NYDIG

MARCH 2022

Bitcoin **Security**

WHAT KEEPS BITCOIN SAFE

TABLE OF CONTENTS

01. Bitcoin Security 3

02. Proof-of-Work 3

03. Decentralization.....4

04. Large Numbers 5

Bitcoin Security

It’s no secret that the Bitcoin Network is secure.

Understanding why isn't so simple. That's because the Bitcoin Network's security model upends how we usually think about protection.

Typically, we think of security as gatekeeping. Banks defend your account by knowing who you are and expecting you to prove it. On the other hand, the Bitcoin Network doesn’t know your identity and doesn’t care to find out. A bank keeps your account balance confidential so as not to attract unwanted attention. As an open network, Bitcoin, though pseudonymous, is free for all the world to see.

So just how does the Bitcoin Network pull it off? When considering Bitcoin’s security, we’ll focus on three attributes: proof-of-work, decentralization, and the power of large numbers. Proof-of-work and decentralization protect Bitcoin at the network level. At the same time, large numbers are, crazy as it may seem, the solution to securing individual accounts.

Proof-of-Work

A blockchain is nothing more than a means of sharing data in a way that is resistant to tampering. In the case of the Bitcoin Network, its ledger is secured through a mechanism known as proof-of-work.

Miners compete to add blocks of transactions to the blockchain in exchange for bitcoin payments. These payments include the block subsidy[1] and transaction fees. But to add a block, Bitcoin’s protocol imposes what amounts to a toll on miners.

The toll comes in the form of requiring a valid proof-of-work for every block. In brief, miners collectively perform quadrillions[2] of computations that generate random numbers. The first miner who generates a

1 Currently, miners receive 6.25 new bitcoins for every block they add to the chain. This reward is cut in half every four years.

2 https://levelup.gitconnected.com/bitcoin-proof-of-work-the-only-article-you-will-ever-have-to-read-4a1fcd76a294

number below a set target wins the block. Proof-of-work is the act of producing these random numbers until a miner finds a sufficient one.

Creating a valid proof-of-work requires specialized hardware and, more importantly, a lot of energy. Miners bear both of those costs. Furthermore, nodes reject blocks that include invalid transactions such as double spends. Therefore, a miner that tries to slip a bad block into the blockchain risks their effort going to waste. Consequently, proof-of-work is a deterrent to adding invalid blocks and ensures that miners have skin in the game.

As more miners compete to add new blocks, generating a valid proof-of-work becomes progressively more difficult. If a miner wanted to attack the blockchain by reordering blocks (that is changing the history of the ledger), they'd need to accumulate 51% or more of the network's computational power, an almost unthinkable task at this point in Bitcoin's evolution.

Decentralization

Unlike the overwhelming majority of websites, the Bitcoin Network isn't run on a centralized server. Instead, the Bitcoin Network lives on computers, known as nodes, that its participants run voluntarily.

The implication is that hacking the Bitcoin Network's software would mean accessing tens of thousands of individual machines. Of course, hackers could attempt to corrupt any single device. However, thousands more would still hold the proper code and an accurate copy of the blockchain.

While Bitcoin's architecture is slower than a centralized network, it's nearly impossible to take down. If even a single node were left unscathed from an attack, the Bitcoin Network could be restored.

Large Numbers

The Bitcoin Network doesn't hold any information about its users. Rather than relying on gatekeeping, addresses (what you might think of as accounts) are secured by private keys (passwords) that are just really large numbers. Hard as it is to believe, the range of numbers is so vast that guessing just one tied to any

bitcoin is practically impossible. A successful guess would theoretically require harnessing the power of a star and take more time than the expected life of the universe.[3]

For a sense of scale, consider the following. People often compare the amount of private key combinations to the number of atoms in the universe.[4] The comparison isn't to galaxies, stars, or grains of sand, but atoms, the building blocks of all matter.

Quite simply, the Bitcoin Network protects addresses through the immutable laws of physics and some clever cryptography. In a world of supercomputers, you might think it'd be possible to have a machine start at one and work its way up until it hit a jackpot. But physics makes such an act prohibitively expensive. Anyone who wanted to try that gambit would be better off, economically speaking at least, using all of that raw energy and processing power to just mine bitcoin.

3 https://medium.com/hackernoon/a-physicists-journey-into-cracking-bitcoin-4631e57158cc

4 https://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/ch04.html#:~:text=The%20size%20of%20bitcoin's%20private,to%20contain%201080%20atoms.

Key Takeaways

01

Proof-of-work ensures that miners have skin in the game and serves as a deterrent to adding invalid blocks to the blockchain.

02

The Bitcoin Network is decentralized. There's no single point of failure to attack.

03

Large numbers protect bitcoin addresses. The enormous amount of energy and time needed to guess a private key (the password that controls an address) make it an economically infeasible proposition.

