Jornada 3

WORKSHOP CRIPTOACTIVOS

CARTA FINANCIERA
IDEAS CONCRETAS

Contenidos

Tercer Día:
Key Take Aways

- U7. Minería
- U8. Renta Fija con criptomonedas
- U9. Aspectos Prácticos

CARTA FINANCIERA
IDEAS CONCRETAS

7 Minería

Minería de Criptomonedas

¿Qué es la minería de criptomonedas?

- Para mantener las blockchain es necesario contar con una red de computadoras al servicio de esa red.
- Se llama minería al proceso por el cual se pone al servicio de la red poder computacional y se obtienen a cambio (como recompensa) tokens nativos de dicha red.
- Por eso, la minería es una manera de obtener tokens.
- No todas las criptomonedas pueden ser minadas. Típicamente se pueden minar los tokens que utilicen un protocolo “Proof of Work” o similar (como Bitcoin o Ethereum) para validar las transacciones de la red.

Minería de Criptomonedas

La minería en Bitcoin (I)

Las transacciones en Bitcoin se validan mediante el protocolo “Proof of Work”.

Es decir, para validar las transacciones y formar un nuevo bloque en la cadena cada nodo intenta resolver un problema matemático complejo.

Cuando un nodo resuelve el problema y forma el nuevo bloque en la blockchain recibe una recompensa en Bitcoins por su trabajo. Esta es la manera en que los Bitcoins son creados. A este proceso se lo llama “minado” de bitcoins, en analogía con el oro.

Recordar: Poner poder computacional al servicio de la red tiene un costo y es por ello que quienes hacen que bitcoin funcione deben recibir algo a cambio.

La minería en Bitcoin (II)

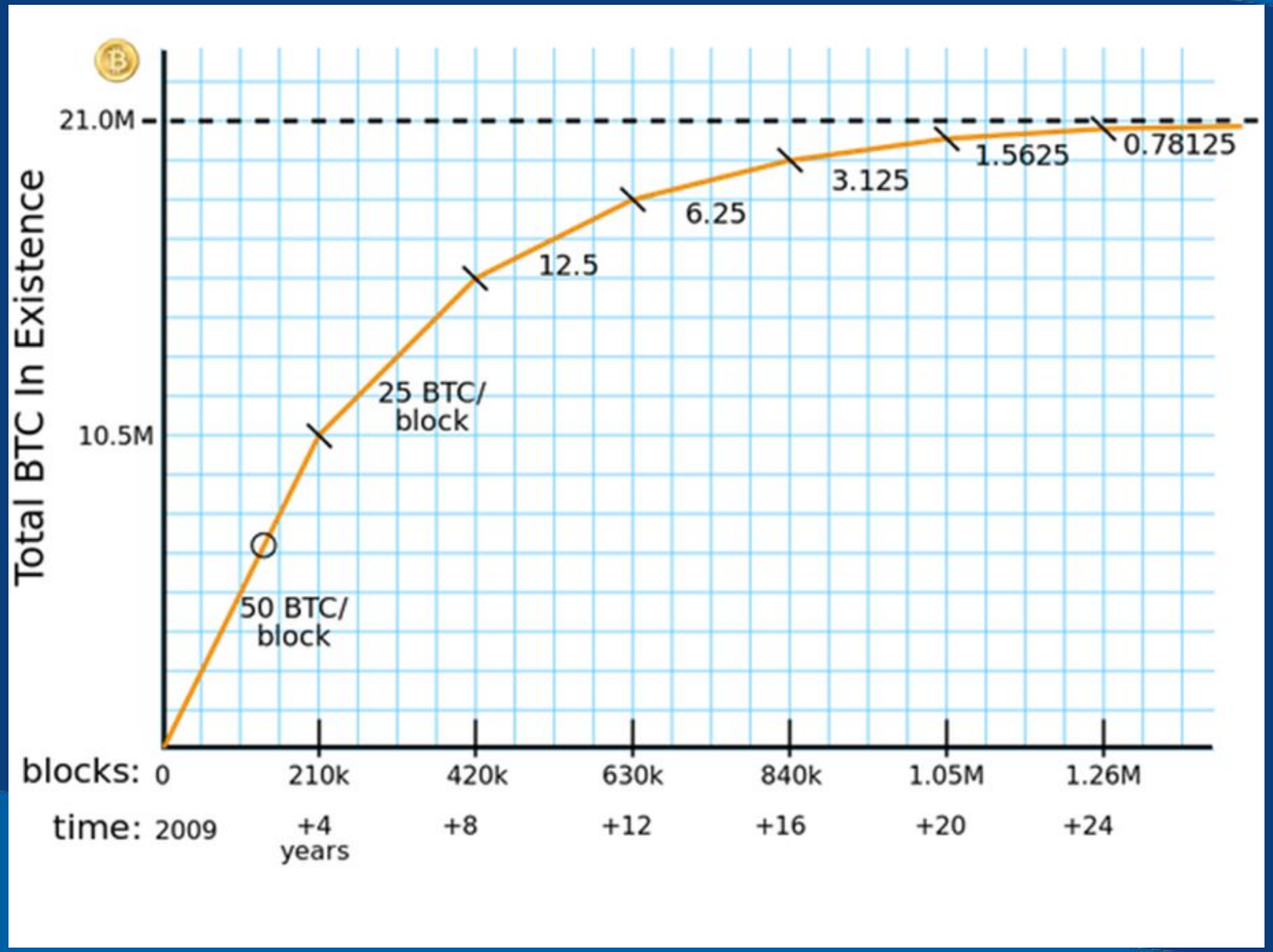
Para ganar Bitcoins minando es necesario resolver un problema matemático.

