Episode 06 -THE UNIVERSE IS A BIG CASINO

"Italic": Excerpt pseudoscience speech or other YouTube videos

[in brackets]: sound effect

OPENING **********

[intro - bass]

Lu - Imagine that you are participating in a game in which there is a white lamp and a red lamp, and one of them will light up, but you don't know which one. Then the red one lights up first... then the white one... and then the red one again. And the question is: which lamp will light up next?

Leo - A few years ago, in the 1960s and 1970s, some studies of this type were carried out in an area of research called probability learning. The objective was to understand how some animals, in their natural habitat, made decisions that were basically probabilistic, that is, they could either go right or wrong.

Lu - For example, in a scarcity scenario, when should a group of birds leave for a new area in search of food? It may very well happen that they find a new place with more food, but it may also happen that they give up the little food they had for another place with even less food. So do the birds learn over time how to make better bets or do they always follow the same instinct?

Leo - Some scientists started to do some experiments similar to the one that Lu mentioned before: they had two lamps, one red and one white, and the animals had to guess which one would light up, and they were rewarded when they got it right. Well, it wasn't exactly like that, but the premise is the same. But the mechanism that controlled these lamps was random, as if it were decided by a coin toss: for heads, the red lamp turned on, for tails, the white lamp turned on. But it wasn't heads or tails with a common coin, it was a biased coin, which had one side heavier than the other: so the chance of getting heads, that is, turning on red, was 70%, compared to 30% of chance of getting tails and turning on the white light. But this mechanism was not openly exposed, the only thing the animals saw were the lights turning on.

Lu - Well, if the experiment is designed like this, then there is an optimal strategy, which maximizes the number of right guesses. In other words, if the animals used this strategy they would have the greatest possible chance of success. Do you already know what this strategy is? The idea is: [radio] always bet that the red lamp will light up.

Leo - It makes sense, because if the pattern that governs the lamps is random, the best thing you can do is always bet on the outcome that has the greatest chance of happening. Always guessing the red lamp, the average success rate is 70%, which in this case is the highest possible.

Lu - Now, do you know what's curious? Not-so-intelligent animals, like pigeons and goldfish, usually understand this and, after a few rounds, learn that one should always guess red. And do you know which animal often doesn't do so well in this type of experiment? The human beings.

Leo - Human beings, who are theoretically so smart and all, are not satisfied with getting things right only 70% of the time, as pigeons learn to do. We want 100% of success. And in this, we often end up convincing ourselves that there is an amazing pattern behind the behavior of the light bulbs, that is, that there is a secret that contains the key to success and that can be deciphered.

Lu - But on certain occasions, like in this particular experiment, this is simply not possible, because the lighting of the lamps is chosen randomly. And it turns out that, in these cases, human beings perform worse than goldfish.

Leo - We wanted to start this episode talking about this experiment because it illustrates well a characteristic of human beings that contributes to the spread of

mysticism and pseudoscience: human beings have a huge difficulty to believe that some events are simply random.

Gláucia - And by chance, this also has a lot to do with quantum theory. I'm Gláucia Murta, physicist and researcher at the University of Düsseldorf in Germany.

Lu - I'm Luciane Treulieb, journalist and science communicator, at the Federal University of Santa Maria.

Leo - And I'm Leonardo Guerini, mathematician and professor at UFSM. [bass] This is the podcast O Q Quântico. In the first block of today's episode, we talk about why these things that we like to call random, like coin toss, in a certain sense are not really random. In block two, we tell you a little more about quantum measurements and why these are truly random. And to finish, in block 3 we talk about cryptography and what it has to do with all of this. Come with us as we start episode 6: The universe is a big casino.

[cat]

BLOCK 1: CLASSICAL DETERMINISM **********

[radio static]

> *"So I would say to people here, open up, so we can open up to the new, open up to possibilities, that quantum physics is the physics of possibilities."*

[radio static]

Leo - Quantum physics is the physics of possibilities. We found this sentence that you just heard on a pseudoscience YouTube channel. This is another one of those cases in which the sentence itself makes sense and with some goodwill we can say that it is scientifically correct... but not for mystical reasons.

Gláucia - But when we talk about possibilities, this is a little vague. A more accurate way of talking about these things is to say that quantum physics is the physics of probabilities.

> **Gabriela Barreto Lemos:** I say this because the study of probability is essential to understanding quantum mechanics. So, if we don't understand probability, nothing done.

Gláucia - This is Gabriela Barreto Lemos, Professor at the Physics Institute at the Federal University of Rio de Janeiro. Probability is a way to quantify each of the possibilities that may occur in a certain event. Perhaps the simplest example we can think of is flipping a coin, in a coin toss. In this case, considering that we have a normal, symmetrical coin, with a regular shape and weight, we usually say that the probability of getting heads is 50% and the probability of getting tails is also 50%.

