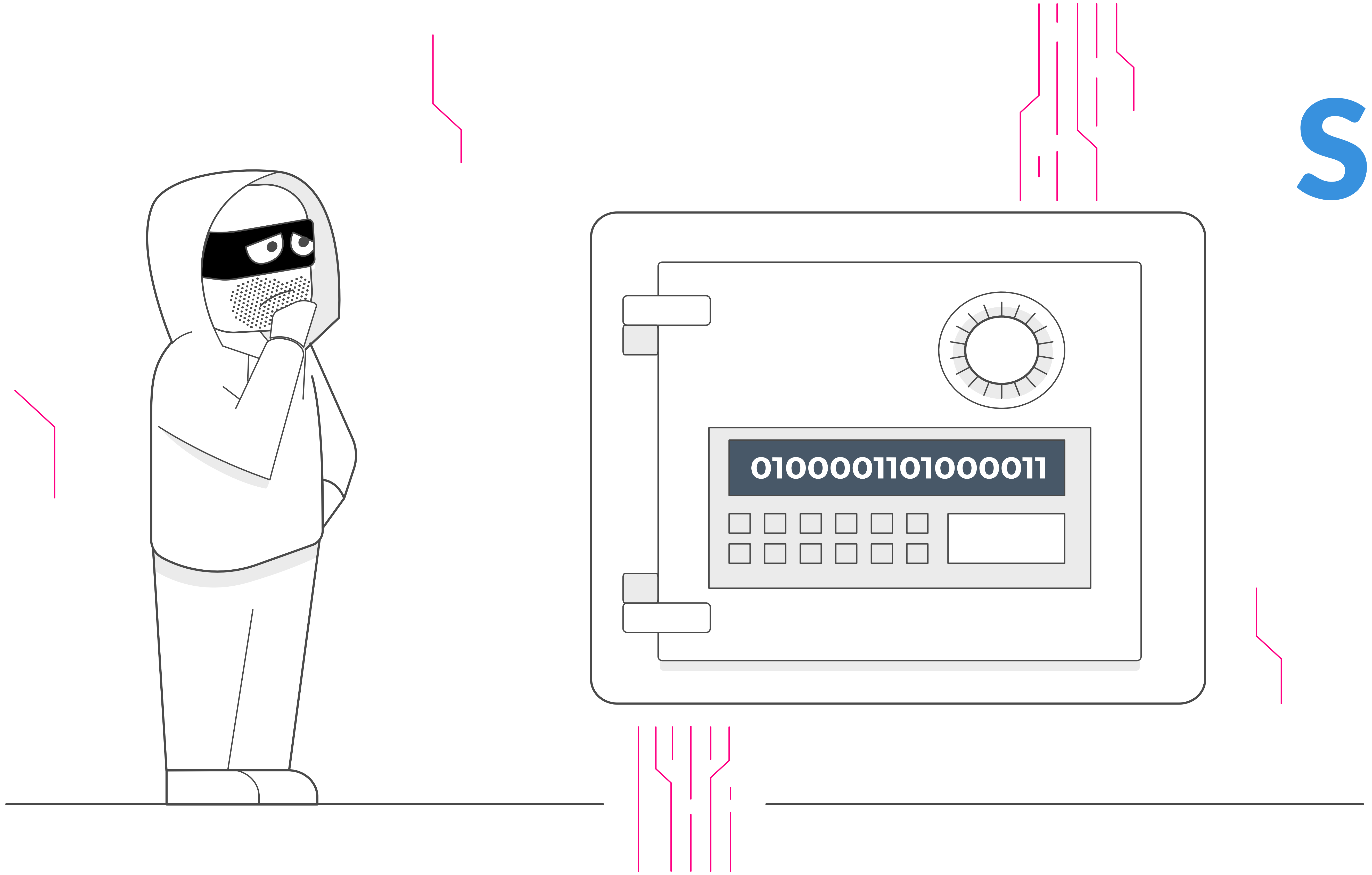
SPEED-SECURITY Tradeoffs in Blockchain Protocols



Team 27

Kritika Prakash

Bakhtiyar Syed

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

OVERVIEW

- **Introduction**

- **Basics**
  - Model
  - Backbone Protocols
  - Security Properties

- **Common Prefix Property**
  - Bound on Common Prefix Property
  - Strong Common Prefix Property

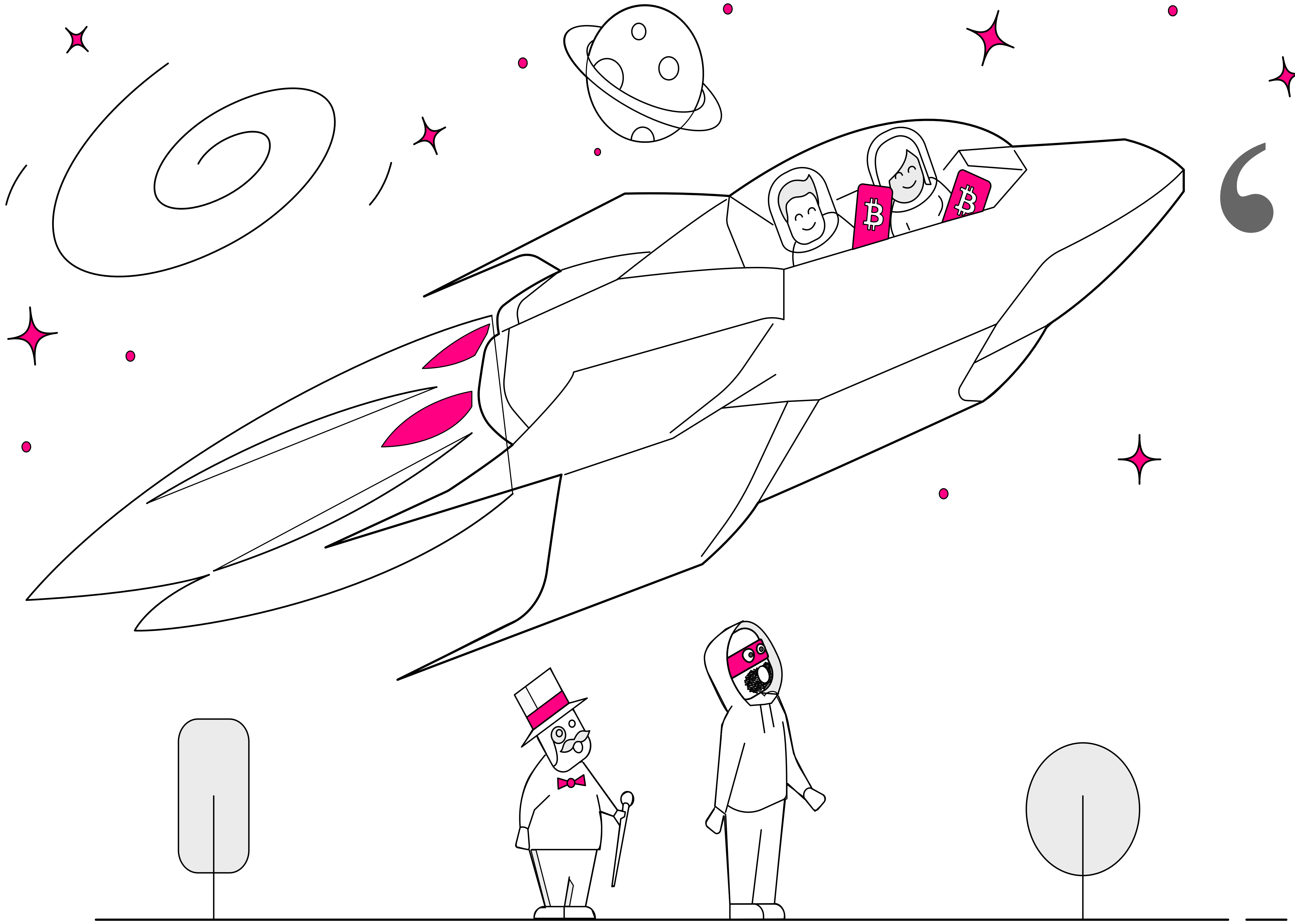
- **Chain Growth Property**

- **Speed - Security Tradeoffs**
  - Attack on Common Prefix

- **Conclusion**

INTRODUCTION

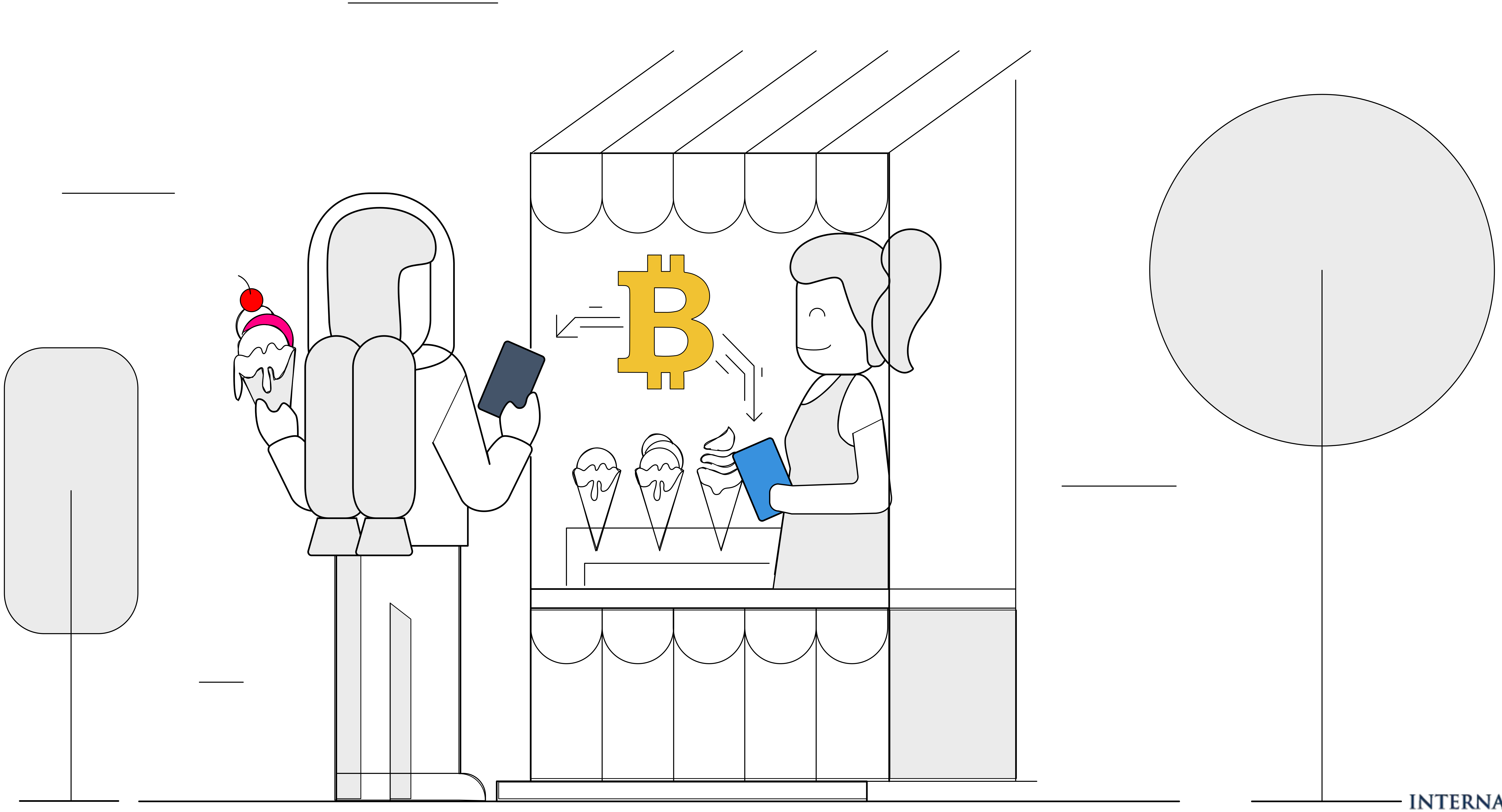
INTRODUCTION



> Speed, security or decentralization, you can only pick two!

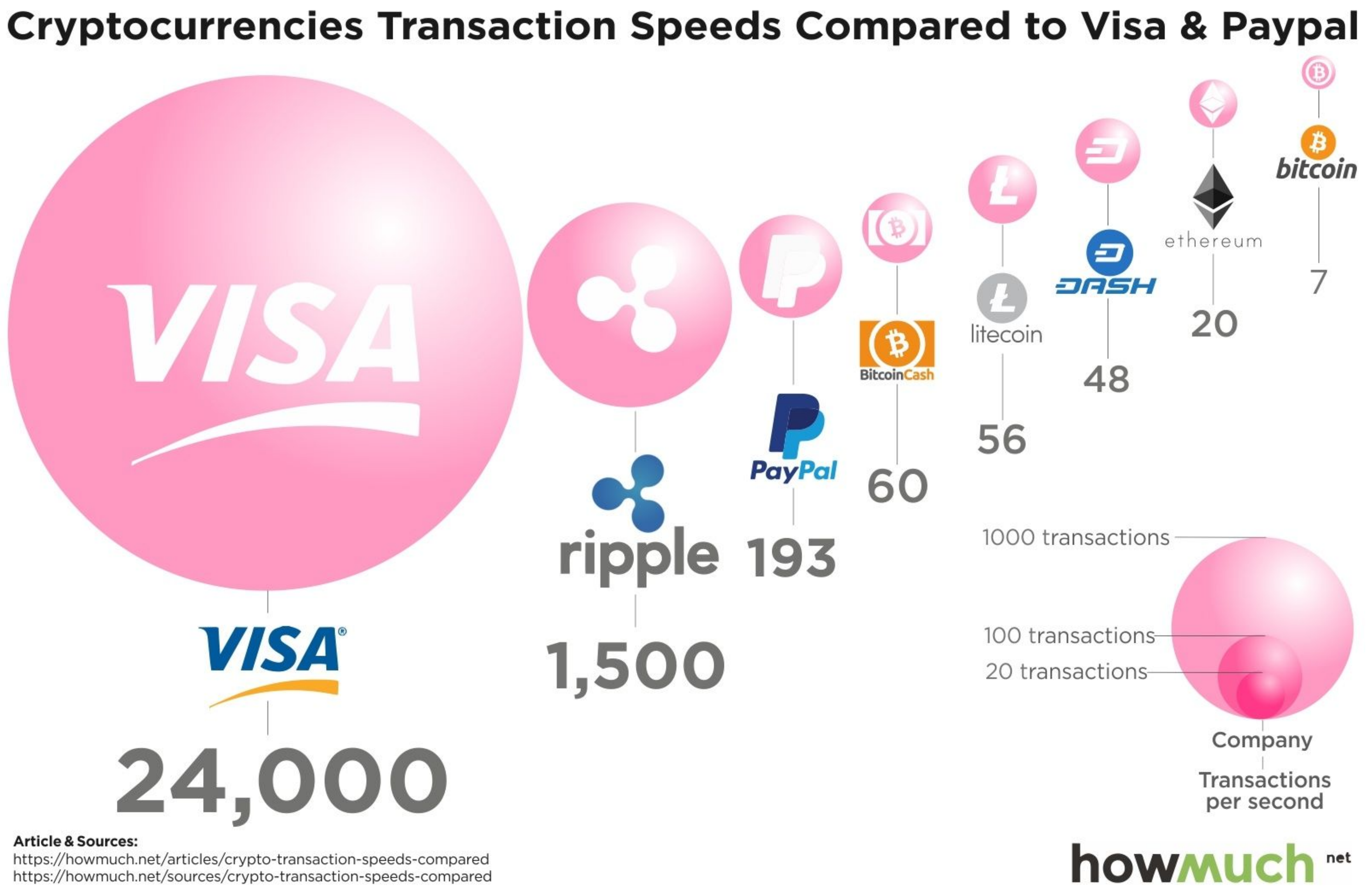
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

BITCOIN - THE FUTURE?



INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

FUTURE? TRANSACTION SPEED

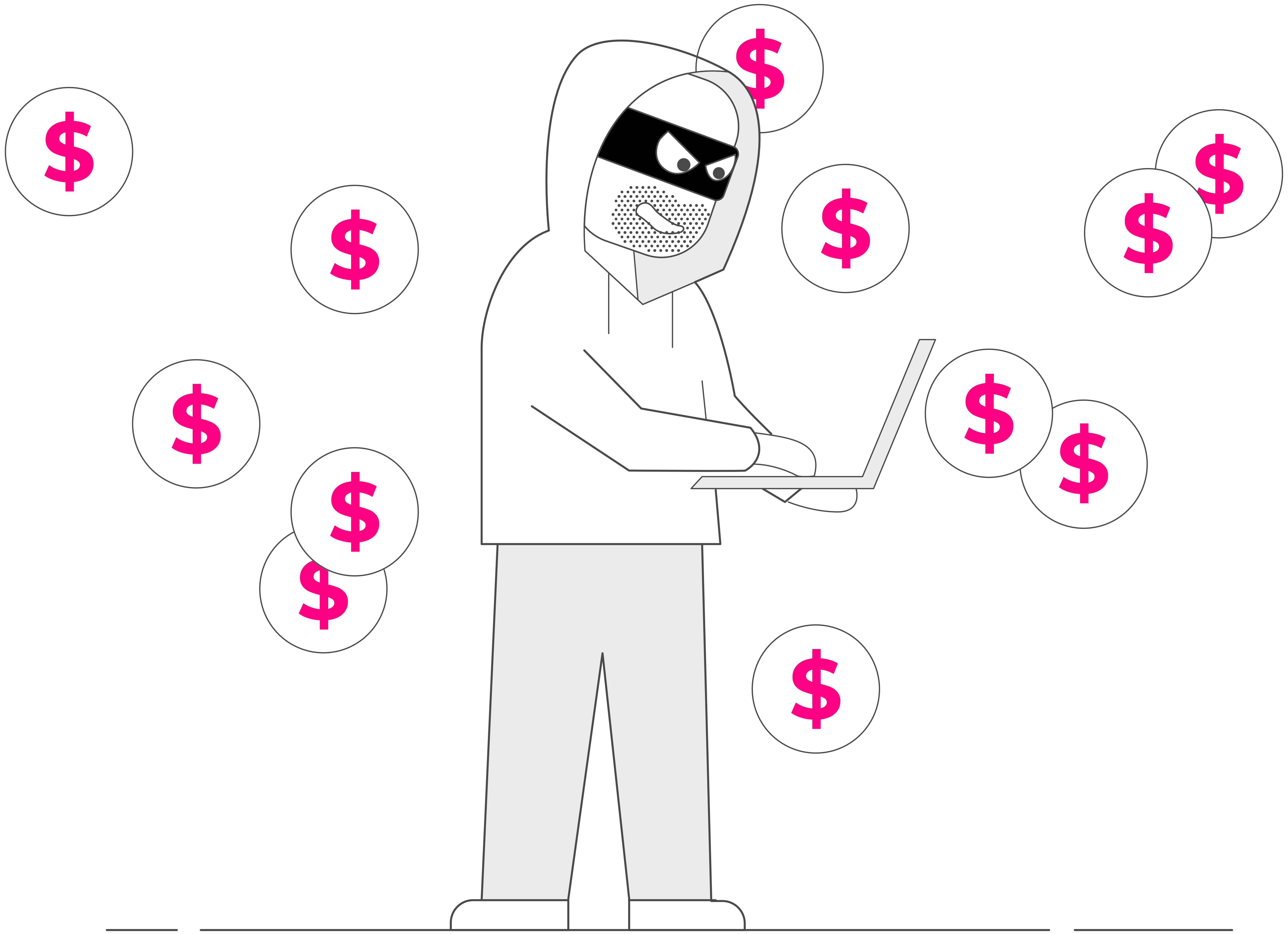


Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared

Bitcoin transaction speed is one of the lowest amongst its peers!

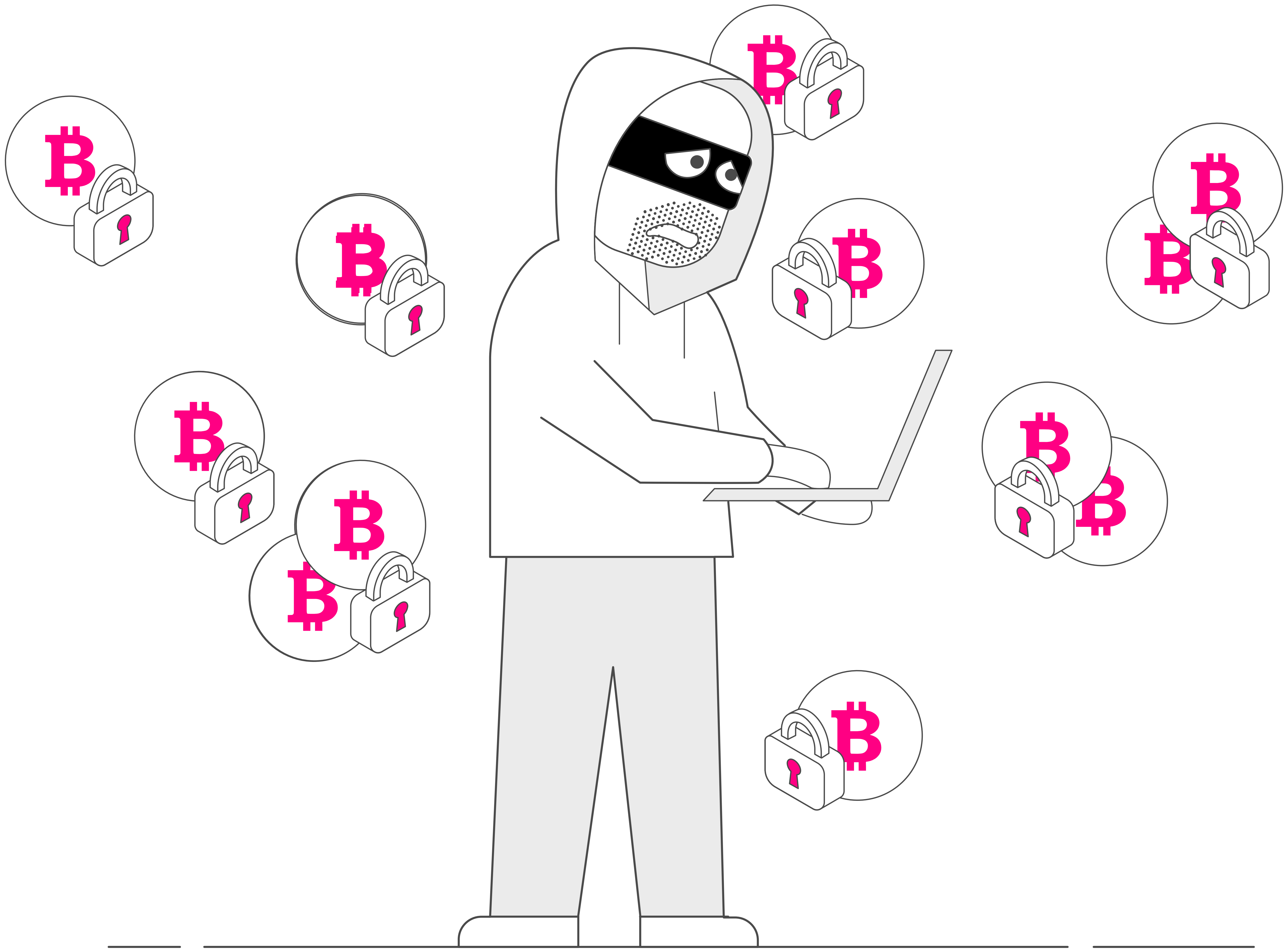
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

SECURITY



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

SECURITY



INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

PROOF of WORK

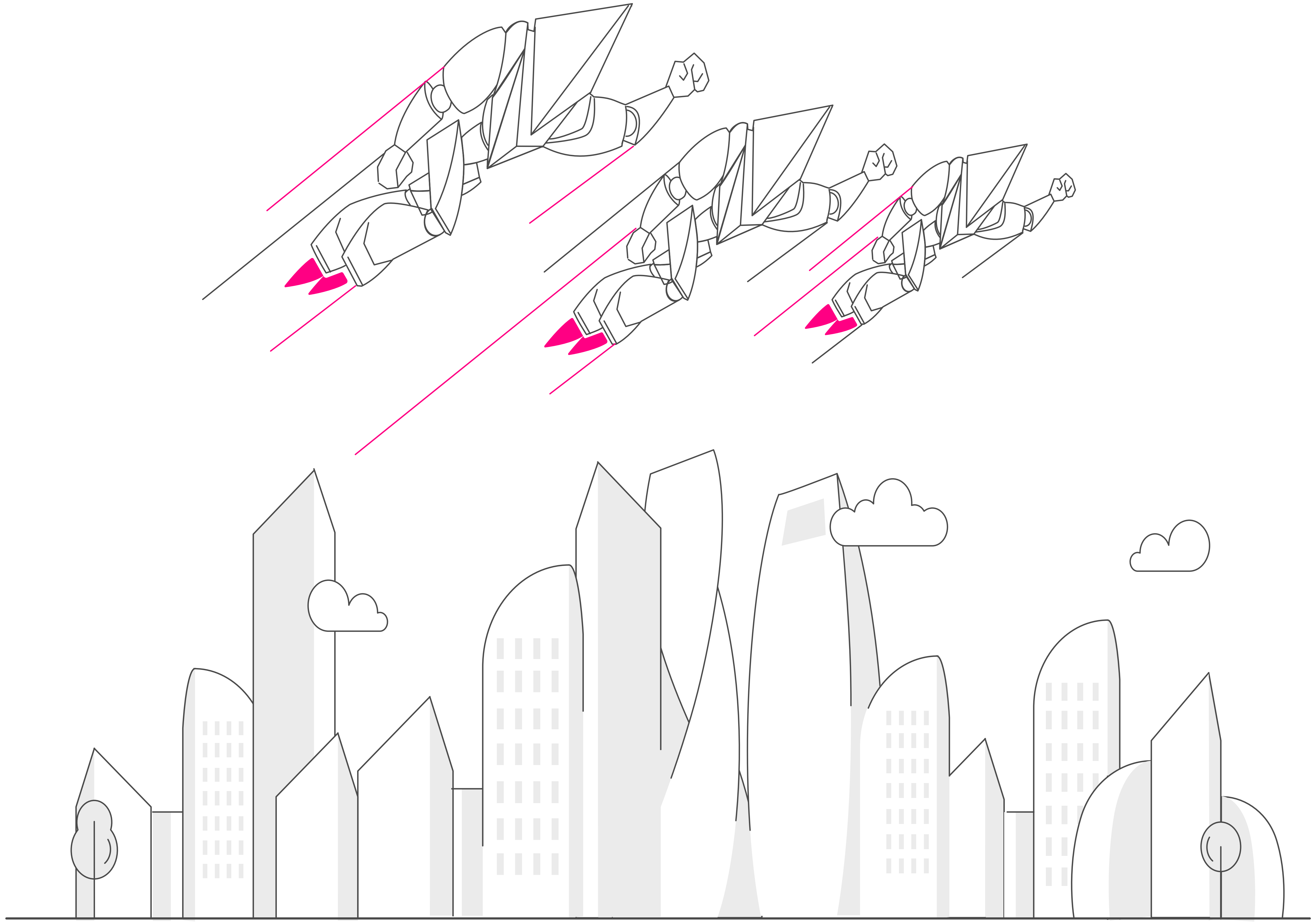
- The transactions in the blockchain are organized in blocks and each block is associated with a POW (Proof-of-Work).

