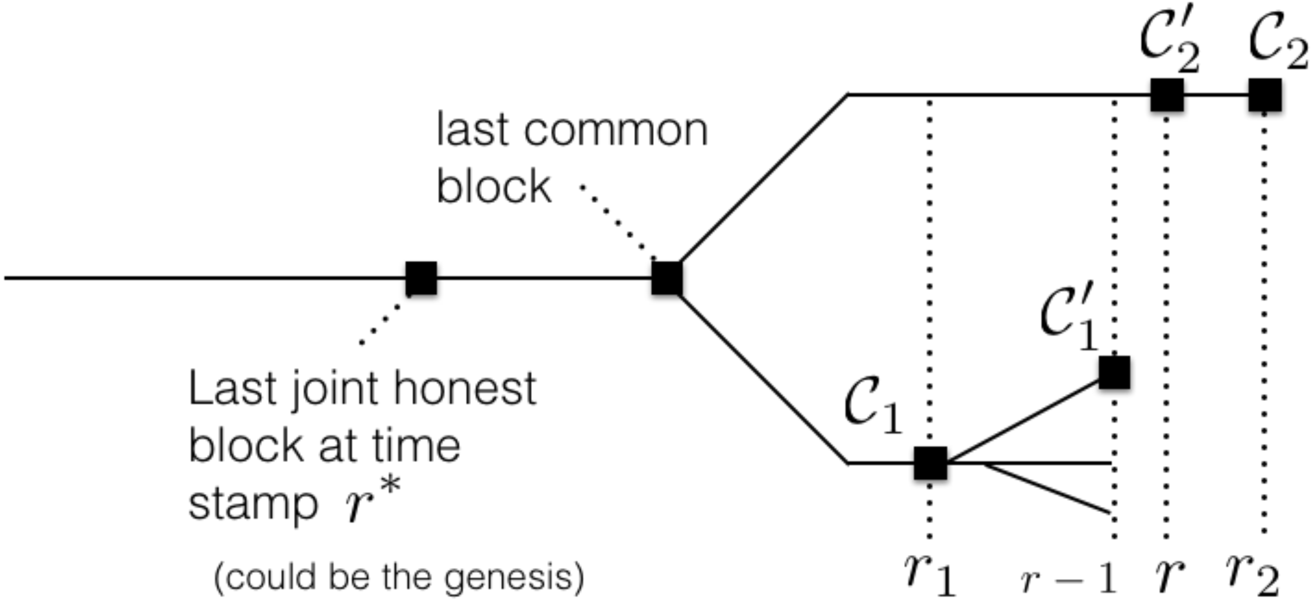
$$\mathcal{C}_1^{\lceil k} \not\preceq \mathcal{C}_2' \qquad |\mathcal{C}_2'| \geq |\mathcal{C}_1|$$

[by assumption]

[by the fact that $\mathcal{C}_2'$ will be accepted at round r by an honest party while at least one honest party at round $r_1 \leq r$ possessed chain $\mathcal{C}_1$]

Proving Common Prefix, III

Consider the set of rounds $S = \{r^* + 1, \ldots, r - 1\}$



Proving Common Prefix, IV

- Consider a uniquely successful round in
  $$S = \{r^* + 1, \ldots, r - 1\}$$
  - **lemma #1.** If a block created in a uniquely successful round at position *m* in a blockchain, then no other honest player will ever mine at position *m in any blockchain.*

- Therefore each uniquely successful round in *S* creates a block that must be matched by another block of the adversary

  - **lemma #2.** Such adversarial block should also be created within *S* (by the choice of *r** and typicality)

Proving Common Prefix, V

- It follows that $Z(S) \geq Y(S)$ and $|S| = \Omega(\kappa)$

By typicality: $Y(S) > (1-\epsilon)E[Y(S)]$

$$Z(S) < (1+\epsilon)E[Z(S)]$$

recall:

$$E[X(S)] \approx pT(n-t)|S|$$

$$E[Y(S)] > (1-f)E[X(S)]$$

$$E[Z(S)] = pTt|S|$$

$$\frac{n-t}{t} > 1+\delta$$

$$(1+\epsilon)pTt|S| > (1-\epsilon)(1-f)pT(n-t)|S|$$

$$\iff \frac{n-t}{t} < \frac{1+\epsilon}{(1-\epsilon)(1-f)}$$

from which we obtain a contradiction as long as

$$1+\delta > \frac{1+\epsilon}{(1-\epsilon)(1-f)}$$

which is implied by: $\delta > 2\epsilon + f$

QED

Proving Chain Growth

Consider a period of S, |S|=*s*, consecutive rounds and the chains that an honest party has at the onset of such rounds denoted by C1, …, C*s*

Let C be the chain that the party adopts after the completion of round *S*.