Leo - In other words, when we flip a coin, we generally don't know what the result will be. So assigning a probability to each of the possible outcomes is a way for us to try to say something about what will happen.

> **Gabriela Barreto Lemos:** And if we don't understand probability, it's not just that we won't understand quantum physics, no, we won't understand the world, right?

Leo - We agree. In fact, there are a lot of things in the world that you only understand if you understand a little about probabilities.

Lu - Here we can mention several important things in our daily lives that involve probability: for example, there is the weather forecast, which indicates the chances of rain tomorrow. Another example is that several drug efficacy tests are carried out to estimate the probability for a person to recover, or be cured. And yet another very relevant topic, which we heard a lot about during the pandemic, are the probabilistic models, which in that case were used to estimate the number of people infected by the virus if this or that prevention policy were put into practice…

Leo - And many of these topics have even generated controversy precisely due to distortions about what probability means, what probabilistic models are and how to interpret them.

Gláucia - But returning to the concept of probability, all areas of science that involve experiments necessarily include statistical studies, where the objective is often to estimate the probabilities of the model in question being right or wrong. So probability really is a central point in science.

> **Gabriela Barreto Lemos:** There's no way you can talk about scientific development without talking about probability, right?

Lu - Okay, so when we flip a normal coin, we say that the probability of getting heads is 50% and the probability of getting tails is also 50%. But at the beginning of the episode, in the description of the blocks, we already said that a coin toss was not something really random. But why?

Gláucia - Well, before we answer that, we first need to define what it means to be random. This is already a difficult task, and there is more than one possible definition. But here in the episode, we want to differentiate two types of randomness: the first type is the randomness that arises due to our lack of knowledge of all the variables that influence an event, and this we will call [eco] apparent randomness. We will soon give examples of this. But on the other hand, there is also the [eco] intrinsic randomness, that is, that involves events that have no way of being predicted with certainty, even if we know everything that is possible to know about that event.

Leo - Let me try to give some examples using sequences of numbers. If we just keep repeating [radio] 0, 1, 0, 1, 0, 1, 0, 1… this doesn't seem like a random sequence, right? I'm just alternating between 0 and 1 one at a time, so it's really easy to predict what number will come up next. Now if I said [radio] 3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5... and continued, perhaps, at first glance, this seems random. But if you identify that these are exactly the first numbers that appear in the decimal expansion of the number pi, that's it, you'll see that they are not random. If you want to know what is the next number that will appear in this list, you just need to look for the number pi on the internet and see which number comes after the last one I mentioned. In other words, there is a formula that predicts what the next number is.

Lu - Hmmm okay. But then, back to the coin toss… you were saying that the outcome might not be random. So does that mean there is a formula that predicts whether it will come up heads or tails?

Leo - So, at first glance it may seem strange, but that's exactly what we're saying. But it's a little different from this example of the pi, in which there was already a list ready with the numbers that were going to come out. In the case of the coin toss, what explains the situation is more physics than mathematics.

Gláucia - Think about it: when I flip a coin, I'm applying a certain force at some point on that coin, which makes it spin in the air. So why is it possible, in principle, to predict what will happen? Because if I know precisely [plim] the dimensions of that coin, [plim] the density of the material, [plim] the force I applied, [plim] the exact point

where this force was applied, [plim] air resistance and [plim] the force of gravity... if I know all this, in principle classical physics tells me how to calculate the trajectory of this coin. They are simply the laws of classical mechanics.

Leo - I may even try to flip the coin in a specific way to manipulate the outcome. For example, an extreme case would be to make the coin not rotate once, that is, it goes up in the air and then comes down with the same side facing up, all the time.

Gláucia - Yes, and we're not saying that doing this is easy, right? Quite the contrary, unless we throw the coin in a somewhat cheating way, as Leo mentioned, simulating the movement of the coin can be a super complex problem. But, in principle, it is possible. If I know this coin well and know exactly what my interaction with it was, there is no chance for luck. The coin will follow a very determined movement. And, theoretically, we can always calculate which side will end up facing up.

Leo - This reasoning is not just restricted to coins. It's the same thing when we roll a dice, or when we see those roulette wheels in casinos. All of these objects, like any other object in our daily lives, move in a deterministic way, that is, in a way that is completely determined by the forces that act on them. The probabilities arise only due to our lack of knowledge of all the possible variables that can influence the event, which means that we cannot know the result with 100% certainty.

Lu - So what you're saying is that a coin toss is not decided by luck. It is decided by physics.

Leo - Essentially, yes. So if you ask me if a coin toss is random, from the point of view of the physical process that is happening, I answer no, because in principle you can predict what will happen.