- 1 MB transaction cap per block

- **POW Difficulty:** Intrinsic feature for security.
  Why? *It prohibits the adversary from flooding the network with messages and gives the opportunity to the honest parties to converge to a unified view.*

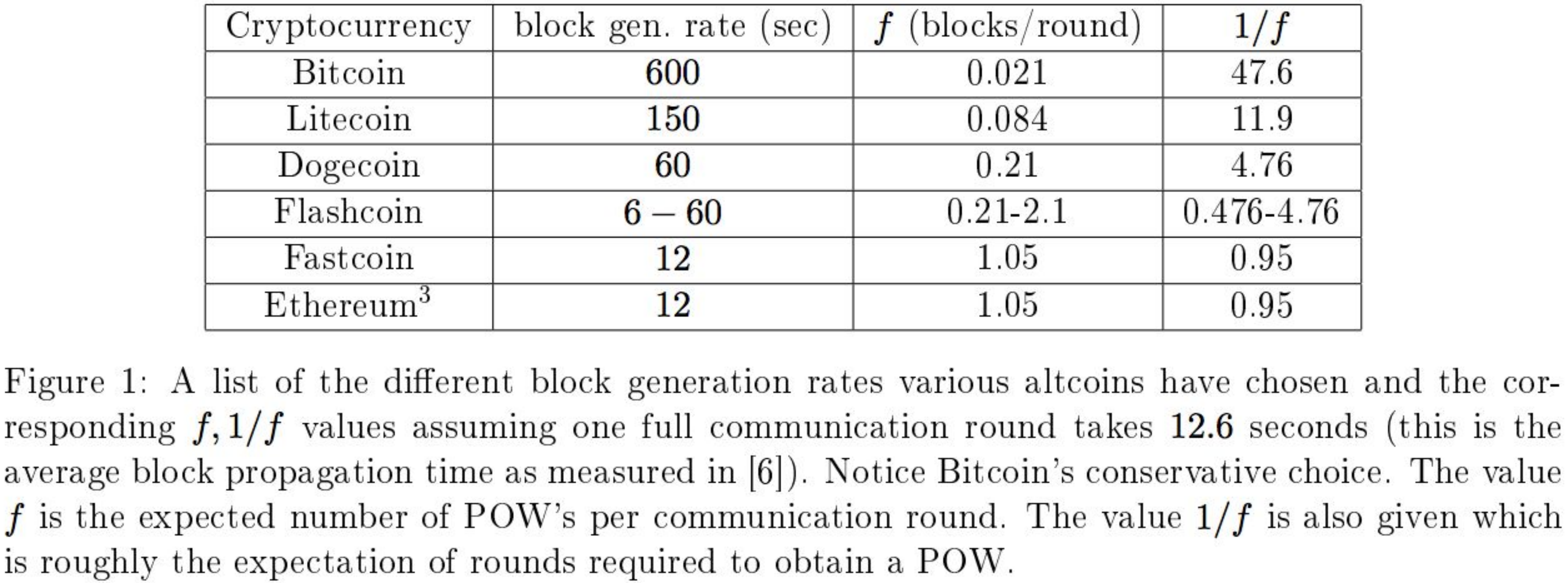
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

SPEED FACTORS



- **Obvious factors:** *network speed, computational power to verify transactions*
- We focus on the **Block Generation Rate.**
- **Block Gen Rate =** ***No. of blocks generated per round of information propagation.***

SPEED FACTORS

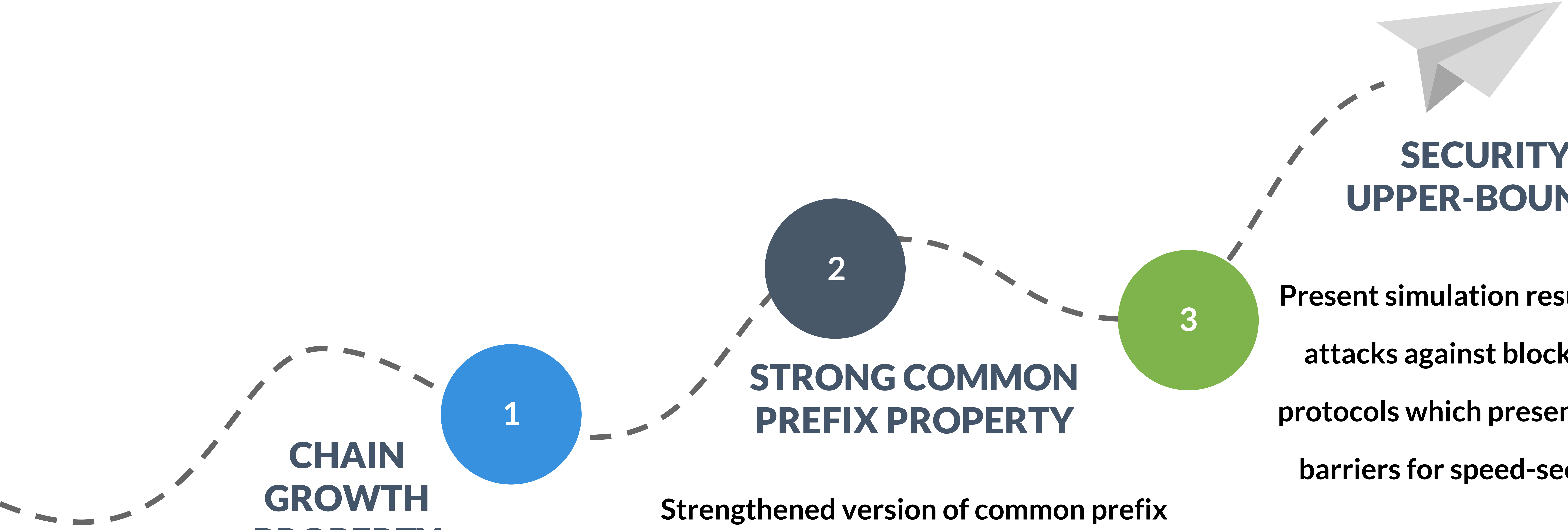


Cryptocurrency	block gen. rate (sec)	f (blocks/round)	$1/f$
Bitcoin	600	0.021	47.6
Litecoin	150	0.084	11.9
Dogecoin	60	0.21	4.76
Flashcoin	$6 - 60$	0.21-2.1	0.476-4.76
Fastcoin	12	1.05	0.95
Ethereum[3]	12	1.05	0.95

Figure 1: A list of the different block generation rates various altcoins have chosen and the corresponding $f, 1/f$ values assuming one full communication round takes 12.6 seconds (this is the average block propagation time as measured in [6]). Notice Bitcoin's conservative choice. The value f is the expected number of POW's per communication round. The value $1/f$ is also given which is roughly the expectation of rounds required to obtain a POW.

INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

What the AUTHORS PROPOSE



1

CHAIN GROWTH PROPERTY

Introduce a new security property which complements *common prefix* and *chain quality*.

2

STRONG COMMON PREFIX PROPERTY

Strengthened version of common prefix property - the third leg.

3

SECURITY UPPER-BOUNDS

Present simulation results and attacks against blockchain protocols which present upper barriers for speed-security.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

THE MAIN QUESTION

For a given block generation rate expressed as the expected number of blocks per round (parameter f), what is *the maximum adversarial hashing power* that can be provably tolerated by a population of honest miners?

THE BASICS

THE MODEL

- Total no. of parties: $\boldsymbol{n}$
- $\boldsymbol{q}$ queries allowed to a random oracle
- Adversary controls $\boldsymbol{t}$ parties $\boldsymbol{(t<n)}$
- Difficulty of finding hash : $\boldsymbol{D}$
- Length of required hash: $\boldsymbol{\kappa}$
- Prob(Single hashing query produces solution) = $\boldsymbol{p = D / 2}^{k}$
- Honest hashing power: $\boldsymbol{\alpha = pq(n-t)}$
- Adversary hashing power: $\boldsymbol{\beta = pqt}$
- Total hashing power = $\boldsymbol{f = pqn = \alpha + \beta}$

- Honest Block: Mined by an honest party
- Adversary Block: Mined by an adversary
- Chain C_1 extends Chain C_2 if $\boldsymbol{prefix(C_1) = suffix(C_2)}$
- Lower bound of a round being successful = $\boldsymbol{\gamma_u = \alpha - \alpha^2}$
- Better Lower Bound => $\boldsymbol{\gamma} = \boldsymbol{\alpha}\ e^{-\boldsymbol{\alpha}}$

  $p(X_i = 1) \geq \boldsymbol{\gamma} \geq \boldsymbol{\gamma_u}$

THE MODEL

q*-bounded setting**: Synchronous communication is assumed that allows each party ***q queries to a random oracle.

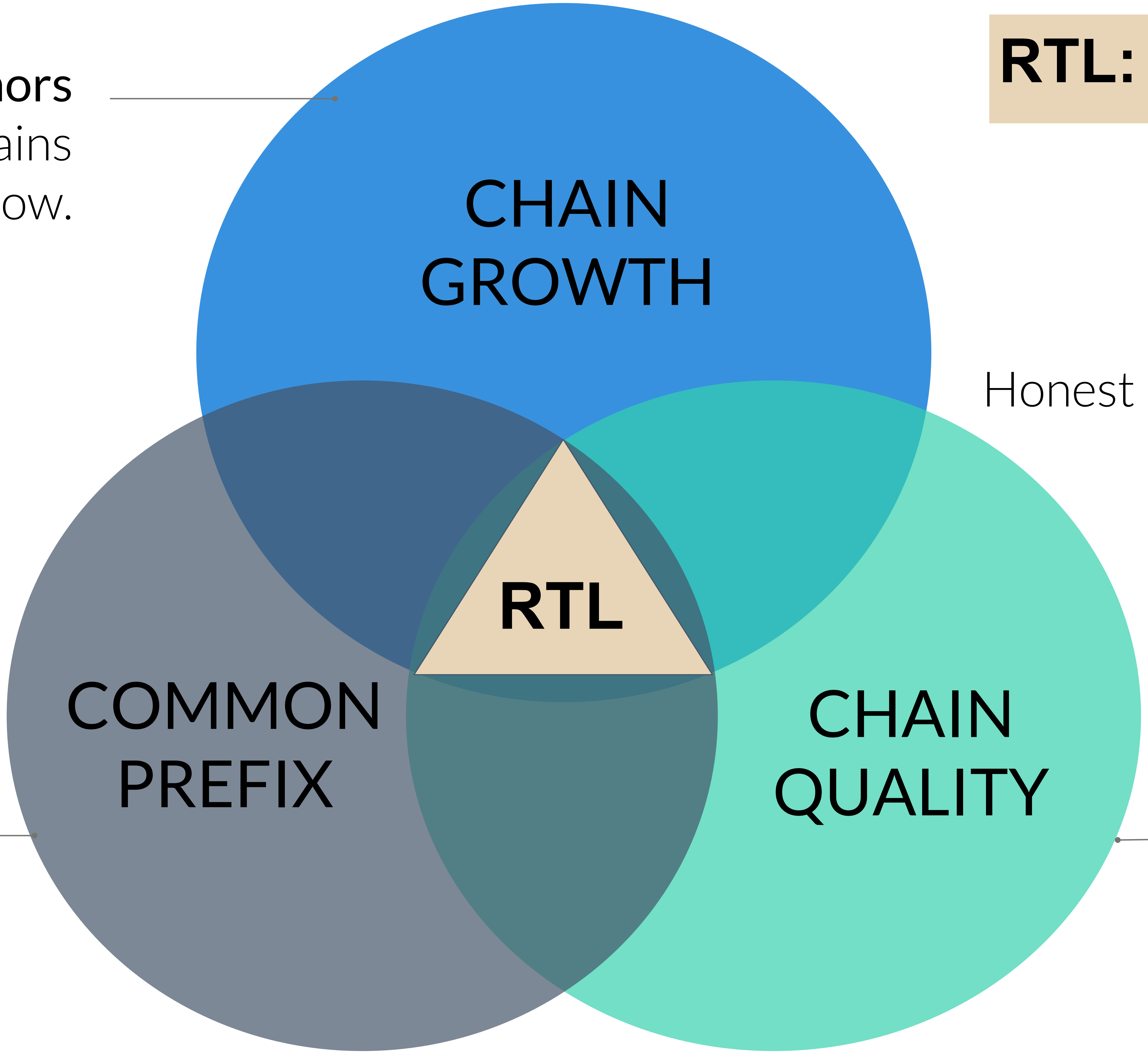
BACKBONE PROTOCOL

On this level of abstraction - we are only interested in properties of the blockchain, *independently* from the data stored inside the blocks.

The main idea is that honest players, at every round, receive new chains from the network and *pick the longest valid one* to mine. Then, if they mine a block, they broadcast their chain at the end of the round.

SECURITY PROPERTIES

RTL: Robust Txn Ledger



Suggested by Authors
Min. rate at which chains of honest blocks grow.

Same chain
Two honest players have the same view of the blockchain if they prune a small number of blocks from the tail.

Quality Metric
Honest players' chains do not contain sequences of adversarial blocks.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

ROBUST PUBLIC TXN LEDGER

→ This primitive captures the notion of a **book,** in which transactions are recorded.

