On Double Spend Races buble Spend Race

Double Spend Races

BY CYRIL GRUNSPAN

Leonard de Vinci Research Center

Finance Lab TYRIL GRUNSPAN
Princi Research Center
Finance Lab
d'Ingénieurs Léonard-BY CYRIL GRUNSPAN
Leonard de Vinci Research Center
Finance Lab
École Supérieure d'Ingénieurs Léonard-de-Vinci

Email: cyril.grunspan@devinci.fr *Web:* cyrilgrunspan.fr rıl.grunspan@devinc
): cyrilgrunspan.fr
February 1, 2018

Mathematical Fondation of
Bitcoin
Article Double Speed Baces in collaboration with **Bitcoin** Mathematical Fondation of

Bitcoin

Article Double Spend Races, in collaboration with

Ricardo Perez-Marco

Mathematical Hitcoin
Bitcoin
Article Double Spend Races
Ricardo Perez-Marco
arXiv:1702.02867 [cs.CR] arXiv:1702.02867 [cs.CR] Article Double Spend Races, in collaboration wi
Ricardo Perez-Marco
arXiv:1702.02867 [cs.CR]
Satoshi Risk Tables, arXiv:1702.04421 [cs.CR]

Ricardo Perez-Marco
arXiv:1702.02867 [cs.CR]
Satoshi Risk Tables, arXiv:1702.04421 [cs.CR]
Section 11. Calculations of Bitcoin: A Peer-to-Peer
Electronic Cash System, Satoshi Nakamoto, 2008. Satoshi Risk Tables, arXiv:1702.04421 [cs.CR]
 Section 11. Calculations of Bitcoin: A Peer-to-Peer

Electronic Cash System, Satoshi Nakamoto, 2008.

Following a previous work by Meni Rosenfeld Satoshi Risk Tables, arXiv:1702.04421 [cs.CR]
Section 11. Calculations of Bitcoin: A Peer-to-Peer
Electronic Cash System, Satoshi Nakamoto, 2008.
Following a previous work by Meni Rosenfeld
Analysis of hashrate-based doubl Section 11. Calculations of Bitcoin: A Peer-to-Peer
Electronic Cash System, Satoshi Nakamoto, 2008.
Following a previous work by Meni Rosenfeld
Analysis of hashrate-based double-spending, 2012

- Correction of Satoshi Transferred alysis of hashrate-based double-spending, 2012

 Correction of Satoshi's calculus for the probability of success of a double spend attack ing a previous work by Meni Rosenfeld
is of hashrate-based double-spending, 2012
Correction of Satoshi's calculus for the
probability of success of a double spend attack
Proof that "the probability drops exponentially
- alysis of hashrate-based double-spending, 2012

 Correction of Satoshi's calculus for the

probability of success of a double spend attack

 Proof that "the probability drops exponentially

as the number of blocks the at Correction of Satoshi's calculus for the
probability of success of a double spend attack
Proof that "the probability drops exponentially
as the number of blocks the attacker has to
catch up with increases" (Satoshi) Correction of Satoshi's calculus for the probability of success of a double spend attack Proof that "the probability drops exponentially as the number of blocks the attacker has to catch up with increases" (Satoshi) Closed probability of success of a double spend attack

• Proof that "the probability drops exponentially

as the number of blocks the attacker has to

catch up with increases" (Satoshi)

• Closed form formula with Beta function
- probability % as the number of blocks the attacker has to
catch up with increases" (Satoshi)
• Closed form formula with Beta function for this
probability
• More accurate risk analysis knowing the time it
took to validate blocks. catch up with increases" (Sa
Closed form formula with Be
probability
More accurate risk analysis l
took to validate blocks.
Underestimation of the pro
- Closed form formula with Beta function for this
probability
• More accurate risk analysis knowing the time it
took to validate blocks.
• Underestimation of the probability of double-
spend attack probability
More accurate risk an
took to validate block
Underestimation of tl
spend attack
-

Two groundbreaking ideas in Bitcoin No groundbreaking ideas in

New framework for the design of a transaction

• Breakthrough in distributed system theory **Example 13 September 13 September 13 September 13 September 14 Se**

-
-

• New framework for the design of a transaction
• Breakthrough in distributed system theory
Concept of "smart-contract" (prophetized by Nick
Szabo) Szabo) • Breakthrough in distributed system theory
Concept of "smart-contract" (prophetized by Nick
Szabo)
ScriptSig / ScriptPubKey (not in the white paper) Concept of "smart-contract" (prophetized by Nick
Szabo)
ScriptSig / ScriptPubKey (not in the white paper)
Use of proof-of-work (rediscovered by Adam Back) to
create a decentralized blockchain

ScriptSig / ScriptPubKey (not in the white paper)
Use of proof-of-work (rediscovered by Adam Back) to
create a decentralized blockchain ScriptSig / ScriptPubKey (not in the white paper)
Use of proof-of-work (rediscovered by Adam Back) to
create a decentralized blockchain
No bibliography at all related with the distributed
system theory! Use of proof-of-wor
create a decentraliz
No bibliography at
system theory!

create a decentralized blockchain
No bibliography at all related with the distributed
system theory!
Main references in cryptography (Haber& Stornetta
for timestamps server) No bibliography at all relat
system theory!
Main references in cryptogra
for timestamps server) system theory!
Main references in cryptography (Haber& Stornetta
for timestamps server)
Variation of two generals problem. Fisher, Lynch et
Paterson, 1985

Main references in cryptography (Haber& Stornetta
for timestamps server)
Variation of two generals problem. Fisher, Lynch et
Paterson, 1985
Theorem. In a asynchronous model, there is no

for timestamps server)
Variation of two generals problem. Fisher, Lynch et
Paterson, 1985
Theorem. In a asynchronous model, there is no
deterministic algorithm to achieve consensus (if at Variation of two generals problem. Fisher, Lynch et
Paterson, 1985
Theorem. In a asynchronous model, there is no
deterministic algorithm to achieve consensus (if at
least one node can crash) Variation of two generals proble

Paterson, 1985
 Theorem. In a asynchronous

deterministic algorithm to acher

least one node can crash) Theorem. In a asynchronous model, there
deterministic algorithm to achieve consensus
least one node can crash)
However, there are randomized consensus.

(*least one node can crash*)
However, there are randomized consensus.
Randomization makes algorithm powerful...

Proof-of-Work Proof-of-Work
Time consuming

Proof-of-Work
Time consuming
Cost function. *A* string, *D* integer, *x* integer
 $\mathcal{F}: C \times [0, D] \rightarrow \{True \ \text{False}\}$ Time consuming
Cost function. A string, D integer, x integer

Time consuming
\nCost function. A string, D integer, x integer
\n
$$
\mathcal{F}: \quad \mathcal{C} \times [0, D_{\text{max}}] \times [0, N] \longrightarrow \{\text{True, False}\}
$$
\n
$$
(A, D, x) \longmapsto \mathcal{F}(A, D, x)
$$
\nProblem. Given A (string) and D (level of difficulty),
\nfind **x** such that
\n
$$
\mathcal{F}(A, D, x) = \text{True} \tag{1}
$$