Gláucia - Now, even if I do all the calculations in advance, it is almost impossible to put this into practice: it's difficult to measure the exact force I have to use and it's difficult to hit the exact spot where I should hit the coin. This is why, in general, we cannot predict the result. And that's where these probabilities of a 50% chance of heads and a 50% chance of tails come from.

Leo - That's why, for all intents and purposes, there's no problem using a coin toss to decide who starts taking penalties in a football match, for example. But it's important to make it clear why: a coin toss may be an impartial way of deciding things, but not because it's something intrinsically random, but because of our ignorance about the

physical conditions of the problem. If you remember what we said earlier, this is exactly what we called apparent randomness. If we precisely controlled all the variables that Gláucia mentioned before, air resistance, the force applied to the coin, etc., we would always be able to make the coin land facing heads, for example.

Lu - So does this mean that we just can't enter a casino and become millionaire because we don't know how hard the ball was thrown onto the roulette wheel? Is that right?

Gláucia - Yes, you would also have to know the force with which the roulette wheel was spun and other details, but basically that. We like to say that these things are decided by luck, but if everything depends on physics, what does luck have to do with it? And another question that I think is cool is: are there other seemingly random processes that, after a lot of training, we can control? And, thinking about it, we realize that this is exactly how magicians and illusionists do most of their tricks.

Leo - True, just as we are talking about coins and heads or tails, we can talk about cards and shuffling. There are several ways to shuffle cards in a deck, but two of them are the most popular. The first is to take the deck in one hand and with the other simply pick up blocks of cards and pass them to the end of the deck.

> [Diaconis] *“People shuffle cards... They shuffle cards this way.”*

Leo - Another way, which is more visually beautiful, is called cascade: we divide the deck into two piles, hold one in each hand, and release the cards so that the two piles end up interspersed.

> [Diaconis] *“Cut 'em about in half; you go like that; you push 'em together, right.”*

Leo - Normally, when someone shuffles the cards this second way, there are two things that apparently are left to luck: the first [plim] is the number of cards in each hand, when we divide the deck into two piles, and the second [plim] is the way the cards are interspersed.

Gláucia - Now, what a person can do is practice this shuffling until they reach the point where there is no longer any uncertainty in these two moments: we can practice cutting until we are able to divide the deck into two piles with exactly the same number of cards and you can train the cascade movement until the cards are

interspersed exactly one by one (one card from one hand, one card from the other, and so on). If you can do this, you know exactly the final order in which the cards will be placed. Thus, this process is deterministic and the shuffling becomes just theater.

Leo - One person who has studied these things, both from a trick point of view and from a scientific point of view, and who I'm a fan of, is Persi Diaconis. He is a well-known American mathematician, who has been a professor at Stanford University for a long time. But, when Diaconis was little, he knew exactly what he wanted to be: his dream was to be a magician. So, when he was 14, he ran away from home to pursue the life of a traveling magician, learning and even inventing a lot of tricks, especially with cards.

> [Diaconis] *“So, for example… take a guess, what do you think the top card is?”*
> [Interviewer] *“Six of spades.”*

Gláucia - In fact, these excerpts that we have heard are from Persi Diaconis in an interview for the YouTube channel Numberphile. When you have talent for it, every form of card shuffling ends up being an opportunity to deceive people, in the best sense of the word. The idea is always the same: to take advantage of this impression that we have that the world is random, when, in fact, the sequence of movements and choices that are happening is completely determined by the magician.

Leo - Diaconis had that kind of talent, but he also had a lot of curiosity. He started to ask himself some questions similar to the ones we already mentioned here in the episode: [radio filter] [plim] If we always flip a coin in the same way, will the result always be the same? [plim] How many parameters are needed to describe a coin toss from a physical point of view? [plim] What is the best way to shuffle cards, from a probabilistic point of view?

> [Diaconis] *“A question is, how many times do you have to shuffle a deck of cards to mix it up?”*

Gláucia - And that's how he ended up becoming a mathematician specialized in probability. Among his various works, he developed, together with his university's engineering department, a “heads or tails machine”, in which the coin was always thrown with the same force, always applied in the same place. Therefore, the result was always the same.

Leo - Another cool result is that Diaconis showed that in fact the probabilities of a coin toss are not necessarily 50-50, but rather that there is a 51% chance of the result being the face that was already facing up at the time of the toss. In other words, if you are going to decide something by flipping a coin, ask for “heads” and flip the coin with the “heads” side facing up, because this way your chance of winning will be a little higher.

Gláucia - But the most famous result of Persi Diaconis is about shuffling. In 1992, he demonstrated a mathematical theorem that says that seven cascade-type shuffles are enough to bring the cards very close to the most random way possible.