Este se resuelve por fuerza bruta.

Por eso, cuanto mayor sea nuestro poder computacional más probabilidades tendremos de resolver el acertijo y ganar la recompensa.

Esto hace que en la práctica la minería de Bitcoins esté muy concentrada (en granjas de minería) y sea muy poco rentable el minado individual o retail.

La minería en Bitcoin (III)



La minería en Ethereum

Al día de hoy, las transacciones en Ethereum también se validan mediante el protocolo “Proof of Work”.

La diferencia con Bitcoin es la política de emisión de Ethereum (la emisión es virtualmente ilimitada, no es decreciente como en Bitcoin).

En general, hoy es más rentable minar Ethereum que Bitcoin.

Sin embargo, algo muy importante: Ethereum planea hacer un upgrade y empezar a validar las transacciones con otro protocolo: “Proof of Stake”.

La minería de Ethereum parece tener los días contados.

Minería de Criptomonedas

Variables que afectan (típicamente) la minería

- El costo de los equipos de minado (hardware)
- La velocidad de internet.
- Costo de electricidad.
- La temperatura (clima frío o refrigeración). En climas de altas temperaturas es mayor el consumo energético.

Minería de Criptomonedas

El hardware de minado

- Lo más común es el uso de placas de video para minería de criptomonedas.

- Hoy en día se fabrican placas de video especiales para el minado. Incluso se venden equipos ya armados listos para minar (“rigs de minería”).

- Sin embargo, otros tokens utilizan distinto hardware:
  - Helium: utiliza unos modems especialmente fabricados para minar su token (no se puede minar otro token).
  - Chia: Se puede minar utilizando discos duros.

Minería de Criptomonedas

Los Pools de minería

- Son agrupaciones que permiten minar de manera colaborativa (integran y juntan todo el poder de minado de mineros individuales).
- De esta manera generan ingresos estables entre los participantes del pool.
- Cada minero pone a disposición del pool su poder computacional y las ganancias luego son divididas entre los mineros según el poder computacional aportado por cada uno.
- Si yo mino Bitcoin de manera individual tal vez no obtenga ninguna recompensa en mucho tiempo. En cambio si participo del pool tengo ingresos más estables.

Minería de Criptomonedas

¿Qué tener en cuenta?

- ¿Cuánto va a rendir mi equipo por mes?
- ¿Cuánto tardo en recuperar la inversión?
- ¿Qué espero que puede pasar con el precio de ese token?
- ¿Sigue siendo rentable la minería si cae un 50% el precio del token?
- ¿Cómo es la emisión de esa criptomoneda? Se mantiene estable o es decreciente (*halvings*)?
- ¿Cuánta gente está minando este token? ¿Cuánto baja el rendimiento si se suma más gente?
- ¿Me sirve el hardware para minar otras criptomonedas?

¿Minería o comprar token?

