NYDIG

MARCH 2022

Private & **Public Keys**

WHAT THEY ARE AND HOW THEY WORK

TABLE OF CONTENTS

Private and Public Keys

The Bitcoin network has no intermediaries. There aren't banks standing in the middle of transactions to verify the sender's identity or that the funds are going to the intended recipient. Instead of relying on go-betweens, Bitcoin uses public key cryptography to establish ownership.

You might be unfamiliar with the term "public key cryptography." Still, if you use messaging services like Signal or WhatsApp, it's already part of your life. Unfortunately, truly understanding how public key cryptography works means grappling with a particularly forbidding branch of mathematics. But fortunately for Bitcoin users, there are just a few simple concepts that need to be understood.

The first is that a private key has a single associated public key. As the names make clear, users should keep private keys secret. In contrast, you can share a public key without compromising your security. Second, private keys create public keys. That means that all you need to remember is the private key since it can undergo a mathematical transformation to produce its public counterpart. The third point is that private keys hold asymmetric information relative to public keys. Knowing a private key means knowing the public key. But knowing a public key tells you nothing about the associated private key. That trick is thanks to the magic that is the mathematical trapdoor function used to derive public keys. Finally, you can distinguish the two types of keys by what they do: private keys are for spending bitcoin, and public keys are for receiving it.

That's all you need to understand about private and public keys. But if you're curious about the nuts and bolts of how they work in tandem to secure bitcoin, you can learn more below.

Private Keys

Private keys are just a random number. Really. There's nothing more to them than that.

Understandably, that notion probably sounds crazy. How can a random number secure millions or billions of dollars in value? Why couldn't someone make wild guesses to potentially unlock untold riches?

Well, they certainly could try, but the set of numbers that could make up a private key is astonishingly large. Specifically, a Bitcoin private key can be any positive number up to about two raised to the 256th power.

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.[1] The comparison isn't to galaxies, stars, or grains of sand, but atoms, the building blocks of all matter. And therein lies the trick. Bitcoin's security hinges on how many possible private keys there are. 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 the 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.

The incomprehensibly low probability of randomly guessing a private key is the crux of why the Bitcoin network is as safe as it is. Anyone who would choose to attack the Bitcoin network would have to do so for reasons other than economic gain.

Now you understand why you should never share your private keys. That number being practically impossible to guess is what keeps your bitcoin safe. Bitcoin investors must safeguard their private keys because recovering a lost key is just as tricky as trying to guess a random one that controls a funded account. Unlike a forgotten ATM pin or email password, no service provider can recover it for you. Anyone who says they can do so is most certainly lying. The Bitcoin network doesn't even store the key itself. A little-known fact is that Bitcoin doesn't create the private key for your account. Wallet software does. So, the point bears repeating: private keys should be stored in an offline device or with a trusted custodian who holds them offline on the user's behalf.

Private keys send bitcoin. They do this by signing transactions much like you would endorse a check. But, as already mentioned, you should never share your private key. So how do you sign a transaction without divulging your private key?

[1] Mastering Bitcoin

Cryptographic Signatures

Here’s where cryptography comes into play. Despite the cryptocurrency moniker, Bitcoin hardly employs encryption. The network itself is open and transparent. It’s pseudonymous, not anonymous. But the one actual deployment of cryptographic science is creating a digital signature from a private key. A signature is an obscured, single-use version of a private key.

In brief, a signature is the product of a private key multiplied by a random number plus transaction data. The protocol requires transaction data to ensure that no one can reuse the signature to falsify future transactions. To get the random number, Bitcoin historically used the Elliptic Curve Digital Signature Algorithm (ECDSA). However, with the adoption of the Bitcoin network's Taproot upgrade, the Schnorr Signature Algorithm is now also supported.

Again, understanding how all of this works is inconsequential to your ability to interact with Bitcoin. Just know that digital signatures remove the need for private keys in Bitcoin transactions. Instead, the signature proves that the sender holds the private key for the account sending bitcoin. And just as public keys can’t be reverse engineered to reveal their private companion, neither can a signature.

Public Keys

But signing a transaction is just one-half of the equation. You also need somewhere to send that bitcoin. Public keys serve two roles, one each for the sender and the recipient. The sender includes the public key so that anyone on the network can verify the digital signature since it’s the only number that will solve the equation. The recipient uses the public key to create the address where they want bitcoin sent.

The relationship between private and public keys is much like a private key and a digital signature. Public keys are also the product of running a private key through ECDSA. But again, it’s a one-way function. Knowing the private key allows you to calculate the public key. But no one can use the public key to uncover the private key because of the trapdoor property of the algorithm. This fact is why you can share public keys.

Ignoring the high-level math that underpins the process, all you need to keep in mind is that the network can only verify a transaction with the sender's public key. No other number will work. Sending the wrong public key means the exchange will be ruled invalid. Providing the correct public key proves that the sender holds the private key that controls those funds.