[Diaconis] *“And there's a practical answer. The answer is about seven.”*

Gláucia - In other words, after seven shuffles, the order of the cards will be completely messed up. Six shuffles are not enough and an octave shuffle doesn't make much difference anymore, seven is the right number! That is, of course, if the person doing the shuffling is an amateur, introducing those uncertainties that we talked about before, when cutting and mixing the cards. Just for comparison, if you shuffle the cards in the other more common way, by blocks, you would need 10 thousand shuffles to obtain the same result.

Lu - In a recent interview to a Portuguese newspaper, Diaconis was asked whether randomness really exists or is it just an invention by mathematicians to represent things they do not control. Do you know what his response was? He said: [radio] “After thinking about it for 50 years, and now forgetting about quantum mechanics, my best guess is that randomness is a statement about a given person's knowledge. It is not a statement about the outside world”.

Gláucia - Here you may have noticed that Diaconis mentions quantum theory in his answer, and we'll get to that in a moment. Before that, I just wanted to say that if we take this way of thinking to its ultimate consequences, we arrive at an idea called [eco] Laplace’s demon. This is an anecdote created by Pierre-Simon, the Marquis de Laplace, who was a French mathematician who lived between the 18th and 19th centuries.

Leo - The idea is more or less like this: if any person, and it would have to be someone with supernatural abilities, that's why we talk about a devil, but if any person knows the precise position and speed of each object in the universe at a

given instant of time, say, yesterday at noon, then, from this, they can predict the movement of anything in the universe at any time, from the past or the future, using the laws of classical physics.

Gláucia - In Laplace's words: [radio] “For such an intellect, nothing would be uncertain, and the future, as well as the past, would be present before his eyes.” In other words, this story shows us that the laws of classical mechanics describe the universe as if it were a clock, where one gear drives another gear, which drives another, and so on, in a completely predictable way. From this point of view, if we have the impression that the universe is random, it is only because we do not have enough information about it, or because we do not know the entire mechanism of the clock, or because we cannot make the calculations.

Leo - Well, of course this argument is quite provocative. Thinking like this is basically saying that everything in the universe, including people and other living beings, comes down to billiard balls colliding with each other, doomed to follow the marked paths. But other than that, you might think that natural phenomena, at least those involving inanimate objects, work like this.

Gláucia - Laplace's demon was an idea that came up in the 19th century. Since then, a lot has changed. [congas] In particular, an event that seriously blew this deterministic conception of the universe was precisely the emergence of quantum theory. This is because, unlike a coin toss or a shuffling of cards, quantum theory, at least as we know it today, is intrinsically probabilistic.

[cat]

BLOCK 2: QUANTUM PROBABILISM **********

> **Barbara Amaral:** So, I think the central question, which I think is the most difficult thing for us to make this transition from thinking about classical systems to thinking about quantum systems, is: what does it mean to measure something?

Leo - This is Bárbara Amaral, who is a Professor at the Department of Mathematical Physics at the University of São Paulo and a researcher in quantum information theory. As Bárbara said, for us to understand the randomness that arises in quantum theory, we first need to understand what a measurement is.

Gláucia - Most of the time, making a measurement, or an observation, of the system you are studying is something so simple that we do it without even paying much attention. For example, think again about the coin toss. How do we check if a coin is heads or tails up? Well, we just look at it. That is, in this case, the measurement is to look at which side of the coin is facing up. No big deal, right? But it is important to note that this measurement is only possible because there is a physical interaction with this coin.

Leo - Again, it's that story that has already appeared here on the podcast a few times: we only see something when there are photons, that is, light, which are reflected by that something and then captured by our eyes. So, in the case of a coin toss, there needs to be this interaction through photons so that we can see the coin and measure whether it is heads or tails facing up.

Gláucia - But we don't usually pay attention to these interactions. This happens mainly because this type of measurement, in practice, does not influence the result I obtain. In other words, if I look or if I don't look at the coin, it won't change which side is facing up. Regardless of my measurement, the face that is up is well defined.

> **Barbara Amaral:** In our classical world, we always think that objects, physical systems, have magnitudes, properties that are well defined, and a measurement, the act of measuring, is a way that we found to reveal this value, which was already there, well-defined, of that system.

Leo - In other words, when we make measurements on everyday objects, whether it's seeing the result of a coin flip, or measuring the speed of a car, or measuring the temperature of a body. For all of them, we need to interact with the respective object that is being measured, but it is a negligible interaction, which does not affect either this object or the measurement result in any way.

> **Barbara Amaral:** So, this notion is the notion of measurement that we have in our daily lives, from classical physics and it is very difficult for us to think that there is anything other than that, right.