 $(A, D, x) \longmapsto \mathcal{F}(A, D, x)$
 F(*A*, *D*) and *D* (level of difficulty),

at
 $\mathcal{F}(A, D, \mathbf{x}) = \text{True}$ (1)

t necessarily unique) is a "proof-of-work"

$$
\mathcal{F}(A, D, \mathbf{x}) = \text{True} \tag{1}
$$

Problem. Given A (string) and D (level of difficulty),
find **x** such that
 $\mathcal{F}(A, D, \mathbf{x}) = \text{True}$ (1)
Solution **x** (not necessarily unique) is a "proof-of-work"
called **nonce**. Problem possibly hard to solve. Use of Froblem. Given A (string) and D (lever of difficulty),
find **x** such that
 $\mathcal{F}(A, D, \mathbf{x}) = \text{True}$ (1)
Solution **x** (not necessarily unique) is a "proof-of-work"
called **nonce**. Problem possibly hard to solve. Use of
c $\mathcal{F}(A, D, \mathbf{x})$ = True
Solution **x** (not necessarily unique) is a "j
called **nonce**. Problem possibly hard to
computational power to solve it. Solution $\mathbf x$ (not necessarily unique) is a "proof-of-work"
called **nonce**. Problem possibly hard to solve. Use of
computational power to solve it.
Pricing via Processing or Combatting Junk Mail, C.
Dwork and M. Naor, (

Solution **x** (not necessarily unique called **nonce**. Problem possibly h
computational power to solve it.
Pricing via Processing or Comba
Dwork and M. Naor, (1993).
Denial-of-service counter measu called **nonce**. Problem possibly hard to solve. Use of
computational power to solve it.
Pricing via Processing or Combatting Junk Mail, C.
Dwork and M. Naor, (1993).
Denial-of-service counter measure technique in a
number computational power to s
Pricing via Processing or
Dwork and M. Naor, (19)
Denial-of-service counter
number of systems
Anti-spam tool Pricing via Processin
Dwork and M. Naor
Denial-of-service com
number of systems
Anti-spam tool Dwork and M. Naor, (1993).
Denial-of-service counter-measure technique in a
number of systems
Anti-spam tool
Hashcash, A Denial of Service Counter-Measure, A.
Back, preprint (2002)

Denial-of-service counter

number of systems

Anti-spam tool

Hashcash, A Denial of Serv

Back, preprint (2002)

Hashcash: a proof-of-work a number of systems
Anti-spam tool
Hashcash, A Denial of Service Counter-Measure,
Back, preprint (2002)
Hashcash: a proof-of-work algorithm
Create a stamp to attach to mail Hashcash, A Denial of Service Counter-Me
Back, preprint (2002)
Hashcash: a proof-of-work algorithm
Create a stamp to attach to mail
Cost functions proposed are different
Selution of (1) by hypto force Hashcash,A Denial of Service Counter-Me
Back, preprint (2002)
Hashcash: a proof-of-work algorithm
Create a stamp to attach to mail
Cost functions proposed are different
Solution of (1) by brute-force. Hashcash, A Denial of Service Co
Back, preprint (2002)
Hashcash: a proof-of-work algorith
Create a stamp to attach to m
Cost functions proposed are differe
Solution of (1) by brute-force.

Hash functions
Use of hash function *h* to create a
Example: $F(A \mid D \mid x) =$ True if *h*(**Hash functions**
Use of hash function *h* to create a puzzle
Example: $\mathcal{F}(A, D, x)$ = True if $h(A|x)$ starts wi **Hash functions**
Use of hash function *h* to create a puzzle
Example: $\mathcal{F}(A, D, x)$ = True if $h(A|x)$ starts with *D*
zeros and false else. **Hash functions**
Use of hash function *h* to
Example: $\mathcal{F}(A, D, x) =$ '
zeros and false else. Use of hash function h to create a puzzle
Example: $\mathcal{F}(A, D, x)$ = True if $h(A|x)$ star
zeros and false else.
Rabin, Yuval, Merkle, late 70.
"Swiss army knife" of cryptography
• input of any size

os and false else.

bin, Yuval, Merkle, late 70.

viss army knife" of cryptogra

• input of any size

• output of fixed-size bin, Yuval, Merkle, late 70.

viss army knife" of cryptograph

• input of any size

• output of fixed-size

• easy to calculate (in $O(r)$

-
-
- bin, Yuval, Merkle, late 70.

viss army knife" of cryptography

 input of fixed-size

 output of fixed-size

 easy to calculate (in $O(n)$ if input is *n*-bit string) string) mput of any size

output of fixed-size

easy to calculate (in $O($

string)

i. collision resistance

i. preimage resistance output of fixed-size

easy to calculate (in $O(n \text{ string})$

i. collision resistance

ii. preimage resistance

ii. second preimage resistance • easy to calculate (in $O(n)$ if in
string)
i. collision resistance
ii. preimage resistance
iii. second preimage resistance
e way function
	-
	-
-

i. collision resistance
ii. preimage resistance
iii. second preimage res
One way function
Random Oracles are Pr 1. collision resistance

ii. preimage resistance

iii. second preimage resistance

One way function

Random Oracles are Practical: A Paradigm for

Designing Efficient Protocols, M. Bellare, P. Rogaway, ii. preimage resistance

iii. second preimage resistance

One way function

Random Oracles are Practical: A Paradigm for

Designing Efficient Protocols, M. Bellare, P. Rogaway,

ACM Conference on Computer and Communication iii. second preimage resistance

One way function

Random Oracles are Practical: A Paradigm for

Designing Efficient Protocols, M. Bellare, P. Rogaway,

ACM Conference on Computer and Communications

Security (1993). m. second premix
One way function
Random Oracles a
Designing Efficient P
ACM Conference on
Security (1993).
Based on block ciphe One way function
Random Oracles are Pract
Designing Efficient Protocols,
ACM Conference on Comput
Security (1993).
Based on block ciphers
Compression function Random Oracles are Practic
Designing Efficient Protocols, M
ACM Conference on Computer
Security (1993).
Based on block ciphers
Compression function
Merkle–Damgård construction Designing Efficient Protocols, M. Bellare
ACM Conference on Computer and Co
Security (1993).
Based on block ciphers
Compression function
Merkle–Damgård construction
Message digest ACM Conference on Con
Security (1993).
Based on block ciphers
Compression function
Merkle–Damgård constru
Message digest
Commitments **Commitments Puzzle** Compression tunction
Merkle–Damgård constr
**Message digest
Commitments
Puzzle**
Digital signature
SHA-1, MD5 broken Merkle–Damgård constructior
**Message digest
Commitments
Puzzle**
Digital signature
SHA-1, MD5 broken
SHA-2

SHA-2

Test of SHA256
Images are uniform & Easy to comput

Test of $SHA256$
Images are uniform $\&$ Easy to compute

Proposition. *If h is a hash function, then the time*
Proposition. *If h is a hash function, then the time*
of resolution before getting a "proof-of-work" for a **Test of SHA256**
Images are uniform & Easy to compute
Proposition. *If h is a hash function, then the time*
of resolution before getting a "proof-of-work" for a
problem of difficulty D has an exponential distributio **Proposition.** If h is a hash function, then the time
of resolution before getting a "proof-of-work" for a
problem of difficulty D has an exponential distribution. **Proposition.** If h is a hash function, then the time of resolution before getting a "proof-of-work" for a problem of difficulty D has an exponential distribution.
Example. Problem: find x such that $SHA256(a|x)$ starts wit

Proposition. If h is a hash function, then the time
of resolution before getting a "proof-of-work" for a
problem of difficulty D has an exponential distribution.
Example. Problem: find x such that $SHA256(a|x)$
starts wit problem of difficulty D has an exponential distribution.
 Example. Problem: find x such that $SHA256(a|x)$

starts with 4 zeros with a an arbitrary string. Sample
 (τ_i) . Mean \approx 4 sec.

Histogram of pow time

 $\frac{1}{10}$ is $\frac{1}{10}$ is $\frac{1}{20}$ $\frac{2}{25}$
 $\frac{1}{10}$ Time before discovery

However, it is not clear that the distribution

is exponential. Tests Cramer-von-Mises and

Kolmogorov-Smirnov fail if size(sample)>6000 software...

