PoissonCoin whitepaper : philosophy, protocols, algorithms and serious mathematics

Vivien Berriche

30th of February 2018, 19:23:12

Version 0.9

Abstract

Let's be honest: we perfectly know that 98,7% of average cryptoenthusiasts who click on a whitepaper pdf file do not understand a goddam thing about it. BUT... as long as it's written in LaTeX, has some texts, charts and mathematical formulas, it's okay, it looks fancy and serious! Well, we enjoy that! let's do it! I will copy-paste this abstract to make it twice longer. Let's be honest: we perfectly know that 98,7% of average cryptoenthusiasts who click on a whitepaper pdf file do not understand a goddam thing about it. BUT... as long as it's written in LaTeX, has some texts, charts and mathematical formulas, it's okay, it looks fancy and serious!

Contents

1 Philosophy

What is Wikipedia?

Wikipedia is a multilingual, web-based, free-content encyclopedia project supported by the Wikimedia Foundation and based on a model of openly editable content. I copy-past some extracts of Wikipedia's articles. **Don't blame me !!** Could you tell me which student hasn't ever made a copy-paste from wikipedia for his/her homework...?

Pataphysics

Pataphysics is a difficult to define literary trope invented by French writer Alfred Jarry (1873–1907). One attempt at a definition might be to say that Pataphysics is a branch of philosophy or science that examines imaginary phenomena that exist in a world beyond metaphysics; it is the science of imaginary solutions.

Pataphysics is a concept expressed by Jarry in a mock-scientific manner with undertones of spoofing and quackery, in his fictional book Exploits and Opinions of Dr. Faustroll, Pataphysician, in which Jarry riddles and toys with conventional concepts and interpretations of reality. Another attempt at a definition interprets Pataphysics as an idea that "the virtual or imaginary nature of things as glimpsed by the heightened vision of poetry or science or love can be seized and lived as real". Jarry defines Pataphysics in a number of statements and examples, including that it is "the science of imaginary solutions, which symbolically attributes the properties of objects, described by their virtuality, to their lineaments". A practitioner of Pataphysics is a pataphysician or a pataphysicist.

> Pataphysics is the science of that which is superinduced upon metaphysics, whether within or beyond the latter's limitations, extending as far beyond metaphysics as the latter extends beyond physics. ... Pataphysics will be, above all, the science of the particular, despite the common opinion that the only science is that of the general. Pataphysics will examine the laws governing exceptions, and will explain the universe supplementary to this one.

2 Poisson distribution

2.1 An ICO according to Poisson distribution

In **probability theory** and **statistics**, the Poisson distribution (French pronunciation named after French mathematician **Siméon Denis Poisson**), is a discrete probability distribution. PoissonCoin's ICO roughly follows a Poisson distribution.

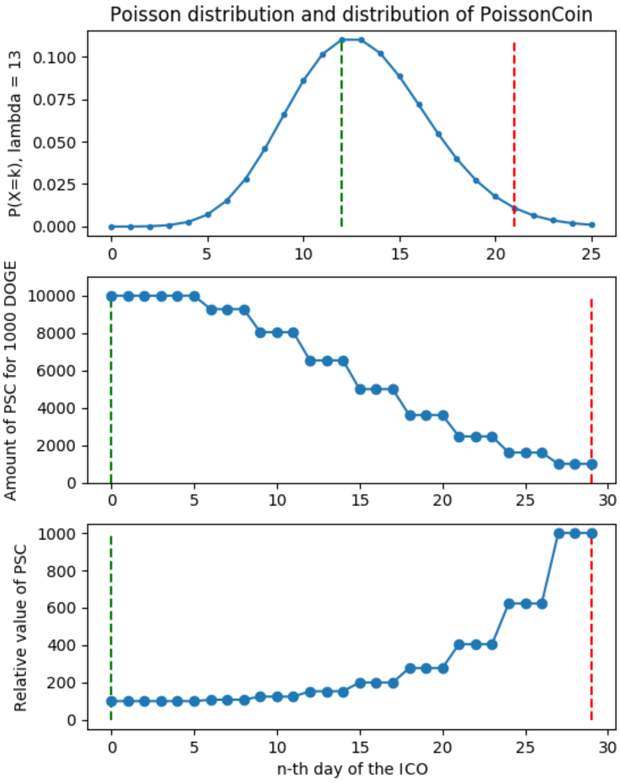
2.2 Details

https://github.com/vberriche/poissoncoin/blob/master/tokens_distribution.py

https://en.wikipedia.org/wiki/Poisson_distribution

2.3 Graphics

Here are the amount of PoissonCoins for 1000 DogeCoins and the relative price of PoissonCoins (100% = first day).