Gláucia - But when we are measuring quantum systems, the story is different. As we said in the last episode, the quantum properties of a system are super sensitive and unstable, and even the interaction with a few photons already causes changes in the system. So, just to make an analogy, if we toss a quantum coin, just looking at the result obtained could change the state in which that coin was.

Lu - This also reminds us of the situation with electrons in the double slit experiment a few episodes ago, in which just by looking at the electrons we changed their behavior, right?

Gláucia - Yes, well remembered. In addition to being very unstable, another difference between the quantum world and the classical world is that, in the quantum world, there are superposition-type phenomena. So imagine that, before being measured, this quantum coin was isolated from everything around it, and in a state of superposition of heads and tails. To measure this currency, we need to interact with it in some way, and this interaction ends isolation. From then on, the, in quotation marks, “quantum natural selection” that we discussed in the last episode ends the superposition and causes the coin to assume one of the classical states: just heads or just tails.

Lu - Wow, so now everything is mixing up, right? All discussions from all episodes are appearing.

Leo - Wait, because now we've reached the main point of this episode. When we measure the quantum coin and it assumes one of these states, heads or tails, the theory itself already describes this process as something random, that is, as something that cannot be determined with 100% certainty. So that's a big contrast with the classic coin, the one from our daily lives. In the last block we were saying that a normal coin only results in 50% heads and 50% tails because we don't know all the details of this coin and the way it was tossed. But in quantum it is different.

Lu - You guys are talking about quantum coins all the time, but what is it? It's not a very small coin, right?

Leo - It's just an analogy. Just as a normal coin only has two sides, heads and tails, there are measurements in quantum systems that can also only give two results, such as measuring the polarization of the photon, for example, which can only result in horizontal or vertical. So measuring photon polarization is analogous to flipping a coin with a quantum coin.

Gláucia - The difference is that, according to quantum theory, even when we know everything that can be known about this photon, the result of this quantum coin toss remains unpredictable [blunt]. It's as if the quantum world were the only cheat-proof casino, with everything really being decided by luck [casino].

Lu - Wow, how crazy.

Leo - Well, quantum theory says that in general, there is no way for us to know in advance what the result of a quantum measurement will be, the best we can do is calculate the probability of obtaining each result. Now, it's not hard to imagine that this type of statement bothers a lot of people. In fact, this is another aspect of quantum that forces us to leave our comfort zone. We, human beings, are used to looking for patterns in everything, and we deal very poorly with randomness, as that red and white light bulb experiment that we talked about at the beginning of the episode showed.

Gláucia - So when you hear that quantum theory is intrinsically random, you might doubt it. Maybe you think: [radio effect] “ok, so the theory can’t predict what the results will be, but that doesn’t mean they are actually unpredictable, right? Eventually science will advance and understand this better.”

Leo - This distrust is quite natural, and dominated much of the philosophical discussions about the theory in the first half of the 20th century, which were led by scientists such as Max Born, Wolfgang Pauli, Werner Heisenberg, Erwin Schrödinger, among others.

Gláucia - And it also had important contributions from figures such as the German mathematician and philosopher Grete Hermann, whose work unfortunately did not gain due visibility in the history of science. Well, but at the heart of these discussions we also have the famous debates between Einstein and Bohr.

Leo - As we already said here, Einstein is one of the great critics of quantum theory, and it was thinking about this probabilistic nature of the theory that he stated another of his famous phrases: [radio effect] “God doesn’t play dice.”

Gláucia - What Einstein meant is that, despite quantum theory being correct, perhaps this probabilistic character indicates that the theory is incomplete. In other words, perhaps there are other elements, other factors, that we do not yet know, but that influence quantum measurements, making this probabilistic character appear.

Leo - In 1935, a scientific article was published on this topic and became known as EPR, due to the initials of its three authors: Einstein, Podolski and Rosen. In this

article, they develop an argument to demonstrate that quantum theory was incomplete, and that therefore its randomness would only be apparent.

Gláucia - Later, it became clear that the hypotheses made in the EPR article were not that obvious. But that doesn't change the fact that it had a huge scientific impact, and even marked the beginning of a new area of research. Following the line of reasoning of its authors, if quantum theory was incomplete, what we should try to do is to complete the theory. Here, Bárbara Amaral again.

> **Barbara Amaral:** So we can try to think about completing quantum physics by thinking that there are additional parameters, beyond those we already know, that would allow us to eliminate these probabilities from the conversation.

Gláucia - So, we could try to build a theory that could answer everything deterministically, that would be an improved version of our current theory, like a quantum theory 2.0.

Leo - These additional parameters that would complete the theory can be called a [eco] completion. But how to achieve this completion? And a key point that appears in these discussions is the term “local”.