Interblock times
Hash function $h = \text{SHA256} \circ \text{SHA256}$ **Interblock times**
Hash function $h = \text{SHA256} \circ \text{SHA256}$
 $\mathcal{F}(A, D, \mathbf{x}) = 1$ **Interblock times**
Hash function $h = \text{SHA256} \circ \text{SHA256}$

$$
\mathcal{F}(A, D, \mathbf{x}) = 1_{h(A|D|x) < \frac{2^{224}}{D}}
$$
\n
$$
A = x_1 |x_2 | x_3 | x_4|
$$
\n
$$
x_1 = \text{Version}
$$
\n
$$
x_2 = \text{Hash Previous Block}
$$
\n
$$
x_3 = \text{Hash Merkle Root}
$$
\n
$$
x_4 = \text{Timestamp}
$$

 x_2 = Hash Previous Block
 x_3 = Hash Merkle Root
 x_4 = Timestamp

Block Header = $A|D|x$. Difficulty adjusted such that

the time of resolution is ≈ 600 sec. $x_2 =$ Hash Previous Block
 $x_3 =$ Hash Merkle Root
 $x_4 =$ Timestamp

Block Header $=A|D|x$. Difficulty adjusted such that

the time of resolution is \approx 600 sec.
 Example. Hash Genesis block & Block 500000
 $\frac{00000000$

000000000019d6689c085ae165831e934763ae46a2a6c172b3f1b60a8ce26f 00000000000000000024fb37364cbf81fd49cc2d51c09c75c35433c3a1945d04

 Block Header $-A|D|x$. Bincury adjusted such the time of resolution is $\approx 600 \text{ sec}$.
 Example. Hash Genesis block & Block 500000
 $\frac{000000000001946689c085a e165831e934\text{ff}763a e46a2a6c172b3\text{ftb}60a8ce26}{000000000000000$ Open-source software platform for Blockchain analysis Example. Hash Genesis block & Diock 000000

000000000000000000000000024fb37364ebf81fd49ec2d51e09e75e35433e3a1945d04

Blocksci (Princeton) github.com/citp/BlockSci

Open-source software platform for Blockchain analysis
 Ex

Mathematics of mining

**Mathematics of mining
The time it takes to mine a block is memoryless
** $\mathbb{P}[T > t_1 + t_2 | T > t_2] = \mathbb{P}[T > t_1]$ **Mathematics of mining**
The time it takes to mine a block is memoryless
 $\mathbb{P}[T > t_1 + t_2 | T > t_2] = \mathbb{P}[T > t_1]$
Proposition. *The random variable T has the*

$$
\mathbb{P}[T > t_1 + t_2 | T > t_2] = \mathbb{P}[T > t_1]
$$

**The time it takes to mine a block is memoryless
** $\mathbb{P}[T > t_1 + t_2 | T > t_2] = \mathbb{P}[T > t_1]$ **

Proposition.** The random variable **T** has the

exponential distribution with parameter $\alpha = \frac{1}{600}$ *i.e.*, **Figure 11 The time it takes to mine a block is memoryless
** $\mathbb{P}[T > t_1 + t_2 | T > t_2] = \mathbb{P}[T > t_1]$ **

Proposition.** The random variable **T** has the

exponential distribution with parameter $\alpha = \frac{1}{600}$ i.e.,
 $f_{\mathbf{m}}(t)$ $\frac{1}{600}$ $i.e.,$ **Proposition.** The random variable **T** has the
exponential distribution with parameter $\alpha = \frac{1}{600} i.e.,$
 $f_{\textbf{T}}(t) = \alpha e^{-\alpha t}$
Parameter α seen as a mining speed, $\mathbb{E}[\textbf{T}] = \frac{1}{\alpha}$.

$$
f_{\bm T}(t) \,\,=\,\, \alpha\, \mathrm{e}^{-\alpha t}
$$

1 $\frac{1}{\alpha}$.

Definition. Let $N(t) = \alpha e^{-\alpha t}$
 Definition. Let $N(t)$ be the number of blocks already

mined at t-time. Start is at $t = 0$. $f_{\mathbf{T}}(t) = \alpha e^{-\alpha t}$
 Parameter α **seen as a mining speed,** $\mathbb{E}[\mathbf{T}] = \frac{1}{\alpha}$.
 Definition. *Let* $N(t)$ *be the number of blocks already*
 mined at t-time. Start is at $t = 0$.
 Proposition. *The random proc* **Definition.** Let $N(t)$ be the number of blocks already
mined at t-time. Start is at $t = 0$.
Proposition. The random process N is a Poisson
process with parameter α i.e.,

Proposition. The random process N is a Poisson

$$
\mathbb{P}[\mathbf{N}(t) = k] = \frac{(\alpha t)^k}{k!} e^{-\alpha t}
$$

Proposition. *The random process IN is a Poisson*
 $\text{process with parameter } \alpha$ *i.e.*,
 $\mathbb{P}[\mathbf{N}(t) = k] = \frac{(\alpha t)^k}{k!} e^{-\alpha t}$
 Notation. *Two group of miners. The letters* $\mathbf{T}, \alpha, \mathbf{S}_n$,
 N (*resp.* $\mathbf{T}', \alpha', \mathbf{S}'_n, \mathbf{N}$) $P[\mathbf{N}(t) = k]$
 $Two\ group\ of\ \prime,\alpha',\mathbf{S}'_n,\mathbf{N})$ a
 (ker) . \mathbf{S}'_n , **N**) are $\begin{array}{l} \left[\begin{array}{l} \epsilon_{k}(t) = k \end{array} \right] \left[\begin{array}{l} \epsilon_{k}(t) = k \end{array} \right] = \frac{(\alpha \, t)^k}{k!} \mathrm{e}^{-\alpha t} \ \text{for } \beta \in \mathbb{R}^{n}, \ \mathbf{N} \left[\begin{array}{l} \epsilon_{k}(t) = k \end{array} \right] = \mathrm{c}^{n} \left[\begin{array}{l} \epsilon_{k}(t) = k \end{array} \right] \left[\begin{array}{l} \epsilon_{k}(t) = k \end{array} \right] \left[\begin{array}{l} \epsilon_{k}(t) =$ $\begin{aligned} \mathbb{P}[\mathbf{N}(t) = \mathbf{Notation.} \; & \; Two \; group \ \boldsymbol{N} \; (resp. \; \boldsymbol{T}', \alpha', \mathbf{S}'_n, \mathbf{N} \; (resp. \; attacker). \end{aligned}$ *n*₈. The letters $\mathbf{T}, \alpha, \mathbf{S}_n$,
rved for honest miners
^{*r*}] *and* $q = 1 - p$. *Then,*

Proposition. Let $p := \mathbb{P}[\mathbf{T} < \mathbf{T'}]$ and $q = 1 - p$. Then,

$$
\alpha = \frac{p}{\tau_0}
$$

$$
\alpha' = \frac{q}{\tau_0}
$$

with $\tau_0 = 600 \text{ sec.}$

Classical Double Spend Attack Classical Double Spend Attack
No eclips attack (kind of Sybill's attack) **Classical Double Spend Att:**
No eclips attack (kind of Sybill's attack)
What is a double spend?
A single output may not be used as an

Classical Double Spend Attack
No eclips attack (kind of Sybill's attack)
What is a double spend?
A single output may not be used as an input to
multiple transactions. No eclips attack (kind of Sybill's attack)
 What is a double spend?

A single output may not be used as an input to

multiple transactions.

• $T=0$. A merchant **M** receives a transaction tx

- **hat is a double spend?**

single output may not be used as an input to

tiple transactions.