- The difference between C and C1 is at least X(S)
- E[X] = *f*|S| ~ *p*T(n-t)|S|
- By typicality, X(S) is at least (1-ε) *f* |S|
- Thus, CG follows with coefficient τ = (1- ε)*f*

Putting things together

Common Prefix => Persistence/Consistency

Chain Growth + Chain Quality => Liveness

Adjusting the difficulty

“maxvalid” rule
is changed so that
parties adopt chain with highest difficulty
linearly related to

$$\sum_i \frac{1}{T_i}$$

The *f* parameter [GKL15]

f = probability of producing a block in a round of interaction
(depends on target *T*, # of miners *n, and duration of round*)

- If *f* becomes too small, parties do not do progress; chain growth becomes too slow. [liveness is hurt]

- if *f* becomes too large, parties “collide” all the time; an adversary, exploiting network scheduling, can lead them to a forked state. [persistence is hurt]

To resolve this in a dynamic environment, bitcoin **recalculates the target** *T* to keep *f* constant

Target recalculation

$n_0 =$ estimation of the number of ready parties at the onset

$T_0 =$ initial target

[recall in this context "party"= single CPU]

$m =$ epoch length in blocks (In Bitcoin) = 2016

$\tau =$ recalculation threshold parameter (In Bitcoin) = 4

$T =$ target in effect

$pT =$ prob of a single miner getting a POW in a round

$$\text{next target} = \begin{cases} \frac{1}{\tau} \cdot T & \text{if } \frac{n_0}{n} \cdot T_0 < \frac{1}{\tau} \cdot T; \\ \tau \cdot T & \text{if } \frac{n_0}{n} \cdot T_0 > \tau \cdot T; \\ \frac{n_0}{n} \cdot T_0 & \text{otherwise} \end{cases}$$

$\Delta =$ last epoch duration based on block timestamps

$$n = \frac{m}{pT\Delta}$$

the "effective" number of parties of the epoch

Bahack’s attack

- The recalculation threshold is essential.
    - Without it, an adversary can create a private, artificially difficult chain that will increase the variance in its block production rate; overcoming the chain of the honest parties becomes a non-negligible event.

Understanding the attack : clay pigeons

clay pigeons

Clay pigeon shooting game

- Suppose you shoot on targets successively from 10m against an opponent
  - your success probability 0.3 vs. 0.4 that of your opponent.
  - You shoot in sequence 1000 targets. The winner is the one that got the most hits.
- What is your probability of winning?

Chernoff Bounds

Let

$$\delta > 0, \mathbf{Prob}[X_i = 1] = p_i, \mu = \sum_{i=1}^{n} p_i$$

Then

$$\mathbf{Prob}[\sum_{i=1}^{n} X_i \geq (1+\delta)\mu] \leq \exp(-\delta^2\mu/(2+\delta))$$

$$\mathbf{Prob}[\sum_{i=1}^{n} X_i \leq (1-\delta)\mu] \leq \exp(-\delta^2\mu/2), \delta \in (0,1)$$

Analysis, I

- You have an expectation of 300 hits and your opponent has an expectation of 400 hits.
- What is your probability of winning?
- Denote by X, whether you hit a target, and similarly Y for your opponent. From Chernoff bounds

$$\mathbf{Pr}[\sum_{i=1}^{1000} X_i \geq 345] \leq \exp(-(0.15)^2 300/2.15) < 4.3\%$$

$$\mathbf{Pr}[\sum_{i=1}^{1000} Y_i \leq 348] \leq \exp(-(0.13)^2 400/2) < 3.5\%$$

Analysis, II

- If the negation of both these events happens you will certainly loose

$$\mathbf{Pr}[X_{<345} \wedge Y_{>348}] = (1 - \mathbf{Pr}[X_{\geq 345}])(1 - \mathbf{Pr}[Y_{\geq 348}]) \geq \boxed{92.3\%}$$

- Thus the probability of you winning is below 8%

Analysis, III

- Now you are given a choice: you can decrease the size of the clay pigeon target by a ratio β and augment your “kills” by multiplying with $1/\beta$.
- Suppose your accuracy is just linear with β.
    - do you accept to play like this (while your opponent will keep playing in the same way) ?

Analysis, IV

Each shot has success $\mathbf{Pr}[X_i' = 1] = \beta \cdot \mathbf{Pr}[X_i = 1]$

- The score expectation of each shot remains the same:

$$E[(1/\beta)X_i'] = (1/\beta)\beta E[X_i] = E[X_i]$$

$$\mathbf{Pr}[\sum_{i=1}^{1000} X_i' \geq 345\beta]$$
$$\leq \exp(-(0.15)^2 300\beta/2.15)$$

decreasing β results in increased variance and our previous concentration argument will fail

β	bound
1,	~4.3%
0.5,	~20.8%
0.25,	~45.6%
0.10,	~73.1%

cc
BY