→ The primitive satisfies two properties: ***persistence*** and ***liveness.***

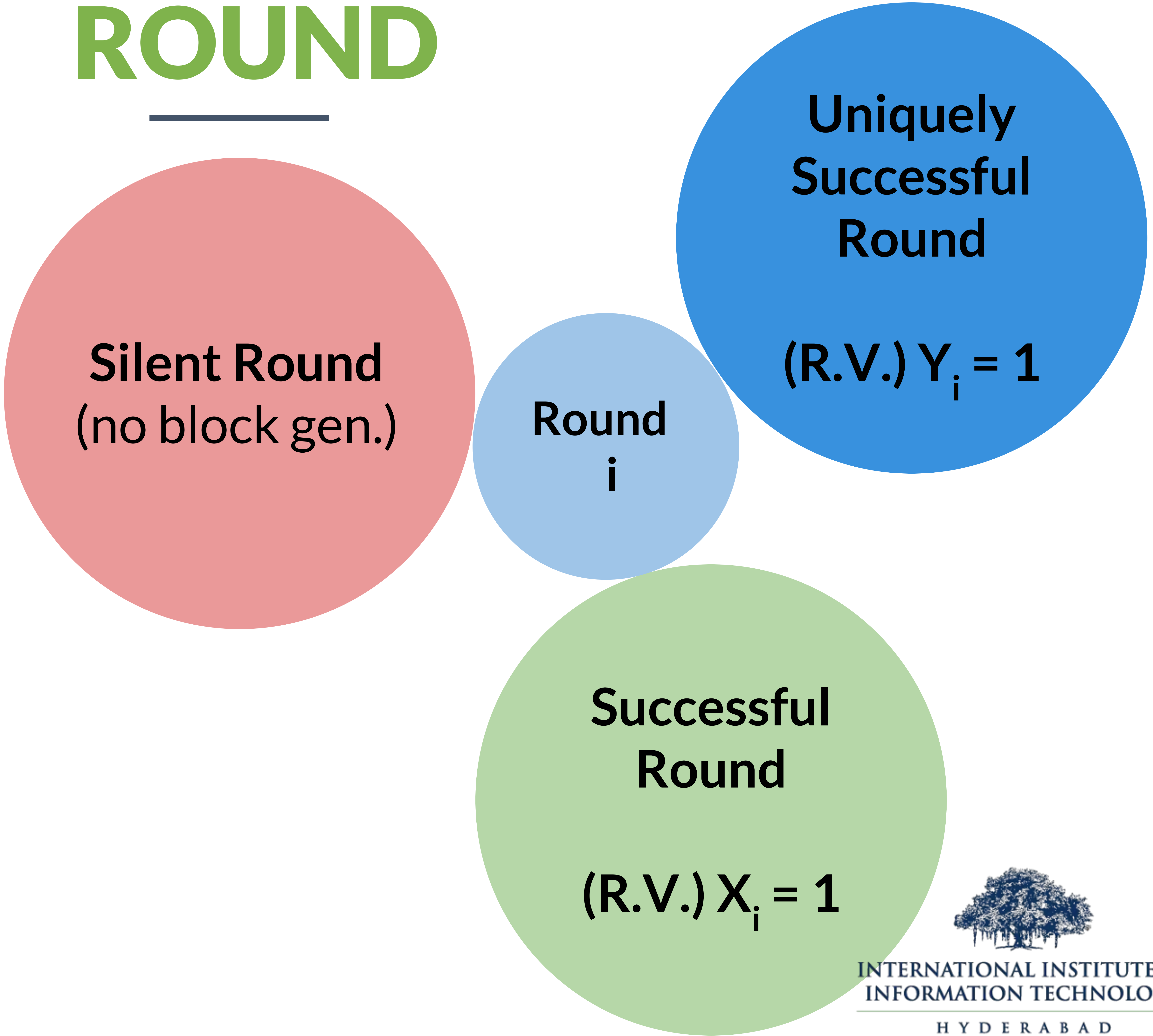
Persistence *ensures that, if a transaction is seen in a block deep enough in the chain, it will stay there.*
Liveness *ensures that if a transaction is given as input to all honest players, it will eventually be inserted in a block, deep enough in the chain, of an honest player.*

COMMON PREFIX

ROUND

Round:

- A round of complete information propagation between all honest parties.
- Useful unit of time to measure the rate of block generation.
- **Successful round**: At least one honest party computes a solution
- **Silent round**: No block is mined



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

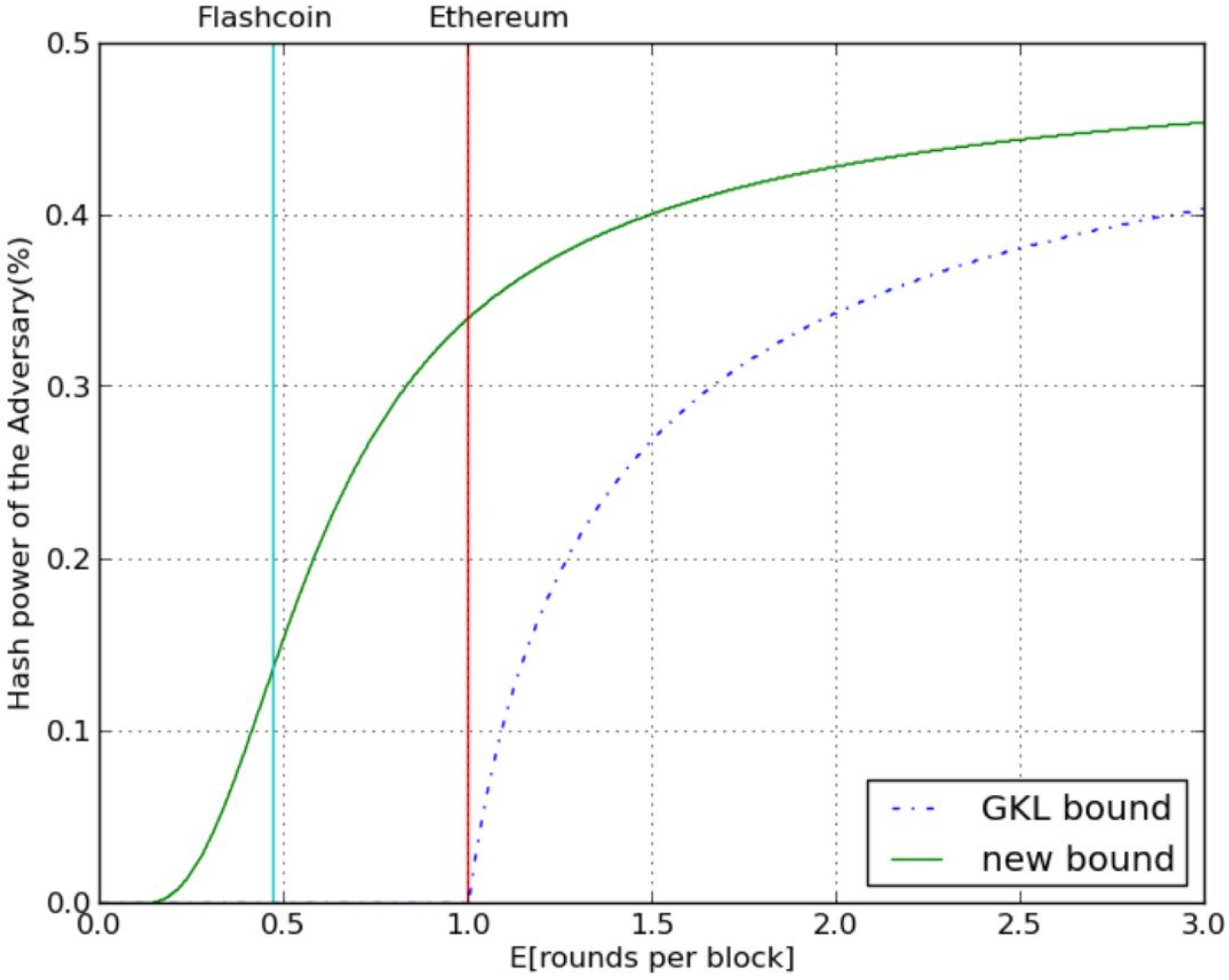
BOUND on Common Prefix

- With this, it is shown that $\gamma_u \geq \frac{f+\sqrt{f^2+4}}{2}\beta$ is sufficient for security in previous work
- Here, authors show that $\boldsymbol{\gamma \geq \beta}$ & $\boldsymbol{\gamma \geq \gamma_u}$
- For the above : *All uniquely successful rounds have to be compensated by the adversary (and not just those that are silent).*

- Lower bound of a round being successful = $\boldsymbol{\gamma_u = \alpha - \alpha^2}$
- Better Lower Bound => $\gamma = \alpha e^{-\alpha}$

  $\mathbf{p(X_i = 1) \geq \gamma \geq \gamma_u}$
- ***β:*** Adversary Hashing Power
- ***f:*** Total Hashing Power

BOUND on SECURITY



1/f

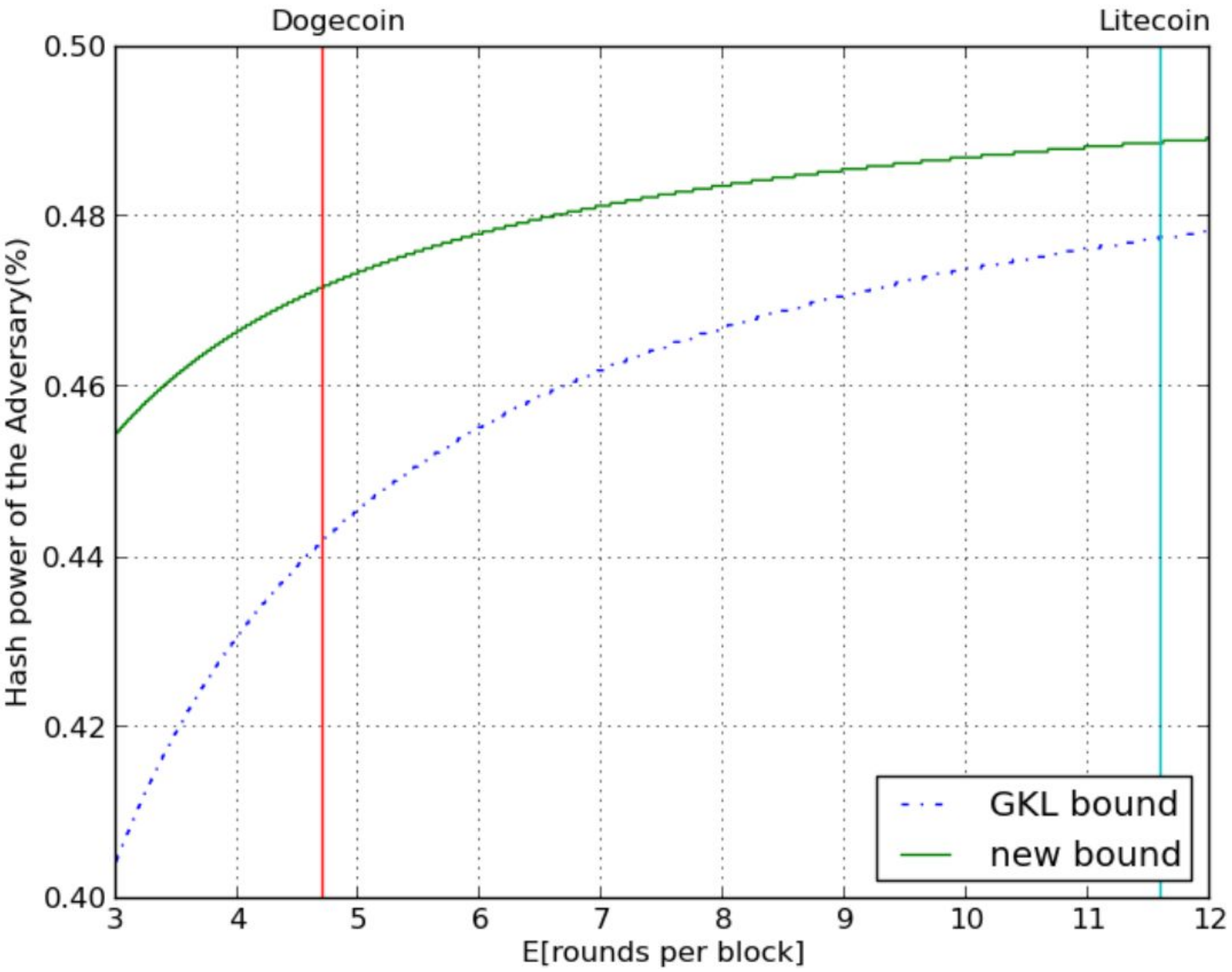
Figure*: The level of insecurity in terms of the hashing power of the adversary as a function of 1/f*

f: *Block Gen Rate per round*

This improvement in the bound has a significant impact in terms of provable security.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

BOUND on SECURITY



1/f →

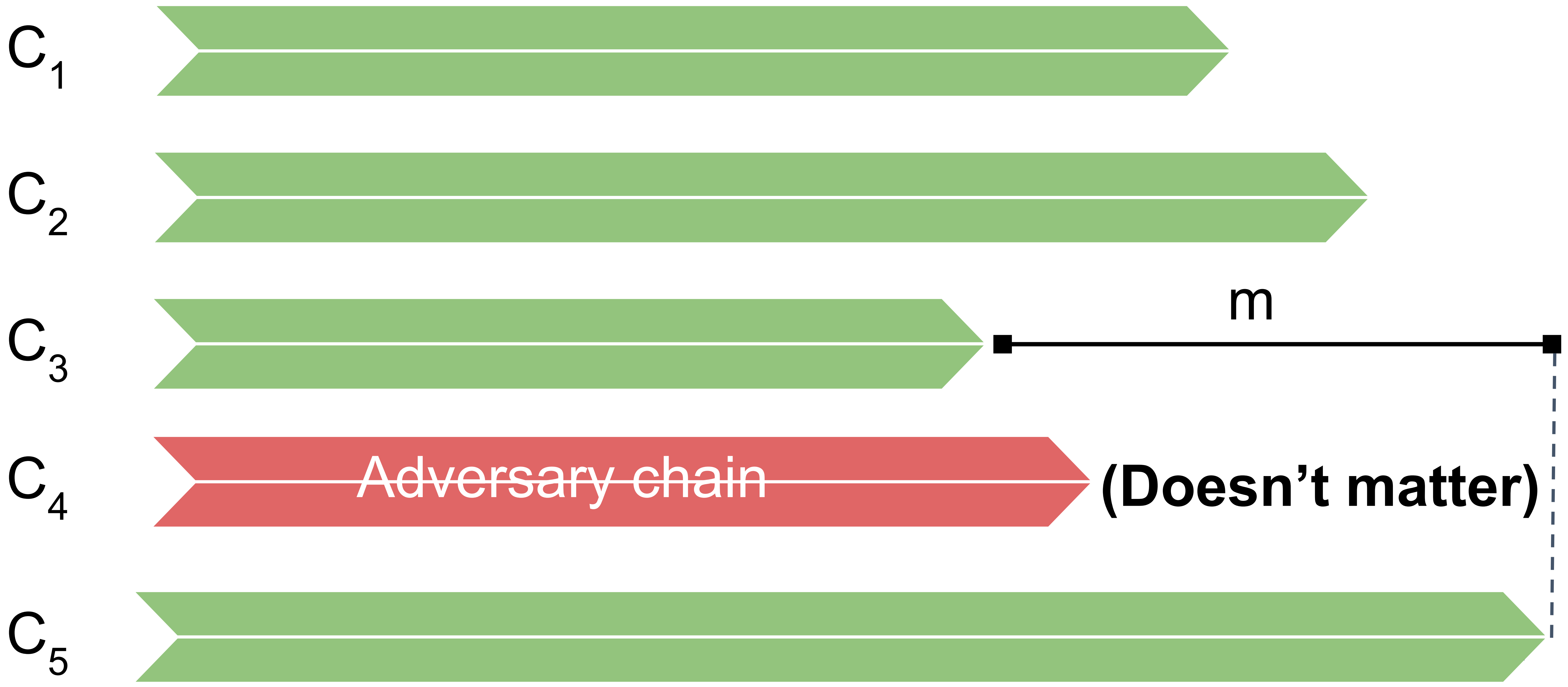
***Figure**: The level of insecurity in terms of the hashing power of the adversary as a function of 1/f*