 $T=0$. A merchant **M** receives a transaction \mathbf{tx}

from \mathbf{A} (= attacker). Transaction \mathbf{tx} is issued **t** is a double spend?
le output may not be used as an input to
le transactions.
 $T=0$. A merchant M receives a transaction \mathbf{tx}
from \mathbf{A} (= attacker). Transaction \mathbf{tx} is issued
from an UTXO $\mathbf{tx0}$ From the used

is transactions.
 $T=0$. A merchant **M** receives

from **A** (= attacker). Transac

from an UTXO $\mathbf{tx0}$

Honest Miners start ltiple transactions.

• $T=0$. A merchant **M** receives a transaction **tx**

from **A** (= attacker). Transaction **tx** is issued

from an UTXO **tx0**

• Honest Miners start mining openly,
 transparently
- transparently from \mathbf{A} (= attacker). Transaction \mathbf{tx} is iss
from an UTXO $\mathbf{tx0}$
• Honest Miners start mining ope
transparently
• Attacker \mathbf{A} starts mining secretly
• One block of honest miners include \mathbf{tx} • Honest Miners start mining openly,
 transparently

• Attacker **A** starts mining secretly

• One block of honest miners include **tx**

• No block of attacker include **tx** • Honest Miners start mining openly,
 transparently

• Attacker **A** starts mining secretly

• One block of honest miners include \mathbf{tx}

• On the contrary, one blocks of the attacker
-
-
-
- Attacker **A** starts mining secretly

 One block of honest miners include \mathbf{tx}

 No block of attacker include \mathbf{tx}

 On the contrary, one blocks of the attacker

includes another transaction \mathbf{tx}' conflicti Attacker **A** starts mining secretly
One block of honest miners include \mathbf{tx}
No block of attacker include \mathbf{tx}
On the contrary, one blocks of the attacker
includes another transaction \mathbf{tx}' conflicting
with $\mathbf{$ One block of honest miners include tx
No block of attacker include tx
On the contrary, one blocks of the at
includes another transaction tx' conf
with tx from same UTXO $tx0$
As soon as the z-th block has been min • No block of attacker include \mathbf{tx}

• On the contrary, one blocks of the attacker

includes another transaction \mathbf{tx}' conflicting

with \mathbf{tx} from same UTXO $\mathbf{tx0}$

• As soon as the *z*-th block has been min On the contrary, one blocks of t
includes another transaction \mathbf{tx}'
with \mathbf{tx} from same UTXO $\mathbf{tx0}$
As soon as the z-th block has bee:
sends his good to $\mathbf A$
 $\mathbf A$ keeps on mining secretly includes another transaction tx'
with tx from same UTXO $tx0$
• As soon as the *z*-th block has been
sends his good to **A**
• A keeps on mining secretly
• As soon as A has mined a blockch
-
-
- As soon as the z-th block has been mined, M

As soon as the z-th block has been mined, M

A keeps on mining secretly

As soon as A has mined a blockchain with a

lenght greater than the official one, A broadcast As soon as the *z*-th block has been mined, M
sends his good to \bf{A}
 \bf{A} keeps on mining secretly
As soon as \bf{A} has mined a blockchain with a
lenght greater than the official one, \bf{A} broadcast
his blockch sends his good to A
A keeps on mining secretly
As soon as A has mined a blockchain with a
lenght greater than the official one, A broadcast
his blockchain to the network • A keeps on mining secretly

• As soon as A has mined a blockchain with a lenght greater than the official one, A broadcast

his blockchain to the network

• Transaction \mathbf{tx} has disappeared from the official blockch
- Transaction \mathbf{tx} has disappeared from the official blockchain.
Free Lunch! lenght greate
his blockchai
• Transaction
official block
Free Lunch!

Nakamoto's Analysis

**Nakamoto's Analysis
Some definitions**
Definition. Let $n \in \mathbb{Z}$. We denote by q_n the probability
of the attacker **A** to catch up honest miners whereas **Nakamoto's Analysis

Some definitions**

Definition. Let $n \in \mathbb{Z}$. We denote by q_n the probability

of the attacker **A** to catch up honest miners whereas **Nakamoto's Analysis

Some definitions**
 Definition. Let $n \in \mathbb{Z}$. We denote by q_n the probability

of the attacker **A** to catch up honest miners whereas
 A's blockchain is n blocks behind. **Some definitions**
Definition. Let $n \in \mathbb{Z}$. We denote by q_n
of the attacker **A** to catch up honest r
A's blockchain is n blocks behind.
Then $q_n = \left(\frac{q}{n}\right)^n$ if $n \geq 0$ and $q_n = 1$ also $n \in \mathbb{Z}$. We denote by q_n the proto catch up honest miners and blocks behind.
if $n \geq 0$ and $q_n = 1$ else. of the attacker **A** to catch up honest miners whereas
A's blockchain is n blocks behind.
Then, $q_n = \left(\frac{q}{p}\right)^n$ if $n \ge 0$ and $q_n = 1$ else.
Definition. For, $z \in \mathbb{N}$, the probability of success of a
double-spend

Then, $q_n = \left(\frac{q}{n}\right)$ if $n \geqslant 0$ $\left(\frac{q}{p}\right)^n$ if $n \geqslant 0$

d s blockchain is n blocks behind.

Then, $q_n = \left(\frac{q}{p}\right)^n$ if $n \ge 0$ and $q_n = 1$ else.
 Definition. For, $z \in \mathbb{N}$, the probability of success of a *double-spending attack is denoted by* $P(z)$.
 Note. The pr **Definition.** For, $z \in \mathbb{N}$, the probability of success of a double-spending attack is denoted by $P(z)$.
Note. The probability $P(z)$ is evaluated at $t = 0$. The double-spending attack cannot be successful before $t = S$ **Solution:** 101, $z \in \mathbb{N}$, the prood double-spending attack is denoted
 Note. The probability $P(z)$ is evaluable-spending attack cannot be \mathbf{S}_z .
 Formula for $P(z)$

When $t = \mathbf{S}_z$, the attacker has m

By con **Note.** The probability $P(z)$ is evaluated at $t = 0$. The
double-spending attack cannot be successful before $t =$
 S_z .
Formula for $P(z)$
When $t = S_z$, the attacker has mined $N'(S_z)$ blocks.
By conditionning on $N'(S_z)$,

double-spending attack cannot be successfu
 S_z .
 Formula for $P(z)$

When $t = S_z$, the attacker has mined $N'(z)$.

By conditionning on $N'(S_z)$, we get:

$$
P(z) = \sum_{k=0}^{\infty} \mathbb{P}[N'(S_z) = k] q_{z-k}
$$

= $\mathbb{P}[N'(S_z) \geq z] + \sum_{k=0}^{z-1} \mathbb{P}[N'(S_z) = k] q_{z-k}$
= $1 - \sum_{k=0}^{z-1} \mathbb{P}[N'(S_z) = k]$
 $+ \sum_{k=0}^{z-1} \mathbb{P}[N'(S_z) = k] q_{z-k}$
= $1 - \sum_{k=0}^{z-1} \mathbb{P}[N'(S_z) = k] (1 - q_{z-k})$

Satoshi's approximation

Satoshi's approximation
White paper, Section 11 Calculations White paper, Section ¹¹ **Calculations**

$$
\boldsymbol{S}_z \; \approx \; \mathbb{E}[\boldsymbol{S}_z]
$$

and

$$
N'(S_z) \approx N'(\mathbb{E}[S_z])
$$

\n
$$
\approx N'(z \cdot \mathbb{E}[T])
$$

\n
$$
\approx N'\left(z \cdot \frac{\tau_0}{p}\right)
$$

\nSo, $N'(S_z) \approx \text{Poisson process with parameter } \lambda \text{ given}$

by

$$
\lambda = \alpha' \cdot z \cdot \frac{\tau_0}{p}
$$

$$
= z \cdot \frac{q}{p}
$$

 $\lambda = \alpha' \cdot z \cdot \frac{\tau_0}{p}$
= $z \cdot \frac{q}{p}$
Definition. We denote by $P_{SN}(z)$ the (false) formula
obtained by Satoshi in Bitcoin's white paper. $\lambda = \alpha' \cdot z \cdot \frac{p}{p}$
= $z \cdot \frac{q}{p}$
Definition. We denote by $P_{SN}(z)$ the (false) form
obtained by Satoshi in Bitcoin's white paper. *pobtained by Satoshi in Bitcoin's white paper.*

Then,

$$
P_{\rm SN}(z) = 1 - \sum_{k=0}^{z-1} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p} \right)^{z-k} \right)
$$

However, $P(z) \neq P_{SN}(z)$ since $N'(S_z) \neq N'(\mathbb{E}[S_z]).$

**A correct analysis of doublespending attack A correct analysis of doubl
spending attack
Meni Rosenfeld's correction
Set** $X_n := N'(S_n)$ **.**

Set $X_n := \mathbf{N}'(S_n)$.