Gláucia -To understand what something being “local” means, let’s go back to the coin toss with the classical, normal coin. In order to be able to determine the result of the coin toss, we only need to know - and this only is in quotation marks, because it is already quite a lot - the properties of the coin and the force applied to it. I don't need to know what's happening on the other side of the planet, or in other very distant points, for example. Because of this, we can call this classic coin toss a local phenomenon, because it is enough to know the physical system that we are measuring, which is the currency, and what happens around this system, for everything to be determined.

Leo - But this is a classic coin. The next question now is: can we assume that quantum systems also behave locally? In other words, does it make sense to assume that everything that affects the measurement of an electron is there, close to that electron?

> **Barbara Amaral:** But then this assumption, along with other assumptions that are completely natural, they end up making predictions that are not consistent

with what we see in the laboratory, when we make measurements in quantum systems.

Gláucia - In other words, what we see in the laboratory is that the attempt to complete quantum theory, assuming that systems depend only on what happens next to them, along with other very natural assumptions like Bárbara said, this attempt fails! [awnn] Then we come to another peculiar characteristic of quantum theory: non-locality [blunt] which, in a simplified way, says that the results of a measurement cannot be pre-determined by any variable that could have influenced the system.

Barbara Amaral: If we want to reproduce what we observe in the laboratory with quantum systems, using this classical intuition, we arrive at a contradiction. And as we know that the experiments are very well done and are correct, we have to conclude that we cannot explain these experiments with classical intuition.

Leo - Experiments of this type appear in the research of physicists Alain Aspect, John Clauser and Anton Zeilinger, who recently won the Nobel Prize in Physics, in 2022. They led several experiments in the 70s, 80s and 90s, exploring photons with another of the counterintuitive aspects of quantum, which is the [eco] entanglement, which we will talk more about in the next block.

Gláucia - And one of the consequences of these experiments was to obtain robust evidence that it is not possible to complete quantum theory, at least when we assume very natural hypotheses. It is true that this evidence does not entirely rule out other counterintuitive ways of completing quantum theory and making it deterministic. But it shows that, in order to have a chance of this happening, it would be necessary, for example, to take into account information that is possibly very distant from the quantum system that we are measuring. [congas] In other words, in order to have any chance of quantum theory seeming deterministic to you, you would have to be a kind of Laplace's demon, who knows everything about every point in the universe.

[cat]

BLOCK 3: QUANTUM CRYPTOGRAPHY ******** **********

Lu - Well, so these experiments by the Nobel Prize winners that you commented on basically show that, for all intents and purposes, quantum systems do have inherently random behavior. But then does this quantum randomness have any practical application?

Gláucia - Yes! This randomness is, for example, one of the pillars of quantum cryptography, which is the area where I do research.

Lu - I know that encryption has to do with exchanging messages securely, like there is encryption in internet banking and also in WhatsApp messages, right?

Gláucia - Well, cryptography studies techniques so that we can communicate securely, exchanging messages in such a way that they cannot be read by third parties. So the idea of encryption is to use a cipher, which is nothing more than a rule to encrypt, that is, to modify the message so that it becomes unintelligible, and then only a person who also knows the details of the cipher can decipher that message.

Leo - There are several famous ciphers that have been used throughout history, such as the Caesar cipher that was used by Julius Caesar in the 1st century BC, in which the idea was simply to translate the position of the letters in the alphabet. For example, if I choose to do a 2-position translation, then A becomes C, B becomes D, C becomes E, and so on. Another much more sophisticated example is the Enigma machine, which was used by the German army in the Second World War and which involves a much more complicated and dynamic algorithm to encrypt the message.

Gláucia - And perhaps, when you were a child, you already used a famous cipher in Brazil, which is the language of P! Do you know it, Lu?

Lu - p-Co p-nhe p-ço! [‘I know!’ in P language] Okay, but so far I can't imagine how quantum helps here.

Gláucia - Well, the problem is that all these ciphers, although some are very ingenious, like the ones we currently use to encrypt our emails, internet banking, etc., in principle they are breakable!

Leo - And being breakable means that if we use a certain cipher to encrypt several messages, one day someone may be able to decipher the secret of our cipher. In

fact, there is a very cool book, The Code Book, by author Simon Singh, which tells the story of the struggle between cryptographers and hackers throughout history.

Gláucia - Think about the P language. If you have an adult who is very attentive, maybe after listening for a while they will be able to understand what is the rule used to mess up the message and from then on they will be able to understand everything the children are saying. So one way to have unbreakable encryption is for me to modify my cipher rule every time I send a new message.

Lu - How can I modify the cipher rule?