3 Presentation of the ROT29 cryptographic system

3.1 Overview

Bitcoin's and PoissonCoin's adresses use a base58 format : "123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz".

ROT29 is a cryptographic system developped by Vivien Berriche. It is inspired by an old technic called "Caesar cipher" and applied to the modern world.

Like most of the cryptographic functions, ROT29 enables to restore the public key from the private key. But unlike most of them, ROT29 enables to restore the **private** key from the **public** key too! We will prove this disruptive feature.

3.2 Mathematical aspect

Let $B = (1, 2, 3, 4, ..., A, B, C, .., a, ..., z)$ be the tuple of base58.

We define canonically the function e :

$$\begin{array}{rccc} e: & B & \longrightarrow & \mathbb{Z}/58\mathbb{Z} \\ & b & \mapsto & e(b) \end{array}$$

where $e(1) = \widehat{0}, e(2) = \widehat{1}, ..., e(A) = \widehat{9}, ..., e(a) = \widehat{34}$, etc.

e is obviously bijective because B and $\mathbb{Z}/58\mathbb{Z}$ have the same cardinal.

We define the function r :

$$\begin{array}{rccc} r: & \mathbb{Z}/58\mathbb{Z} & \longrightarrow & \mathbb{Z}/58\mathbb{Z} \\ & \widehat{x} & \mapsto & \widehat{x} + \widehat{29} \end{array}$$

r is also obviously bijective.

The ROT29 function $\Re$ is defined :

$$\begin{array}{rccc} \Re: & B & \longrightarrow & B \\ & b & \mapsto & (e^{-1} \circ r \circ e)(b) \end{array}$$

3.3 Mathematical proof of its disruptive feature

Let's start with a lemma.

Lemma : r is involutive.

Let $\widehat{x}$ be an element of $\mathbb{Z}/58\mathbb{Z}$.

$r^2(\widehat{x}) = r(\widehat{x}) + \widehat{29} = \widehat{x} + \widehat{29} + \widehat{29} = \widehat{x} + \widehat{0} = \widehat{x}$ because $58 \equiv 0 \ \ [58]$

Therefore, $r^2 = Id$, ie. r is involutive. □

We prove now that $\Re$ is involutive too.

Let's take $b \in B$.

$$\begin{aligned} \Re^2(b) = \ & (e^{-1} \circ r \circ e) \circ (e^{-1} \circ r \circ e)(b) & \\ = \ & (e^{-1} \circ r \circ r \circ e)(b) & \text{because } e \circ e^{-1} = Id \\ = \ & (e^{-1} \circ e)(b) & \text{because } r \text{ is involutive (lemma)} \\ = \ & Id & \end{aligned}$$

Therefore, $\Re$ is involutive. ■

3.4 Implementation in JavaScript

```
<script type="text/javascript">

var base58 = "123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz" ;
var base58d = "WXYZabcdefghijkmnopqrstuvwxyz123456789ABCDEFGHJKLMNPQRSTUV" ;

function rot29(texte) {

 var converted =’’ ;

 for (var i = 0 ; i < texte.length ; i++ ) {
 if ( base58.indexOf(texte.charAt(i)) != -1 )
  { converted = converted + base58d.charAt(base58.indexOf(texte.charAt(i))) ; }
}
 return converted ;
}
```

4 Serious mathematics for a serious work

Academics, this part is only for newbies. They don't see the differences between fake and real math ;-)

4.1 Fancy equations

$$\widehat{\lambda}_\mathrm{MLE} = \frac{1}{n}\sum_{i=1}^{n} k_i. \qquad \lambda = \frac{\sum_{i=1}^{n} k_i}{n}$$

$$P(\mathbf{x}) = \prod_{i=1}^{n} \frac{\lambda^{x_i} e^{-\lambda}}{x_i!} = \frac{1}{\prod_{i=1}^{n} x_i!} \times \lambda^{\sum_{i=1}^{n} x_i} e^{-n\lambda}$$

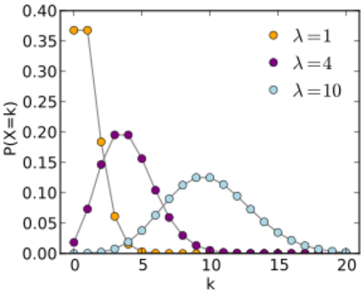
$$\ell(\lambda) = \ln \prod_{i=1}^{n} f(k_i \mid \lambda) = \sum_{i=1}^{n} \ln\!\left(\frac{e^{-\lambda}\lambda^{k_i}}{k_i}\right)$$