Proposition. *The random variable* X_n *has a negative*
Proposition. *The random variable* X_n *has a negative*
binomial distribution with parameters (n, p) , *i.e., for* **binding** $\mathbf{X}_n := \mathbf{N}'(\mathbf{S}_n)$ **.
Proposition.** The random variable \mathbf{X}_n has a negative binomial distribution with parameters (n, p) , i.e., for $k \geqslant 0$ $k \geqslant 0$

$$
\mathbb{P}[\boldsymbol{X}_n = k] = p^n q^k \binom{k+n-1}{k}
$$

 $\mathbb{P}[\mathbf{X}_n = k] = p^n q^k \binom{k+n-1}{k}$

"The attacker's potential progress" is not "a Poisson

distribution with expected value $\lambda = z \frac{q}{p}$ "... $\mathbb{P}[\mathbf{X}_n = k] = p^n q^k \binom{k+n-1}{k}$

"The attacker's potential progress" is not "a Pois"

distribution with expected value $\lambda = z \frac{q}{p}$ "... *q p* ... "The attacker's potential progress" is not "a Poisson
distribution with expected value $\lambda = z \frac{q}{p}$ "...
Proposition. The probability of success of a double-
spending attack is Free attacker's potential
distribution with expected
Proposition. The probal
spending attack is

Proposition. The probability of success of a double-
spending attack is\n
$$
P(z) = 1 - \sum_{k=0}^{z-1} (p^z q^k - q^z p^k) \binom{k+z-1}{k}
$$
\n**Numerical Applications**\nFor $q = 0.1$,

For $q = 0.1$,

For $q = 0.3$,

Solving for P less than 0.1%:

Satoshi underestimates $P(z)$...

A closed form formula
Definition. *The incomplete Beta function* **A closed form formula**
Definition. *The incomplete Beta function is
defined for* $a, b > 0$ *and* $x \in [0, 1]$ *by* **definition.** The **incomplete Beta function** P *and* $x \in [0, 1]$ *by*
R $(a, b) := \int_{a}^{x} t^{a-1}(1-t)^{b-1} dt$ **Definition.** The **incomplete Beta function** is

defined for a, b > 0 and $x \in [0,1]$ by
 $B_x(a, b) := \int_0^x t^{a-1}(1-t)^{b-1} dt$

The **regularized Beta function** is defined by
 $L(a, b) := \frac{B_x(a, b)}{a}$

Eq. 10TIM IOTMula
\n**n.** The **incomplete Beta function**
\n
$$
r a, b > 0
$$
 and $x \in [0, 1]$ by
\n $B_x(a, b) := \int_0^x t^{a-1} (1-t)^{b-1} dt$
\n**larized Beta function** is defined by
\n
$$
I_x(a, b) := \frac{B_x(a, b)}{B_1(a, b)}
$$

$$
I_x(a,b) \,\, \mathrel{\mathop:}= \,\, \frac{B_x(a,b)}{B_1(a,b)}
$$

The **regularized Beta function** is defined by
 $I_x(a, b) := \frac{B_x(a, b)}{B_1(a, b)}$

Classical result: for $a, b > 0, B(a, b) = \frac{\Gamma(a) \Gamma(b)}{\Gamma(a+b)}$

Theorem. We have: $\Gamma(a) \Gamma(b)$ $\Gamma(a+b)$ *T_x*(*a*,*b*) :=
Classical result: for *a*,*b* > 0
Theorem. We have:
 $P(z) =$

$$
P(z)\enskip = \enskip I_s(z,1/2)
$$

Classical result: for $a, b > 0$, $B(a, b) = \frac{C}{\Gamma(a+b)}$
 Theorem. We have:
 $P(z) = I_s(z, 1/2)$

with $s = 4 p q < 1$.
 Proof. It turns out that the cumulative distribution

function of a negative binomial random variable **X** $P(z) = I_s(z, 1/2)$
with $s = 4 p q < 1$.
Proof. It turns out that the cumulative distribution
function of a negative binomial random variable *X*
(same notation as above) is with $s = 4 p q < 1$.
 Proof. It turns out that the cumu

function of a negative binomial ra

(same notation as above) is
 $F_{\mathbf{Y}}(k) = \mathbb{P}[\mathbf{X} \leq k]$ Figure 1.1 That the cumulative distribute binomial random variable

pve) is
 $= \mathbb{P}[\mathbf{X} \le k]$
 $= 1 - I_p(k+1, z)$

(same notation as above) is
\n
$$
F_{\mathbf{X}}(k) = \mathbb{P}[\mathbf{X} \le k]
$$
\n
$$
= 1 - I_p(k+1, z)
$$
\nBy parts,

$$
F_{\mathbf{X}}(k) = \mathbb{P}[\mathbf{X} \leq k]
$$

= 1 - I_p(k + 1, z)

$$
I_p(k, z) - I_p(k + 1, z) = \frac{p^k q^z}{k B(k, z)}
$$

$$
P(z) = 1 - I_p(z, z) + I_q(z, z)
$$

So,

$$
P(z) \ = \ 1 - I_p(z, z) + I_q(z, z)
$$

Classical symmetry relation for Beta function:
 $I(a, b) + I(b, a) = 1$ etry relation for Beta function:
 $I_p(a, b) + I_q(b, a) = 1$

able $t \mapsto 1 - t$ in the definition). So Classical symmetry relation for Beta function:
 $I_p(a, b) + I_q(b, a) = 1$

(change of variable $t \mapsto 1 - t$ in the definition). So,
 $I(z, z) + I(z, z) = 1$

$$
I_p(a,b) + I_q(b,a) = 1
$$

etry relation for Beta function:
 $I_p(a, b) + I_q(b, a) = 1$

able $t \mapsto 1 - t$ in the definition). So
 $I_p(z, z) + I_q(z, z) = 1$ $I_p($ (change of variable $I_p($ We also use:

$$
I_p(z, z) + I_q(z, z) = 1
$$

(change of variable *t* → 1 − *t* in the definition). So,
\n
$$
I_p(z, z) + I_q(z, z) = 1
$$
\nWe also use:
\n
$$
I_q(z, z) = \frac{1}{2} I_s(z, 1/2)
$$
\nwith $s = 4 p q$.