Gláucia - Well, we can use the Caesar cipher as an example. In principle, I can think of the Caesar cipher as follows: I choose a number between 1 and 26, which is the number of letters in the alphabet, and this number will tell me how many positions I need to shift the alphabet to encrypt the message. But the idea now is: for each letter in my message I will draw a different number to define the shift of that letter.

Lu - Let me see if I understood, so if I want to encrypt the word OI [Hi] I need to draw two numbers, for example if I draw 3 and 1 then the O moves 3 positions and becomes R and I moves 1 position and becomes J. Hence the encrypted word OI becomes RJ, is that it?

Gláucia - Exactly, and now as each letter was encrypted using a number that was chosen randomly, there is no general rule to be discovered. So if you send me this encrypted message, the only way I can read it is if I know what numbers you used to encrypt it. And if these numbers are really random, there is no way for me or anyone else to discover them unless you tell me.

Lu - I think now I see where quantum randomness is coming into play...

Leo - Well, if you use the randomness that comes from measurements in quantum systems, which is an intrinsic randomness and not just apparent, to choose the numbers you use in your cipher, your message is completely safe! But there's a catch. As Gláucia said, for the other person to be able to decode your message, you need to find some way to send these random numbers to them.

Gláucia - In cryptography, we call these random numbers that you use in your cipher the [eco] secret key, so what Leo described is called secret key distribution, which is

a central problem in cryptography, since people would basically have to meet to exchange these keys.

Lu - Do you mean to meet in person? Seriously?

Gláucia - In principle yes. In fact, this event, which is called a key ceremony, is still used today when it comes to encrypting very sensitive information, such as communication between banks and credit card companies, for example.

Leo - So quantum, in addition to providing the necessary randomness, at the same time solves the problem of distributing these secret keys. The idea is to use measurements in quantum systems to generate this secret key remotely, without the need for the parties to meet.

Gláucia - But for this we need an essential ingredient: entanglement, which is one of those strange quantum properties that appeared in block 2, when we talked about the experiments that led to the 2022 Nobel Prize.

Leo - We are not going to go into this phenomenon in depth, which has several very interesting subtleties and consequences, but to try to give you an idea, let's go back to the example of coins. Imagine that I split a coin in half, so that each half has one face, then I put each of these halves in an envelope and hand one of these envelopes to you, Lu, and another envelope to Gláucia. When you open your envelope and see that you got the heads face, what will be in Gláucia's envelope?

Lu - If I ended up with heads, Gláucia must have ended up with tails.

Leo - Exactly. So this is an example of correlation, the coin halves you received are not just any halves, they are not independent of each other, we say they are correlated. As we are talking about two sides of the same coin, the side you receive and the side Gláucia receives have to be opposites. So when you look inside your envelope, you also deduce what is in Gláucia's envelope.

Gláucia - But so far this is just a classic correlation. Now, if we use a quantum system to play the role of this coin, if instead of talking about two halves of a coin we talk about two photons, for example, we have these strange quantum properties at our disposal. In particular, we can use a pair of entangled photons.

Leo - The entanglement, in very simplified terms, is a superposition of correlations. Speaking in terms of a coin, it's as if each of you were given half of the coin again, only it's neither the ‘heads’ half nor the ‘tails’ half, because what we have is a superposition of the case in which Lu receives heads and Gláucia receives tails and the opposite case, in which Lu receives tails and Gláucia receives heads.

Lu - Wow, this is difficult, I can't visualize it.

Leo - Yes, it's difficult to visualize, but in other words, it's as if each of you had half of a coin in superposition of heads or tails, but in a correlated way. Whenever you measure, or observe, your half, and get 'heads', Gláucia will get 'tails' on her half. And whenever you measure it and find ‘tails’, Gláucia will find ‘heads’ in hers.

Gláucia - This definition of entanglement, as a superposition of correlations, does not make clear all the nuances and impressive consequences that this phenomenon generates. But, this already shows us that the entanglement of coins guarantees that at the moment we open our envelopes, which is the analogue of measuring the system, there is a 50% chance that Lu will have heads and I will have tails and 50 % chance that Lu will have tails and I will have heads.

Leo - So, if Gláucia and Lu are far from each other and want to choose between 0 or 1 at random, they can use two entangled photons to act as the two halves of the coin. So they can agree, for example, that the result will be 0 if Gláucia gets heads and 1 if Gláucia gets tails. Gláucia only needs to measure her half of the coin, her photon, and Lu will always know what Gláucia's result is because it will be exactly the opposite of the result of her photon.

Gláucia - And remembering that the photon is a little package of light, so when Leo talks about sending entangled photons to two distant points, here we can simply think about sending a light signal, for example, through an optical fiber. The big challenge is how to manipulate this signal so that it has the properties we need, and find ways to fight against decoherence, so that the signal reaches its destination without losing its quantum properties.