- Es muy importante nuestro horizonte de inversión. Si el horizonte es corto, siempre va a convenir comprar el token directamente.
- También depende el precio del token bajo análisis (según su market cap). Si tiene un precio alto y es buen negocio el minado probablemente convenga esto.
- Especialmente es importante saber en cuánto tiempo estaríamos recuperando la inversión si minamos. Si tenemos que esperar un año o más probablemente el riesgo es muy elevado.

8 Renta Fija con Criptomonedas

Renta fija con criptomonedas

¿Renta fija o criptomonedas?

- En una época de tasas de interés en cero y bonos que no rinden nada, el mundo cripto ofrece la oportunidad de invertir en proyectos con estas características a tasas muy atractivas.
- ~~Claro está que los riesgos son altos (caída del precio de los~~ tokens, riesgo de contraparte, riesgos de ciberseguridad, etc.).

Renta fija con criptomonedas

Distintos negocios de renta fija en criptoactivos

- **Staking**
- **Préstamos en criptomonedas (DeFi).**
- **Pools de liquidez (*liquidity pools*).**

Renta fija con criptomonedas - Staking

¿Qué es el staking?

- El “Proof of Stake” es un protocolo para validar transacciones en la blockchain distinto del ya conocido “Proof of Work”.
- Básicamente consiste en poner en garantía una determinada cantidad de tokens y eso te da el derecho a validar las transacciones.
- Como recompensa por tu aporte te pagan un interés sobre esa garantía.
- Sin embargo, si el nodo intenta validar transacciones ilegítimas tiene el riesgo de perder los tokens en garantía.

Renta fija con criptomonedas - Staking

Proof of Stake

- El problema con el protocolo “Proof of Work” es que consume mucha energía y es lento para validar transacciones (escalabilidad).
- “Proof of Stake” busca dar una solución a este doble problema: baja el consumo energético y aumenta cantidad de transacciones que se pueden verificar por segundo.
- Sin embargo, una de las críticas es que puede tender a la centralización de la red.
- El caso más importante hoy es Ethereum 2.0.

Renta fija con criptomonedas - Staking

Pools de Staking

- Funcionan de forma similar a los pools de minería.
- La diferencia es que en vez de poner a disposición poder computacional, se ponen los tokens. OJO: Esto es más riesgoso.
- ¿Por qué existen? Porque hay montos mínimos requeridos para hacer *Staking* (que suelen ser muy elevados). Por ejemplo, para ser un nodo validador en Ethereum 2.0 se necesitarán 32 ETH (Hoy aprox. USD 96.000).

Renta fija con criptomonedas - Préstamos DeFi

Préstamos con criptomonedas

- Hoy existen plataformas DeFi que ofrecen la posibilidad de dar y tomar créditos en criptomonedas.
- El funcionamiento es similar a las plataformas que ya existían para dinero fiat: se da en préstamo una X cantidad de determinado token y se recibe de vuelta esa cantidad más un interés.
- Típicamente a la contraparte (quien toma el préstamo) se le exige una garantía que también será en tokens (en general esa garantía es en BTC o ETH).

Renta fija con criptomonedas - Liquidity Pools

Pools de liquidez

- Es una alternativa para ganar tokens en proyectos nuevos donde en general hay poca liquidez.
- Típicamente debemos “congelar” montos equivalentes del token en cuestión y de una stablecoin.
- Nuestros tokens se suman al “pool” para aumentar la liquidez y a cambio nos dan unos tokens sintéticos que representan el par que enviamos.
- En general se ofrecen tasas muy altas pero también el riesgo es alto.
- Ejemplo: Pancake swap.

9 Aspectos Prácticos

The Real Danger of this *Wild World of Crypto*!