 $I_q(z, z) = \frac{1}{2} I_s(z, 1/2)$
with $s = 4 p q$. \square
Classical function pbeta implemented in R gives the
true double-spending attack success probability. with $s = 4 p q$. \Box
Classical function pbeta implemented in R gives the true double-spending attack success probability. $I_q(z, z) = \frac{1}{2} I_s(z, 1/2)$
with $s = 4 p q$.
Classical function pbeta implemented in l
true double-spending attack success proba
Asymptotic analysis
According to Satoshi,

Asymptotic analysis
According to Satoshi,

nptotic analysis
ing to Satoshi,
Given our assumption that $p > q$, the
probability drops exponentially as the
number of blocks the attacker has to **Inprofile analysis**
ing to Satoshi,
Given our assumption that $p > q$, the
probability drops exponentially as the
number of blocks the attacker has to ing to Satoshi,
Given our assumption that $p > q$, the
probability drops exponentially as the
number of blocks the attacker has to
catch up with increases. Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. Given our assumption that $p >$
probability drops exponentially a
number of blocks the attacker l
catch up with increases.
Theorem. When $z \to \infty$, we have:
 $P(z) = s^z$

Theorem. When
$$
z \to \infty
$$
, we have:
\n
$$
P(z) \sim \frac{s^z}{\sqrt{\pi(1-s) z}}
$$
\nwith $s = 4$ $p q < 1$.

A more accurate risk analysis

A more accurate risk analysis
The merchant waits for *z* blocks. Once it has been
done, he knows how long it took... Denote this number **A more accurate risk analysis**
The merchant waits for z blocks. Once it has been
done, he knows how long it took... Denote this number
by τ_1 . In average, it should take $\mathbb{E}[z\,] = \frac{z\,\tau_0}{p}$. **A more accurate risk analysis**
The merchant waits for z blocks. Once it has been
done, he knows how long it took... Denote this number
by τ_1 . In average, it should take $\mathbb{E}[z\,] = \frac{z\,\tau_0}{p}$. it has bee:
this numbe
 $\frac{z \tau_0}{p}$. $\frac{\tau_0}{p}$. $\frac{p}{\text{d}}$ it took..

hould take
 $\frac{p}{z\tau_0}$ $\frac{p \, \tau_1}{z \, \tau_0}$

Definition. *Set* $\kappa := \frac{p \tau_1}{z \tau_2}$ **Definition.** *Set* $\kappa := \frac{p \tau_1}{z \tau_0}$
Dimensionless parameter.
Satoshi's approximation: $\kappa = 1...$

Dimensionless parameter.

Dimensionless parameter.

Satoshi's approximation: $\kappa = 1...$

Instead of computing $P(z)$, let us compute $P(z, \kappa)$.

Probability for a successful double-spending attack

knowing that z blocks have been mined by the honest Instead of computing $P(z)$, let us compute $P(z, \kappa)$.
Probability for a successful double-spending attack
knowing that z blocks have been mined by the honest
miners at $S_z = \tau_1$. Instead of computing $P(z)$,
Probability for a successfu
knowing that z blocks have
miners at $S_z = \tau_1$. Probability for a successful double-spending attack
knowing that *z* blocks have been mined by the honest
miners at $S_z = \tau_1$.

Note. We have $P_{SN}(z) = P(z, 1)$.
Note. Two different probabilities.

- **te.** We have $P_{SN}(z) = P(z, 1)$.
 te. Two different probabilities.

 Theoretical probability $P(z)$ calculated at $T = 0$ by the attacker or the merchant. Two different probabilities.
Theoretical probability $P(z)$ calculated
0 by the attacker or the merchant.
- Theoretical probability $P(z)$ calculated at $T = 0$ by the attacker or the merchant.
• concrete probability $P(z, \kappa)$ calculated at $T = \tau_1$ by the merchant. Theoretical probability P
0 by the attacker or the n
concrete probability $P(z,$
 τ_1 by the merchant.

Number of bocks mined by the attacker at $T = \tau_1$
unknown to the merchant = Poisson distribution Number of bocks mined by the attacker at $T = \tau_1$
unknown to the merchant = Poisson distribution
parameter $\lambda(z, \kappa)$: Number of bocks mined b
unknown to the merchan
parameter $\lambda(z,\kappa)$:
 $\lambda(z,\kappa) =$ (*z*) contained by the attack

(*z*) = $\alpha' \tau_1$
 $\lambda(z,\kappa) = \frac{\alpha' \tau_1}{\tau_0 \cdot \frac{z \kappa \tau_0}{n}}$ *z* 0

$$
\lambda(z,\kappa) = \alpha' \tau_1
$$

=
$$
\frac{q}{\tau_0} \cdot \frac{z \kappa \tau_0}{p}
$$

=
$$
\frac{zq}{p} \kappa
$$

i.e.,

$$
= \frac{2q}{p}\kappa
$$

$$
\mathbb{P}[\mathbf{N}'(\tau_1) = k] = \frac{\left(\frac{zq}{p}\kappa\right)^k}{k!} e^{-\frac{zq}{p}\kappa}
$$

i.e.,
 $\mathbb{P}[N'(\tau_1) = k] = \frac{\left(\frac{zq}{p}\kappa\right)^k}{k!} e^{-\frac{zq}{p}\kappa}$
 Definition. *The regularized Gamma function is defined by:* $\mathbb{P}[N'(\tau)]$
Definition. The *defined by:* **Definition.** The regularized Gamma function is **Definition.** The regularized Gamma function is
 defined by:
 $\Gamma(s,x) := \int_x^{+\infty} t^{s-1} e^{-t} dt$

The regularized incomplete Gamma function is:
 $\Omega(s,x)$

$$
\Gamma(s, x) := \int_{x}^{+\infty} t^{s-1} e^{-t} dt
$$

ized incomplete Gamma function is:

$$
Q(s, x) := \frac{\Gamma(s, x)}{\Gamma(s)}
$$

The regularized incomp
 $Q(s, x)$
It turns out that

$$
Q(s,x) \,\, \mathrel{\mathop:}= \,\, \frac{\Gamma(s,x)}{\Gamma(s)}
$$

$$
Q(s, x) := \frac{\Gamma(s, x)}{\Gamma(s)}
$$

It turns out that

$$
Q(z, \lambda) = \sum_{k=0}^{z-1} \frac{\lambda^k}{k!} e^{-\lambda}
$$

So,
Theorem. We have:

$$
P(z, x) = 1 - Q\left(z^{-Kz}q\right) + \left(q\right)^z e^{\frac{z-p-q}{n}}Q(z, x).
$$

So,

So,
\n**Theorem.** We have:
\n
$$
P(z, \kappa) = 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^{z} e^{\kappa z \frac{p-q}{p}} Q(z, \kappa z)
$$

Proof. We have:
\n
$$
P(z, \kappa) = \mathbb{P}[N'(\tau_1) \geq z] + \sum_{k=0}^{z-1} \mathbb{P}[N'(\tau_1) = k] q_{z-k}
$$
\n
$$
= 1 - \sum_{k=0}^{z-1} \frac{\lambda(z, \kappa)^k}{k!} e^{-\lambda(z, \kappa)}
$$
\n
$$
+ \sum_{k=0}^{z-1} \left(\frac{q}{p}\right)^{z-k} \cdot \frac{\lambda(z, \kappa)^k}{k!} e^{-\lambda(z, \kappa)}
$$
\n
$$
= 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^{z} e^{\kappa z \frac{p-q}{p}} Q(z, \kappa z)
$$
\n**Asymptotics Analysis**

\nProposition. We have $P_{\text{CM}}(z) \sim \frac{e^{-z(z(\frac{q}{p}))}}{z}$ with

Asymptotics Analysis
Proposition. We have $P_{SN}(z) \sim \frac{e^{-zc(\frac{q}{p})}}{2}$ with
 $c(u) := u - 1 - \ln u$ $e^{-zc\left(\frac{q}{p}\right)}$ *p* / $\sqrt{2}$ $\frac{1}{2}$ *with* $c(\mu) := \mu - 1 - \ln \mu$ **Proposition.** We have $P_{SN}(z) \sim \frac{e^{-zc(\frac{q}{p})}}{2}$ with
 $c(\mu) := \mu - 1 - \ln \mu$

More generally, we have 5 different regimes.
 Proposition 1. When $z \to +\infty$, we have:

or equivalently, we have 5 different regimes.