Bitcoin Addresses

Addresses stem from the recipient's public key. Some wallet software can create unique addresses from a public key for each transaction to maintain data hygiene. You still only have a single public key, but it can yield multiple addresses through math and clever coding.

To receive bitcoin, the recipient shares one of these addresses with the sender. The sender then can direct the payment to that address. Because the address correlates to a specific public key, only the receiver's private key can use the bitcoin sent in that transaction.

Key Takeaways

01 A private key is just a random number among an unfathomably large number of possibilities.

02 Private keys should never be shared and should always be safeguarded offline either by using a hardware wallet or a trusted custodian.

03 A private key has one corresponding public key.

04 Private keys send bitcoin; public keys receive bitcoin.

05 Wallet software creates a public key from a private key. But there's no way to decipher a private key from a public key. This property is due to the mathematical trapdoor function used to create public keys.

DISCLOSURES

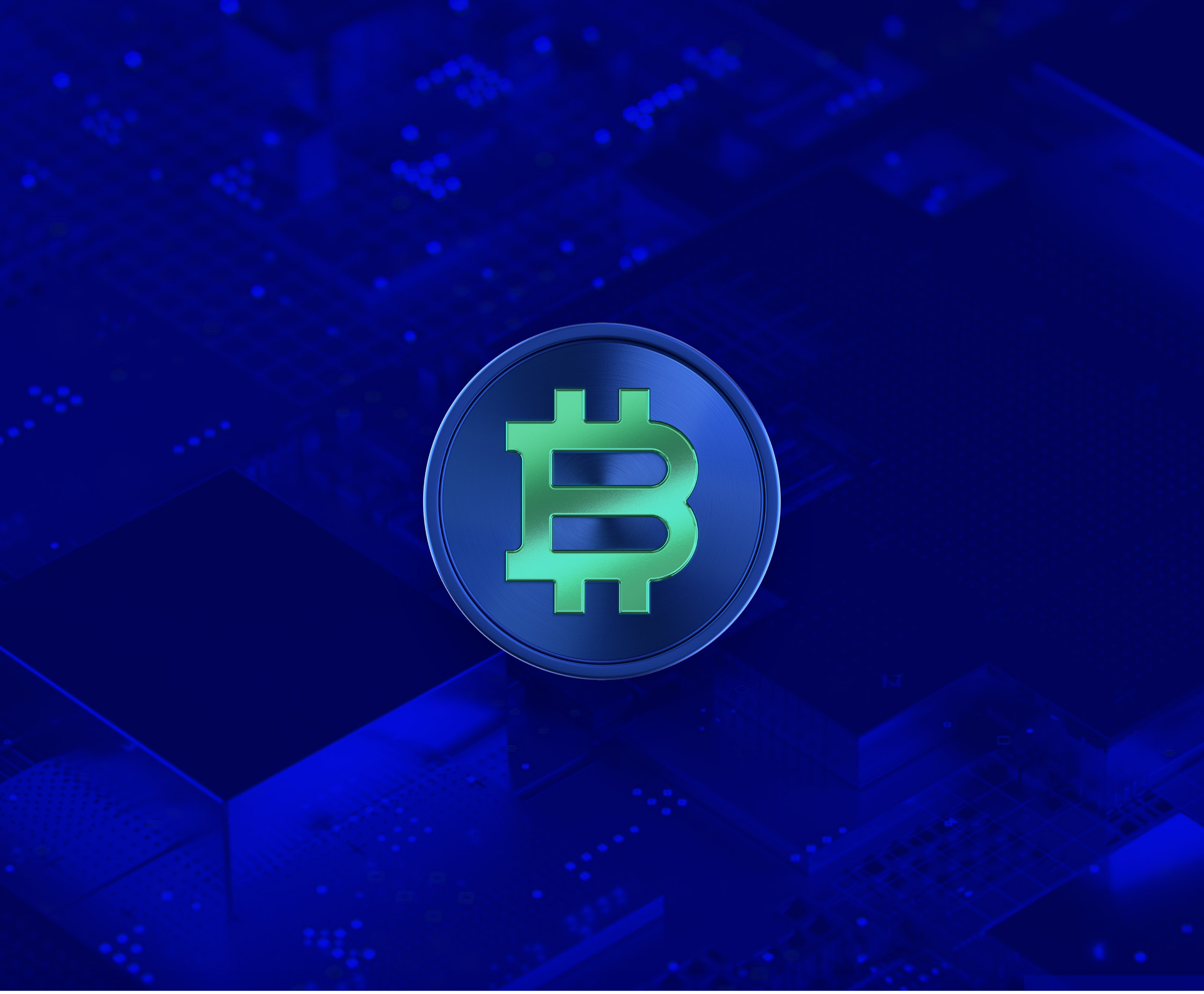
This report has been prepared solely for informational purposes and does not represent investment advice or provide an opinion regarding the fairness of any transaction to any and all parties nor does it constitute an offer, solicitation or a recommendation to buy or sell any particular security or instrument 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