Leo - So in short, quantum theory, through entanglement, gives us the two essential ingredients for cryptography: [plim] the randomness to ensure that no one has information about the secret key and [plim] the correlation to make that two people far away from each other obtain the same key.

Lu - That's cool, but what is the status of that? Is this idea of quantum cryptography still only in theory or are there services and products available today?

Gláucia - Quantum cryptography, or more specifically quantum secret key distribution, is one of the most mature quantum technologies we have at the moment. There are several startups that offer products ranging from components to complete encryption systems, such as the Swiss startup ID Quantique, which has been on the market for over 20 years. And in the last two decades, several quantum cryptography networks, covering small distances, have been implemented in different places around the world, and there are also some initiatives emerging in Brazil, such as the project Rede Rio Quântica.

Leo - An interesting point is that these quantum networks will make use of existing communication infrastructures, such as optical fibers and satellites.

Gláucia - Indeed, and we have quantum communication being implemented even using satellites, which allows us to cover much larger distances. And China is the great leader in this technology. In other words, it has been a long time since this technology got off the ground and this was only possible due to advances in our understanding of quantum theory.

[cat]

CLOSING **********

Lu - Ok, after all this talk about probabilities, shuffling, entanglement and quantum cryptography, my role here in the podcast is to ask: why did we bring up these discussions and what do they have to do with pseudoscience?

Leo - So, we decided to dedicate an entire episode to talking about the probabilistic nature of quantum theory precisely because it is very difficult for human beings to accept that something is essentially probabilistic. It just seems like we don't really understand these phenomena and that the theory needs some complement. And when pseudoscience is faced with this situation, it has a simple way out: for pseudoscience, what is missing in quantum theory, the piece that fits perfectly and that scientists are too prejudiced to admit is the [eco] human consciousness.

[radio static]

“Quantum physics only calculates possibilities, but if we accept this, then the question immediately arises: who or what chooses among these possibilities to bring about the actual event of experience? So we directly, immediately see that consciousness must be involved.”

[radio static]

Gláucia -These lines were taken from the film What the Bleep Do We Know!?, from 2004. We have already commented in past episodes that this film illustrates well how much the ideas of quantum theory are distorted and transported to another context. And the concepts that we brought up here in this episode, such as probabilities and the possible incompleteness of the theory, are also frequently explored by pseudoscience.

[radio static]

“All these things are nothing more than possible movements of consciousness. I am choosing moment by moment from these movements to bring my true experience into manifestation.”

[radio static]

Leo - You can see that these lines resonate with the points we discussed here in the episode, it's not like they were invented out of nowhere. [bass] So, deep down, can't they make any sense? After all, what is the relationship between quantum theory, as we know it today, and the human consciousness? That's the topic of our next and final episode.

[cat]

CREDITS **********

Leo - On our website, you will find articles about learning probability by animals, mathematical articles by Persi Diaconis, a video of him talking about card shuffling and the seminal article by the EPR trio that discusses the completeness of quantum theory. In this episode you heard excerpts from our interviews with Gabriela Barreto Lemos and Bárbara Amaral. We also used excerpts from the YouTube channels Tiago Benevides, Numberphile and the 2004 film What the Bleep Do We Know!?.

Gláucia - If you liked the episode, you can help us by recommending the podcast to a friend who is interested in the topic. Also follow O Q Quântico on Instagram @oqquantico and be sure to rate the podcast on your favorite podcast platform.

Lu - Q Quantico is presented by me, Luciane Treulieb, Glaucia Murta and Leonardo Guerini.
In addition to the three of us, Samara Wobeto and Vitor Zuccolo complete the team of podcast producers
The script for the episode is by Leonardo Guerini and Gláucia Murta, with contributions from me and Samara Wobeto
The project was conceived by Leonardo Guerini and Gláucia Murta
The script consultancy is carried out by the team from the Ciência Suja podcast
Sound editing is by Leonardo Guerini
The mixing is by Felipe Barbosa
The recording support is by Pablo Ruan
The original music is by Pedro Leal David
and the visual identity and cover illustrations are by Augusto Zambonato
The person who takes care of our social media is Milene Eichelberger and
Our website was developed by Daniel Carli

Glaucia - O Q Quântico is produced within public universities. We had the support of several employees from our institutions who contributed to the podcast reaching its final format. We are grateful for the financial support from the National Council for Scientific and Technological Development (CNPq) and the “Matter and Light for Quantum Computing” cluster of excellence in Germany. And the support and infrastructure of the Heinrich-Heine-Universität Düsseldorf and the radio stations of the Federal University of Santa Maria.

Thanks for listening and see you in the next episode!

[transition - cat]