\noposition 1. When
$$
z \to +\infty
$$
, we have:

\n\n- For $0 < \kappa < 1$, $P(z, \kappa) \sim \frac{1}{1 - \kappa \frac{q}{p}} \frac{1}{\sqrt{2\pi z}} e^{-zc\left(\kappa \frac{q}{p}\right)}$
\n- For $\kappa = 1$, $P(z, 1) = P_{\text{SN}}(z) \sim \frac{e^{-zc\left(\frac{q}{p}\right)}}{2}$
\n- For $1 < \kappa < \frac{p}{q}$,
\n

\n- For
$$
0 < \kappa < 1
$$
, $P(z, \kappa) \sim \frac{1}{1 - \kappa \frac{q}{p}} \frac{1}{\sqrt{2 \pi z}} e^{-z c \left(\kappa\right)}$
\n- For $\kappa = 1$, $P(z, 1) = P_{\text{SN}}(z) \sim \frac{e^{-z c \left(\frac{q}{p}\right)}}{2}$
\n- For $1 < \kappa < \frac{p}{q}$,
\n- (1, 9)
\n

• For
$$
1 < \kappa < \frac{p}{q}
$$
,

or
$$
\kappa = 1, P(z, 1) = P_{SN}(z) \sim \frac{e^{-(p)}}{2}
$$

\nor $1 < \kappa < \frac{p}{q}$,
\n
$$
P(z, \kappa) \sim \frac{\kappa \left(1 - \frac{q}{p}\right)}{(\kappa - 1) \left(1 - \kappa \frac{q}{p}\right)} \frac{1}{\sqrt{2 \pi z}} e^{-zc\left(\kappa \frac{q}{p}\right)}
$$

• For
$$
\kappa = \frac{p}{q}
$$
, $P(z, \frac{p}{q}) \rightarrow \frac{1}{2}$ and
\n
$$
P(z, \frac{p}{q}) - \frac{1}{2} \sim \frac{1}{\sqrt{2\pi z}} \left(\frac{1}{3} + \frac{q}{p-q}\right)
$$
\n• For $\kappa > \frac{p}{q}$, $P(z, \kappa) \rightarrow 1$ and
\n
$$
1 - P(z, \kappa) \sim \frac{\kappa \left(1 - \frac{q}{p}\right)}{\left(\kappa \frac{q}{p} - 1\right)(\kappa - 1)} \frac{1}{\sqrt{2\pi z}} e^{-z c \left(\kappa \frac{q}{p}\right)}
$$
\n**Comparison between** $P(z)$ and
\n $P_{SN}(z)$

$P_{\rm SN}(z)$ **Comparison between** P **
** $P_{SN}(z)$
 Asymptotic behaviours

The asymptotic behaviours of $P(z)$ and $\lim_{z \to 0} \frac{1}{z}$ **Comparison between** $P(z)$ **and** $P_{SN}(z)$ **
Asymptotic behaviours
The asymptotic behaviours of** $P(z)$ **and** $P_{SN}(z)$ **are quite different**

Asymptotic behaviours
The asymptotic behaviours of $P(z)$ a
quite different
Proposition. We have $P_{SN}(z) \prec P(z)$ **Asymptotic behaviours**
The asymptotic behaviours of $P(z)$ and P_{SN}
quite different
Proposition. We have $P_{SN}(z) \prec P(z)$ The asymptotic behaviours of $P(z)$ and P_{SN}
quite different
Proposition. We have $P_{SN}(z) \prec P(z)$
Bounds for $P(z)$ **and** $P_{SN}(z)$
Goal: compute an explicit rank z_0 such that

Proposition. We have $P_{SN}(z) \prec P(z)$
 Bounds for $P(z)$ **and** $P_{SN}(z)$

Goal: compute an explicit rank z_0 such that *P*SN(*z*) **and** $P_{SN}(z)$
(*z*) **and** $P_{SN}(z)$
explicit rank z_0 such the $P_{SN}(z) < P(z)$ **Example 3 Bounds for** $P(z)$ **and** $P_{SN}(z)$ **

Goal: compute an explicit rank** z_0 **such that
** $P_{SN}(z) < P(z)$ **

for all** $z > z_0$ **.

Upper and lower bounds for** $P(z)$

Remember that $s = 4 p q$.

$$
P_{\rm SN}(z) \ < \ P(z)
$$

for all $z > z_0$.
 Upper and lower bounds for $P(z)$

Remember that $s = 4 p q$.

We'll use Gautschi's inequalities.

Proposition 2. For any $z > 1$,

Proposition 2. For any
$$
z > 1
$$
,
\n
$$
\sqrt{\frac{z}{z+1}} \frac{s^z}{\sqrt{\pi z}} \leqslant P(z) \leqslant \frac{s^z}{\sqrt{\pi (1-s) z}}
$$
\n**An upper bound for** $P_{SN}(z)$
\n**Lemma.** Let $z \in \mathbb{N}^*$ and $\lambda \in \mathbb{R}_+^*$. We have:
\n*i.* If $\lambda \in [0,1]$, then

Lemma. Let $z \in \mathbb{N}^*$ and $\lambda \in \mathbb{R}_+^*$. We have

An upper bound for
$$
P_{SN}(z)
$$

\nLemma. Let $z \in \mathbb{N}^*$ and $\lambda \in \mathbb{R}_+^*$. We have:
\n $i. \text{ If } \lambda \in]0,1[, \text{ then}$
\n $1-Q(z,\lambda z) < \frac{1}{1-\lambda} \frac{1}{\sqrt{2\pi z}} e^{-z(\lambda - 1 - \ln \lambda)}$
\n $ii. \text{ If } \lambda = 1, Q(z,z) < \frac{1}{2}.$
\nProposition. We have

Proposition. We have
\n
$$
P_{\text{SN}}(z) < \frac{1}{1 - \frac{q}{p}} \frac{1}{\sqrt{2 \pi z}} e^{-zc\left(\frac{q}{p}\right)} + \frac{1}{2} e^{-zc\left(\frac{q}{p}\right)}
$$
\nwith $c(\mu) := \mu - 1 - \ln \mu$.
\n**An explicit rank** z_0
\n**Theorem.** Let $z \in \mathbb{N}^*$. A sufficient condition to get

 $\begin{array}{ll}\n\sqrt{2\pi z} & 2 \\
\frac{1}{2} & \n\end{array}$
 A sufficient condition to get with *P*
 *P*SN(*z*) *z*) *<i>P*(*z*) *is z z E N*^{*} *A sufficient*
 *P*_{SN}(*z*) *<P*(*z*) *is z* > *z*₀ *with*
 P

An explicit rank
$$
z_0
$$

\n**Theorem.** Let $z \in \mathbb{N}^*$. A sufficient condition to get
\n
$$
P_{SN}(z) < P(z) \text{ is } z > z_0 \text{ with}
$$
\n
$$
z_0 := \text{Max}\left(\frac{2}{\pi \left(1 - \frac{q}{p}\right)^2}, \frac{1}{2\sqrt{2}} - \frac{1 + \frac{1}{\sqrt{2}}}{2} \frac{\ln\left(\frac{2\psi_0}{\pi}\right)}{\psi_0}\right)
$$
\nwith
\n
$$
\psi_0 := \frac{q}{p} - 1 - \ln\left(\frac{q}{p}\right) - \ln\left(\frac{1}{4pq}\right) > 0
$$

with

$$
\psi_0 \ := \ \frac{q}{p} - 1 - \ln\left(\frac{q}{p}\right) - \ln\left(\frac{1}{4\,p\,q}\right) > 0
$$

Conclusion. What sould the
merchant do?
Set $\bar{P}(z, t)$ = probability of success of a double spend **Conclusion.** What
merchant do?
Set $\bar{P}(z,t) =$ probability of succes
attack knowing that z blocks h