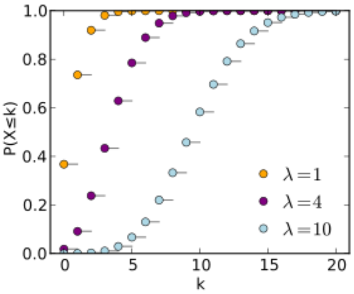
$$\ell(\lambda) = -n\lambda + \left(\sum_{i=1}^{n} k_i\right) \ln(\lambda) - \sum_{i=1}^{n} \ln(k_i).$$

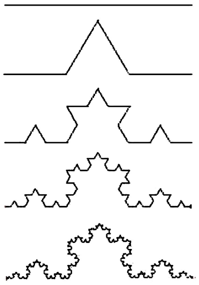
$$\frac{\mathrm{d}}{\mathrm{d}\lambda}\ell(\lambda) = 0 \iff -n + \left(\sum_{i=1}^{n} k_i\right)\frac{1}{\lambda} = 0.$$

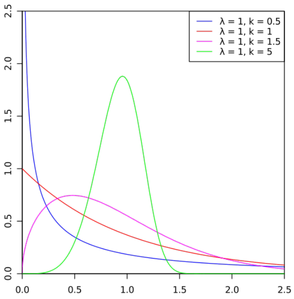
$$\frac{\partial^2 \ell}{\partial \lambda^2} = -\lambda^{-2}\sum_{i=1}^{n} k_i$$

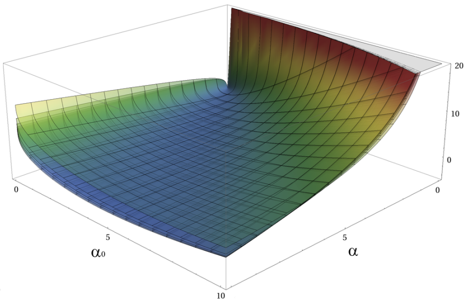
4.2 Complicated charts











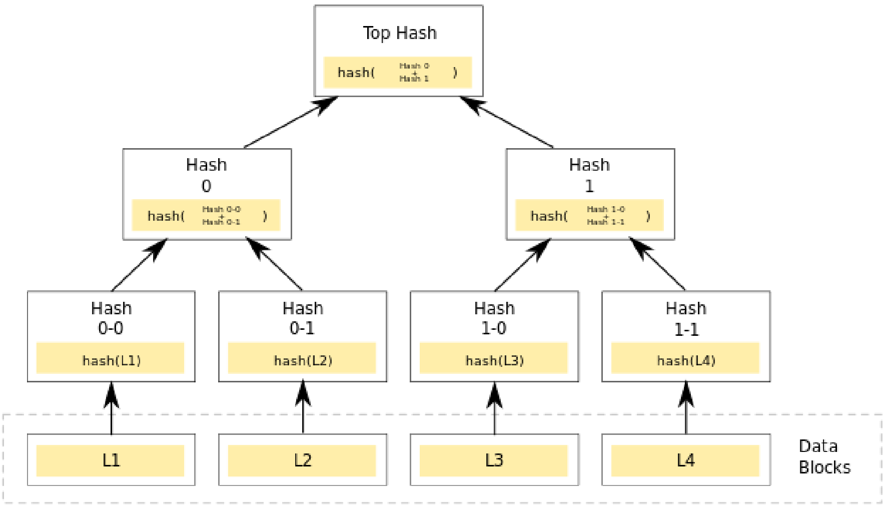
4.3 Merkle trees

Merkle trees have no relations with the Chancellor of Germany Angela Merkel. Actually, Angela Merkel does not like trees as she wants to cut an cute forest in Germany, the Hambach forest (Have a look on the internet!).

In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

Demonstrating that a leaf node is a part of a given binary hash tree requires computing a number of hashes proportional to the logarithm of the number of leaf nodes of the tree;[1] this contrasts with hash lists, where the number is proportional to the number of leaf nodes itself.

The concept of hash trees is named after Ralph Merkle who patented it in 1979.



5 Acknowledgements

Big up to Rami Malek, Alexander Grothendieck and Geronimo.
Rami Malek, because the scene of the party in Mr Robot (S03E07) is cynically lucid...
Alexander Grothendieck, because he was the most aware mathematician.

> "Only when the last tree is cut down, the last fish caught and the last stream poisoned, may the cryptoenthusiasts realize that bitcoin can't be eaten". Satoshi Geronimo