NOT JUST AMA BUT MY WARNING SINCERELY! SINCE I HAVE NO WAY HEARING ALL YOUR VOICE, I AM VERY WORRIED THAT SOME OF YOU GUYS MAY NOT UNDERSTAND THE REAL DANGER OF THIS WILD WORLD OF CRYPTO! HOPE THE MEDIA COULD BROADCAST MY VOICE SERIOUSLY: I HAVE SPENT A LOT OF TIME EXPLAINING THE SECURITY STUFF. I CLAIMED THAT I WAS SUPER ANONYMOUS AND SECURE, WHY? BOASTING MYSELF? SOME PEOPLE READS IT AS "HE IS BLUFFING BECAUSE OF FEAR AND THE SECURITY TEAMS WHO HAVE TRACED HIM ARE ON THE WAY". WAKE UP BOYS! THEY ARE NOT THE GOD, THEY CAN NOT SAVE YOU! I CAN NOT SAVE YOU! YOU SHOULD LEARN TO PROTECT YOURSELF! I HAVE EXPLAINED THE SITUATION OF SECURITY INDUSTRY (SEE P6Q1Q3), AS EXPERIENCED SECURITY EXPERTS, WE KNOW ALL THE WAYS OF TRACING THE BAD GUYS, THAT IS TO SAY, WE KNOW ALL THE WAYS OF HIDING FROM GOOD GUYS. IN THE REAL WORLD, THE GOVERNMENT AND POLICE MAY STAND ON YOUR SIDE, BUT THERE IS NO SUCH A UTOPIA IN THE CRYPTO WORLD! THE POINT OF CLAIMING MY ANONYMITY, ALONG WITH THE LESSONS ABOUT FEARLESS LAUNDERING, IS TO CONVINCE YOU THAT THERE ARE ALWAYS PERFECT HACKS THAT CAUSE PERMENANT DAMAGE FOR REAL! DON'T BE NAIVE! DON'T BELIEVE IN SO CALLED EXPERTS, ESCPECIALLY THOSE WHO CONCLUDE THAT "IT'S THE EVIDENCE THAT THE CRYPTOWORLD IS STILL SOMETHING CAN BE REGULATED"! PROTECT YOURSELF, OR JUST LEAVE THE CASINO!

The Real Danger of this *Wild World of Crypto!*

Poly Network
@PolyNetwork2

Important Notice:
We are sorry to announce that #PolyNetwork was attacked on @BinanceChain @ethereum and @0xPolygon Assets had been transferred to hacker's following addresses:
ETH:
0xC8a65Fadf0e0dDAf421F28FEAb69Bf6E2E589963
BSC:
0x0D6e286A7cfD25E0c01fEe9756765D8033B32C71

9:38 AM · Aug 10, 2021

Cross-Chain DeFi Site Poly Network Hacked; Hundreds of Millions Potentially Lost

DeFi platform Poly Network was attacked on Tuesday, with the alleged hacker draining roughly $600 million in crypto.

By Eliza Gkritsi, Muyao Shen · Aug 10, 2021 at 10:56 a.m. · Updated Sep 14, 2021 at 10:37 a.m. ·

Address 0x5dc3603C9D42Ff184153a8a9094a73d461663214

Heist Exploit

Sponsored: **Merchant Token** - Join the LARGEST crypto consumer protection project! **Join the project**

⚠ This address is reported to be involved in a PolyNetwork exploit.

After the attack, the hacker said that he'd stolen the funds to keep them safe, saying that putting the coins in a "trusted account" was a way to highlight the bug without giving someone else the opportunity to make away with them. He's had a somewhat continuous banter with Poly Network, who even took to calling him "Mr. White Hat" in their series of update notes. Poly Network also invited the hacker to act as the company's chief security advisor, which the hacker has (seemingly cheekily) acknowledged, signing off a message to the company with "your chief security advisor." *Chainalysis* points out that the transparency of blockchain tech can make it difficult to get away with spending stolen funds.

"We call on miners of affected blockchain and crypto exchanges to blacklist tokens coming from the above addresses," the Poly team tweeted.

The $600 million figure would place the Poly Network hack among the largest in crypto history.

Tether froze approximately $33 million in relation to the hack, Tether CTO Paolo Ardoino tweeted.

About one hour after Poly announced the hack on Twitter, the hacker tried to move assets including USDT through the Ethereum address into liquidity pool Curve.fi, records show. The transaction was rejected.

Meanwhile, close to $100 million has been moved out of the Binance Smart Chain address in the past 30 minutes and deposited into liquidity pool Ellipsis Finance.

Poly Network hacker gave back more than $600 million in stolen crypto

The hacker began returning the funds almost two weeks ago

By Mitchell Clark | Aug 23, 2021, 3:55pm EDT

The Real Danger of this *Wild World of Crypto*!