Conclusion. What sould the
merchant do?
Set $\bar{P}(z,t)$ = probability of success of a double spend
attack knowing that z blocks have been validated
before t date. **Conclusion.** What sould the merchant do?
Set $\bar{P}(z,t)$ = probability of success of a double spend attack knowing that z blocks have been validated before *t*-date. before *t*-date. Set $\bar{P}(z, t)$ = probability of success of a double spend
attack knowing that z blocks have been validated
before t-date.
Shipment condition: Good will be sent to the buyer
as soon as $\bar{P}(z, t) < 0.1\%$ for any $q < 0.2$

Set $P(z, t)$ = probability of success of a double spend
attack knowing that z blocks have been validated
before *t*-date.
Shipment condition: Good will be sent to the buyer
as soon as $\bar{P}(z, t) < 0.1\%$ for any $q < 0.2$ (f attack knowing that z blocks have been validatefore t -date.
Shipment condition: Good will be sent to the buy as soon as $\bar{P}(z, t) < 0.1\%$ for any $q < 0.2$ (for instan where $t =$ time used to mine z blocks and of Sa before *t*-date.
Shipment condition: Good
as soon as $\bar{P}(z, t) < 0.1\%$ for
where $t =$ time used to mine
cf Satoshi Risk Tables. Shipment condition: Good will be sent to the buyer
as soon as $\bar{P}(z, t) < 0.1\%$ for any $q < 0.2$ (for instance)
where $t =$ time used to mine *z* blocks and
cf Satoshi Risk Tables.
Shipment_time = Inf{ $t > 0/\bar{P}(N(t), t) < \varepsilon$

 $\label{eq:2.1} \begin{split} \text{Shipment_time} &= \text{Inf}\{t>0/\bar{P}(N(t),t)<\varepsilon\}.\\ \text{On average, this will happen after z blocks have been validated and $P(z)<\varepsilon$.} \end{split}$ his will happe
 $P(z) < \varepsilon$.

. One has $P(z)$

as above.

and $P(z)$
 ion. One
 $\frac{p S_z}{z \tau_0}$ as abo $\frac{p S_z}{z \tau_0}$ as abo **Proposition.** One has $P(z) =$
and $\kappa := \frac{p S_z}{z \tau_0}$ as above.
So, by Markov inequality,

$$
\frac{p S_z}{z \tau_0}
$$
 as above.
\narkov inequality,
\n
$$
\forall \varepsilon > 0, \quad \mathbb{P}[P(z, \kappa) > \varepsilon] \le \frac{P(z)}{\varepsilon}
$$
\n
$$
\to 0
$$

 $\forall \varepsilon > 0, \quad \mathbb{P}[P(z, \kappa) > \varepsilon] \leq \frac{P}{\rightarrow 0}$
 Note. If $\kappa > 1, \mathbb{P}[\kappa > \kappa] \sim \frac{1}{\kappa - 1} \frac{1}{\sqrt{2\pi z}} e^{-\frac{1}{2}}$

asymptotics in DSR. 1 $\kappa - 1 \sqrt{2 \pi z}$ $\frac{1}{\sqrt{2\pi z}}e^{-zc(\kappa)}$. Oth . Other $\forall \varepsilon > 0$, $\mathbb{P}[P(z$
 Note. If $\kappa > 1$, $\mathbb{P}[\kappa > \kappa]$

asymptotics in DSR.

So $\mathbb{P}[\text{Shimmet Time} < 1]$ $\rightarrow 0$

Note. If $\kappa > 1$, $\mathbb{P}[\kappa > \kappa] \sim \frac{1}{\kappa - 1} \frac{1}{\sqrt{2\pi z}} e^{-zc}$

asymptotics in DSR.

So, $\mathbb{P}[\text{Shipment-Time} < +\infty] = 1$.

Submissions

- Submissions

Long list of rejections from

 arxiv.org (section probability) **ibmissions**
arxiv.org (section probability)
• European Journal of Operational Re
- **IDMISSIONS**

19 list of rejections from

19 arxiv.org (section probability)

19 European Journal of Operational Research: "I

19 came to conclusion that your paper does not fit Compared in the conclusion from that your paper does not fit
came to conclusion that your paper does not fit
the scope of EJOR. Your list of references also st of rejections from
arxiv.org (section probability)
European Journal of Operational Research: "I
came to conclusion that your paper does not fit
the scope of EJOR. Your list of references also
gives support to this concl arxiv.org (section probability)
European Journal of Operational Research: "I
came to conclusion that your paper does not fit
the scope of EJOR. Your list of references also
gives support to this conclusion.", Emanuele
Borg Borgonovo European souther of operational research.

came to conclusion that your paper does not fit

the scope of EJOR. Your list of references also

gives support to this conclusion.", Emanuele

Borgonovo

• Acta Informatica: "[..
	- the scope of EJOR. Your list of references also
gives support to this conclusion.", Emanuele
Borgonovo
Acta Informatica: "[...]the list of references, [...]
is comparably short and does not refer to any
paper of the typica example of the typical Acta Information.", Emanuele
Borgonovo
Acta Informatica: "[...]the list of references, [...]
is comparably short and does not refer to any
paper of the typical Acta Informatica areas.",
Christel Baie Borgonovo
Acta Informatica: "[.
is comparably short
paper of the typical
Christel Baier
SIAM Journal on Mathematica: "[...]
the list of references, [...]
is comparably short and does not refer to any
paper of the typical Acta Informatica areas.",
Christel Baier
SIAM Journal on Financial Mathematics:
"Overall, the authors bas The automatical properties of federatios, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

	(i) is comparably short and does not refer to any

	paper of the typical Acta Informatica areas.",

	Christel Baier

	SIAM Journal on Financial Mathematics:
	- be comparatly short and does not refer to any
paper of the typical Acta Informatica areas.",
Christel Baier
SIAM Journal on Financial Mathematics:
"Overall, the authors basically just recast really
basic probability result Peper of the typical from intermatica areas,

	SIAM Journal on Financial Mathematics:

	"Overall, the authors basically just recast really

	basic probability results using bitcoin jargons.

	I think rejection outright is the SIAM Journal on Final

	"Overall, the authors basica

	basic probability results us

	I think rejection outright is

	Jean-Pierre Fouque

	Journal of Economic Theo SHIM SOGNIGHT IN THEORGE INCREDIBLE THEORGENDERITY

	SHIM SOGNIES USIBY JUST FECAST FOR DISPONSITY

	SAGGE THEORY: The paper does

	Theory: "The paper does

	not contribute to any ongoing conversations in basic probability results using bitcoin jargons.

	I think rejection outright is the right decision.",

	Jean-Pierre Fouque

	Journal of Economic Theory: "The paper does

	not contribute to any ongoing conversations in

	econom
- Example Deaming Testates and Second I think rejection outright is the right de
Jean-Pierre Fouque
Journal of Economic Theory: "The pay
not contribute to any ongoing conversate
economics.", Laura Veldkamp
submitted to Inter Jean-Pierre Fouque

• Journal of Economic Theory: "The paper does

not contribute to any ongoing conversations in

economics.", Laura Veldkamp

Finally submitted to International Journal of

Theoretical and Applied Finance

• Journal of Economic Theory: "The paper does
not contribute to any ongoing conversations in
economics.", Laura Veldkamp
Finally submitted to International Journal of
Theoretical and Applied Finance: "We will send
the pape not contribute to any ongoing conversations in
economics.", Laura Veldkamp
Finally submitted to International Journal of
Theoretical and Applied Finance: "We will send
the paper to referees and the process will take
approx ally submitted to Internative of the Pinally submitted to Internative original and Applied Finance paper to referees and the approximately 5-6 months."