DISCLOSURES

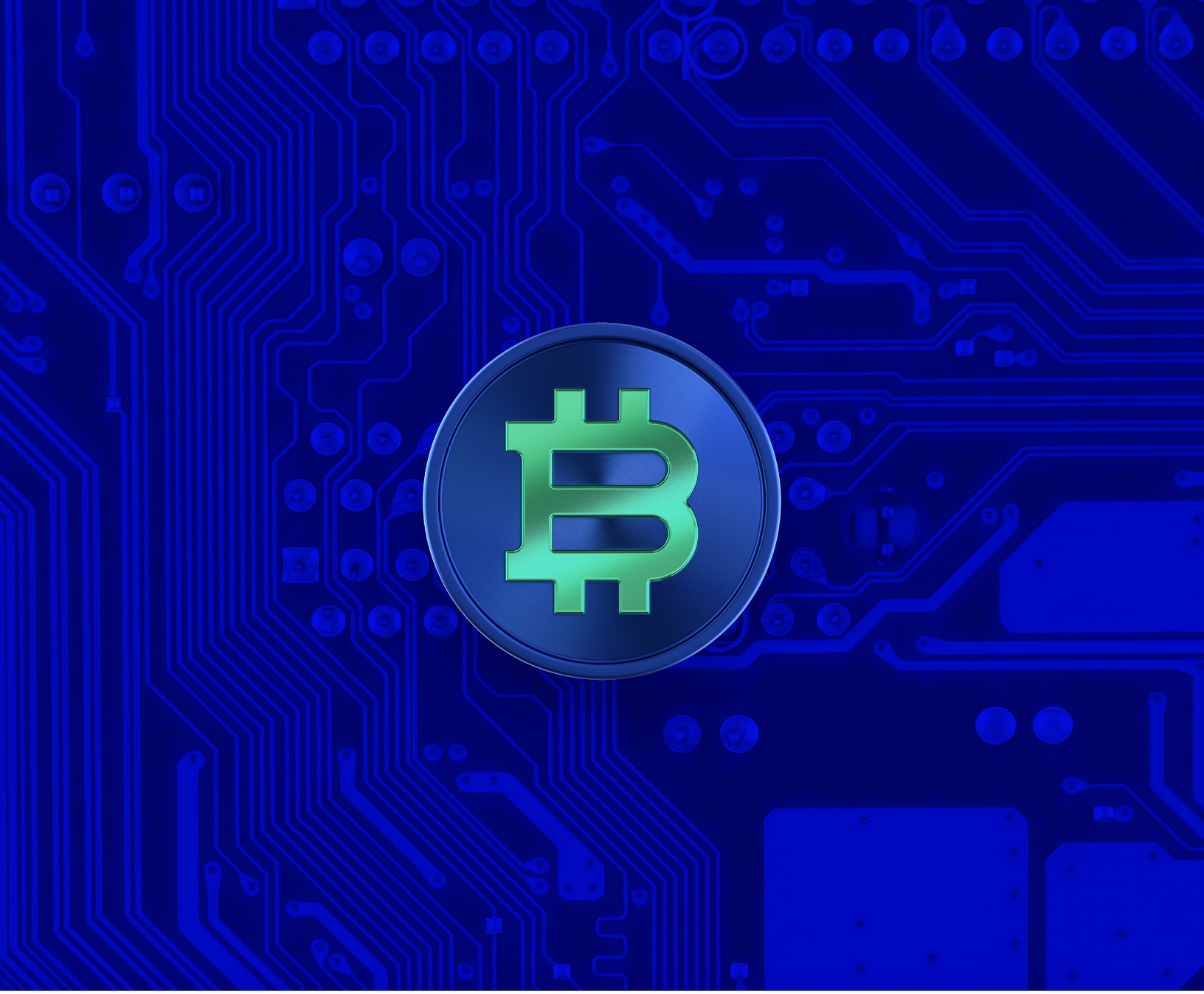
This report has been prepared solely for informational purposes and does not represent investment advice or provide an opinion regarding the fairness of any transaction to any and all parties nor does it constitute an offer, solicitation or a recommendation to buy or sell any particular security or instrument or to adopt any investment strategy. This report does not represent valuation judgments with respect to any financial instrument, issuer, security or sector that may be described or referenced herein and does not represent a formal or official view of New York Digital Investment Group or its affiliates (collectively, "NYDIG").

It should not be assumed that NYDIG will make investment recommendations in the future that are consistent with the views expressed herein, or use any or all of the techniques or methods of analysis described herein in managing client accounts. NYDIG may have positions (long or short) or engage in securities transactions that are not consistent with the information and views expressed in this report.

The information provided herein is valid only for the purpose stated herein and as of the date hereof (or such other date as may be indicated herein) and no undertaking has been made to update the information, which may be superseded by subsequent market events or for other reasons.

Information furnished by others, upon which all or portions of this report are based, are from sources believed to be reliable. However, NYDIG makes no representation as to the accuracy, adequacy or completeness of such information and has accepted the information without further verification. No warranty is given as to the accuracy, adequacy or completeness of such information. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions that occur subsequent to the date hereof.

Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision. Legal advice can only be provided by legal counsel. NYDIG shall have no liability to any third party in respect of this report or any actions taken or decisions made as a consequence of the information set forth herein. By accepting this report, the recipient acknowledges its understanding and acceptance of the foregoing terms.



NYDIG

Interested In Learning More?

NYDIG.COM/RESEARCH