The Complete List Of Crypto Exchange Hacks

SEP 24, 2021 / TRADING

→ Desde 2012, hubo *46 ciberataques* a Exchanges. Solo en 2019 hubo hubo *19 hacks* por valor de 292M U$d; en 2020 hubo *5 hacks* por valor de casi 300M U$D worth

→ En total, casi *2.6 Billons worth tokens han sido robados de Exchanges en 9 años*

→ En *2021 el target de hacks fueron las plataformas de DeFi*: el hack a Poly Network representó el mismo valor de todos los hacks a Exchanges de 2019 + 2019…

→

The Real Danger of this *Wild World of Crypto*!

LILY HAY NEWMAN SECURITY 05.18.2020 09:00 AM

Cryptocurrency Hardware Wallets Can Get Hacked Too

New research shows vulnerabilities in popular cold-storage options that would have revealed their PINs.

A 15-year-old hacked the secure Ledger crypto wallet

John Biggs @johnbiggs / 2:32 PM GMT-3 • March 21, 2018

A 15-year-old programmer named Saleem Rashid discovered a flaw in the popular Ledger hardware wallet that allowed hackers to grab secret PINs before or after the device was shipped. The holes, which Rashid described on his blog, allowed for both a “supply chain attack” – meaning a hack that could compromise the device before it was shipped to the customer – and another attack that could allow a hacker to steal private keys after the device was initialized.

The Real Danger of this *Wild World of Crypto*!

BUSINESS 2 SEPTEMBER 2021

Steve Kaaru 

South African man loses $1M BTC fortune after losing private keys

A bit over a decade ago, BTC was barely in the conversation and it was confined to geeks and tech nerds who scoured the Internet looking for the latest cool trends to try out. That was when one South African man learned about the digital currency and started to mine it. He accumulated 20 BTC, worth little at the time. This fortune would be worth almost a million dollars, but the man lost his private keys.

If you believe in the concept of **"Not Your Keys, Not Your Crypto"** you probably take personal responsibility for your crypto portfolio by keeping it on a non-custodial solution (preferably a versatile hardware wallet like the CoolWallet) instead of centralized exchanges, which come with their own litany of horror stories of hacks and scams (the author may or may not have thousands of Dogecoins floating around the wreckage of the hacked and now-defunct Cryptopia exchange, forever lost).

The road to crypto riches is paved with Bitcoin gold but unfortunately also littered with the wreckages of poorly managed, lost or hacked wallets. In fact, research shows that up to a **staggering 20%, or 3.7 million**, of all Bitcoins have been lost forever. And it's not stopping there.

The Real Danger of this *Wild World of Crypto*!

1) This British guy threw out a hard drive containing 7,500 bitcoin ($375m)

2. This Russian politician lost 400 bitcoin ($200 million) after deleting his private key

4. The German engineer who forgot the password to his encrypted device containing 7,002 bitcoin ($350m)

5. The exchange CEO who went to India and “died”, taking 26.5k BTC and 430,000 ETH with him

Aspectos prácticos

Top Estafas

- *"Phishing"*: Existen infinitos mecanismos para intentar robar tus datos. NUNCA pero NUNCA debemos dar nuestra clave privada / semilla a NADIE.
- "Rug Pulls": Son proyectos fraudulentos donde los desarrolladores juntan inversiones y abandonan el barco (con los fondos de los inversores). Cuidado con los tokens nuevos.
- Falsos exchanges: Hay sitios que emulan ser un exchange de criptomonedas y en verdad son una pantalla.
- Falsas wallets: Software malicioso donde típicamente te dan una semilla corrupta para vaciar la wallet luego de depositados los fondos.
- Falsos NFTs: toman un NFT de moda y lo replican intentando venderlo como si fuera el original.

Aspectos prácticos

¿Qué tener en cuenta antes de invertir en un token?

- Conocer el proyecto detrás del token. ¿Cuál es el valor que aporta? ¿Qué problema intenta resolver?
- Conocer al equipo detrás del proyecto. ¿Quiénes son? ¿Cuál es su Track Record? Desconfiar de los proyectos donde el equipo no muestra la cara!
- Política de emisión.
- Cuidado con engaños y seguridad.
- Invertir siempre lo que se está dispuesto a perder. Riesgo de perder el 100%.

Algunas métricas on-chain

https://coinmarketcap.com/

MUCHAS GRACIAS POR SU TIEMPO

Sebastian Heredia Querro

Martín Bertoni