***f:** Block Gen Rate per round*

This improvement in the bound has a significant impact in terms of provable security.

m-Uniform ROUND

- We call a round ***m***-uniform if, at that round, ***m*** is the minimum value such that for all chains C_1, C_2 that any two honest parties adopt at this round, it holds that $||C_1| - |C_2|| \leq \boldsymbol{m}$

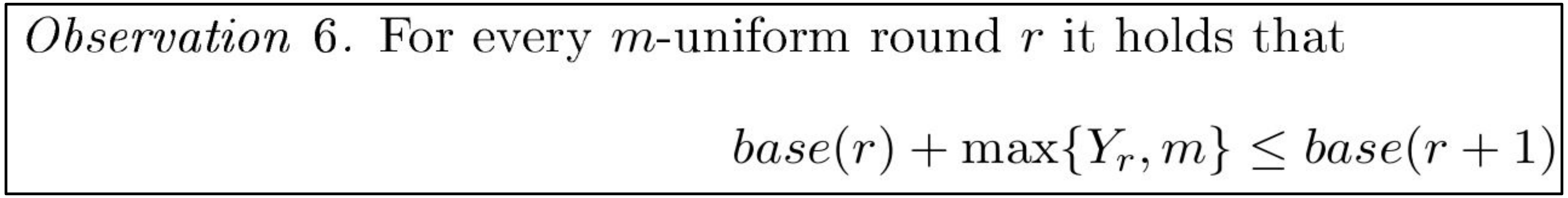


Base(*r*): Length of shortest chain adopted by honest party in round ***r***

$|C_3|$ = base(***r***)

INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

OBSERVATIONS



Observation 6. For every m-uniform round r it holds that

$$base(r) + \max\{Y_r, m\} \leq base(r+1)$$

- **Uniform Round: *m = 0***

$||C_1|-|C_2|| = 0$ for all chains of honest nodes in round ***r***

- **Non-Uniform Round: *m > 0***

$||C_1|-|C_2|| > 0$ for all chains of honest nodes in round ***r***

Y_r : Indicator R.V. = 1 if ***i*** is a uniquely successful round and 0 otherwise.

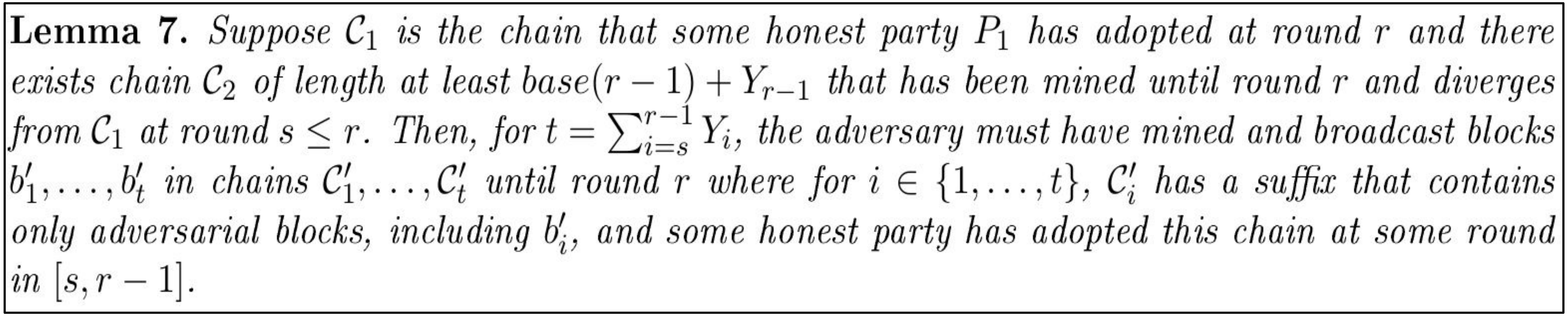
Uniquely Successful Rounds: Bad for Adversary

m-Uniform Rounds: Good for Adversary (Hash queries of short chains get wasted)

- Does not happen naturally in the system
- Adversary must mine his own blocks to make a round non-uniform (*m > 0)*

The adversary must compensate for all uniquely successful rounds independently of uniformity.

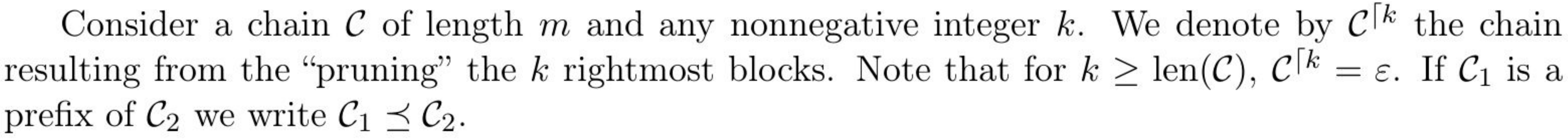
OBSERVATIONS



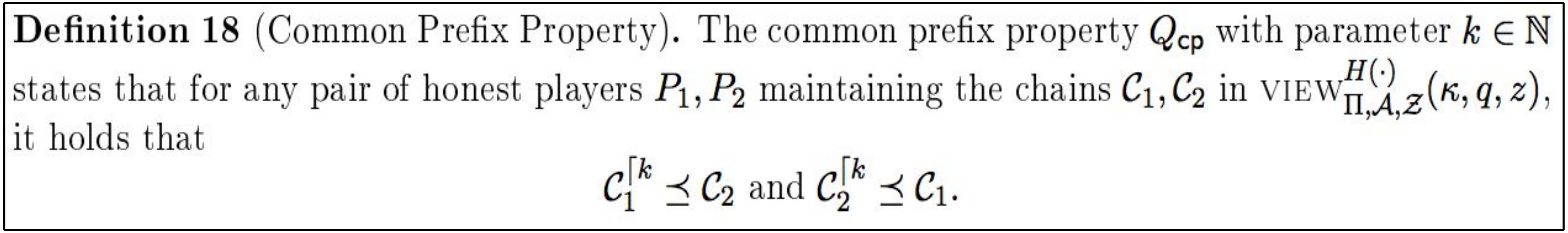
Lemma 7. *Suppose $\mathcal{C}_1$ is the chain that some honest party P_1 has adopted at round r and there exists chain $\mathcal{C}_2$ of length at least* $\mathrm{base}(r-1)+Y_{r-1}$ *that has been mined until round r and diverges from $\mathcal{C}_1$ at round $s \leq r$. Then, for $t = \sum_{i=s}^{r-1} Y_i$, the adversary must have mined and broadcast blocks $b'_1, \ldots, b'_t$ in chains $\mathcal{C}'_1, \ldots, \mathcal{C}'_t$ until round r where for $i \in \{1, \ldots, t\}$, $\mathcal{C}'_i$ has a suffix that contains only adversarial blocks, including b'_i, and some honest party has adopted this chain at some round in $[s, r-1]$.*

All uniquely successful rounds have to be compensated by the adversary!

COMMON PREFIX PROPERTY

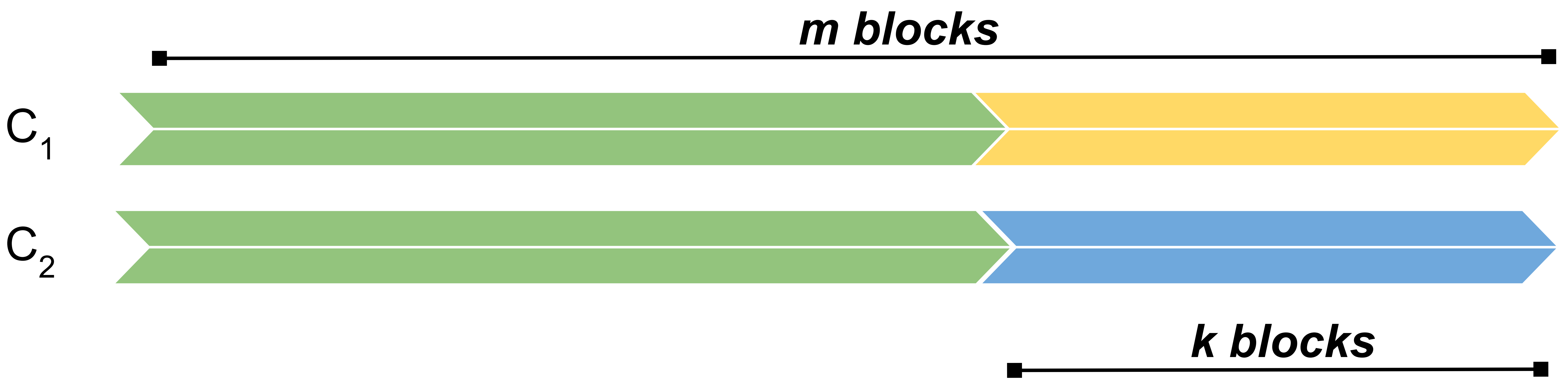


Consider a chain $\mathcal{C}$ of length m and any nonnegative integer k. We denote by $\mathcal{C}^{\lceil k}$ the chain resulting from the "pruning" the k rightmost blocks. Note that for $k \geq \text{len}(\mathcal{C})$, $\mathcal{C}^{\lceil k} = \varepsilon$. If $\mathcal{C}_1$ is a prefix of $\mathcal{C}_2$ we write $\mathcal{C}_1 \preceq \mathcal{C}_2$.



Definition 18 (Common Prefix Property). The common prefix property Q_{cp} with parameter $k \in \mathbb{N}$ states that for any pair of honest players P_1, P_2 maintaining the chains $\mathcal{C}_1, \mathcal{C}_2$ in $\textsc{view}^{H(\cdot)}_{\Pi,\mathcal{A},\mathcal{Z}}(\kappa, q, z)$, it holds that

$$\mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2 \text{ and } \mathcal{C}_2^{\lceil k} \preceq \mathcal{C}_1.$$

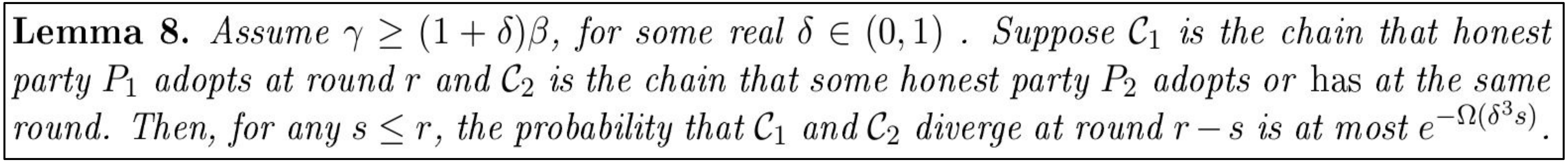


Not sufficient to prove persistence!

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

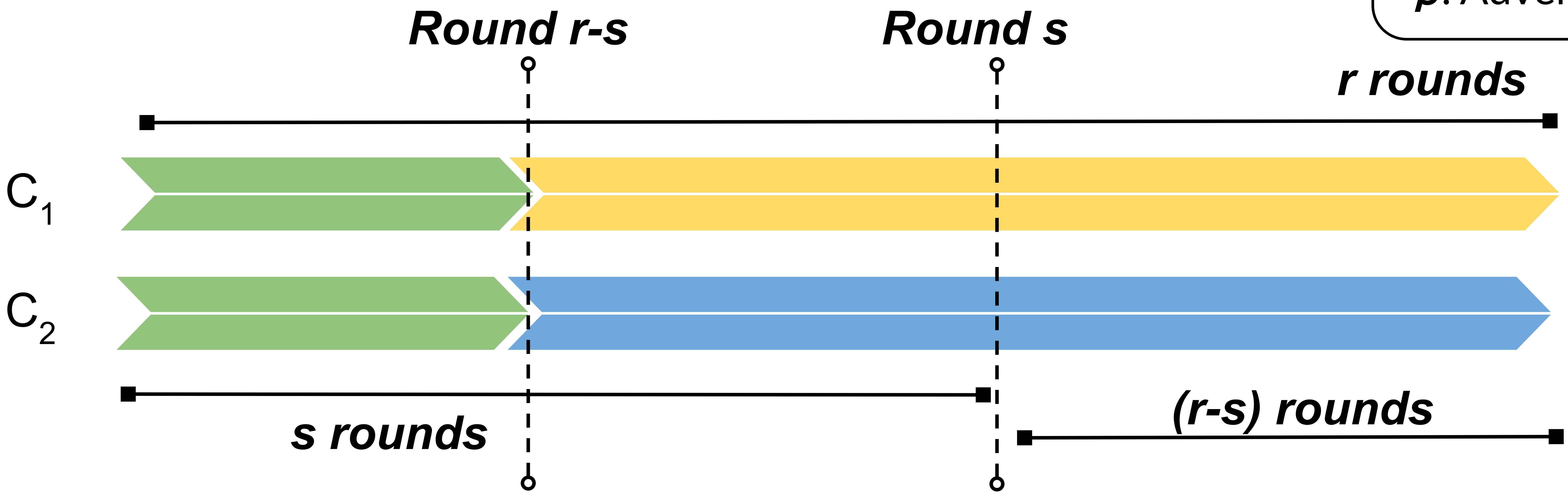
COMMON PREFIX PROPERTY



Lemma 8. *Assume* $\gamma \geq (1+\delta)\beta$*, for some real* $\delta \in (0,1)$. *Suppose* $\mathcal{C}_1$ *is the chain that honest party* P_1 *adopts at round* r *and* $\mathcal{C}_2$ *is the chain that some honest party* P_2 *adopts or* has *at the same round. Then, for any* $s \leq r$*, the probability that* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *diverge at round* $r-s$ *is at most* $e^{-\Omega(\delta^3 s)}$.

γ: Lower bound on round being successful

β: Adversary's hashing power



e

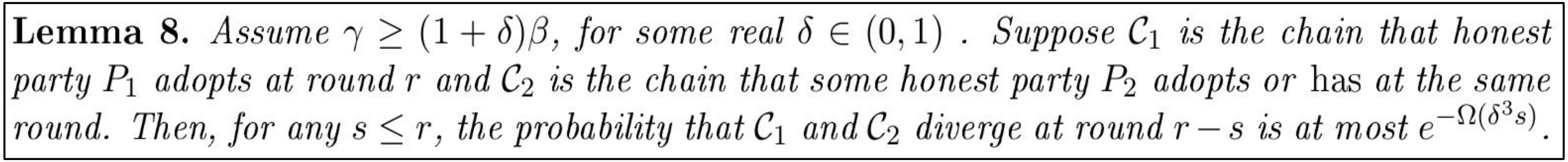
$e^{-\Omega}$

(δ^3.s)

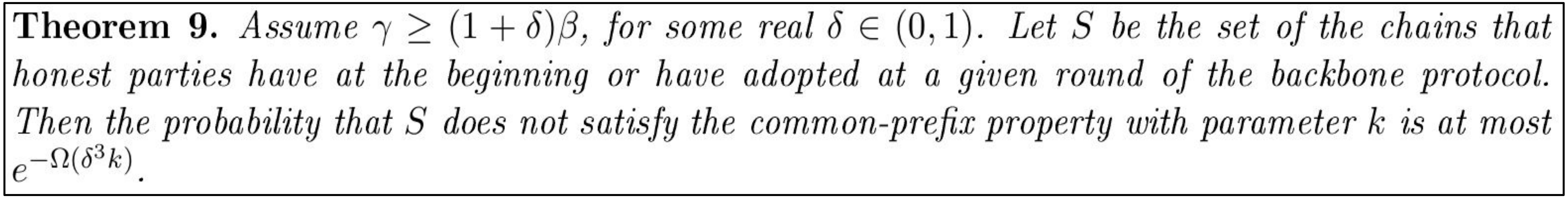
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

COMMON PREFIX PROPERTY



Lemma 8. *Assume* $\gamma \geq (1+\delta)\beta$*, for some real* $\delta \in (0,1)$. *Suppose* $\mathcal{C}_1$ *is the chain that honest party* P_1 *adopts at round* r *and* $\mathcal{C}_2$ *is the chain that some honest party* P_2 *adopts or* has *at the same round. Then, for any* $s \leq r$*, the probability that* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *diverge at round* $r-s$ *is at most* $e^{-\Omega(\delta^3 s)}$.

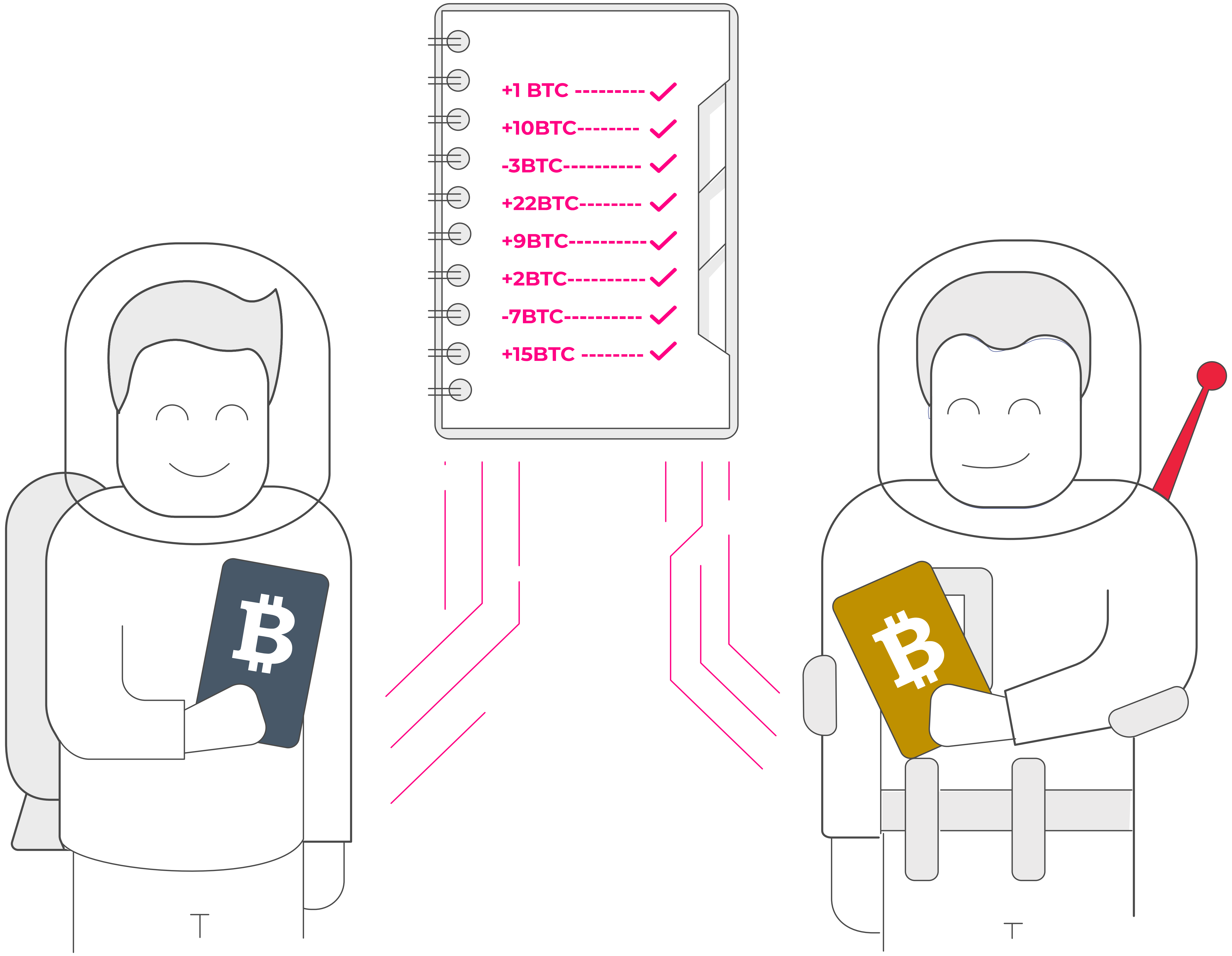


Theorem 9. *Assume* $\gamma \geq (1+\delta)\beta$*, for some real* $\delta \in (0,1)$*. Let* S *be the set of the chains that honest parties have at the beginning or have adopted at a given round of the backbone protocol. Then the probability that* S *does not satisfy the common-prefix property with parameter* k *is at most* $e^{-\Omega(\delta^3 k)}$.

INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

STRONG COMMON PREFIX PROPERTY

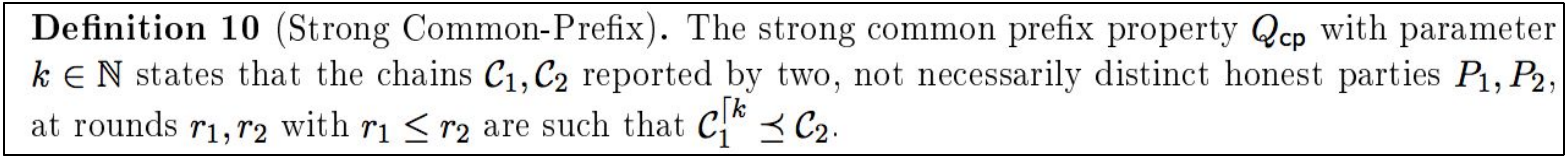
STRONG COMMON-PREFIX



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

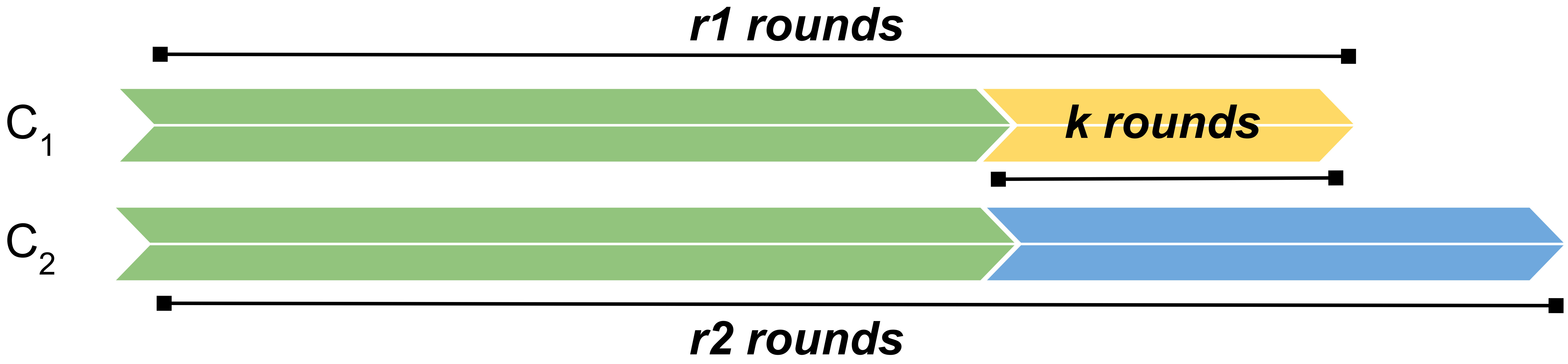
STRONG COMMON-PREFIX



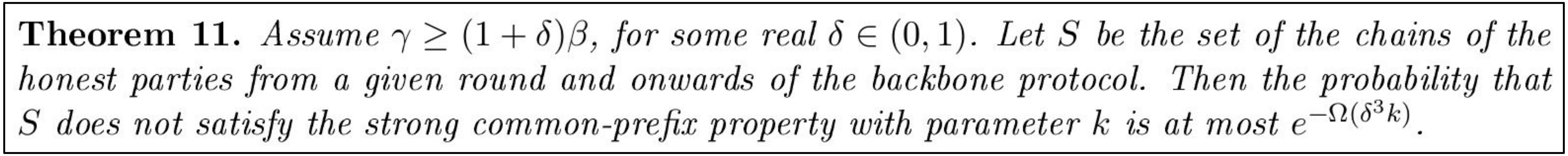
Definition 10 (Strong Common-Prefix). The strong common prefix property Q_{cp} with parameter $k \in \mathbb{N}$ states that the chains $\mathcal{C}_1, \mathcal{C}_2$ reported by two, not necessarily distinct honest parties P_1, P_2, at rounds r_1, r_2 with $r_1 \leq r_2$ are such that $\mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2$.

Sufficient to prove Persistence in a black-box fashion

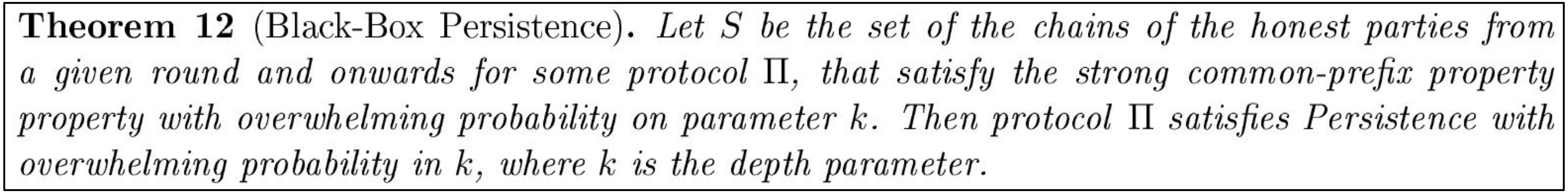
Stronger Property catering to larger possibilities



STRONG COMMON-PREFIX

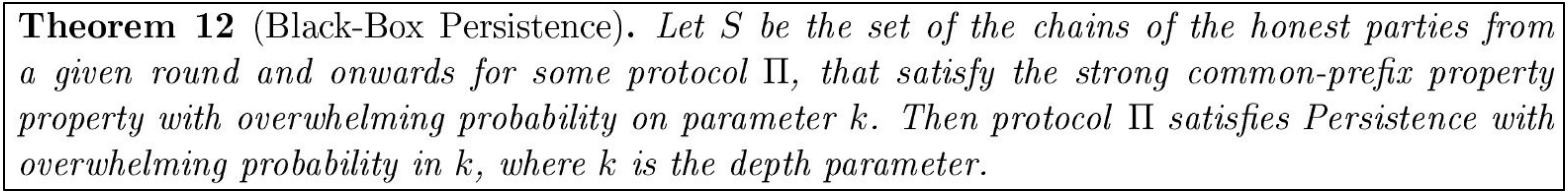


Theorem 11. *Assume $\gamma \geq (1+\delta)\beta$, for some real $\delta \in (0,1)$. Let S be the set of the chains of the honest parties from a given round and onwards of the backbone protocol. Then the probability that S does not satisfy the strong common-prefix property with parameter k is at most $e^{-\Omega(\delta^3 k)}$.*

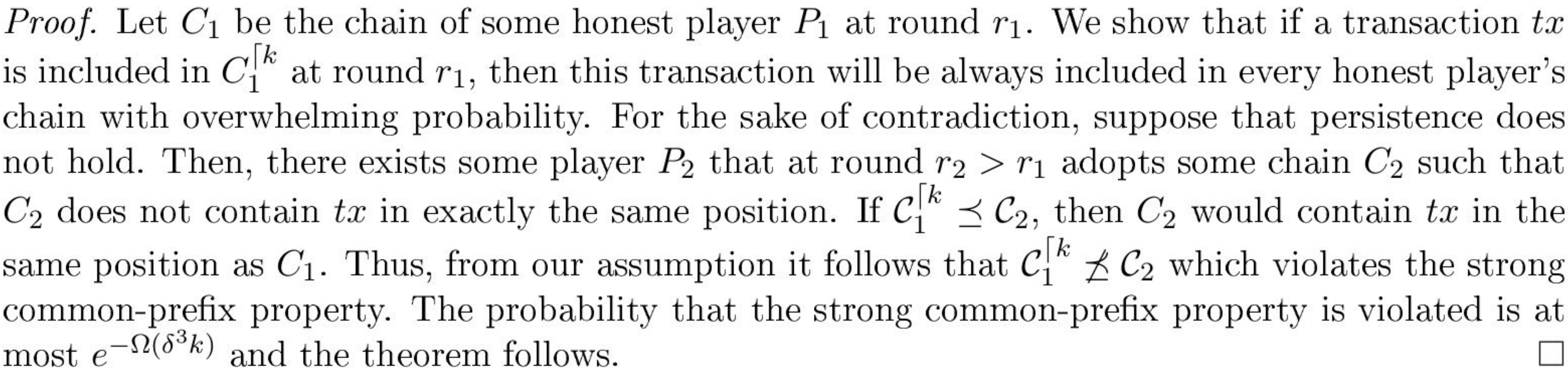


Theorem 12 (Black-Box Persistence)**.** *Let S be the set of the chains of the honest parties from a given round and onwards for some protocol Π, that satisfy the strong common-prefix property property with overwhelming probability on parameter k. Then protocol Π satisfies Persistence with overwhelming probability in k, where k is the depth parameter.*

STRONG COMMON-PREFIX



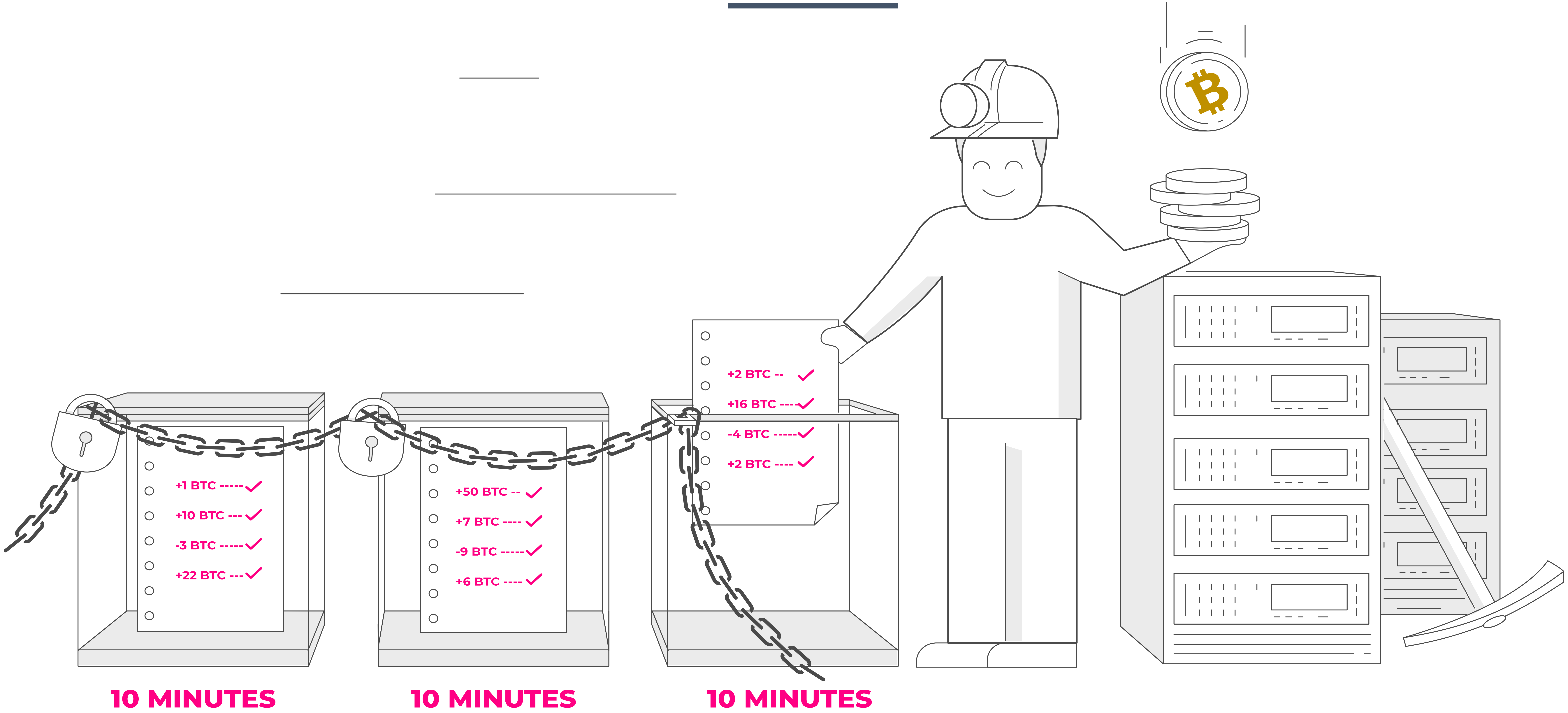
Theorem 12 (Black-Box Persistence). *Let S be the set of the chains of the honest parties from a given round and onwards for some protocol Π, that satisfy the strong common-prefix property property with overwhelming probability on parameter k. Then protocol Π satisfies Persistence with overwhelming probability in k, where k is the depth parameter.*



Proof. Let C_1 be the chain of some honest player P_1 at round r_1. We show that if a transaction tx is included in $C_1^{\lceil k}$ at round r_1, then this transaction will be always included in every honest player's chain with overwhelming probability. For the sake of contradiction, suppose that persistence does not hold. Then, there exists some player P_2 that at round $r_2 > r_1$ adopts some chain C_2 such that C_2 does not contain tx in exactly the same position. If $\mathcal{C}_1^{\lceil k} \preceq \mathcal{C}_2$, then C_2 would contain tx in the same position as C_1. Thus, from our assumption it follows that $\mathcal{C}_1^{\lceil k} \npreceq \mathcal{C}_2$ which violates the strong common-prefix property. The probability that the strong common-prefix property is violated is at most $e^{-\Omega(\delta^3 k)}$ and the theorem follows. □

CHAIN GROWTH

CHAIN GROWTH



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

CHAIN GROWTH

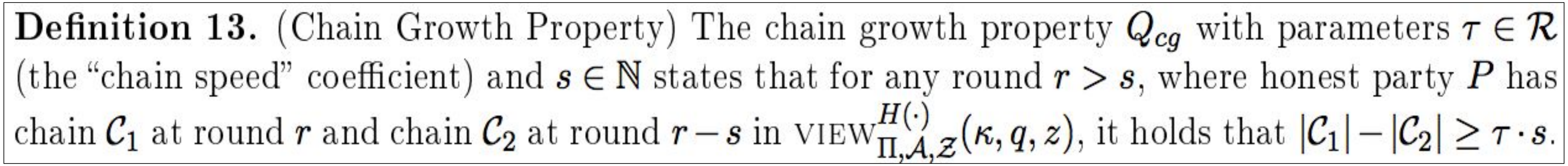
- **This property aims at expressing the minimum rate at which the chains of honest parties grow.**

Motivation: *It is motivated by an attacker that has objective to slow down the overall transaction processing time of the blockchain system.*

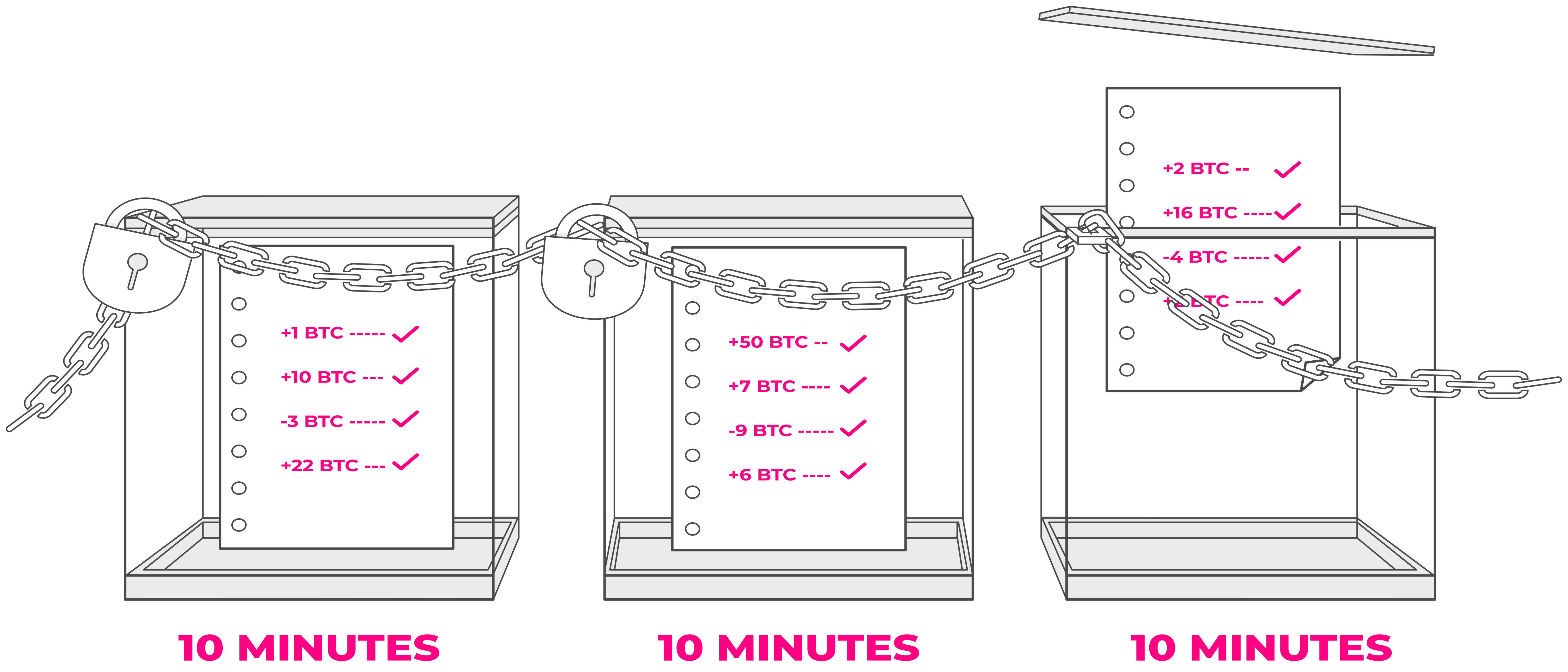
The common prefix and chain quality properties do not explicitly address this issue, and this can be seen from the fact that both properties can hold even if honest parties' chains do not grow at all.

CHAIN GROWTH

τ : Speed Coefficient



Definition 13. (Chain Growth Property) The chain growth property Q_{cg} with parameters $\tau \in \mathcal{R}$ (the "chain speed" coefficient) and $s \in \mathbb{N}$ states that for any round $r > s$, where honest party P has chain $\mathcal{C}_1$ at round r and chain $\mathcal{C}_2$ at round $r - s$ in $\text{VIEW}^{H(\cdot)}_{\Pi,\mathcal{A},\mathcal{Z}}(\kappa, q, z)$, it holds that $|\mathcal{C}_1| - |\mathcal{C}_2| \geq \tau \cdot s$.

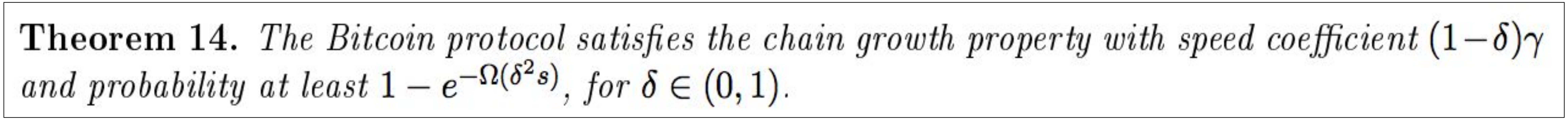


INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

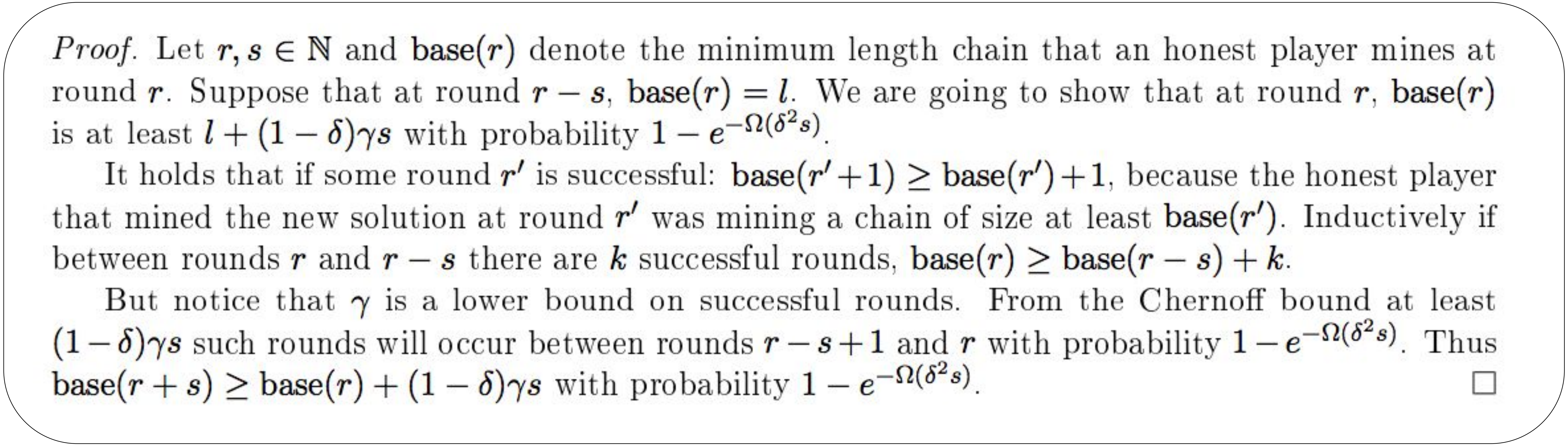
HYDERABAD

CHAIN GROWTH

THE BITCOIN PROTOCOL SATISFIES THE CHAIN GROWTH PROPERTY!



Theorem 14. *The Bitcoin protocol satisfies the chain growth property with speed coefficient* $(1-\delta)\gamma$ *and probability at least* $1 - e^{-\Omega(\delta^2 s)}$, *for* $\delta \in (0, 1)$.

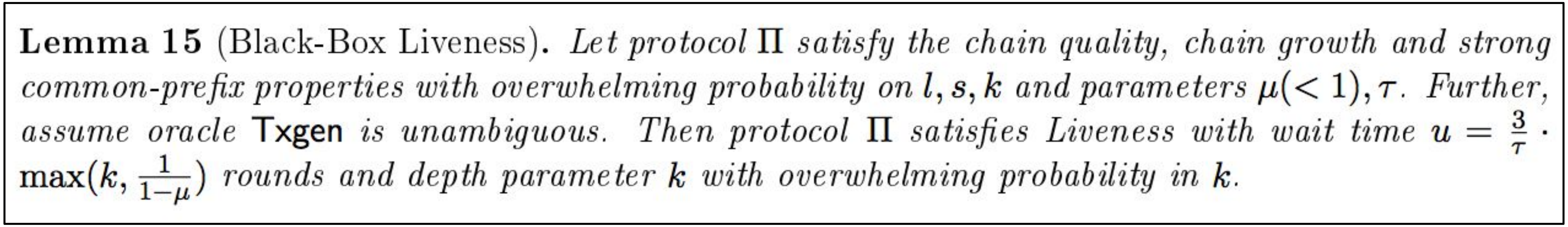


Proof. Let $r, s \in \mathbb{N}$ and $\mathsf{base}(r)$ denote the minimum length chain that an honest player mines at round r. Suppose that at round $r - s$, $\mathsf{base}(r) = l$. We are going to show that at round r, $\mathsf{base}(r)$ is at least $l + (1 - \delta)\gamma s$ with probability $1 - e^{-\Omega(\delta^2 s)}$.

It holds that if some round r' is successful: $\mathsf{base}(r'+1) \geq \mathsf{base}(r')+1$, because the honest player that mined the new solution at round r' was mining a chain of size at least $\mathsf{base}(r')$. Inductively if between rounds r and $r - s$ there are k successful rounds, $\mathsf{base}(r) \geq \mathsf{base}(r - s) + k$.

But notice that γ is a lower bound on successful rounds. From the Chernoff bound at least $(1-\delta)\gamma s$ such rounds will occur between rounds $r - s + 1$ and r with probability $1 - e^{-\Omega(\delta^2 s)}$. Thus $\mathsf{base}(r + s) \geq \mathsf{base}(r) + (1 - \delta)\gamma s$ with probability $1 - e^{-\Omega(\delta^2 s)}$. □

OBSERVATIONS



Lemma 15 (Black-Box Liveness). *Let protocol Π satisfy the chain quality, chain growth and strong common-prefix properties with overwhelming probability on l, s, k and parameters $\mu(< 1), \tau$. Further, assume oracle* Txgen *is unambiguous. Then protocol Π satisfies Liveness with wait time $u = \frac{3}{\tau} \cdot \max(k, \frac{1}{1-\mu})$ rounds and depth parameter k with overwhelming probability in k.*

By *liveness* we are guaranteed that *new transactions will be confirmed by at least one honest party after a predetermined amount of rounds*, where confirm here means that some party has some transaction at least k blocks deep in its chain!

SPEED SECURITY Tradeoffs

Attack on Common Prefix

INTERNATIONAL INSTITUTE OF
INFORMATION TECHNOLOGY
HYDERABAD

ATTACK on COMMON PREFIX

- *51% attacker* can break the common prefix with an arbitrarily long fork. (When *f* is large, even below 50% is possible)

- ***Adversary*: Rushing** - In any given round he gets to see all honest players' messages before deciding his own strategy. After seeing the messages he is not allowed to query the hashing oracle again in this round. Adversary has complete control of the order that messages arrive to each player.
- ***Attack:*** When a fork of depth 1 happens, adversary splits it's hashing power along with honest parties' power on the two branches.

ATTACK on COMMON PREFIX

Step 1: Honest party publishes a new solution in branch 1
Step 2: Adversary publishes solution in branch 2
(or)
Step 1: Honest parties extend both branches by same length
Step 2: Adversary reschedules messages of honest players

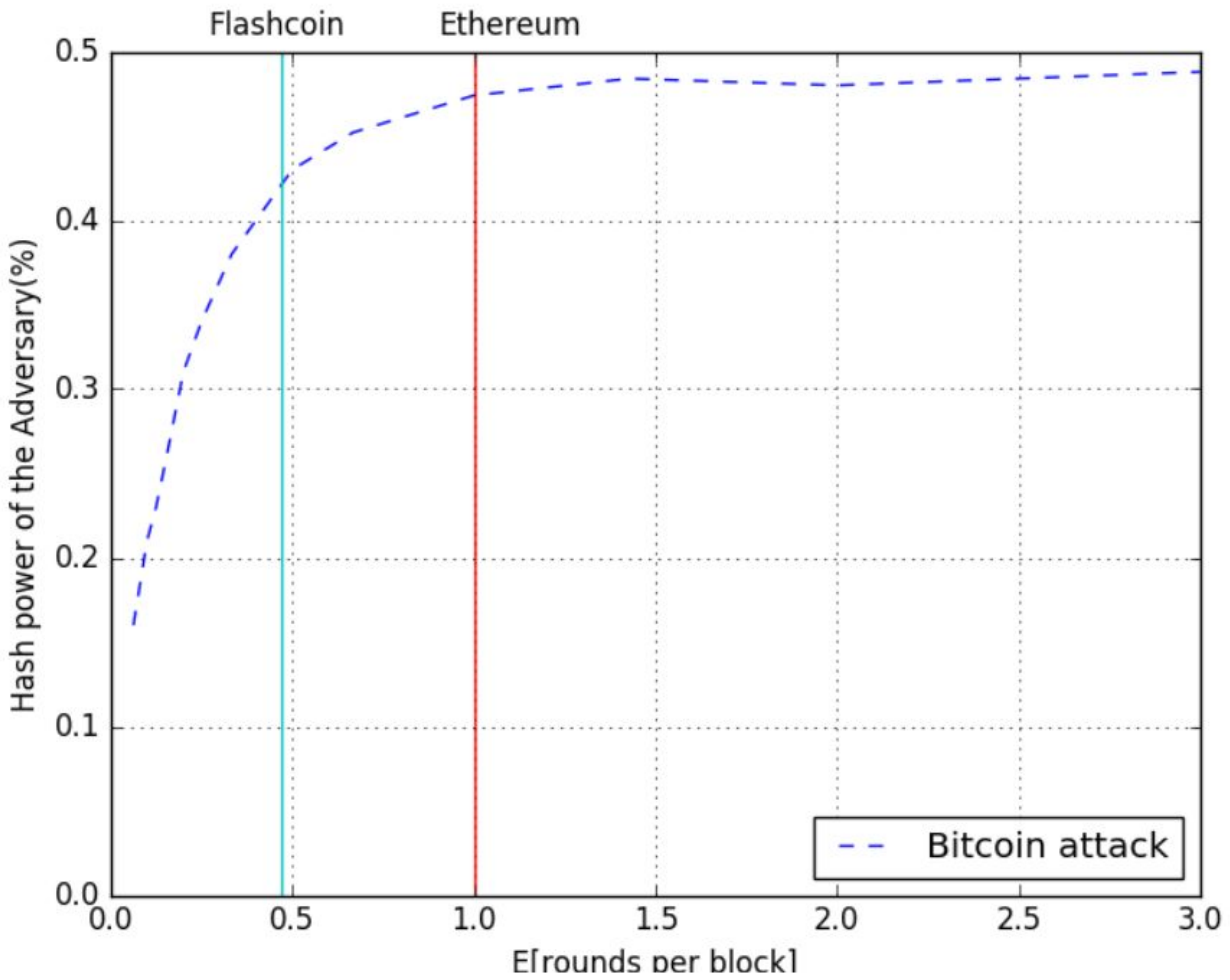
Protocol is robust against attack when ***f*** < 1
When ***f* >> 1,** security deteriorates :'(

Optimal Provable Security Bound: Bitcoin (49%)
Security Analysis doesn't hold: Flashcoin

Adversary lengthens the shorter chain to keep the fork running.

***f*:** Block generation rate per round

ATTACK on COMMON PREFIX



1/f

***Figure**: The level of insecurity in terms of the hashing power of the adversary as a function of 1/f*

Above the curve, the attack breaks common prefix with a fork that is 100 blocks deep with probability of success at least 1%.

Ethereum (f ≈ 1)
Provable security bound = 35%
Dogecoin and Litecoin
Provable security bound = 47%
Bitcoin
*Provable security bound = 49% **(Optimal)***

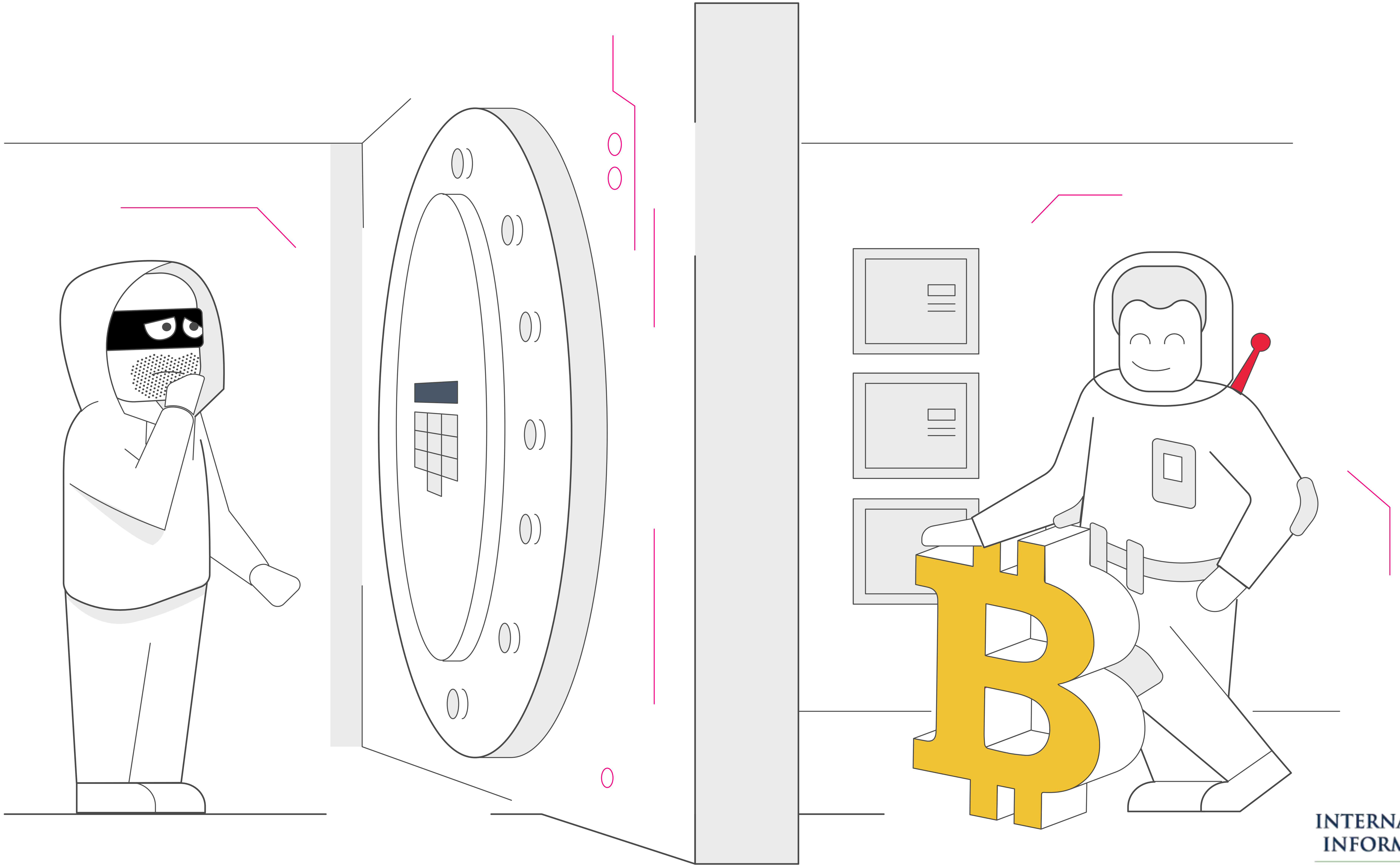
INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

CONCLUSION

CONCLUSION

- **Improve Security Bounds** of the Bitcoin backbone protocol.
- **Introduced the Property**
  Chain Growth > Fundamental to a Robust Txn Ledger
- **Measure of Speed**
  Chain Speed Coefficient
- Identified **Strong Common Prefix Property**
  That - along with the chain quality and chain growth properties, is sufficient for proving that a protocol implements a robust public transaction ledger in a black-box manner.

CONCLUSION



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

REFERENCES

1. https://steemit.com/bitcoin/@ronald20/the-good-the-bad-and-the-ugly-of-bitcoin-security
2. https://www.upfolio.com/ultimate-bitcoin-guide
3. The Bitcoin Backbone Protocol: Analysis and Applications

THANK YOU!

Team 27

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD