

EDUCATIONAL
WORKBOOK



MY FIRST ZCASH

PUBLISHED BY MASS ADOPTION ALLIANCE

ENGLISH VERSION
MAY 2024 - V1

*Mass Adoption Alliance has developed this work,
which was created by members of the Zcash Community,
and made it freely available under Creative Commons.
This work is licensed under Creative Commons
Attribution-ShareAlike4.0 International (CC BY-SA 4.0).
Some content and design elements are
the original work of **Mi Primera Bitcoin***



PUBLISHED BY MASS ADOPTION ALLIANCE

ENGLISH VERSION
MAY 2024 - V1



About Mass Adoption Alliance

Mass Adoption Alliance is a 501(c)(3) public charity. Our mission is empowering youth worldwide through education about decentralized cryptocurrencies and financial privacy. Educating youth in turn educates their families and communities; this aligns with the overarching goal of mass adoption as a means to a more peaceful world.

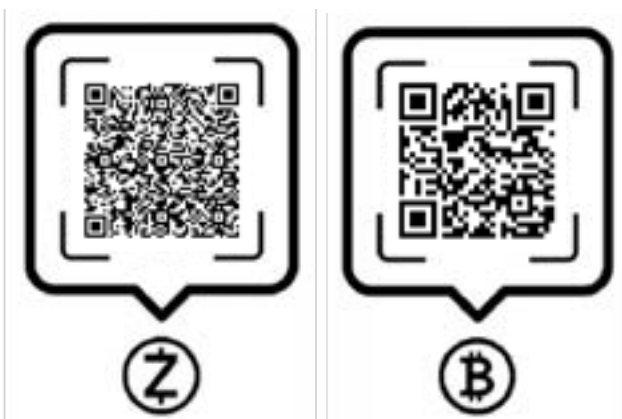
We partner with organizations and communities to curate educational content and experiences to share with students across the globe. Would you like us to develop an educational resource for your organization, community or school? Let's connect!

Support for the establishment of Mass Adoption Alliance was provided by a grant from Zcash Foundation.

Learn more at: massadoption.org

Follow us on X: [@massadoptionorg](https://twitter.com/massadoptionorg)

Please donate to support our mission



ACKNOWLEDGEMENTS

This book exists because Zcash Foundation supported the establishment of Mass Adoption Alliance through a ZF grant a couple years ago. Thank you for believing in my vision.

My First Zcash is a community-created resource, written and designed by Zcashers around the world, including this group of unbelievably talented volunteers:

A collection of talented writers authored the beautiful, expert content found within the pages of this book. Their contributions will live on in this and future iterations of My First Zcash and ultimately be translated into multiple languages. My sincere thanks to:

Alfredo Garcia (Chapter 7), **Chris Tomeo** (Chapter 5), **Marek** (Chapter 8), **Pacu** (Chapter 6), **Pili Guerra** (Chapter 7), and **zksquirrel** (Chapter 5).

And that spectacular Glossary! Have you seen it? That’s **Tripleyouwu** hard at work.

The design work across every page in this book exceeded expectations–by a mile! It’s gorgeous from cover to cover!

Creative Director, **Mine**, spent countless hours working tirelessly to deliver the author’s content with beautiful, full-color effect across every page of the book, including chapter page layout for Chapters 1 and 2. Mine also designed the MFZ merch over in the Zechub store. **Thank you for your dedication, Mine!**

Design work of magnitude from illustrations to page layout was also undertaken by a team of skilled experts including:

Geffen, who contributed generous design leadership as well as chapter layout design for Chapters 5-7 and all of the gorgeous chapter cover pages!

logy not only supported Mine in daily life while she was leading the design work, but also created lovely page layout design for Chapters 3 and 8.

Zerodartz provided great support with illustration work, was always willing to lend a hand, and championed page layout design for Chapter 4.

There are so many people to thank who truly went above and beyond in getting this project over the finish line in time for ZconV. Additional contributors to whom I am incredibly grateful are:

Decentralistdan: For spinning up that amazing list of every Zcash video in existence the second the task sheet was published, but most of all for regularly reaching out to check-in, your kind willingness to listen, and offering your always-brilliant ideas during our syncs.

Franklynstein: For transforming that Zcash video list into QR codes—at least three times. And they didn’t even make it into v1 of the book! Oh boy. v2 for sure! And hey, you didn’t know it but you were the very first person who submitted a volunteer form. Thank you for jumping right in!

Vito: For answering so, so many Discord questions when I was getting started, you always responded with unbelievable patience, speed and kindness.

Zcash Foundation: For donating use of your Cypherpunk Zero NFT collection in this publication and for cheering me and MFZ on from inception.

Speedfox: For cataloging every Cypherpunk Zero NFT that Zcash Foundation donated to this project. We’re going to use that resource a lot in v2!

Electric Coin Co: For generously donating use of the fabulous Cypherpunk Zero collection of images for use in this publication and on merch in the Zechub store.

Dismad and zksquirrel: For making MFZ merch look so good in the Zechub store!

Ryan and the ZFAV squad: For support and help getting the word out right from Day 1.

ICE: For taking Zcash forward to the next generation!

And to the many, many others who contributed to this book: THANK YOU!

To those who are still waiting to get involved: **v2 is coming in hot!**

Gratefully,

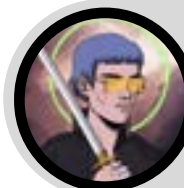
Elise

Elise Hamdon
Executive Director
Mass Adoption Alliance

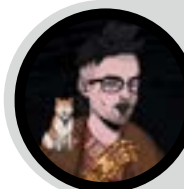
THE PEEPS WHO DID ITZ



Ice [*@frostbyte11211*]
Ice is a high schooler interested in privacy and computers. She hopes to study both cryptography and psychology in college to better understand users.



Pacu [*@thecodebuffet*]
Pacu has been a Zcash wallet developer since mid-2019. Four years at ECC (maintaining the mobile SDKs, collaborating with partners, and organizing the Light Client Working Group) has been followed by a grant from ZCG to be Zcash Wallet Developer for the community!



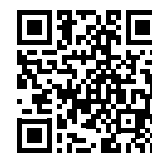
Marek
Marek is an engineer at the Zcash Foundation.



Alfredo Garcia
Alfredo Garcia is a Rust systems engineering working in the Zebra team at the Zcash Foundation



Pili [*@mpguerra*]
Pili is the Engineering Manager at the Zcash Foundation. She has 20 years of experience working in the tech industry as a software developer, solutions engineer, consultant and project manager. Work includes the Tor Project: Browser, Community and UX Teams.



Zksquirrel
Community Note Taker for Zcash Arborist and contributor to ZecHub, an open source education hub for Zcash education.



Tripleyouwu
Community Support Coordinator at the Zcash Foundation



Mass Adoption Alliance
Empowering youth worldwide through education about decentralized cryptocurrencies and financial privacy.



TABLE OF CONTENTS

1 THE POWER OF THE MONEY

1.0	READY?	17
1.1	CLASS DISCUSSION: WHAT IS MONEY?	17
1.2	THE LIMITED WORLD: NAVIGATING SCARCITY IN A GROWING ECONOMY	17
1.3	DEFINITION OF MONEY	21
1.3.1	WE CAN USE IT, BUT CAN WE DEFINE IT?	21
1.3.2	FUNCTIONS OF MONEY	22
1.3.3	MONEY CHARACTERISTICS	23
1.3.4	TYPES OF MONEY	25

2 FROM BARTER TO BITCOIN AND CBDCS: A HISTORY OF MONEY

2.0	INTRODUCTION	31
2.1	EARLY FORMS OF MONEY	32
2.2	COMMODITIES TO I.O.U'S	34
2.3	TRANSITION FROM SOUND MONEY TO UNSOUND MONEY	34
2.4	TRACING THE EVOLUTION: FROM PLASTIC TO DIGITAL	36
2.5	THE RISE OF A CASHLESS SOCIETY	37

3 DISCOVERING THE DARK SIDE OF FIAT

3.0	DRAWBACKS OF THE FIAT SYSTEM	45
3.1	THE GREATEST THREATS TO YOUR MONEY: INFLATION, DEBASEMENT, AND THE LOSS OF PURCHASING POWER	47
3.1.1	THE EFFECTS OF INFLATION: AN AUCTION ACTIVITY	47
3.1.2	SAVING MONEY IN HARD TIMES	52
3.1.3	THE TIME VALUE OF MONEY AND ITS ROLE IN ECONOMIC GROWTH	53
3.2	CENTRALIZED CONTROL: HOW THE GOVERNMENT AND BANKS MANIPULATE THE MONEY SUPPLY	53
3.3	THE MAGIC OF MONEY CREATION	53
3.3.1	FRACTIONAL RESERVE BANKING	55
3.3.2	EXERCISE: FRACTIONAL RESERVE BANKING	56
3.4	DEBT: THE BURDEN THAT CRUSHES THE MIDDLE AND LOWER CLASSES	58
3.5	ADDRESSING WEALTH INEQUALITY: A NEW APPROACH TO MONEY	59

4 THE DECENTRALIZED FUTURE: EMPOWERING COMMUNITIES AND INDIVIDUALS

4.0	THE PRICE OF CONTROL: A LOOK AT SURVEILLANCE, CENSORSHIP, AND REGULATION	63
4.0.1	SURVEILLANCE	63
4.0.2	FINANCIAL REGULATIONS AND CENSORSHIP	63
4.1	FROM CRISIS TO INNOVATION: THE CYPHERPUNKS AND THE CREATION OF A DECENTRALIZED DIGITAL CURRENCY	66
4.2	CENTRALIZED SYTEMS	66
4.2.1	CENTRALIZED SYTEMS	63
4.2.2	THE INTERMEDIARIES IN A CREDIT CARD TRANSACTION	68
4.3	OVERCOMING CENTRALIZATION WITH DECENTRALIZED SYSTEMS	68
4.4	TRANSACTIONS ARE JUST AGREEMENTS TO TRADE	71
4.4.1	TO TRUST OR NOT TO TRUST	71
4.4.2	LET´S SWAP TRUST FOR RULES	72
4.5	UNLOCKING THE POWER OF THE BLOCKCHAIN: A TECHNOLOGY REVOLUTIONIZING THE FUTURE	73
4.5.1	CONSENSUS BUILDING IN A PEER-TO-PEER NETWORK	74
4.6	EMPHASIZING THE IMPORTANCE OF TRUE DECENTRALIZATION IN BLOCKCHAIN PROJECTS FOR ACHIEVING FREEDOM AND EMPOWERMENT	75

5 INTRO TO ZCASH

5.0	THE ENIGMA OF SATOSHI NAKAMOTO: BITCOIN AND THE PRIVACY REVOLUTION	79
5.1	INTRODUCTION TO ZCASH AND BITCOIN	79
5.1.1	WHAT IS BITCOIN? WHAT IS ZCASH?	79
5.1.2	WHAT IS THE DIFFERENCE BETWEEN BITCOIN AND ZCASH?	80
5.1.3	WHY LEARN ABOUT ZCASH?	80
5.1.4	WHAT GIVES ZCASH ITS VALUE?	81
5.1.5	WHY SHOULD I CARE?	81
5.2	WHAT IS ZCASH MADE OF?	81
5.2.1	HOW DO NEW ZCASH COINS ENTER THE NETWORK?	79
5.2.2	INTRODUCTION TO ZCASH PRIVACY	80
5.2.3	HOW DOES THE BLOCKCHAIN KEEP TRACK OF WHO SPENDS WHICH ZCASH?	80
5.2.4	ARE ZCASH TRANSACTIONS SECURE?	84
5.2.5	WALK ME THROUGH AN ACTUAL ZCASH TRANSACTION	84
5.2.6	EXERCISE: ZCASH TRANSACTIONS IN ACTION	84
5.2.7	CAN ZCASH BE SHUT DOWN?	84
5.3	WHO'S WHO AND WHAT'S WHAT IN THE ZCASH WORLD?	85

6 ZCASH WALLETS

6.0	FROM NOVICE TO PRO: NAVIGATING THE WORLD OF THE ZCASH WALLET	89
6.1	THE PROCESS OF ONBOARDING AND SECURING YOUR ZCASH	92
6.1.1	THROUGH KYC EXCHANGES	93
6.1.1.1	RISKS ASSOCIATED WITH KYC-EXCHANGES	93
6.1.2	ONBOARD YOURSELF THROUGH EARNING ZEC.	94
6.2	EXCHANGE AND HARDWARE WALLETS	94
6.2.1	CENTRALIZED EXCHANGES	95
6.2.1.1	KYC'D CENTRALIZED EXCHANGES	95
6.2.1.2	NON-KYC CENTRALIZED EXCHANGES	95
6.2.2	DECENTRALIZED EXCHANGES	95
6.3	PRIVACY-FOCUSED WALLETS	96
6.3.1	TO SHIELD OR NOT TO SHIELD	96
6.3.1.1	UNIFIED ADDRESSES	96
6.3.1.2	WHAT IS AUTOSHIELDING?	96
6.3.2	ZCASH SHIELDED WALLETS	98
6.3.2.1	NIGHTHAWK WALLET	98
6.3.2.2	YWALLET	98
6.3.2.3	ZASHI WALLET	98
6.3.2.4	ZINGO! WALLET	98
6.4	HARDWARE WALLETS	99

7 ZCASH INNER WORKINGS

7.0	INTRODUCTION	103
7.1	TRANSPARENT WORLD	104
7.1.1	GENERATING PRIVATE KEYS	104
7.1.2	TRANSPARENT PUBLIC KEYS AND ADDRESSES	108
7.2	SHIELDED WORLD	109
7.2.1	VALUE POOLS	109
7.2.2	EVOLUTION OF SHIELDED TECHNOLOGY	109
7.2.3	SHIELDED ADDRESSES AND KEYS	111
7.2.3.1	SPROUT SHIELDED ADDRESSES AND KEYS	111
7.2.3.2	SAPLING SHIELDED ADDRESSES AND KEYS	112
7.2.3.3	ORCHARD SHIELDED ADDRESSES AND KEYS	113
7.2.3.4	UNIFIED ADDRESSES	114
7.2.4	SHIELDED ADDRESSES AND KEYS	115
7.2.4.1	SPROUT TRANSACTIONS	116
7.2.4.2	SAPLING TRANSACTIONS	116
7.2.4.3	ORCHARD TRANSACTIONS	117
7.3	CONCLUSION	119

8 PROOF OF WORK AND CONSENSUS

8.0	A PRELUDE ON HASH FUNCTIONS	123
8.0.1	INTEGRITY CHECKS	123
8.0.2	HASH FUNCTIONS ARE IRREVERSIBILITY	123
8.0.3	COLLISION RESISTANCE	124
8.0.4	OTHER PROPERTY	124
8.1	THE ZCASH NETWORK AND BLOCKCHAIN	124
8.1.1	NOBODY CAN TELL YOU WHAT YOU OUGHT TO DO	125
8.1.2	THE ZCASH BLOCKCHAIN	125
8.2	PROOF OF WORK	126
8.2.1	NOBODY CAN TELL YOU WHAT YOU OUGHT TO DO	126
8.2.2	WHY DO MINERS EVEN BOTHER?	126
8.3	DESCENTRALIZED CONSENSUS	129
8.3.1	SYBIL RESISTANCE	131
8.3.2	MODIFYING THE CONSENSUS RULES	132
8.3.2.1	SOFT FORKS	133
8.3.2.2	HARD FORKS	133
8.3.2.3	NETWORK UPGRADES	133
8.3.3	DECENTRALIZATION IS A SPECTRUM	134
8.3.3.1	MINING POOLS	135
8.3.3.2	51% ATTACKS	135
8.4	ZEC ISSUANCE	136
8.4.1	THE FOUNDERS' REWARD AND DEV FUND	136
8.5	A CLOSING NOTE	138

9 APENDIX

BRINGING ZCASH TO HIGH SCHOOLS	142
GLOSSARY	144



THE POWER OF THE MONEY

1.0

READY?

Bitcoin has been called many things - a fad, a scam, “magic internet money.”

But behind the hype, there is a powerful technology that has the potential to change the way we think about and use money; the potential to change the world in a way that “normal people” like you and me have the opportunity to build wealth, become truly free and live the lives we want to live. In this course, we will explore the flaws and limitations of our current financial system and how Bitcoin offers a potential solution.

So, if you’re ready to go beyond the headlines and learn about the real possibilities of Bitcoin, **let’s dive in!**



1.1

CLASS DISCUSSION: WHAT IS MONEY?

- Please do not eat the piece of candy placed on your desk yet.
- Who would be willing to trade their candy for a US\$1 bill?
- Now, keep your hands up if you would still be willing to do the trade your candy for a \$1 monopoly bill instead for your piece of candy?

WHY OR WHY NOT?

- What makes one bill so desirable and another one as good as trash?
- What gives money its “value”?
- Where does money come from and who decides how much of it to print?
- Why not print more money and distribute among everyone equally?



NOTE

The only difference between these two notes, is your belief that one has more value than the other.

1.2

THE LIMITED WORLD: NAVIGATING SCARCITY IN A GROWING ECONOMY

- Is money backed by gold? Or, by any other commodity?
- How many people still use cash anyways?



Imagine you are stranded in a desert and you only have one bottle of water left. You are thirsty and desperate for a drink, but you also know that you will need the water to survive until you can find more.

This is a classic example of scarcity - you only have a limited amount of a resource (water) and you must make a choice about how to use it.



Scarcity forces us to weigh the pros and cons of how we use our resources and make trade-offs.



In this situation, you might decide to ration it and take small sips over a longer period of time, in order to make it last as long as possible.

Alternatively, you might decide to drink as much as you can in one go, hoping that the burst of hydration will give you the energy you need to find more water. Regardless of which choice you make, you are faced with a difficult decision.

In this case, the choice is between quenching your immediate thirst and conserving the water for later.

This concept of scarcity applies to all kinds of resources, not just water. Whether it's money, time, or even love and attention, we are constantly faced with choices about how to allocate our limited resources.

➔ There are two types of scarcity: **human-made scarcity** and **natural**.

Human-made scarcity, also known as *centralized scarcity*, includes things like limited edition designer bags, rare sports cards, and numbered art pieces. These can be easily replicated or counterfeited.

Natural scarcity, also known as *decentralized scarcity*, includes things like salt, shells, and precious metals like gold. These are harder to replicate or counterfeit.

➔ The main difference between the two is control. Centralized scarcity is controlled by a single entity, like a company or government, while decentralized scarcity is not controlled by anyone.

➔➔ An example of centralized scarcity that disproportionately affects the poor is the control of essential resources like clean water. In some regions, access to clean water is managed by private companies or government entities that may limit its distribution, leading to a scarcity of this vital resource.

This centralized control can result in price increases or unequal access to clean water, with impoverished communities often bearing the brunt of the impact. Limited access to clean water not only affects their health and well-being but also perpetuates poverty as they may be forced to pay higher prices for water or travel long distances to obtain it.

Scarcity affects our choices. Understanding it can improve our decision-making. We often have to choose between immediate gains and long-term benefits, and these trade-offs shape our path to achieving our goals.



Time preference refers to the idea that people generally prefer to have something NOW rather than later.

ANOTHER EXAMPLE:

Let's say you have the option to receive \$100 today or \$110 in a year. If you have a high time preference, you might choose to receive the \$100 today, because you value having the \$100 now more than the benefits of waiting a year for the extra \$10. On the other hand, if you have a low time preference, you'll prefer to wait for the larger reward, because you are more focused on long-term planning and less concerned with immediate gratification.

CLASS ACTIVITY

1. Listen to the teacher's explanation of the candy choice.
2. Decide whether you would like to receive a small candy or marshmallow now, or wait until the end of the class to receive two candies or a larger, more desirable candy.
3. Commit to your decision and let the teacher know your choice. Receive your candy either immediately or at the end of the class,



CONCLUSION AND DISCUSSION

➔ What factors influenced your decision to take the candy now or wait for a larger reward later?

➔ How do you feel about your decision now that the activity is over?

➔ Can you think of real-life examples where high time preference might be harmful and where low time preference might be beneficial?

➔ What are some potential consequences of choosing high time preference over low time preference?

➔ In the context of the desert example, this means that you might be more inclined to drink all of the water right away, even if it means that you won't have any left for later. This is because the thirst you feel right now is more pressing than the potential thirst you might feel in the future.

➔ On the other hand, if you choose to ration the water and drink it slowly over time, you are demonstrating a lower time preference. This means that you are willing to wait to satisfy your thirst and improve your chances of survival.

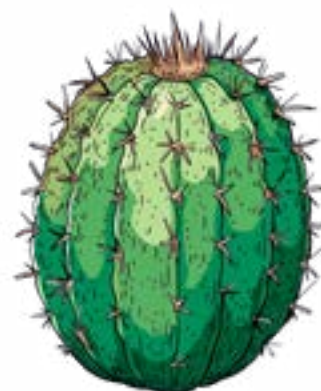
The concept of **opportunity cost** is closely related to the idea of **scarcity** and **time preference**.



Opportunity cost refers to the value of the next best alternative that you give up when you make a decision.

TODAY'S CHOICE	NOW	LATER
		
Buying a \$7 strawberry smoothie.	Benefiting from \$7 saved regularly.	Spending \$7 another way.

- In the desert example, the opportunity cost of drinking all of the water right away is the survival benefits you would have gained from rationing the water and using it over a longer period of time.
- Let's say that you decide to ration the water and take small sips over a longer period of time. As a result, you have the energy and hydration you need to search for more water.
- However, while you are searching, you come across a cactus that has a small amount of water inside. It's not a lot, but it's enough to quench your thirst for the moment. If you had decided to drink all of your water at once, you might not have had the energy to search for more water and come across the cactus. In this case, the **opportunity cost** of drinking all of your water at once would have been the chance to find the cactus and get more hydration.



This example illustrates how opportunity cost involves not just the immediate **trade-off** between two options, but also the potential future opportunities that may be gained or lost as a result of our choices. Our willingness to give up a larger reward in the future in exchange for a smaller reward now is influenced by our **time preference**, or how much we value immediate gratification versus long-term planning.

CORPORATIONS, GOVERNMENTS, AND SOCIETIES ALSO HAVE TO MAKE CHOICES.

CORPORATIONS	GOVERNMENTS / SOCIETIES
Firing 200 Employees vs. Freezing Wages	Funding Cancer Treatment Research vs. Clean Energy
Asking for a Loan vs. Bringing in more Shareholders	Building a New Highway vs. Increasing Teacher Salaries

1.3

DEFINITION OF MONEY

1.3.1 WE CAN USE IT, BUT CAN WE DEFINE IT?

Have you ever stopped to think about what money really is? Ever even wonder what makes money, well, money? Most of us know how to use it, but not many of us understand where it comes from or how it works.

Money is essentially a way to exchange goods and services. It represents the value of these items in a form that can be easily traded.

This can take many different forms, such as paper notes, metal coins and electronic payments. Governments or other authorities typically issue and control money.

But money is so much more than just a physical or digital medium of exchange. It's like a universal language that allows us to trade with people all around the world, even if we don't speak the same language or have the same culture. For example, you can be on the other side of the world and still "speak" money by placing a product on the counter and exchanging it for the local currency or using a credit card. Money is like a social contract that allows us to make exchanges without having to rely on bartering or finding someone who specifically wants what we have to offer. If a group of people started accepting chocolate as payment for most goods and services, chocolate would become money. (Although, since it would melt in some parts of the world, we might consider it bad money.)

As French economist Jean Baptiste Say pointed out, "Money performs but a momentary function in an exchange; and when the transaction is finally closed, it will always be found that one kind of commodity has been exchanged for another."



Transaction is an exchange or transfer of goods and services. It is a way of exchanging value between two or more parties.

Without money, how easy or feasible would this trade be?
Would you trade one cow for 1,000,000 strawberries?
Or is it 600,000 strawberries?
How about 50,000?



In other words, money itself doesn't have the power to satisfy human wants. It's just a tool that allows us to trade one commodity for another.

There are many different types of transactions, ranging from simple exchanges (such as buying a sandwich at a deli) to more complex financial transactions (such as buying a house or investing in stocks or bonds).

Transactions can be conducted in person, over the phone, online, or through other means, and they can involve a wide range of parties, including individuals, businesses, and financial institutions.

IN SUMMARY, MONEY:

- Facilitates trade because everyone accepts it as final payment.
- Allows us to measure the value and to make comparisons between different goods and services.
- Lowers our time preference, as it allows us to save and spend it in the future.



Money IS the value BY which goods are exchanged.
Money IS NOT the value FOR which goods are exchanged.



Unit of Account

Consumers know the value of something when you assign a price (monetary value) to it.

1.3.2 FUNCTIONS OF MONEY

When it comes to buying and selling goods and services, money is the key player. It has several important jobs, like:

- Making exchanges easier:** With money, you Medium of Exchange don't have to find someone who wants exactly what you have to trade. Instead, you can use money to buy and sell anything you want. This makes trading and commerce much more convenient and efficient.
- Being a unit of account:** Money provides a universal standard of value that allows people to express and compare the price of different goods and services. This allows for a more efficient and transparent market, where people can make informed decisions about what to buy and sell.

Think of it like this: if you wanted to buy a new car, you could compare prices from different dealerships and make an informed decision about which one to buy based on the price in dollars.

Without a unit of account, you'd have to try to compare the value of one car to another using something else, like the number of cows it was worth or the length of time it took to make the car.

- Being a store of value:** Money should maintain its value over time, making it useful as a way to save and invest the value of human labor. This lets people use money to plan for the future and to borrow and lend money.
So next time you're saving up for something special, remember that money is more than just a way to pay for things - it's a tool to help you plan and invest in your future.

WHAT'S YOUR STORE OF VALUE?

	BTC (USD)	Gold (USD)	USD (EUR)	ETH (USD)
March 14, 2019	\$3,846	\$1,293	€0.8817	\$136.86
March 14, 2020	\$5,258	\$1,529	€0.90056	\$127.76
Gain/Loss	+36.71%	+18.25%	+2.14%	6.65%

So next time you're saving up for something special, remember that money is more than just a way to pay for things - it's a tool to help you plan and invest in your future.

These three functions are what allow economies to become complex and dynamic. Without money, it would be much harder to buy and sell goods and services, and our economy would be much less developed.

CLASS EXERCISE

WHAT FUNCTION OF MONEY IS THIS AN EXAMPLE OF?

- Roby decided to save a portion of his weekly paychecks to buy a puppy.
- Jim buys two slices of pizza for \$8.30 at Ray's Pizza.
- Marc can't decide whether to buy concert tickets for \$75 or buy a ski pass for \$95.



1.3.3 MONEY CHARACTERISTICS

Over time, people ultimately have realized that money must possess certain qualities in order to be effective as a medium of exchange. These characteristics include durability, portability, divisibility, fungibility, scarcity, and acceptability.

- Durability** refers to the ability of money to resist physical deterioration and last over time. deterioration and last over time. This ensures that money can circulate in the economy in an acceptable and recognizable state.
Gold is a durable material that can withstand wear and tear, making it a good representation of the durability characteristic of money.

- Divisibility** refers to the ability of money to be divided into smaller units, so that people can use it to make purchases of varying amounts.
Paper bills can be easily divided into smaller denominations, making them a good representation of the divisibility characteristic of money.

- Portability** refers to the ease with which money can be transported and carried around. This allows people to use money to buy and sell goods and services without difficulty.
Credit cards are portable, as they can easily be carried in a wallet or purse, making them a good representation of the portability characteristic of money.

- Scarcity** refers to the limited supply of money, which helps to maintain its value and prevent us from having to spend more money to buy the same amount of goods.
Collectible stamps, especially rare and valuable ones, can be a good form of money because they are scarce and can appreciate in value over time. Stamp collectors often use their stamps as a way to invest their wealth and to diversify their portfolio.

- Acceptability** refers to the widespread acceptance of money as a form of payment, so that people can use it to buy and sell goods and services with confidence.
The US dollar is widely accepted as a form of payment, making it a good representation of the acceptability characteristic of money.

- Fungibility** refers to the interchangeability of money, so that one unit of money is equivalent to another unit of the same value.
Money should be **uniform**.



Copper coins are uniform in size and weight, making them a good representation of the uniformity characteristic of money.

One cent is always one cent.

Overall, these characteristics make money a useful and effective tool for facilitating trade and commerce, and they are essential for the development and stability of economies.

Use the following questions to help you determine how well the different items in the table meet the characteristics of money.



CLASS EXERCISE

Different assets have different properties and perform the functions of money to varying degrees. Society ultimately determines which asset is used as money based on factors such as its stability, scarcity, divisibility, transferability, and acceptance as a medium of exchange.

To determine how well different items meet the specific characteristics of money, you can score each item on a scale from 1 to 5 for each characteristic. By tallying up the scores for each item, you can determine which one is best suited to be a form of money.

[0 = Terrible; 3 = Okay; 5 = Excellent]

*Please do not fill in the column for Zcash; we will return to it later in the course.

Durability: Can the money withstand wear and tear over time?






Fungibility: Is the money interchangeable with other forms of money?

Acceptability: Is the money widely accepted as a form of payment?

Scarcity: Is the money scarce and not too abundant?

Portability: Can the money be easily transported and used in different locations?

Divisibility: Can the money be divided into smaller units for transactions?

CHARACTERISTIC OF GOOD MONEY	 Cows	 Chocolates	 Diamonds	 Euros	 Zcash
DURABLE					
PORTABLE					
UNIFORM					
ACCEPTABLE					
SCARCE					
DIVISIBLE					
TOTAL					

1.3.4 TYPES OF MONEY


Money can be divided into two main categories: physical and digital.

Physical money includes:


Fiat money, which is the paper bills and coins issued by governments and accepted as a medium of exchange.

Representative money, which represents a claim on a physical commodity.


Commodity money, which is a physical object that has intrinsic value and is widely accepted as a medium of exchange. For example, gold and silver.




Commodity money
Objects like this gun powder once served as commodity money.



Representative money
Representative Money like this silver certificate could be exchanged for silver.



Fiat money
Today, Federal Reserve notes are fiat money, decreed by the federal government to be an acceptable way to pay debts.



DIGITAL CURRENCIES, on the other hand, can be used for online transactions and include electronic currencies, stablecoins, and cryptocurrencies.

ELECTRONIC CURRENCIES are digital versions of regular money, like dollars or euros, and can be used to buy and sell things online via digital payment rails.

Cash

ACH

Checks

Whire transfer

Card Network

Crypto

Payment rails are the infrastructure that enables the movement of electronic currencies and other digital assets from one place to another. However, in the traditional financial system, there is always a middleman, such as a bank or financial institution, that charges a fee and has the authority to accept, cancel, revert, or delay transactions.

In the intermediated financial system, the main types of digital payment rails include card networks, which facilitate the transfer of funds between financial institutions and merchants when a customer makes a purchase using a debit or credit card, and digital wallets, which are online accounts that allow users to store and manage their electronic currencies and make payments by transferring funds from their account to the recipient's account.



Central Bank Digital Currencies (CBDCs): are digital versions of a country's fiat currency, which are issued and backed by the central bank and intermediated by the government. CBDCs are not cryptocurrencies, as they are issued by a central authority and do not use decentralized payment rails.

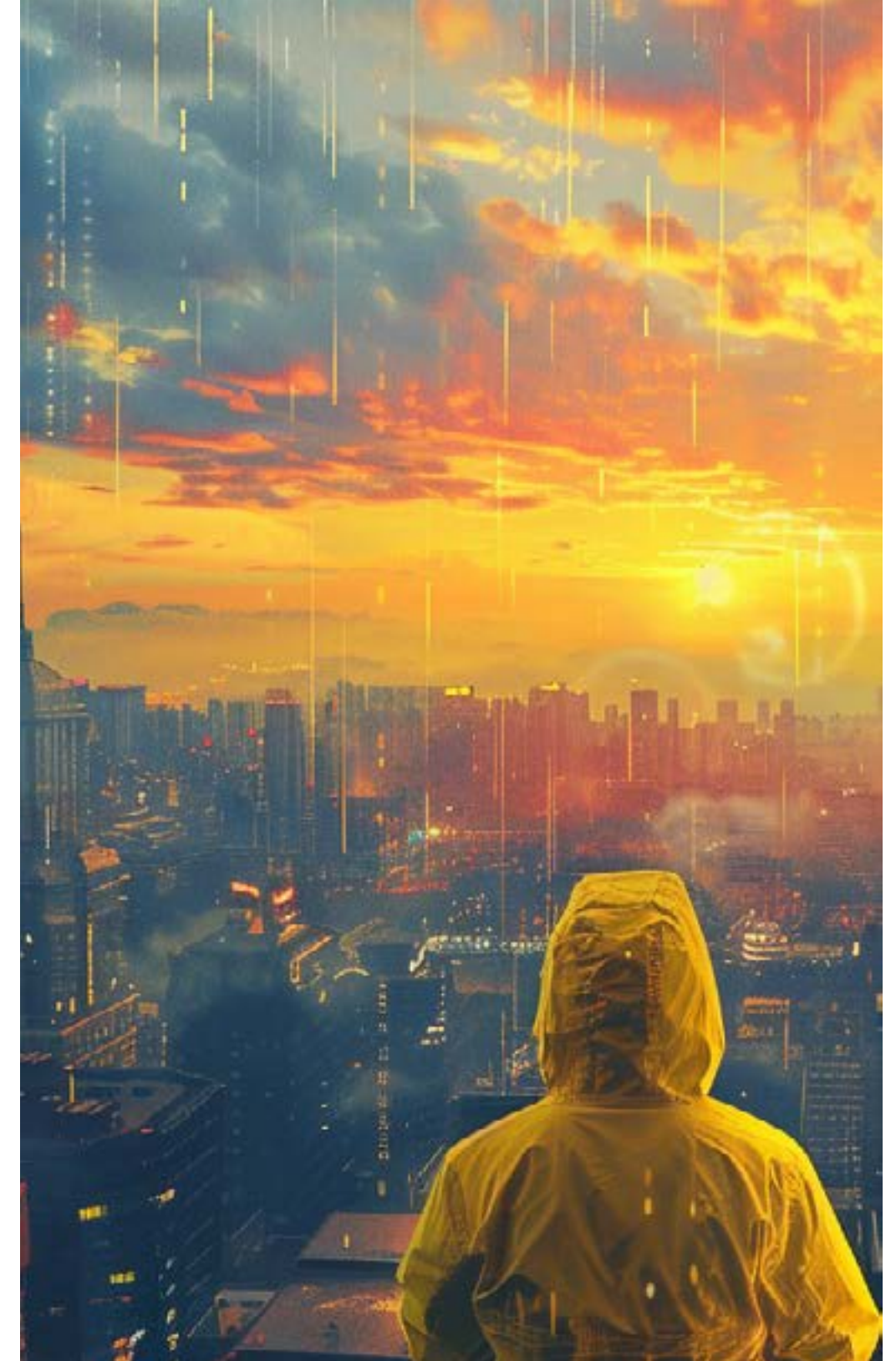


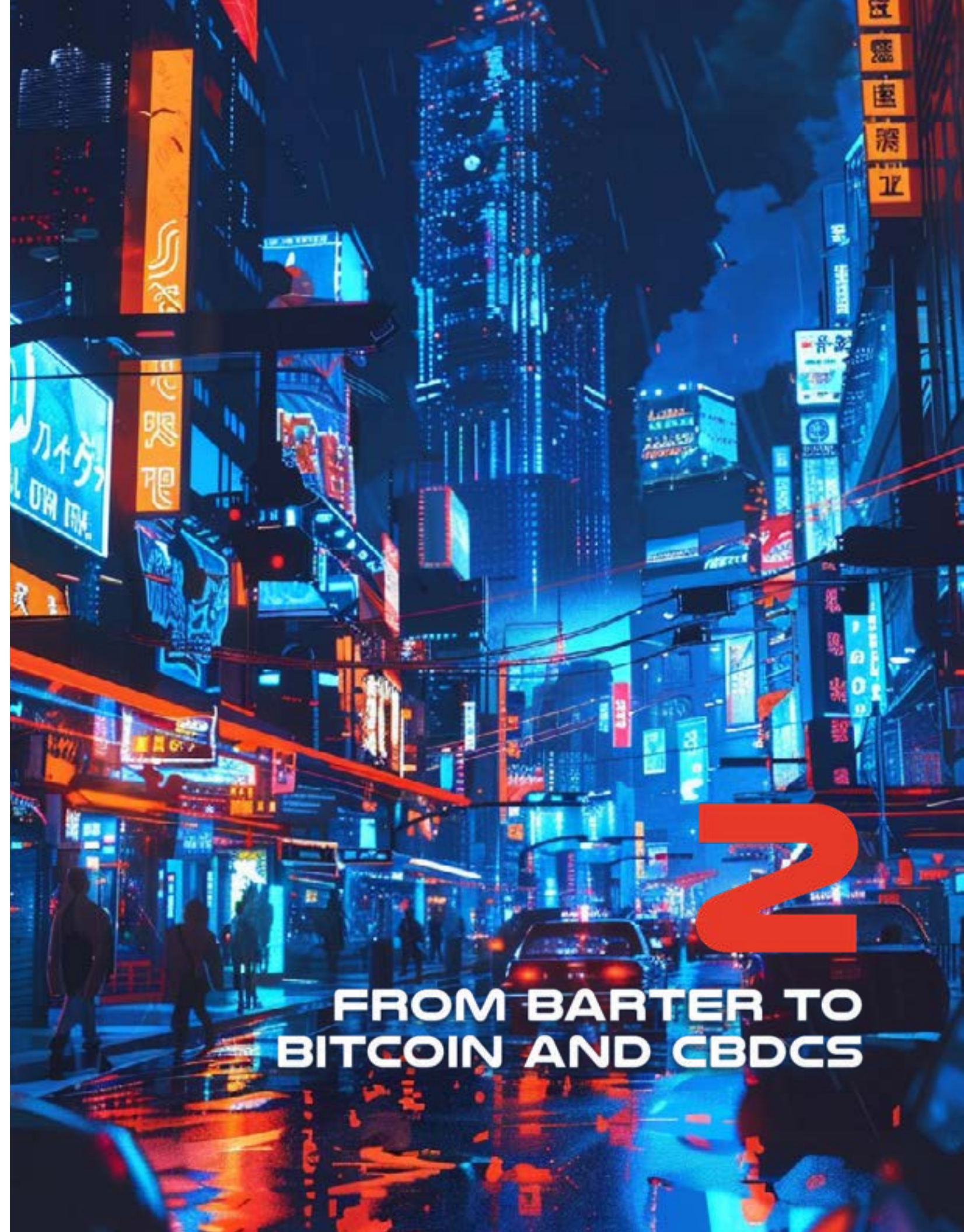
Stablecoins are cryptocurrencies that are designed to maintain a stable value relative to an asset, like the US dollar. Some stablecoins are intermediated, meaning they require a middleman like a bank to operate, while others are decentralized and do not require intermediaries.



Cryptocurrencies are a type of digital currency that use decentralized payment rails to move from one place to another online. They can be transferred and exchanged directly, without the need for a middleman like a bank. Cryptocurrencies are not intermediated, meaning they do not require a central authority or intermediary to operate.

Ultimately, a currency that operates without intermediaries is more efficient and beneficial for society, as it prevents a few individuals from controlling the money supply and concentrating their power. However, creating such a currency that facilitates secure transactions without relying on trust between parties has been a challenge throughout history. To achieve this, a currency must be created that operates like the internet, where control is distributed among everyone and no one at the same time. This requires the agreement of all parties, including those who hold power, to relinquish control for the greater good.





2

**FROM BARTER TO
BITCOIN AND CBDCS**

INTRODUCTION

The concept of money has evolved over time. In its early forms, money was used to facilitate trade and exchange of goods and services.

- In ancient civilizations, people relied on bartering, a system of direct exchange of goods and services without the use of a medium of exchange.
- Later, metal coins and paper currency were introduced as more convenient forms of money, paving the way for the sophisticated financial systems we have today.

In this chapter, we will embark on a journey through time, experiencing the evolution of money firsthand. We'll trace its origins and observe how it has changed and adapted through history.

EXERCISE: BARTER GAME

Your teacher has given you a small piece of paper. Your goal is to trade what you **"have"** with what you **"want"** in a game of commerce throughout history. Please write your name on the top of the paper in small legible letters.

ROUND #1 BARTER

It is the year 6000 B.C.E. Needless to say, money as we know it has not been invented. You are in Mesopotamia and directly exchange goods and services with one another through **bartering**.



As a side-note, many businesses still accept non-monetary payments for their services, and governments treat these bartered transactions the same as currency transactions for tax reporting purposes.

Cut your sheet of paper at the dashed line. Your goal is to trade away your have as many times as you need to finally get your original **"want"**. You cannot change your original **"want"**. You will have 5 minutes to accomplish the goal of this exercise.

When your new **"have"** matches your original **"want"**, return to your seat. After the time is up, if you have not found a trading partner, return to your seat anyway. Raise your hand if you were able to get what you wanted after one trade. Two? Three?



Zcash
2016



Electronic
Money



Plastic Cards
1959



Bretton Woods
System
1945-1971



Paper
Money



Metal Coins
700 BCE



Gold



Barter System
9,000 BCE

QUESTIONS

Answer the following questions briefly but substantially.

1. Why were some of you able to get someone to trade with and others were not?
2. What are the benefits of barter?
3. Based on your experience with this exercise, what are the drawbacks to using barter?

ROUND #2- COMMODITY MONEY

Fast forward and travel to the western coast of Africa sometime around the 14th century BCE. Bartering has become tedious and inefficient. We have evolved as a civilization and are now using *commodity money*.

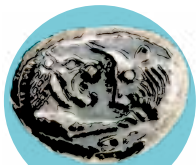
COWRY SHELLS TO COINS



1,300 BCE



1,000 BCE



687 BCE

1,300 BCE
Cowry shells are the predominant form of payment in most of Asia, Africa, Oceania, and some parts of Europe.

1,000 BCE
China's Western Zhou dynasty begins using metal coins.

687 BCE
King Alyattes of Lydia (present-day Turkey) orders the first metal coins to be minted in the Western world.

FUN FACT
Cowry shells were accepted as legal tender in some parts of Africa until the 20th century.

These proto-coins were oval-shaped, made from "electrum" (a gold/silver alloy), and had a design on one side only.

Your teacher has given you one macaroni (for simplicity purposes). Let's assume that by convention, the price of each good is worth one macaroni. Your goal again is to obtain what you "want" . But now, our species has smartened up a bit and found a way to solve certain problems.

- Why do we consider macaroni commodity money?
- How do we get the things we want now?
- Was the macaroni round easier?
- Why do you think money has replaced commodities?
- In what ways is using commodity money more efficient than bartering?
- What are the drawbacks to using macaroni as money?
- What do you think happened when Spain started to bring back boatloads of macaroni into your community (gold and silver from the Americas back to Spain)?



2.1

EARLY FORMS OF MONEY

In barter economies, people trade with each other based on the relative value of the goods and services that they have to offer. Barter economies are inefficient and can be difficult to manage, especially in complex societies.

A situation, known as the double coincidence of wants, is necessary in any bartering system since people must always find someone who has what they want but also wants what they have to offer.

LET'S SUPPOSE

- Joseph wants to trade his banana for Yael's coconut.
- But Yael only wants to trade her coconut for Tammy's mango.
- And Tammy only wants to trade her mango for Joseph's banana.
- They are stuck in a never-ending cycle of fruit trading without a double coincidence of wants.
- Joseph suggests they just trade their fruits for a nice cold soda, but they realize they are on a remote island and there is no soda.
- They decide to just sit on the beach and enjoy their fruits in silence.



Using a common unit of account, such as a "soda" , makes trade and commerce much more efficient. In ancient times people began by using beads, shells, and other items that had value in their society as mediums of exchange.

2.2

FROM COMMODITIES TO I.O.U'S

As you and your community become more involved in trade and commerce, you realize the limitations of using bartering and other forms of non-monetary exchange. You decide to adopt the use of metal coins as a form of money.



These metal coins are made of valuable materials like gold and silver, and they serve as a medium of exchange and unit of account to facilitate trade and commerce: commodity money.

However, as you begin to use metal coins more frequently, you encounter some drawbacks. They can be heavy and inconvenient to carry in large transactions, and you notice that some people are taking advantage of the system by melting down the coins and creating new ones by mixing them with cheaper metals, which causes prices to rise and undermines trust in the system.

In an effort to address these issues, you and your community start to use paper receipts as a form

of money. These paper receipts, which have their origins in ancient China, are a convenient and easily exchangeable form of currency. They are backed by gold and other valuable metals, and can be converted into these metals during the seventeenth through the nineteenth century. This allows you to have a more portable and easily transferable form of money, while still maintaining the value and security of precious metals.



2.3

TRANSITION FROM SOUND MONEY TO UNSOUND MONEY

Fast forward to the 17th century in Sweden. Now you are completely dependent on banks to store your valuable assets. However, you start to notice something fishy going on with these bankers. It seems they are issuing more paper receipts than they have gold in storage, allowing them to create more money than they have assets to back it up. This sneaky practice allows the bankers to profit from the difference between the value of the paper receipts and the value of the gold they are holding for their customers.

You realize that this marks a major shift in the way money works. You are moving from a system of sound money (i.e. money backed by precious metals) to a system of unsound money (i.e. fiat currency not backed by a physical commodity). This transition didn't happen overnight, but rather was a gradual process influenced by several factors. The Industrial Revolution, with its mass production and urbanization, played a role, as did the growth of advanced financial systems like banks and stock markets. The emergence of central banks and other monetary authorities contributed to the centralization or the control of money, leading to the issuance of fiat currencies to support economic growth.

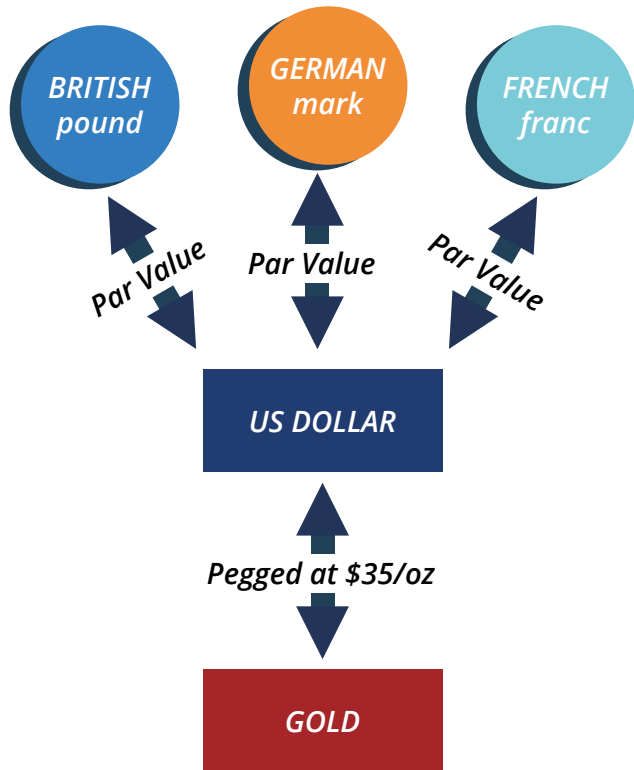


However, you also begin to see the downsides of this centralization, including irresponsible consumption, an increase in debt, and manipulation of citizens through economic incentives.

Until World War I, you were able to convert your paper money into a preset amount of gold. But the two world wars and the 1929 economic crisis put an end to that. In 1944, the Bretton Woods agreement is signed, establishing the U.S. dollar as the world's reserve currency and fixing the value of the U.S. dollar to the price of gold at a rate of \$35 per ounce. Other countries' currencies are pegged to the dollar, which helps to stabilize international financial markets.



BRETTON WOODS SYSTEM (1945-1972)



Unfortunately, the system begins to break down in the late 1960s, leading to the Nixon Shock in 1971, when the U.S. government suspends the convertibility of the dollar into gold. This marks the end of the gold standard and the beginning of a world driven by the creation and accumulation of debt.

As you go about your daily life, you begin to notice that the value of money is no longer as stable as it used to be. Just like a flexible ruler makes it difficult to accurately measure the length of a table, living in a fiat world where the value of money is subject to the unpredictability of those in power can also make it difficult to accurately measure the value of goods and services. You feel confusion and unease adjusting to a world where the value of money is no longer tied to a physical commodity like gold.

You see the impacts of this shift on the global economy and start to question the stability and reliability of fiat currencies. You realize that in this modern world, the dollar is no longer fixed and consistent as it was when it was pegged to gold, but instead becomes subject to fluctuation. This makes it more difficult to use the dollar as a unit of account, as its value is affected by various factors including inflation (rising prices), interest rates, the strength of the country's economy, political events, market speculation, and demand in international trade. It can be a confusing and unpredictable time, as you try to navigate the constantly shifting value of the dollar and its impact on your daily life.

Despite efforts to improve quality of life through modern monetary systems, increased efficiency, greater access to information, and enhanced communication, the majority of people's standards of living begin to decline due to:

- Abuse of centralization.
- Rising prices.
- Stagnated real wages.
- Weakening currencies.
- The need to spend more money for fewer things.



This has challenges for those with lower economic resources, who may have limited access to education, credit, resources, social networks, and political representation, leading to potential disadvantages in their ability to succeed.

As a result, the rich seem to keep getting richer and the poor seem to keep getting poorer.

"I don't believe we shall ever have good money again until we take the thing out of the hands of government... all we can do, is by some sly, roundabout way, introduce something that they can't stop."

Friedrich Hayek,
Nobel Prize Winner of Economics

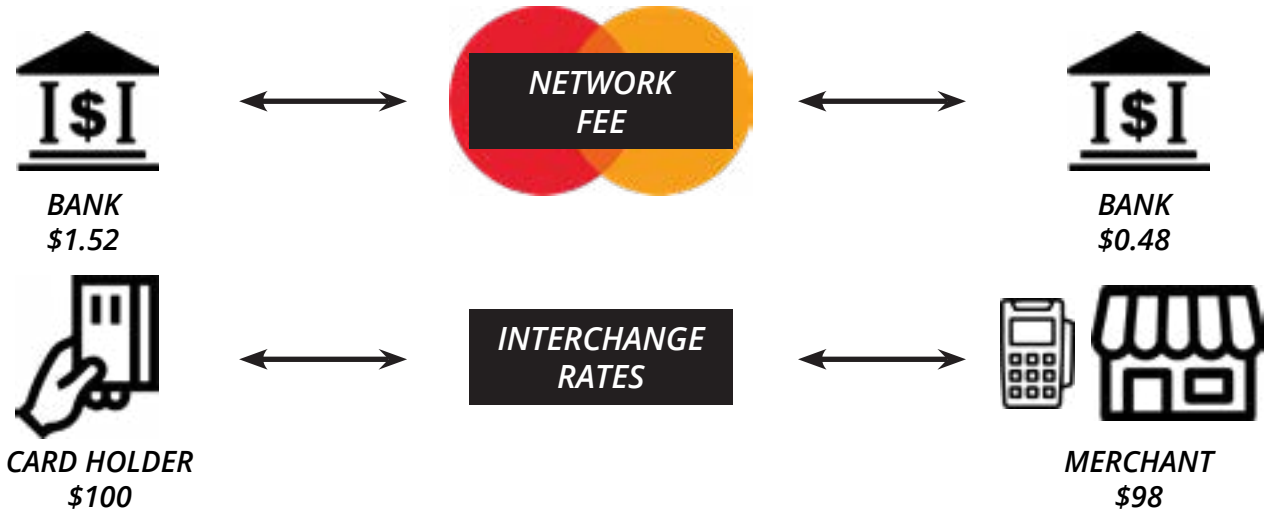


2.4

TRACING THE EVOLUTION: FROM PLASTIC TO DIGITAL

Today, we've come a long way from the introduction of the first credit card back in the 1950s. With a simple swipe of plastic, we can buy whatever we want, whenever we want, without any hassle. It's like opening up a world of endless possibilities, and the excitement of discovering what it holds is palpable... or so we thought. Little did we know that our reliance on credit would have painful aftereffects - like raising the overall cost of goods, and incentivizing a certain economy doomed to fail.

As technology advances, so does the way we handle money. The internet becomes a major player in the financial world, with online banking and e-commerce websites making it possible to manage and spend money entirely online.



Then, in 2009, the first decentralized cryptocurrency, bitcoin, is created. As its popularity grows, it inspires the creation of new technologies and unknown frontiers for the future of money. And so, as we'll learn, we've come full circle from sound money to unsound money and back again, sound money finding new wind in its sails for the first time in almost a hundred years.

2.5

THE RISE OF A CASHLESS SOCIETY

When the first credit card was introduced in the 1950's and people rejoiced at the thought of never having to carry around actual cash again. No more fumbling for loose change or awkward check- writing moments at the checkout counter. All those pesky intermediaries can now take their cut without you even realizing it, just like a toll on a network. Ah, the convenience of modern finance.

But with the rise of digital currencies like CBDCs, it's like we've gone from paying a fee for using the network to having to ask permission. Worse, now we expect to be searched, scanned, and scrutinized by the government every time we pass through. Control and surveillance has taken the place of convenience. And just like the fee from the network, these intrusions into our financial lives come with a cost, whether it's monetary, a violation of privacy, or the loss of autonomy.



The question is, are we willing to pay the price for the convenience of modern finance, or will we seek out alternative options that prioritize our freedom and privacy?

As more of our daily transactions move online, the use of cash declines. Governments and financial institutions around the world are promoting the use of electronic payments and cracking down on the use of physical money.

This trend has sparked a debate about the future of cash and the potential consequences of a cashless society.

The war on cash is a term that refers to the various efforts to reduce the use of physical money, remove high-denomination bills and promote the use of electronic payments.

Proponents of the war on cash argue that it will make transactions faster, more convenient, and more secure. Critics, however, fear that it could lead to a loss of privacy and financial inclusion and increased risks of fraud and cyber-attacks.

The Global War on Cash There is a global push by lawmakers to eliminate the use of physical cash around the world. This movement is often referred to as "The War on Cash", and there are three major players involved:

- ✳ **The Initiators**
- ✳ **The Enemy**
- ✳ **The Crossfire**

Desjardins, Jeff. "The Global War on Cash." *Visual Capitalist*, 27 Jan. 2017, <https://www.visualcapitalist.com/globalwar-cash/>.

Q: How do traditional banking methods put individual's financial data at risk?

A: With credit cards, debit cards, wire transfers, and other centrally controlled payment networks, individuals are giving their private financial transaction data to a third party and potentially sacrificing their rights to privacy.

In this infographic, we will provide an overview of the war on cash and explore all sides of the debate. We will look at the reasons behind the push for a cashless society, the challenges and concerns that it raises, and the potential impacts on individuals, businesses, and society as a whole.



THE INITIATORS

WHO?

Governments, central banks

WHY?

The elimination of cash will make it easier to track all types of transactions, including those made by criminals.



THE ENEMY

WHO?

Criminals, terrorists

WHY?

Large denominations of banknotes make illegal transactions easier to perform, and increase anonymity.



THE CROSS FIRE

WHO?

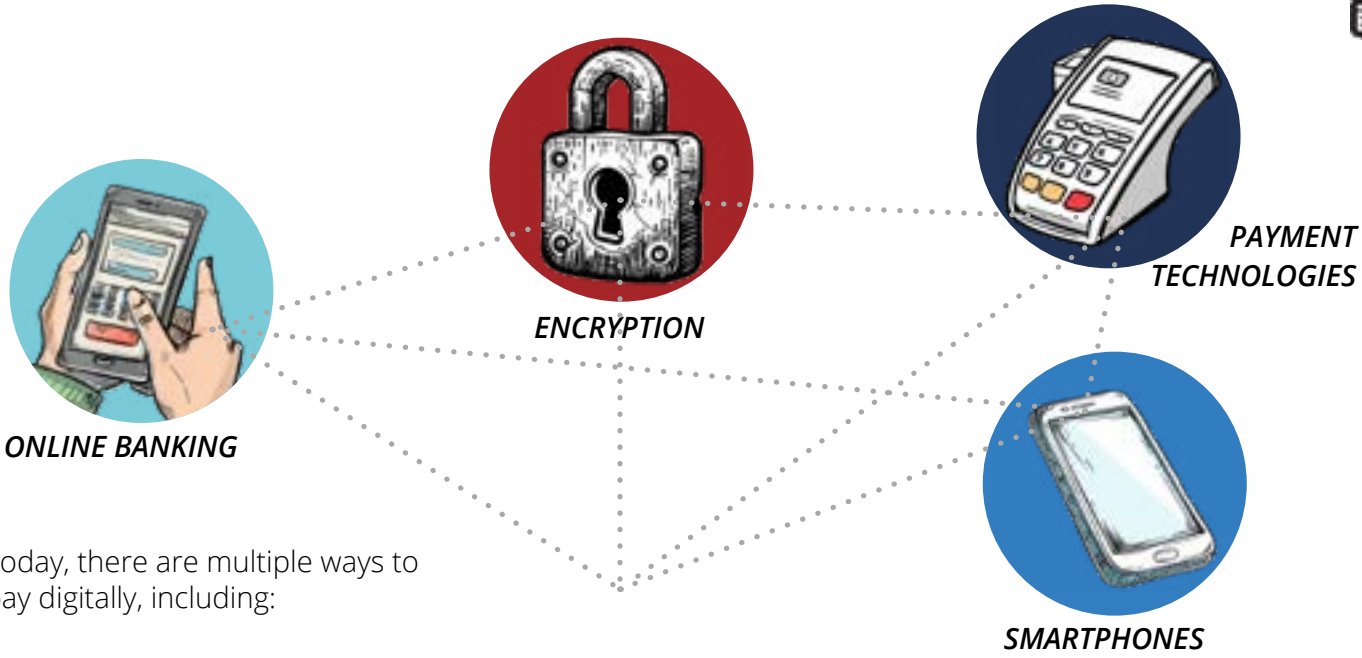
Citizens

WHY?

The coercive elimination of physical cash will have potential repercussions on the economy and social liberties.

IS CASH STILL KING?

Cash has always been king - but starting in the late 1990s, the convenience of new technologies have helped make non-cash transactions to become more viable:

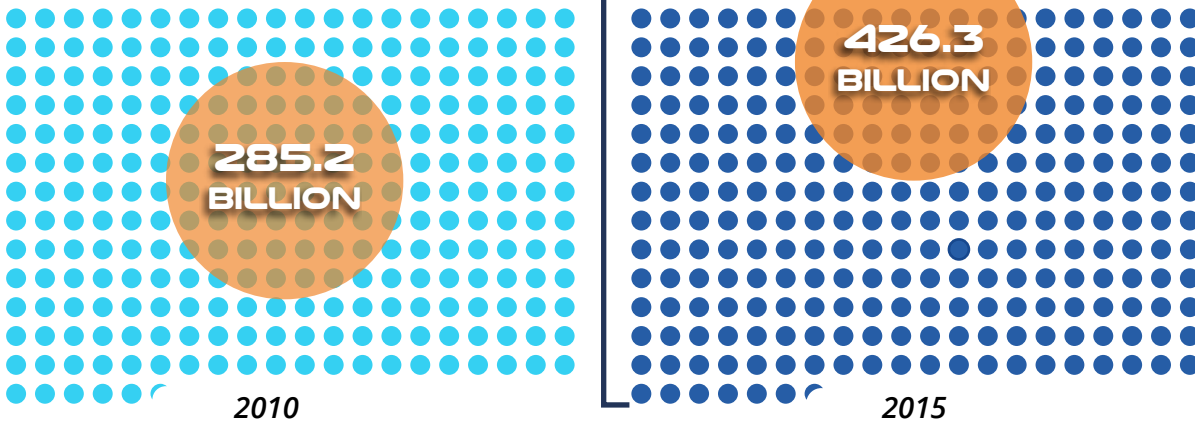


Today, there are multiple ways to pay digitally, including:



By 2015, there were 426 billion cashless transactions worldwide

- a 50% increase from five years before.



THE FIRST SHOTS FIRED

The success of these new technologies has prompted lawmakers to posit that all transaction should be now digital. Here is their case for a cashless society:

Removing high denominations of bills from circulation makes it harder for terrorists, drug dealers, money launderers, and tax evaders.

1

\$1 million in \$100 bills weighs only ten kilograms (22lbs).

Criminals move \$2 trillion per year around the world each year.

The U.S. \$100 bill is the most popular note in the world, with 10 billion of them in circulation.



Money that is traceable means higher tax revenues.

It also means there is a third-party involved with all transactions.

Central banks can dictate interest rates that encourage (or discourage) spending to try to manage inflation. This includes ZIRP or NIRP policies.

2

This gives regulators more control over the economy.

3

Banks would incur less costs by not having to handle cash.

It also makes compliance and reporting easier.

The "burden" of cash can be up to 1.5% of GDP, according to some experts.



Cashless transactions are faster and more efficient

For this to be possible, they say that cash, especially large denomination bills, must be eliminated.



After all, cash is still used for about 85% of all transactions worldwide.

CAUGHT IN THE CROSSFIRE

Cashless transactions would always include some intermediary or third party.

Increased government access to personal transactions and records.

Certain types of transactions (gambling, etc.) could be barred or frozen by governments.

Decentralized cryptocurrency could be an alternative for such transactions.



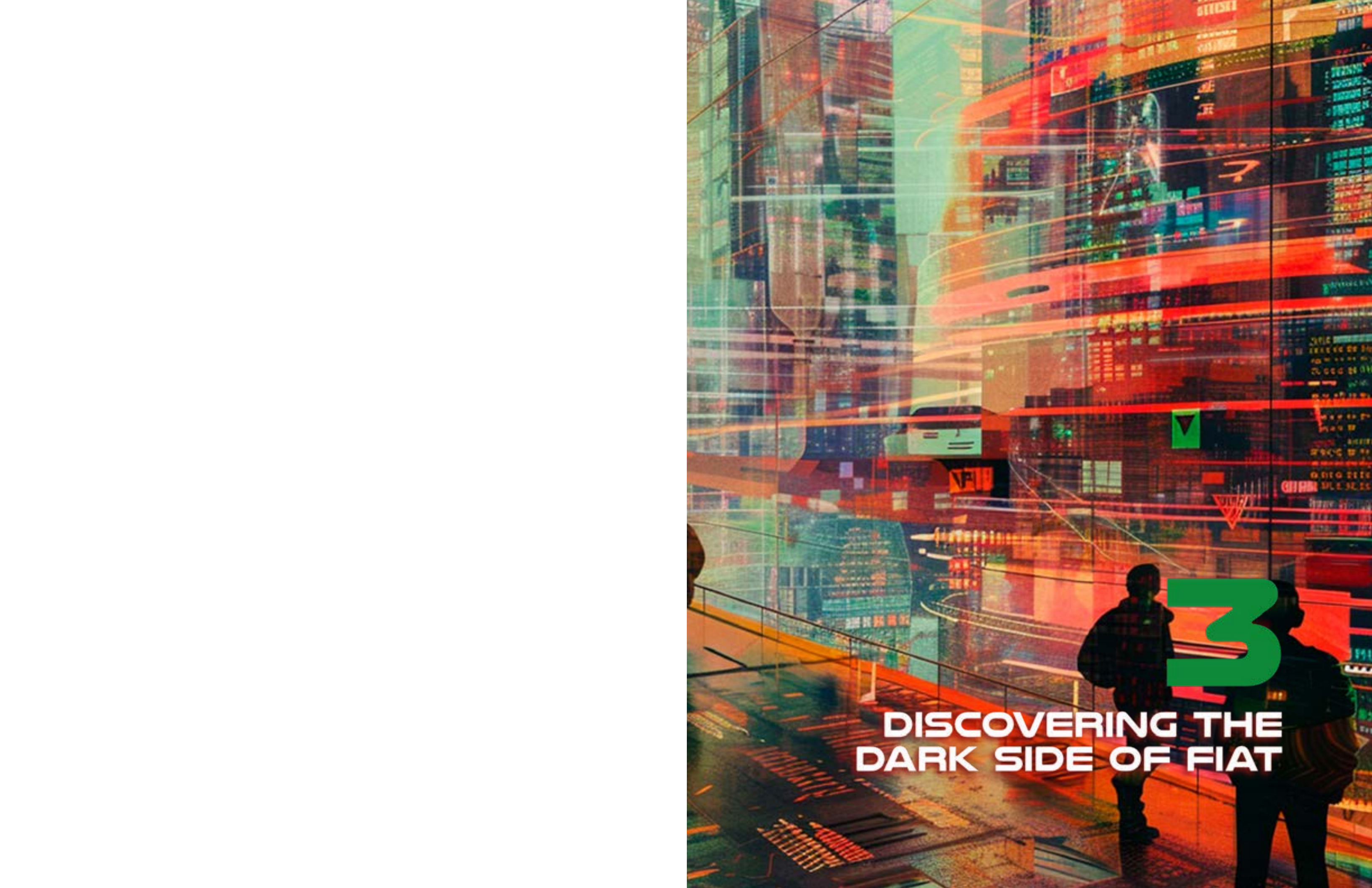
- ▶ Savers could no longer have the individual freedom to store wealth "outside" of the system.
- ▶ Eliminating cash makes negative interest rates (NIRP) a feasible option for policymakers.
- ▶ A cashless society also means all savers would be on the hook for bank bail-in scenarios.
- ▶ Savers would have limited abilities to react to extreme monetary events like deflation or inflation.

Rapid demonetization has violated people's rights to life and food. In India, removing the 500 and 1,000 rupee notes has caused multiple human tragedies, including patients being denied treatment and people not being able to afford food. Demonetization also hurts people and small businesses that make their livelihoods in the informal sectors of the economy.



- ▶ For this to be possible, they say that cash, especially large denomination bills, must be eliminated. The shots fired by governments fighting the war on cash may have several unintended casualties.
- ▶ With all wealth stored digitally, the potential risk and impact of cybercrime increases.
- ▶ Hacking or identity theft could destroy people's life savings. The cost of online data breaches is reached \$2.1 trillion by 2019, according to Juniper Research.





DISCOVERING THE DARK SIDE OF FIAT

3.0

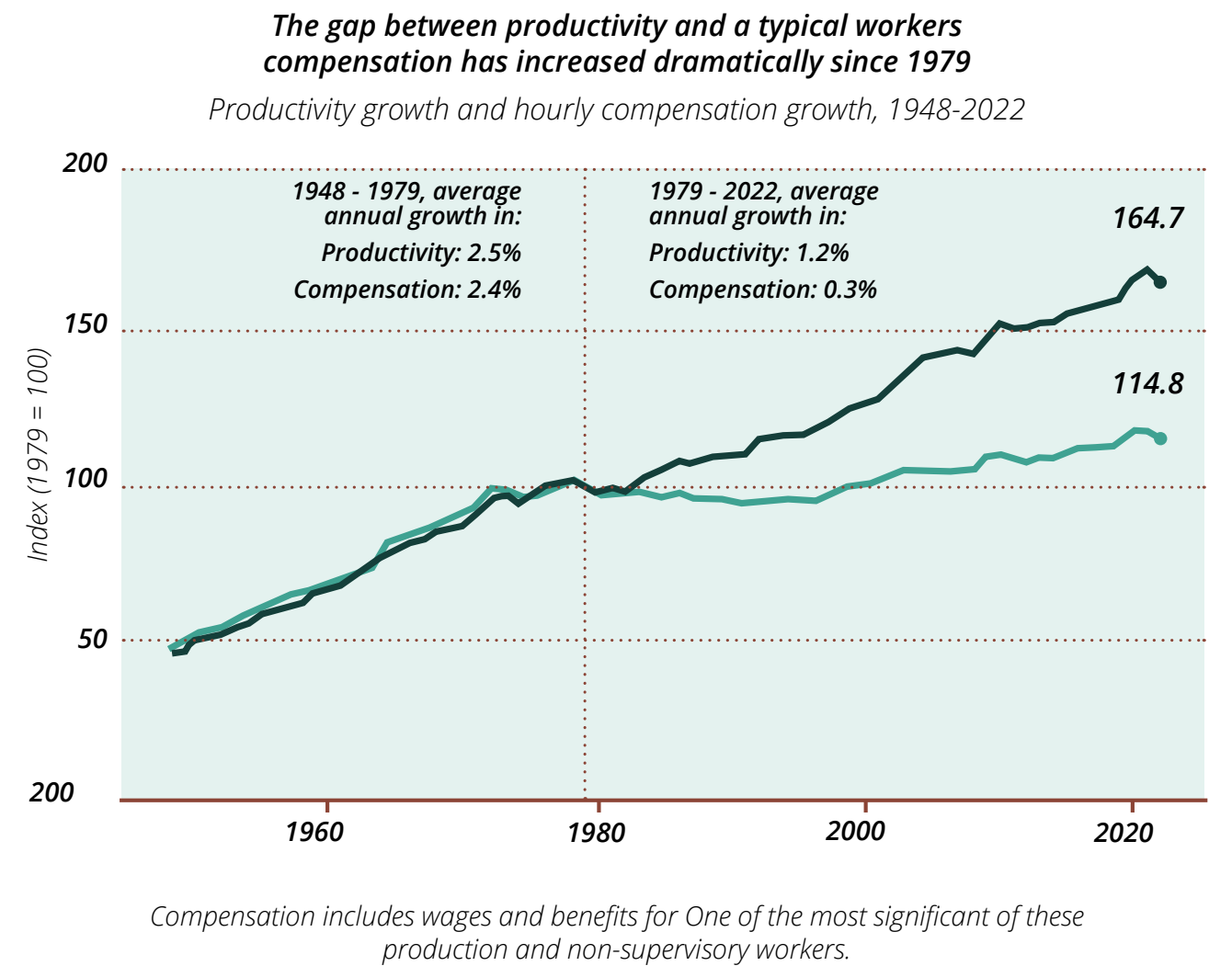
DRAWBACKS OF THE FIAT SYSTEM

In this chapter, we will explore the drawbacks **Growth in Productivity and Hourly** of the traditional fiat system and how it benefits those in power at the expense of the majority.

The fiat system is a monetary system that is based on government-issued currency that is not backed by a physical commodity like gold or silver. Instead, the value of fiat currency is based on the faith and credit of the government that issued it.

Although the fiat system has its benefits, such as stability and flexibility, it also has significant drawbacks. One of the most significant of these is the way it perpetuates power dynamics and wealth inequality.

History often echoes through time, revealing patterns that are strikingly familiar.



For instance, during the 2008 financial crisis, the US government bailed out large corporations such as AIG, Citigroup, and Bank of America. These bailouts were paid for with taxpayer money, but they disproportionately protected the interests of the wealthy while leaving ordinary citizens to bear the burden of economic hardship. In fact, a study by the Congressional Budget Office found that the top

1% of income earners received 95% of the income gains from the recovery after the 2008 crisis, while the bottom 90% of income earners experienced a decline in their income.

Furthermore, the manipulation of the money supply by governments and central banks can exacerbate the problem of wealth inequality. **Inflation** and **debasement** of currency pose significant threats to the value of money in a fiat system, often disproportionately affecting the middle and lower classes.

Inflation occurs when the general level of prices of goods and services in an economy increases over time. It reflects a reduction in the purchasing power of money and results in a loss of real value in the medium of exchange and unit of account within an economy

Purchasing power refers to the amount of goods or services that can be purchased with a certain amount of money. In other words, it's a measure of how much you can buy with your money.

➤ For example, if you have \$100 and the price of a loaf of bread is \$2, you can purchase 50 loaves of bread with your money. However, if inflation occurs and the price of bread increases to \$4, your purchasing power decreases and you can only purchase 25 loaves of bread with your \$100.

In addition, debasement of currency occurs when the government reduces the value of its currency by increasing the money supply or decreasing the quality of the currency.

To better illustrate the impact of inflation and debasement on the middle and lower classes, let's look at some statistics. According to a report by the Economic Policy Institute, the top 1% of income earners in the US have seen their income grow by 205% since 1979, while the bottom 90% have seen their income grow by only 62%. This means that the rich are getting richer while the poor are getting poorer. Inflation and debasement only serve to exacerbate this problem by decreasing the purchasing power of the middle and lower classes, who are already struggling to make ends meet.

In addition to wealth inequality, the fiat system can also perpetuate power dynamics by giving governments and central banks control over the money supply. This control can be abused to benefit those in power at the expense of the majority. For example, the government and central bank can manipulate interest rates to favor certain groups or industries over others. They can also

use monetary policy to stimulate economic growth or control inflation, but these policies can have unintended consequences that disproportionately affect the middle and lower classes.

Furthermore, the fiat system allows for the accumulation of debt on a massive scale. Governments and corporations can borrow money with relative ease, but this debt must be paid back with interest. This interest can become a significant burden on the economy and future generations, who may be left to bear the consequences of decisions made by their predecessors.

While the fiat system has its benefits, it is important to recognize its drawbacks and consider alternatives like Zcash. By understanding the power dynamics and wealth inequality perpetuated by the fiat system, we can work towards creating a more equitable and transparent financial system for all.

3.1

THE BIGGEST THREATS TO YOUR MONEY: INFLATION, DEBASEMENT, AND THE LOSS OF PURCHASING POWER

3.1.1 THE EFFECTS OF INFLATION: AN AUCTION ACTIVITY

Objective: To understand the concept of the **money supply** and how it affects the prices of goods and services in an economy.

DEFINITION :

➔ The **money supply** is the total amount of money in circulation within an economy at a specific time. This includes:

- Physical currency, such as coins and bills
- Electronic money held in bank accounts

+The money supply is an important concept in economics, as it can affect the overall health of an economy.

➔ **Auction:** A public sale in which goods or property are sold to the highest bidder.



Societies can often be unpredictable and unjust, exemplified by the simulation of a teacher randomly giving a significant amount of money to only a select few students. This mimics real-life situations where unequal distribution of resources and opportunities can occur, highlighting the inherent randomness and unfairness in many situations.



CLASS EXERCISE

FOLLOW THE INSTRUCTIONS BELOW:

- 1. You will receive a random amount of monopoly money from the teacher. This represents the money supply in a society.
- 2. Write down the total money supply in the chart provided.
- 3. The teacher will auction a candy bar to the students. To win the candy bar, you will need to make the highest bid using your monopoly money. Record the winning bid next to the money supply.
- 4. The teacher will then add a significant amount of monopoly money to the total money supply. This represents an increase in the money supply in an economy. Later, you will learn how money supply is added or reduced in an economy.
- 5. The teacher will auction a second candy bar to the students using the same process as before. Record the winning bid next to the money supply on the chart.
- 6. The teacher will repeat the auction a third time.

Round	Money Supply	Winning Bid
1		
2		
3		

Conclusion:

- 1. How did the increase in the money supply affect the winning bids for the candy bars?
- 2. What is the relationship between the money supply and inflation?
- 3. How is the money supply relevant in the real world?
- 4. Can you think of any other factors that can affect the prices of goods and services?

Understanding how inflation impacts not only individuals, but entire communities, can help people make informed decisions about saving and spending, while recognizing the challenges posed by economic conditions. Let’s begin with an example:

Jaime is a college student who lives in a small apartment. He works part-time at a coffee shop to pay for his living expenses and tuition. As soon as he began living independently, Jaime became a pro at managing his own **ledger**.



A **ledger** is a detailed record of all of your monetary transactions. Whether it’s money you’re earning or spending, a ledger helps you keep track of it all.

At the beginning of the year, he budgeted \$10,000 for his living expenses, including rent, food, and other necessities.

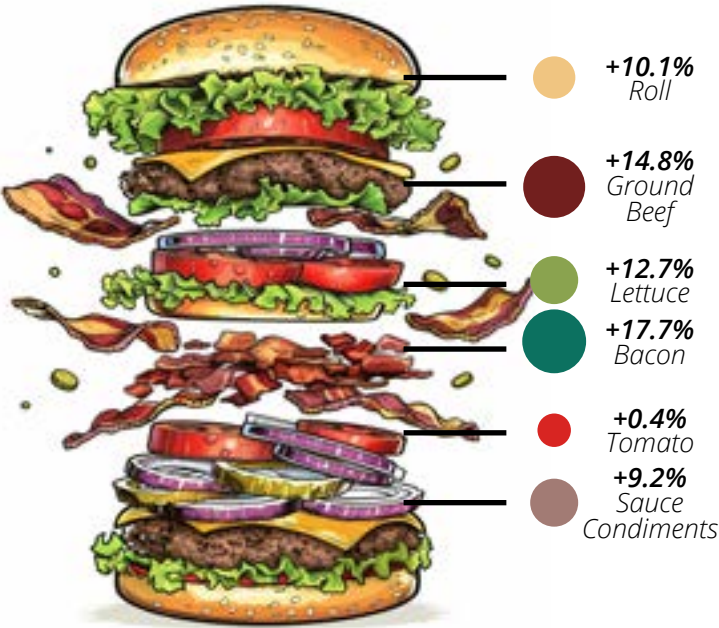
These were his transactions for January:

Date	Description	Amount	Type	Balance
01/01/2023	Starting Balance			\$1,600.00
01/01/2023	Rent for January	\$800.00	Debit	\$800.00
01/05/2023	Groceries	\$100.00	Debit	\$700.00
01/15/2023	Part-time paycheck	\$500.00	Credit	\$1,200.00
01/20/2023	Gas for car	\$350.00	Debit	\$850.00
01/30/2023	Texbooks	\$150.00	Debit	\$650.00

This ledger shows that Jaime’s starting balance on his checking account on January 1st was \$1,600, out of which he spent \$800 to pay rent for the month. He then spent (a debit) \$100.00 on groceries and received \$500.00 (a credit) in pay from his part-time job, bringing his balance to \$1200.00. He then spent money on gas and textbooks, bringing his balance down to \$650.00 at the end of the month.

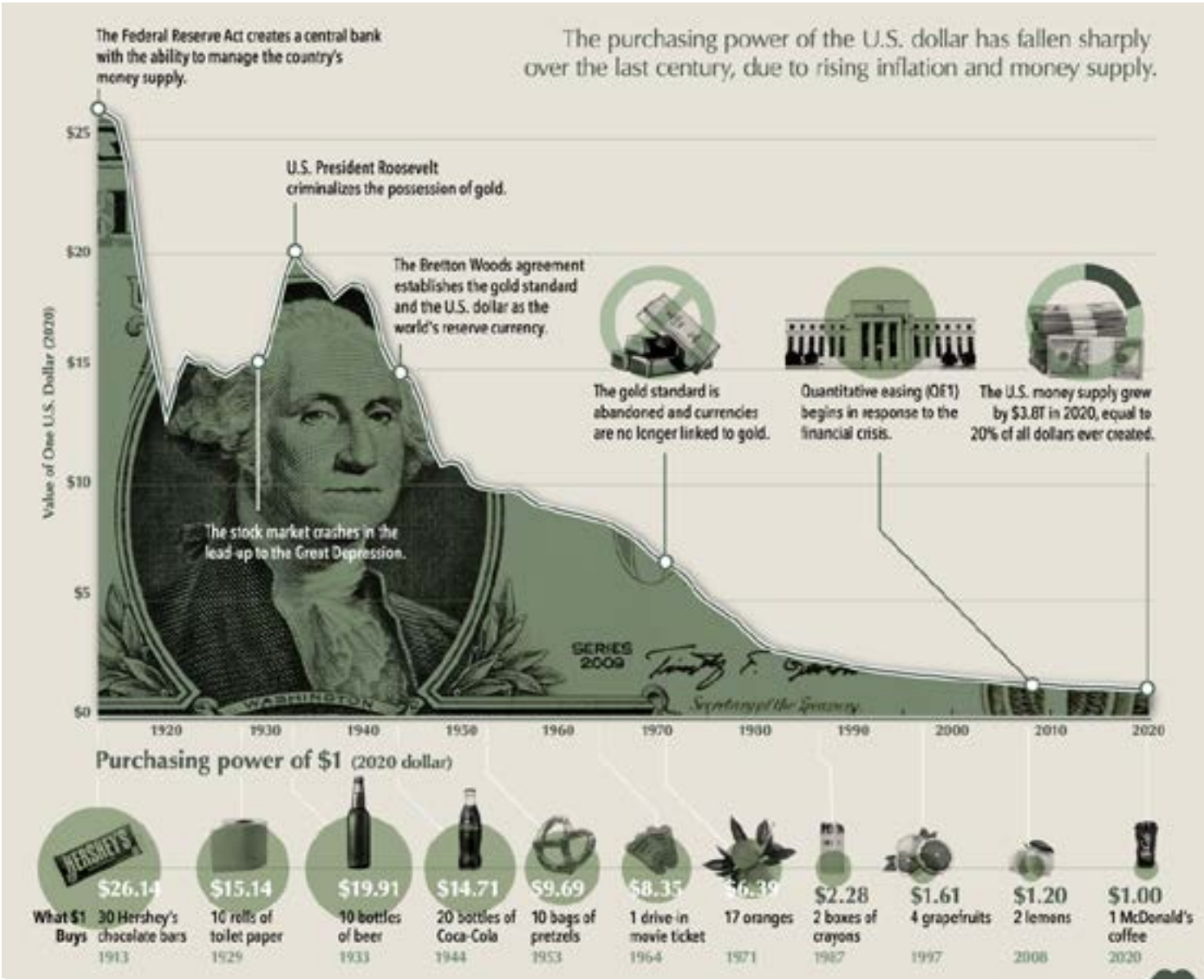
HOW INFLATION CHANGED THE PRICE OF A HAMBURGER

Year-over-year change in the price of selected ingredients of a hamburger (April 2021 – April 2022)



* Based on retail prices, urban consumers. gredients of a hamburger (April 2021 – April 2022)

A DOLLAR'S WORTH
Purchasing Power of the U.S. Dollar



In 2020, purchasing 30 Hershey's Chocolate bars would cost you \$26.14. However, if we go back in time to 1913, the cost for the same quantity of bars would only be \$1. This significant difference in price highlights the change in purchasing power over time and demonstrates how the value of currency has shifted over the years due to inflation.

Jaime: "What? That's crazy. I can't even imagine what my rent would have cost back then."

Grandfather: "Well, let me see. If we take inflation into account, \$1USD would have bought me about 10 bags of pretzels back then."



Jaime needs to budget an additional \$1,000 for the same basket of goods and services that he purchased the previous year.

This means that his purchasing power has decreased by \$1,000, as he now has to spend more money to buy the same goods and services.

The basket of goods and services includes rent for his apartment, groceries, and other necessities.

The following table shows the cost of each item in the basket in the first year and the second year, as well as the percentage increase in price:

Actually, according to the US Bureau of Labor Statistics, today's prices are 30.39 times as high as average prices since 1913 meaning that a dollar today only buys about 3% of what a dollar bought

Item	Cost Year #1	Cost Year #2	% Increase
Rent	\$4,000	\$4,500	12.5%
Groceries	\$2,000	\$2,300	15%
Necessities	\$4,000	\$4,200	5%
Total	\$4,000	\$4,000	10%

back then. Now, imagine someone gave Jaime a time-travel choice: either take \$100 in 1913 or wait till 2023 and receive a mere \$3. It's like deciding between a shopping spree in the past or grabbing just a couple of small treats today. The difference is huge, and it really highlights how much the value of money has changed over the years!

Jaime earns more in a year than his grandfather ever did, but this also disincentivizes saving. It's more advantageous to spend money now since its value decreases. This hinders the ability to plan for the future.

As shown in a previous graph (in section 3.0), salary growth year over year in the United States has remained stagnant for the average citizen, meaning most people aren't receiving raises at the same rate as the decreasing value of their money, despite working harder.

It could have been worse for Jaime. For example, Zimbabwe experienced hyperinflation in the late 2000's, when the country's economy was hit by a combination of political instability, economic mismanagement, and external factors such as drought and sanctions. As a result, the value of the Zimbabwean dollar (ZWD) plummeted, and the government was forced to print more money.

The 100,000,000,000 ZWD bill was introduced in Zimbabwe in 2008. Because of hyperinflation, it was worth only a few US dollars at the time.

Despite its high face value, the 100,000,000,000 ZWD bill was not enough to buy basic necessities like food or fuel, and people had to carry large bundles of cash to make everyday purchases.

The 2008 financial crisis exemplified the failure of a fiat system. Irresponsible lending practices, lack of oversight, and excessive money creation by banks led to a collapse in the housing market, massive job losses, and global economic turmoil.

Another example is the hyperinflation crisis in Venezuela. Poor economic policies, mismanagement, and excessive money printing caused the Venezuelan Bolivar to experience severe inflation, leading to widespread poverty, food shortages, and political instability.



3.1.2 SAVING MONEY IN HARD TIMES

The current global economic situation, which was negatively affected by the pandemic, has brought about challenges such as high inflation and low interest rates on savings accounts. These conditions can make it tough to effectively save money, as inflation eats away at the value of currency over time. Even if you save today, you may end up with less purchasing power in the future. But don't worry! There are still ways to save money and be financially secure. Here are a few ideas to try:

Make a budget: A budget is a plan for how you will use your money. It can help you see where you are spending too much money and where you can save. Set aside some money each month for saving, and look for ways to cut back on your expenses.

Start investing: Investing is a way to make your money grow over time. There are many types of investments to choose from, and you can find one that fits your budget and your level of risk.

Get creative: There are many creative ways to save money. You can try cutting your own hair or bartering with others for goods and services. Be open to trying new things and looking for non-traditional solutions to your financial problems.

THE 50/30/20 SPENDING PLAN



- It is **generally acceptable** to **take on debt as long as the money is used to generate income and increase purchasing power in the future**. This is because borrowing money can allow an individual or business to make investments that increase their productivity and efficiency, ultimately leading to greater profits and financial stability.
 - For example, if a farmer takes out a loan to purchase new equipment that allows them to harvest their crops more quickly and efficiently, they may be able to generate more income and increase their purchasing power as a result. On the other hand, if the money is used to waste resources or make unproductive investments, it can lead to financial difficulties and wouldn't be a wise decision.
- By taking charge of your finances and being flexible, you will be better able to weather the storm of a tough economy and come out on top.

3.1.3 THE TIME VALUE OF MONEY AND ITS ROLE IN ECONOMIC GROWTH

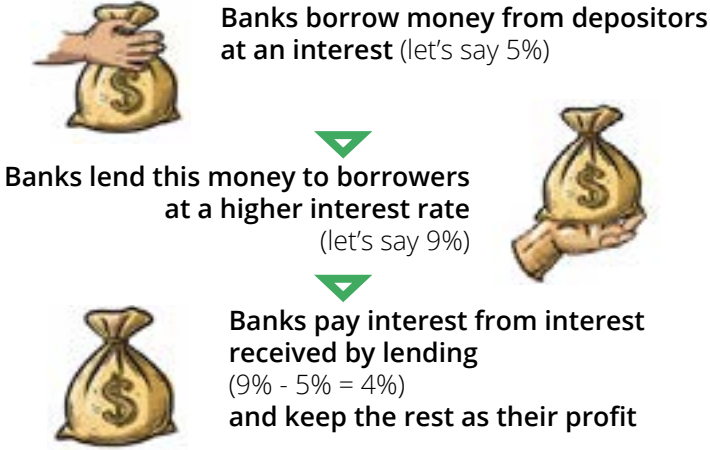
Have you ever wondered why banks offer so many services to their customers? While it may seem like they are being generous, it's important to remember that banks are businesses, and their primary goal is to make a profit. But how do they make a profit if they are giving away money in loans?

In addition to earning interest on deposits, banks generate revenue in other ways, including:

1. Charging interest on loans they give out.
2. Charging fees for services like ATM usage and account maintenance
3. Earning money through investments, like buying and selling securities or investing in real estate.
4. Keeping a percentage of loans in reserve and investing or lending out the rest
5. Paying interest on deposits and charging fees on checking and savings accounts.

By borrowing money at low interest rates and lending it out at higher rates, banks are able to turn a profit. They also generate income through fees and investment activities.

But why should this matter to you as an individual? Well, have you heard the phrase "a dollar today is worth more than a dollar tomorrow"? This concept is known as the time value of money, and it's all about the idea that money is worth more in the present than in the future. This is because **money can be invested to earn interest and because money can lose value over time due to inflation**.

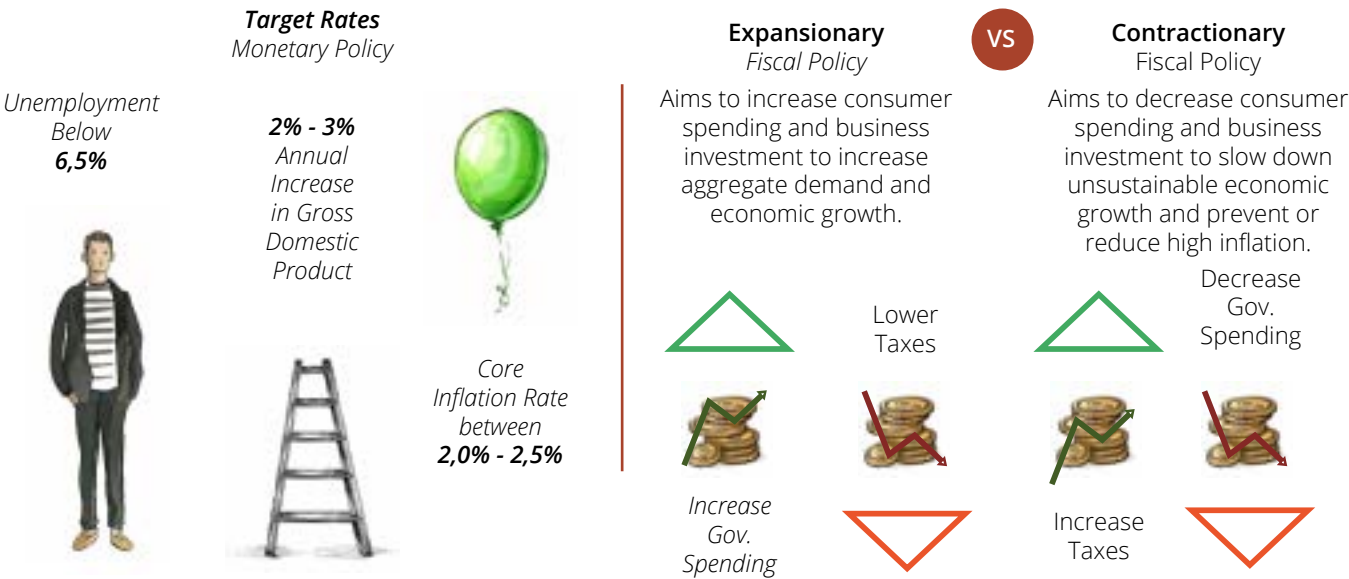


In other words, if you have money sitting in a savings account earning a low interest rate, it's not going to be worth as much in the future as it is today. On the other hand, if you invest your money in something that has the possibility of earning a higher return, you might come out ahead.

3.2 CENTRALIZED CONTROL: HOW THE GOVERNMENT AND BANKS MANIPULATE THE MONEY SUPPLY

Understanding where trillions of dollars in stimulus funds come from, and who gets to decide their allocation, is critical for comprehending the broader financial system. Governments use several tools to manage the money supply at specific moments in time.

Central banks and governments can use monetary and fiscal policy tools to influence the money supply and the economy. For example, the United States Federal Reserve (The Fed) uses monetary policy to adjust interest rates, affecting the amount of money in circulation. Fiscal policy, on the other hand, involves using spending and tax policies to influence economic activity.



Exchange rate policies, supply shocks, and price controls are additional tools that can be used to manage the money supply and influence trade and the economy. These policies can help stabilize prices and manage inflation.

To ensure that your money retains its value over time, the goal of investing is to earn a return that is higher than the rate of inflation. This way, your money will be worth more in the future than it is today.

Example: "Too big to fail" refers to financial institutions so large and interconnected that their failure would have catastrophic repercussions on the entire financial system. During the 2008 financial crisis, several large banks were deemed "too big to fail," leading the U.S. government to intervene and provide bailouts to prevent their collapse.

➔ One of the most prominent examples of a "too big to fail" institution during the financial crisis was investment bank Lehman Brothers. When Lehman Brothers filed for bankruptcy in September 2008, it set off a domino effect of events, including the near-collapse of insurance giant AIG and a massive drop in the stock market. The U.S. government had to intervene and provide bailouts to other major financial institutions to avert further chaos and safeguard the broader economy.

➔ Grasping how these policies function is vital for understanding the limitations of centralized monetary systems and the context in which Zcash emerged. As a decentralized currency, Zcash addresses some of the issues associated with centralized control over the money supply by offering a system that operates independently of central banks and governments.

3.3 THE MAGIC OF MONEY CREATION

3.3.1 FRACTIONAL RESERVE BANKING

In the previous sections, we discussed how central banks like the Federal Reserve manage the money supply, how banks earn profits, and some strategies to save money. However, we haven't yet talked about how new money is created and introduced into an economy. It may seem like magic, but there is an interesting process behind it.

So, how does new money actually enter circulation and fuel economic growth? Unlike physical resources like food or water, money has no fixed limit. The government, the central bank, and private banks all play a role in this process.

Let's take a closer look at how the Federal Reserve (Fed) can add \$100 million into circulation:

1. The Fed decides to increase the money supply by \$100 million based on its monetary policy goals, such as boosting economic growth or stabilizing prices.
 2. The Fed instructs a commercial bank to create a \$100 million deposit in its account at the Fed. This deposit is created out of thin air and not backed by any physical assets.
➔ When a commercial bank creates a deposit at the Fed, it essentially borrows money from the Fed. The Fed provides the bank with funds for the deposit, and in return, the bank pays interest on the loan and eventually pays the loan back.
 3. The bank uses the new \$100 million deposit to make loans to businesses, individuals, or purchase securities such as government bonds.
 4. The businesses or individuals who receive these loans can then use the money to make purchases, pay bills, or invest in other assets. This increases the overall supply of money in the economy.
 5. The circulated money eventually ends up in other banks, which can then use it to make their own loans and investments. This process continues until the \$100 million has been fully injected into circulation.
- It's important to note that banks create new money every time they lend to customers or make investments. When a bank makes a loan, it creates money by adding new funds to the borrower's account for the loan amount. The borrower can then use this money to make purchases or pay bills, effectively increasing the overall supply of money in the economy.

Overall, the Fed's ability to add new money into circulation through the banking system helps to stimulate economic growth and achieve its monetary policy goals. The process of creating new money can be complex, but it is sometimes essential for the economy to function and grow. Other times, it can lead to dire consequences, such as excessive money printing and growing wealth inequality.

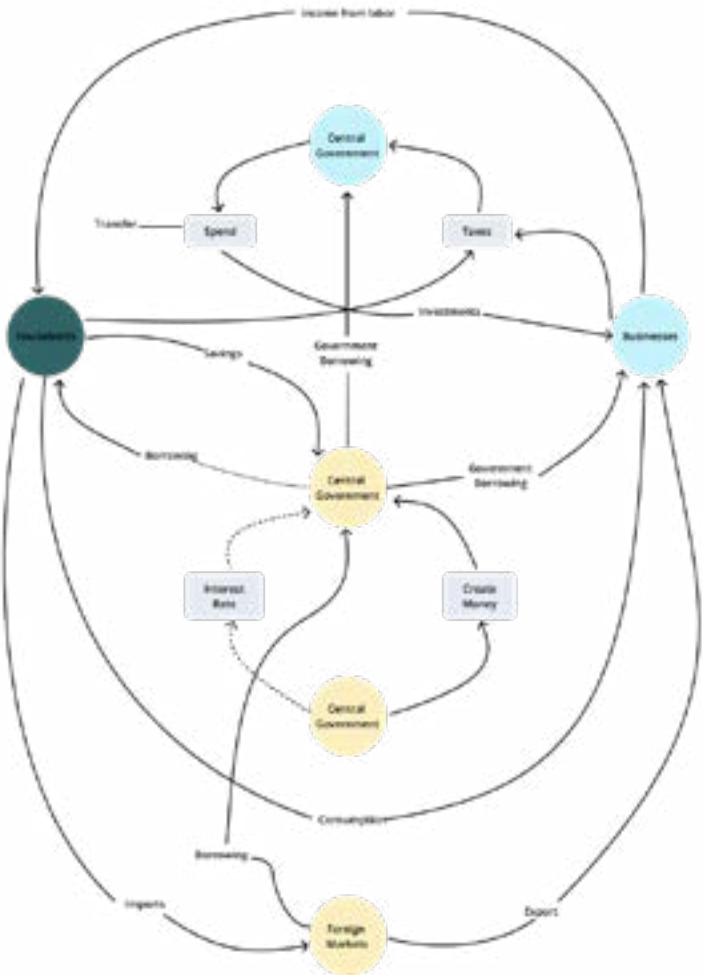
Excessive money printing can foster wealth inequality in several ways. For example, **the Cantillon effect** suggests that when new money is created, it primarily benefits those who receive it first—usually large corporations and wealthy individuals. These early recipients can spend or invest the new money before prices rise, accumulating more wealth. In contrast, those further down the chain, like the middle and lower classes, experience the negative effects of inflation without reaping any direct benefits from the newly created money.

The COVID-19 pandemic provided a recent example of the Cantillon effect. Central banks worldwide, including the U.S. Federal Reserve, implemented large-scale quantitative easing measures, purchasing government bonds and other financial assets to increase the money supply and stimulate the economy.

As a result, a significant amount of newly created money flowed into the hands of large corporations, financial institutions, and wealthy individuals. They could obtain low-interest loans or invest in assets like stocks, bonds, and real estate. The increased demand for these assets drove up their prices, leading to substantial gains for those who could invest early.

Conversely, the middle and lower classes, without the same access to capital or investment opportunities, dealt with the consequences of inflation. As the newly created money trickled down through the economy, it led to higher prices for goods and services, reducing the purchasing power of those unable to benefit directly from the central banks' actions.

This example demonstrates how the Cantillon effect can exacerbate wealth inequality, disproportionately benefiting those closest to the source of new money while leaving the majority to grapple with the negative consequences of inflation.



3.3.2 EXERCISE: FRACTIONAL RESERVE BANKING

Fractional reserve banking is a system where banks maintain only a fraction of their deposits as reserves and lend out the remainder. As long as they adhere to the reserve ratio set by the central bank, they can create more money than they have on hand. However, this ability to create new money carries the risk of excessive borrowing and financial instability if not managed carefully.

The reserve ratio is a regulation that dictates how much money banks must keep in reserve and how much they can lend out. It is established by the central bank, which is responsible for ensuring a healthy economy.

In the following exercise, we'll explore how fractional reserve banking can lead to currency debasement, inflation, and a decrease in purchasing power. We'll use a simplified example involving six participants, one of whom will act as a bank, and a reserve ratio of 10%.

FRACTIONAL RESERVE BANKING

Keeps 1/2



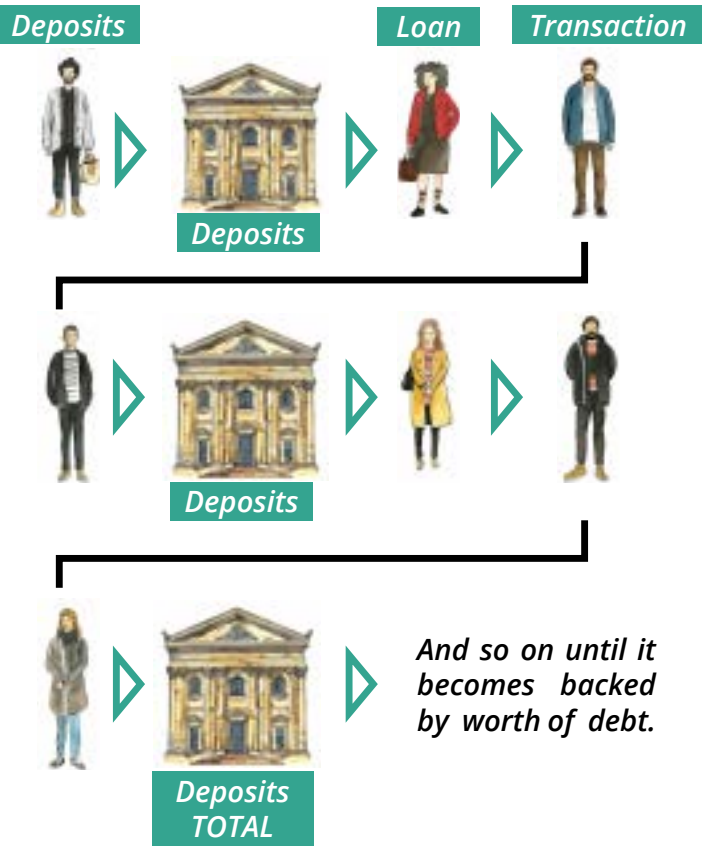
We need the following volunteers:

- A = Depositor (Lottery Winner) (Light Blue)
- B = Bank Cashier (Bank)
- C = Debtor #1 (Dark Blue)
- D = Property Owner/ Depositor (Red)
- E = Debtor #2 (Light Purple)
- F = Art Gallery Owner/ Depositor (Green)

1. A just won \$100,000 from the lottery and deposits it in the bank (B). With a 10% reserve ratio, B must keep \$10,000 in its vault and can lend out the remaining \$90,000.
2. C borrows the maximum amount (\$90,000) from B and uses it to buy a house from D.
3. D deposits the \$90,000 received from C into the bank (B). The total deposits in the bank are now \$190,000.
4. E requests a loan from B, and the bank lends out 90% of the new deposit, which is \$81,000.
5. E uses the \$81,000 loan to buy an art piece from F, who then deposits the money in the bank (B). The total deposits recorded are now \$271,000.

In this scenario, the initial \$100,000 deposit has resulted in a total of \$271,000 in deposits after circulating through the economy. If the reserve ratio were lowered to 1%, the amount of money created would be significantly higher ($\$100,000 / 0.01 = \$10,000,000$).

It's important to note that as of 2020, the Federal Reserve (the Central Bank of the USA) reduced reserve requirement ratios to zero percent in order to stimulate the economy. Through this exercise, we can see that fractional reserve banking has the potential to fuel economic growth by increasing the availability of credit. However, it also carries risks that need to be carefully managed to avoid inflation and financial instability. So, how much money is actually created with those 100,000 USD if the money continues to circulate throughout the economy?



Just out of curiosity, how much money would be created in an economy if its reserve ratio was lowered to 1%? (Make sure you divide $\$100,000/0.01$). Surprised?

As of 2020, the Federal Reserve (the Central Bank of the USA) **reduced reserve requirement ratios to zero percent** in order to stimulate the economy.

3.4

DEBT: THE BURDEN THAT CRUSHES THE MIDDLE AND LOWER CLASSES

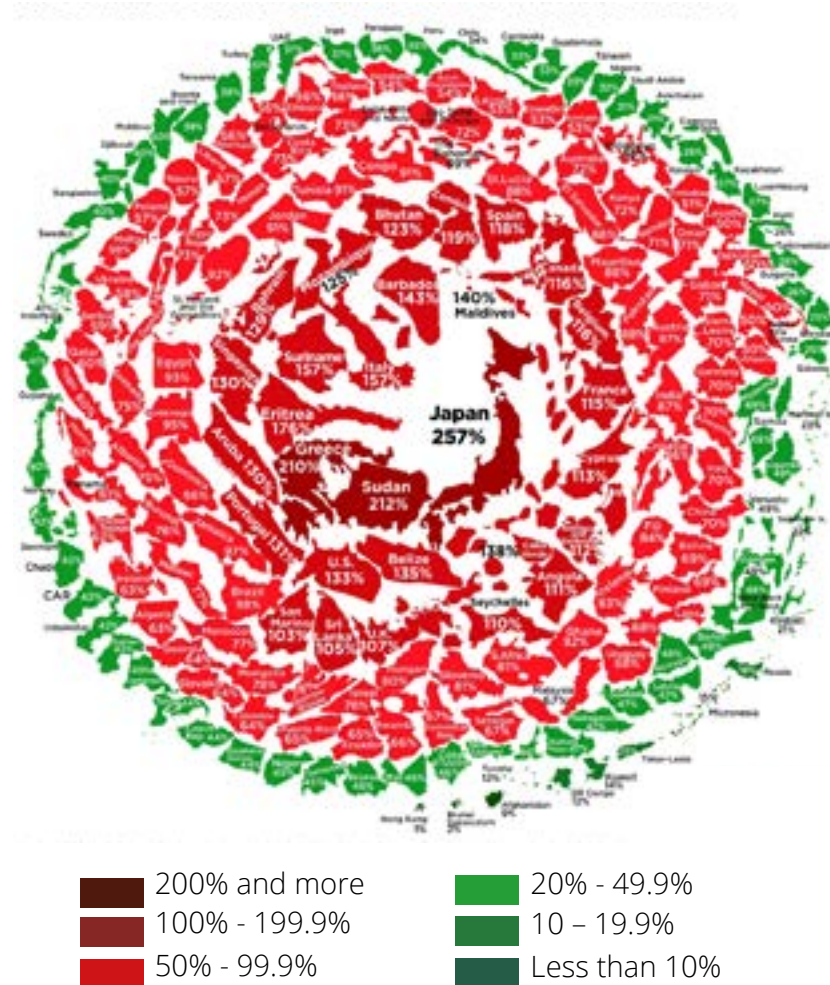


Debt is money that is owed by one person or organization to another. When you have debt, you are required to pay back the money you owe, usually with interest, by a certain date.

The State of the World's Government Debt

Debt is a double-edged sword. It's true that borrowing money can provide a much-needed financial boost, whether it's for individuals making a big purchase, businesses investing in their growth, or governments funding important services. But borrowing too much can lead to financial ruin. When you can't pay the interest on your debts, it becomes harder to pay your bills and stay afloat. This is especially true when an entity takes on more debt to pay off existing debt, and gets caught in a vicious cycle known as a "debt spiral".

The debt crisis is a worldwide problem, including in the United States. Currently, the government is spending more money than it is earning. To pay its bills, it has been borrowing more and more money.



However, this cycle of debt and higher borrowing costs can soon harm the government's credit rating. If the debt becomes too much, the government may have financial difficulties and potentially go bankrupt, just as many other countries have in the past.

- Debt taken on by the government can have long-term effects on future generations.
- Printing more money to fund expenses can result in currency devaluation and a possible collapse of the monetary system.

In the late 2000s, Greece faced a severe debt crisis when it was revealed that the government had been hiding the true extent of its debt. As a result, the country was unable to repay its creditors, leading to austerity measures, skyrocketing unemployment, and a significant decline in economic growth.

But how can we measure the risk of a country taking on too much debt? One way is through the debt-to-GDP ratio, which shows the amount of a country's total debt as a percentage of its GDP.

- It's important to remember that the debt-to-GDP ratio is only one part of understanding a country's money situation.

- The debt-to-GDP ratio is a way to see if a country can pay its debts.

- If the ratio is high, the country may have trouble paying its debts in the future.

- If the ratio is low, the country may be able to pay its debts easily and be in good financial shape.



Gross Domestic Product (GDP) is a measure of the total value of goods and services produced within a country over a specific period of time, typically a year. It is often used as a measure of the size and health of an economy.

3.5

ADDRESSING WEALTH INEQUALITY: A NEW APPROACH TO MONEY

The transition from commodity-based currencies to the modern fiat system has brought about several challenges. Issues with the current monetary system include inflation, debasement, excessive debt, and wealth inequality, as well as concerns about privacy, control, and financial censorship. The need for a viable alternative is increasingly urgent in today's digital, interconnected world.

Zcash was invented as a potential solution to these issues with traditional money. Operating independently of central banks, Zcash enables peer-to-peer transactions without intermediaries, making it a groundbreaking innovation in the financial industry. Key features of **Zcash** include its decentralized network, which makes it resistant to government interference and manipulation, and its finite supply. These attributes make **Zcash** scarce and valuable, similar to gold, contributing to its growing popularity as a store of value and investment opportunity.

It's important to note that one of the key benefits of **Zcash** is that it operates without a central authority or boss. Nobody controls Zcash, and it has been operating perfectly fine since 2013, without any major crashes or shutdowns. This decentralized nature of **Zcash** means that it is not subject to the same vulnerabilities as traditional financial systems, which can be manipulated or controlled by governments, banks, or other centralized institutions. This lack of control has also been a major factor in addressing wealth inequality, as Zcash is accessible to anyone with an internet connection, regardless of their socioeconomic status.

In the following sections, we'll explore **Bitcoin's** origins, technology, and how it addresses the concerns of the current monetary system.

A person is shown in profile, wearing a VR headset. The background is a vibrant, futuristic cityscape with neon lights and digital overlays. The overall color palette is dominated by blues, greens, and oranges.

THE DECENTRALIZED FUTURE: EMPOWERING COMMUNITIES AND INDIVIDUALS

4

THE PRICE OF CONTROL: A LOOK AT SURVEILLANCE, CENSORSHIP, AND REGULATION

4.0.1 SURVEILLANCE

Surveillance is a tricky business. On the one hand, it helps catch people doing bad things like money laundering. But the more fraud that happens, the more surveillance is needed, which can lead to invasions of privacy through technology. Private companies may also collect and trade your personal information for their own benefit, and the risks of this surveillance can include scams, harassment, extortion, identity theft, and even tracking your card purchases. Plus, with the rise of AI and machine learning, it's becoming even easier for governments and companies to invade our privacy. Moreover, it's often the people who are already disadvantaged or underprivileged who are hit the hardest.

THE IMPACT OF AI AND TECHNOLOGY ON FUTURE PRIVACY AND SURVEILLANCE

Future Effect	The Rich	The Poor
Access to personal information.	May have access to extensive personal information and can use it to make informed decisions.	May lack this information and may have to rely on outdated or unreliable sources.
Ability to shape the world in their own interests.	May use their access to data to shape the world in their own interests.	May have little influence on what happens.
Control over others.	May exert control over the poor through their access to data, leading to a loss of individual freedom.	Little control; are often the controlled.
Vulnerability to digital scams, online harassment, extortion, and identity theft.	Likely less vulnerable to these issues with more information and more protection from such scams.	May be more vulnerable to these issues due to a lack of access to resources and information.

4.0.2 FINANCIAL REGULATIONS AND CENSORSHIP

Financial regulations, censorship, and prohibitions can be an emotionally and financially taxing reality for society and its citizens. They come in many forms, such as:

➔ **Capital Controls or Sanctions:** When spending gets out of control, governments may impose price controls to try and fix the problem. But sometimes these controls make things worse. Governments may also limit how much money citizens can transfer, exchange, or take out of the country.

EXAMPLES

➔ How does China's Social Credit Score system work? In China, financial transactions and other data of all citizens are centrally collected, and used to create a Social Credit Score system that can be used to control citizens.

➔ Consider what happened in Greece in 2015 — citizens were only able to withdraw 60 euros per day by government mandate. Similarly, the Chinese are only able to send limited amounts of Renminbi out of the country.

➔ There have been several instances in Argentina when the government imposed strict currency controls to try to stabilize the peso. One such instance was in 2011, when the government implemented capital controls to stem the flow of dollars out of the country and to prevent further devaluation of the peso. Another instance was in 2019.

➔ **Restrictive Banking Policies:** Have you ever tried to withdraw cash from an ATM only to find out you've reached your daily limit?

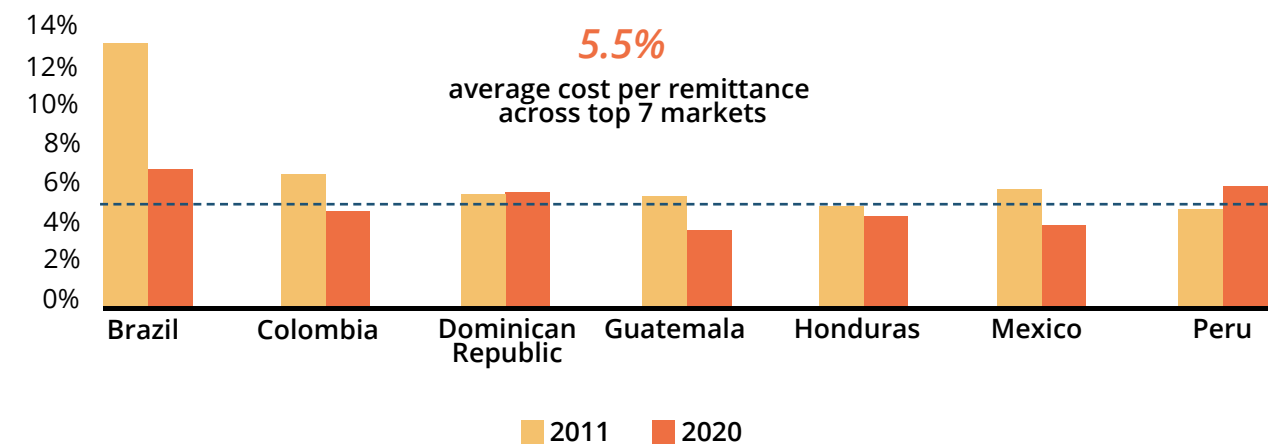
Or maybe you've tried to transfer money to a friend only to be told there's a maximum amount you can send. These are just a few examples of restrictive banking policies that can make it tough to access your own money and do what you like with it.

Banks can also charge fees for most transactions and may only be open during certain hours, making it hard to get to your cash or make financial decisions. Carrying around lots of cash increases your risk of getting robbed. On top of all that, banks sometimes offer lower interest loans to the wealthy, while opening up the poor to loan sharks and higher-interest loans. In so doing, the financial system often profits from the gap between the rich and the poor.

➔ **Expensive Remittances:** Sending money to other countries can be expensive due to fees from banks and other financial institutions. Many low-income families in developing countries rely on money from relatives living abroad to get by. But high fees for international money transfers can eat into how much money is actually received by the recipient. This can make it hard for families to afford basic necessities like food, housing, and education.

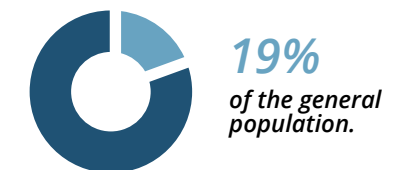
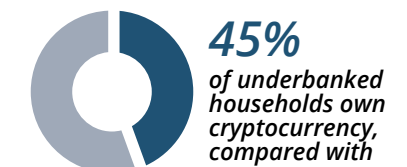


Average Remittance Fees in Latin America
(% of transaction)



➔ Imagine a family in a rural village in Brazil that relies on money from a relative working in the US. If the relative sends \$100, but the bank charges a \$7 fee for the transfer, the family only gets \$93. This may not seem like a lot, but for a family living on a tight budget, losing \$7 can make a big difference.

➔ **The Unbanked and Underbanked:** Unfortunately, not everyone has access to **traditional banking services**, whether it's because they don't meet the requirements to open an account or because they live in areas where banking services aren't available. This can make it difficult for people to access financial services and participate in the global economy.



➔ But wait, there's more! Governments may also control the exchange rate of their currency, which can make it hard for people to exchange money between countries or lead to **unfavorable exchange rates**. Financial institutions may **block donations** to certain organizations or individuals, or take away your bank account altogether. Social media platforms and financial institutions may remove certain content if they believe it is spreading misinformation or violating their community standards or policies. This is sometimes referred to as **ensorship** and can include a wide range of activities, such as blocking or suppressing content, limiting access, or removing information altogether.



Surveillance, control, and hidden fees are only the political downsides of the current system we live in. Unfortunately, there are a series of hidden economic costs as well — ones that we often never get to learn about.

FROM CRISIS TO INNOVATION: THE CYPHERPUNKS AND THE CREATION OF A DECENTRALIZED DIGITAL CURRENCY

Before the creation of **Zcash**, people were searching for ways to address the problems of traditional finance, such as fraud, corruption, and a lack of trust in financial institutions. These issues were made even more pressing by the global financial crisis of 2008. In response, a group of tech-savvy and forward-thinking individuals known as the Cypherpunks set out to create a **digital currency** that could be used for online transactions **without the need for intermediaries** like banks.

The Cypherpunks were rebels and visionaries who believed in the power of technology to bring about positive change and challenge traditional power structures. Many of them were involved in activism and civil liberties issues, and they were united by a shared passion for technology and a desire to use it to shape the future.



Q: How can individuals regain their financial self-sovereignty?

A: The Cypherpunks movement aims to create a new financial system that respects individuals security, privacy, and freedom, as a solution to regain financial self-sovereignty.

And so, they set out to create bitcoin, a digital currency that would revolutionize the way we think about money and financial transactions. To do this, they needed to find a way to record transactions that was more secure and transparent than traditional centralized ledger systems. Why did they feel this way?

ABUSE OF CENTRALIZATION

4.2.1 CENTRALIZED SYSTEMS

Centralization of power often leads to corruption, which can result in the mismanagement of resources, including financial resources. This can disproportionately affect those lower in the hierarchy and without as much influence or power, causing them to bear the greatest burden of the consequences of corruption and mismanagement.

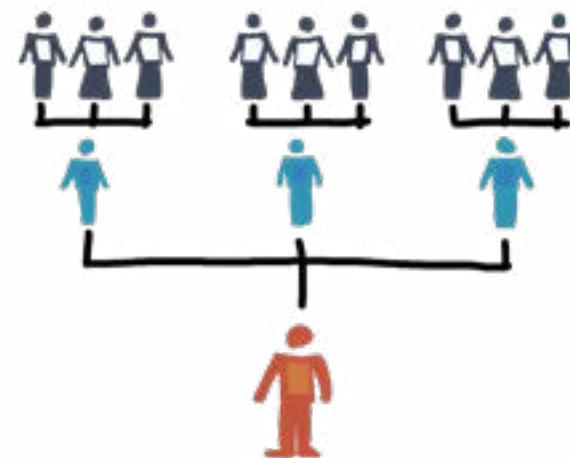
The modern fiat system is characterized by centralization of control, with a small group of banks and other financial institutions holding significant weight over the economy.

A centralized system can be thought of as a tree with a single trunk. The trunk represents the central authority or point of control, and the branches represent the various parts of the system that are controlled by the central authority. In this analogy, the tree is vulnerable if the trunk is damaged or diseased, because the entire tree relies on the trunk for support.



There are many drawbacks to centralized systems including:

- ➔ **Vulnerability:** A centralized system relies on a single point, so if that point fails, the whole system can fail.
- ➔ **Control and power:** Those in control of centralized systems have a lot of power and influence over how they work.
- ➔ **Inefficiency and intermediaries:** Centralized systems often use intermediaries, which can make them slow and add extra costs.
- ➔ **Lack of autonomy:** People may not be able to make their own financial decisions.
- ➔ **Censorship and restriction:** There is a risk of being blocked from accessing certain financial resources in centralized systems.



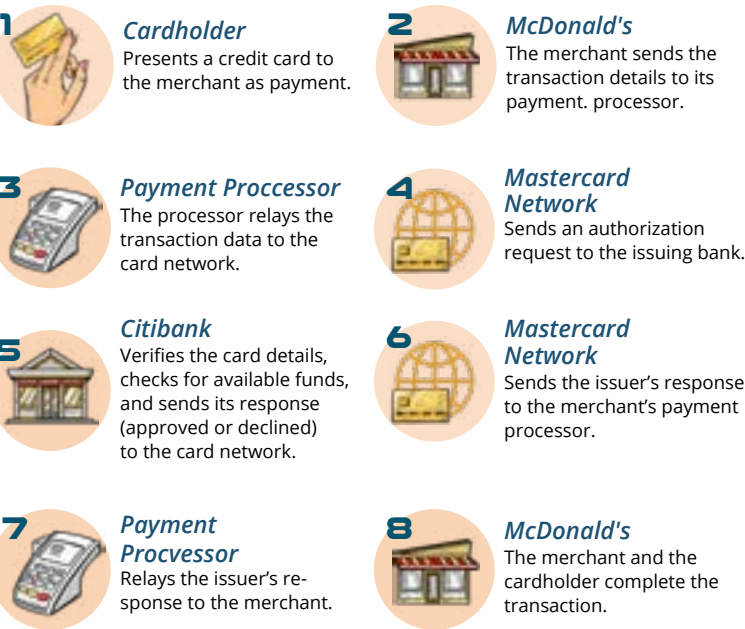
➔ **Scaling challenges:** Centralized systems may struggle to keep up with increasing demand for financial services and resources.

➔ **Security risks:** Centralized systems can have weaknesses that hackers can use to gain access or cause damage.

➔ **Lack of transparency and trust:** It can be hard to understand how centralized systems work and to make informed decisions about them because they may not be transparent or trustworthy.

4.2.2 THE INTERMEDIARIES IN A CREDIT CARD TRANSACTION

A credit card transaction, such as buying a hamburger, might appear simple but involves multiple intermediaries. Let's break down the process concisely to reveal its complexity and hidden costs.



- 1. You order a hamburger at McDonald's using your Citibank MasterCard card.
- 2. McDonald's sends an authorization request to its payment processor.
- 3. The processor forwards the request to Mastercard.
- 4. Mastercard sends the request to the issuing bank, Citibank.
- 5. Citibank sends an authorization code back to Mastercard.
- 6. Mastercard returns the authorization to the processor.
- 7. The processor sends the authorization back to McDonald's.
- 8. You receive your hamburger.

In this process, each intermediary adds fees, which are ultimately passed on to the consumer. These fees remain hidden in the cost of the hamburger.

NOTE

Real-world Examples of Centralized and Decentralized Systems

Centralized System: Facebook

Facebook is a centralized social media platform where users' data is stored and controlled by the company. In 2018, the Cambridge Analytica scandal revealed that personal data of millions of Facebook users had been harvested without their consent, leading to questions about privacy and security.

Decentralized System: Tor

Tor (The Onion Router) is a decentralized network that allows users to browse the internet anonymously. Instead of relying on a central authority, Tor routes users' data through multiple nodes, protecting privacy and security. This has made it popular among journalists, activists, and others seeking to evade censorship and surveillance.

Research, Data, and Statistics

- 1. A study by the Federal Reserve Bank of Kansas City found that the average interchange fee for credit card transactions in the United States was 2.04% in 2019 [1]. This means that for every \$100 spent, \$2.04 goes to intermediaries in the credit card transaction process.
- 2. According to the International Data Corporation (IDC), global spending on blockchain solutions is expected to reach \$15.9 billion by 2023, a compound annual growth rate of 60.2% between 2018 and 2023 [2]. This indicates that investment in decentralized systems is growing rapidly.
- 3. Research by GlobalWebIndex showed that 40% of respondents were concerned about how Facebook uses their personal data [3]. This highlights the potential drawbacks of centralized systems when it comes to privacy and security.

Modern banking. Simple, right? Take something as seemingly simple as buying a hamburger with a credit card. At first glance, it may seem undemanding and harmless. But if we break down the steps and see the intermediaries involved, you might be surprised at what we discover. Are there inconveniences, inefficiencies, maybe even hidden dangers lurking in the shadows? Let's find out.

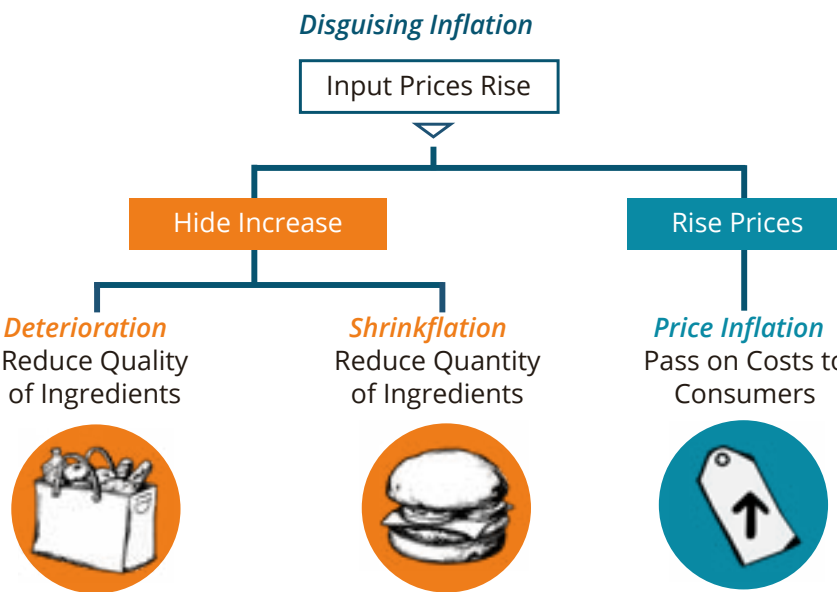
At this point, no actual funds have changed hands, except perhaps a small authorization fee. The transaction only exists on "paper." McDonald's needs to close or batch-out its sales for the day. The closing process might look like this:

- 1. McDonald's terminal or point-of-sale (POS) system sends the day's transactions to the processor.
- 2. The processor sends the transaction information to Mastercard.
- 3. Mastercard sends the transactions to Citibank.
- 4. Citibank confirms the authorizations, holds back their interchange fees (there are over 900 possible fee codes in North America), and transfers the funds back to Mastercard.
- 5. Mastercard takes its assessment fee and sends the funds to the processor.
- 6. The processor takes its cut, as set out in the merchant agreement, and deposits the funds to McDonald's bank account.

Who do you think paid for the fees? Of course YOU. But, did anybody inform you of this? Oh, no! They were hidden in the cost of the hamburger.

And all of this happens believe it or not because we rely on centralization.

The modern banking world comes with various risks, including accidental double swipes, credit card fraud, human and computer errors, and potential hacks.



4.3

OVERCOMING CENTRALIZATION WITH DECENTRALIZED SYSTEMS

Decentralized systems resemble a forest, where each tree represents an independent participant, and the forest symbolizes the entire system. In this analogy, the forest is more resilient than a single tree as it does not rely on a single point of failure. If one tree is damaged, the forest can continue to thrive. Decentralized systems, like forests, are more effective with diverse and collaborative participants, instead of a single central authority dictating the rules.



Advantages of decentralized systems:

- Enhanced resilience and reliability due to no single point of failure
- Increased security with the right encryption, as there's no central point of control for hackers
- Greater sovereignty for participants, who have more control over assets and decisions
- Improved transparency, as all nodes access the same information
- Permissionless and limitless nature, allowing anyone to join or participate
- Equal opportunities for all nodes to contribute and influence the network
- Enhanced privacy and security through the use of pseudonyms or nickname



A node is a computer connected to a network that can share and/or receive information and communicate with the other nodes.



A network is a group of nodes that are connected to each other in some way. This connection allows the devices to exchange information and communicate with each other.

Challenges of decentralized systems:

- Increased effort required to achieve consensus among nodes
- Greater vulnerability to malicious nodes that could harm the network

In a centralized financial system, a small group of entities or individuals has control over the entire system, making decisions that impact all participants. In contrast, a decentralized system can empower each participant to be in charge of themselves, eliminating the influence of a central authority. This power shift restores financial control to the people, fostering a more equitable and democratic financial landscape.

4.4

TRANSACTIONS ARE JUST AGREEMENTS TO TRADE

Welcome to The **Decentralized** Micronesian island of Yap! It is a bit remote, but fascinating because people use a special kind of currency called "Rai stones." A feature that makes them a great form of money is their **scarcity**. The total number of Rai stones is limited, which means that they cannot be easily reproduced or inflated like fiat currencies. This fixed supply helps to maintain the purchasing power of the Rai stones over time and makes them a reliable store of value. These Rai stones are like giant coins that are used to purchase stuff on the island. The thing is, they can weigh a ton. Rai stones can actually crush you, so they're a bit impractical to carry around. How then, can people conveniently use Rai stones as mediums of exchange without having to physically take them from one place to another?



4.4.1 TO TRUST OR NOT TO TRUST

While the US Dollar is now the official currency of Yap Island, Rai stones still are a type of money. Unlike the dollars, the Rai stones on Yap Island are not controlled by a single authority or stored in banks. Instead, the transactions are based on oral history and trust, with people keeping track of their own records of who owns which stones.

This system has both benefits and drawbacks. On the one hand, it allows for a certain degree of independence from one central authority. On the other hand, it can also lead to disagreements and potential for cheating. Why?

Decentralization is easy to achieve in small groups. Life is simple as there are fewer people to coordinate; it is often possible for everyone to have a say in decision-making processes and for those decisions to be implemented relatively quickly. As a group gets larger, it becomes more difficult to reach an agreement and for decisions to be implemented effectively.

➤ Imagine that you have a field full of ripe corn that needs to be harvested. You need some help, so you approach your neighbor, Raquel, and offer her a deal: if she helps you harvest the corn, you will give her a 10 kg stone in exchange. Raquel agrees, and for the next day, she works alongside you in the fields, helping to gather the corn and bring it in. At the end of the day, you both shake hands and instead of physically handing over the stone, you simply show her that her payment (the Rai stone) is in your backyard.

➤ From that point on, you both agree that the stone now belongs to Raquel. This type of **transaction**, where no currency actually is handed from one individual to the other as a form of payment, but instead a physical object is used as a **symbol of value**, is common on Yap Island and has been used for centuries as a form of currency.

➤ Five years later, you decide to try and claim the Rai stone as your own. You present evidence to the community that the stone has been passed down through your family for generations, and that you are the rightful owner.

➔ However, Raquel remembers the agreement that you both made and provides evidence by bringing witnesses of the exchange to give a statement. She argues that the stone rightfully belongs to her, as it was given to her in exchange for her help with the harvest.

➔ Some members of the community might agree with your claim, citing the tradition and history of your family's ownership of the stone. However, others might side with Raquel, pointing to the agreement that was made and the fact that the stone has been in her possession (figuratively speaking) for five years without any objections from other members of the community. Factors that might be considered include the history and tradition of ownership, the terms of the agreement between you and Raquel, and any relevant evidence or arguments. Not a very solid solution, is it?



So then, how can thousands of strangers all agree on one truth without anyone having the final say? This is something that has puzzled people for a long time, and it's an important question to consider. It turns out that the internet has helped us find a solution to this problem. The solution is called the **blockchain**.

4.4.2. LET'S SWAP TRUST FOR RULES

Imagine you and your friends are in a group chat where you can buy and sell things with each other. Every time a purchase is made, it's recorded in a shared document for everyone to see and each person's balance is updated. This chat uses a digital ledger to keep track of all the transactions that have happened. The ledger is like a record book that everyone can see.

In a decentralized system like this, all the participants have a copy of the ledger. This makes it hard for any one person or group to change any information without being noticed. It's like a security measure to make sure that the records are accurate and no one can cheat. This is similar to how a blockchain works.



Instead of relying on personal relationships and subjective interpretations of trust, a decentralized system can operate effectively if it is based on a set of clear, transparent rules that everyone agrees to follow. This way, decisions can be made and conflicts can be resolved in a fair and objective manner, without relying on the trust of individual parties. It might not be as romantic as relying on trust, but it's a much more reliable way to ensure that a decentralized system operates smoothly.

➔ If Yap Island had a set of unbreakable rules and a written record of all transactions between its members, the conflict between you and Raquel could have been avoided. These rules and records would have made it clear to all members of the village what their rights and responsibilities were.

But is it that simple? Not really; there was a lot of trial and error before blockchain technology was actually a success.

- ✳ What are the exact rules that must be followed Who makes these rules ?
- ✳ Why will people want to follow the rules?
- ✳ How do rules get distributed across the network?
- ✳ What will happen if someone breaks the rules?
- ✳ How can the rules be changed or updated later?
- ✳ How will the rules be enforced to make sure everyone follows them?
- ✳ How can the rules be made clear and easy to find for everyone in the system?

4.5

UNLOCKING THE POWER OF THE BLOCKCHAIN: A TECHNOLOGY REVOLUTIONIZING THE FUTURE

Despite numerous setbacks, one very enigmatic person (or group of people) finally found the key to developing a game-changer methodology for the world of trade and finance. This masterpiece made it incredibly easy to track and verify transactions, streamlining the process of exchanging money, goods, and other assets. With its innovative approach and advanced technology, this system revolutionized the way we think about economic transactions, making them faster, safer, and more efficient than ever before.



A blockchain is a decentralized digital ledger that securely records and verifies all transactions across multiple computers in a transparent manner.

A **blockchain** is like a history book. Each page (or "**block**") has a list of things that happened (**transactions**). As more things happen, we need to add new pages (blocks) to the book. Anyone can read the book for free, but only special helpers (**miners**) can add new pages. They make sure that what's written is true. Once something is written in the book, it can't be changed or erased. It's a permanent record of all the **transactions** that have happened on the **blockchain**.

➔ A **blockchain** does not have a central authority (like an author, a publisher or an editor) that can edit, delete or change the information recorded in it, hence it's considered a more secure and reliable method of record keeping compared to a traditional central database.

What is a blockchain?

All records of actions on the blockchain are called transactions.





If the helpers (**miners**) are not in **consensus** about the validity of the pages (**blocks**), they will be rejected and will not be added to the **blockchain**.

4.5.1 CONSENSUS BUILDING IN A PEER-TO-PEER NETWORK

1. Understand your role: You have been assigned to either Group A or Group B.
2. If you are in Group A:
 - ➔ Select a leader who will create a drawing on a piece of paper, which represents a **transaction** to be added to the **blockchain**.
 - ➔ Pass the paper around the group until everyone has had a chance to replicate the drawing.
 - ➔ Compare the original drawing to the final drawing to see if there are any discrepancies.
 - ➔ If there are discrepancies, discuss and try to reach a consensus on what the correct drawing should be.
3. If you are in Group B:
 - ➔ Select a leader who will create a different drawing on a piece of paper, which represents a **transaction** to be added to the **blockchain**.
 - ➔ Pass the paper around the group until everyone has had a chance to replicate the drawing.
 - ➔ Compare the original drawing to the final drawing to see if there are any discrepancies.
 - ➔ If there are discrepancies, discuss and try to reach a consensus on what the correct drawing should be.
4. Try to complete the task as quickly as possible.
5. Discuss the similarities between this activity and the process used by nodes in a peer-to-peer network to verify **transactions** and add them to the **blockchain**.
6. Compare the activity to the concept of proof of work, where nodes compete to solve a complex mathematical problem to add a new block to the **blockchain**.
7. Discuss the benefits of consensus-building in a **blockchain** network, such as decentralization, security, and immutability.

This activity helps students to visualize the concept of consensus-building in a **blockchain** network, where nodes must agree on the validity of a transaction before it can be added to the **blockchain**. By working together to reach a consensus on the correct drawing, students can better understand the importance of collaboration and agreement in a decentralized system. Additionally, the timed aspect of the activity adds a sense of urgency, which reflects the importance of speed and efficiency **in blockchain transactions**.

4.6

EMPHASIZING THE IMPORTANCE OF TRUE DECENTRALIZATION IN BLOCKCHAIN PROJECTS FOR ACHIEVING FREEDOM AND EMPOWERMENT

Decentralization is a key principle of **blockchain** technology that eliminates the need for intermediaries and enables peer-to-peer interactions. In a truly decentralized system, there is no central authority or control, and all participants have an equal say in the decision-making process. Bitcoin, the first and most well-known blockchain-based cryptocurrency, was designed with decentralization as a central principle. By creating a decentralized monetary system, Bitcoin sought to eliminate the need for intermediaries and empower individuals to take control of their financial transactions. The decentralized nature of Bitcoin makes it immune to government or institutional control, and its open-source code allows anyone to participate in the network.

True decentralization is important in blockchain projects because it ensures that power is distributed among all participants and that no single entity can control the system. This aligns with the principles of Bitcoin and the larger goal of the freedom and empowerment of individuals. When power is centralized, it can be easily abused, leading to unequal access to resources and control over financial transactions. Decentralization allows for a more transparent and equitable system where all participants have an equal say in decision-making.

Unfortunately, not all blockchain projects prioritize decentralization. Some projects create new blockchain and tokens, which are still controlled by a central authority or company. This defeats the purpose of blockchain technology, which is to create a decentralized and trustless system. These projects may market themselves as decentralized, but in reality, they are not truly decentralized by design.

Incorporating true decentralization into blockchain projects is essential for creating a more equitable and transparent society. By eliminating intermediaries and creating a peer-to-peer system, individuals can take control of their financial transactions and participate in a global economy in unprecedented ways. Additionally, true decentralization can help prevent abuse of power and promote fairness and equal access to resources.

As we continue to explore the possibilities of blockchain technology, we recognize that the true revolutionary power lies in the open source, peer-to-peer networks that implement true decentralization and unstoppable freedom in our society. This aligns with the principles of Bitcoin and the larger goal of the freedom and empowerment of individuals. By challenging traditional power structures and creating transparent and secure systems, blockchain technology has the potential to transform many aspects of our society, creating a future that is more equitable, transparent, and decentralized. While the potential of blockchain technology to revolutionize finance is well-known, we are only beginning to scratch the surface of its potential to transform many other industries as well. By prioritizing true decentralization and aligning with the principles of Bitcoin, we can create a future that empowers individuals and promotes greater freedom and equality.





5

INTRO TO ZCASH

5.0

THE ENIGMA OF SATOSHI NAKAMOTO: BITCOIN AND THE PRIVACY REVOLUTION

Satoshi Nakamoto, a mysterious and brilliant innovator, dreamed of a future where financial transactions were borderless, transparent, and secure—free from the control of governments and banks. In 2008, Satoshi sparked a Freedom Revolution with the Bitcoin whitepaper. It described the first practical implementation of blockchain technology. Bitcoin emerged as a symbol of hope and resilience in a world rocked by financial crises and eroding trust in centralized institutions. The first Bitcoin transaction occurred in January 2009.

Driven by a desire to establish a decentralized financial system, Satoshi's Bitcoin returned power to the people, igniting a global movement that challenged the status quo and championed financial freedom.

5.1

INTRODUCTION TO ZCASH AND BITCOIN

Seven years later, in 2016, a group of scientists and researchers launched Zcash. Their objective was to improve on the game-changing power of Satoshi's Bitcoin, namely by adding privacy features. (More on this later.)

Zcash is, in fact, a fork of Bitcoin, which means the code from Bitcoin was essentially copied and modified. The idea for Zcash was first described in a white paper published in 2014 by professors and academic researchers from MIT, Johns Hopkins University, the Technion, and Tel Aviv University, and it was developed over the course of several years by Zooko Wilcox-O'Hearn and his team at Electric Coin Co. (ECC; formerly called Zcash Company).

People use ZEC to transact efficiently and safely with low fees. It's private, fast, flexible, and accessible to everyone — built for the digital age. Use it to buy nearly anything, from bagels to beach vacations.

You can use your mobile phone to privately pay a friend in Zcash, send money overseas, buy groceries, or send a donation to a worthy cause. Use third-party apps like Flexa SPEDN to pay with Zcash at Lowe's, Nordstrom, Baskin Robbins, and more. Services like Moon allow you to use Zcash online anywhere Visa is accepted.

5.1.1 WHAT IS BITCOIN? WHAT IS ZCASH?

Bitcoin (BTC) is a form of electronic cash that can be sent and received by anyone on the Bitcoin network. Bitcoin can be stored in digital wallets, on mobile phones or desktop computers, that tap into a distributed ledger system. Think of this like a giant online spreadsheet, accessible to everyone, where all transactions are logged.

Like Bitcoin, Zcash is a digital currency, based on an open-source, blockchain-based ledger, but unlike Bitcoin, Zcash features a sophisticated zero-knowledge proving system that safeguards the ledger against fraud while allowing users to keep their transaction information private.



5.1.2 WHAT IS THE DIFFERENCE BETWEEN BITCOIN AND ZCASH?

The simplest way to describe Zcash is that it is a digital currency like Bitcoin but it protects a user's privacy instead of exposing their financial history.

When Bitcoin was released in 2009, it was the first-ever decentralized cryptocurrency. All Bitcoin transactions are verified and recorded on a public blockchain, the ledger, which means that anyone in the world can see user balances and transaction data. This lack of privacy is what inspired the Zcash scientists to build something better, and in 2016, these cryptography experts took Bitcoin's open-source code and added zero-knowledge proofs (among other improvements) to create Zcash. Zcash offers all the conveniences of Bitcoin, but with full encryption to protect users' financial information.

There are other important differences, e.g., a self-funding mechanism for Zcash development, shorter confirmation times, a private memo field, faster transactions, and more.

5.1.3 WHY LEARN ABOUT ZCASH?

Zcash gives people the opportunity to transfer digital cash and other data privately and permissionlessly, without a middleman like a bank or a government institution. Having a private, peer-to-peer, permissionless money system gives people the ability to store their money and transact with others, independent of centralized entities who often impose controls or fees. Zcash gives people the freedom to choose if and when they want to disclose information about their finances with others.

Zcash solves Bitcoin's biggest flaw: private ownership and transfer of data. In a world where blockchain applications and cryptocurrencies are becoming more widely accepted, pseudonymous transactions, like those in Bitcoin, are no longer a viable option to protect user privacy. Surveillance applications are becoming more sophisticated by the day and are widely used by people and institutions to analyze and track blockchain transactions.



5.1.4 WHAT GIVES ZCASH ITS VALUE?

People can use ZEC to store wealth in a hard, privacy protecting, asset. There will only ever be 21 million ZEC units, meaning that the asset has a fixed supply. Once the 21 millionth ZEC is mined into circulation, the asset will become anti-inflationary. Anti-inflationary assets are a good hedge against inflation in the event that centralized gatekeepers inflate national money supplies.

Zcash has come a long way since its original network launch in late 2016, and it continues to offer blockchain and crypto users control over their privacy. Zk-SNARK cryptographic proofs have helped set the privacy standard for blockchain-based use cases in the global marketplace. A wide variety of users and enterprise clients alike demand the type of privacy, flexibility, and performance that the Zcash protocol provides.

5.1.5 WHY SHOULD I CARE?

Zcash gives people the choice to transact outside of centralized systems that can censor and/or exploit people, and to disclose information about your finances with others or to keep that information private.

This censorship-resistant digital payment mechanism protects freedom of speech and freedom of association — and the freedom to be human, be silly, or be whatever they want to be! Zcash users can donate to organizations, send money overseas, or just send it to a friend, without exposing their identity and without fear of repercussion.

And because Zcash has a fixed supply of 21 million, just like Bitcoin, users can feel assured their ZEC won't be devalued by a centralized party printing more on a whim.

5.2 WHAT IS ZCASH MADE OF?

Zcash gives users the option of two transaction types, transparent (available for anyone to see) and shielded (private). Both are executed on the same Zcash blockchain, but amounts and proofs for transactions are handled in different ways. To keep shielded transactions private, Zcash utilizes what are known as zero-knowledge proofs.

Specifically, Zcash uses zk-SNARKs, a type of zero-knowledge proof. The acronym zk-SNARK stands for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, and refers to a proof construction where one can prove possession of certain information, e.g., a secret key, without revealing that information, and without any interaction between the prover and verifier.

More simply, a zero-knowledge proof is a cryptographic method that can prove something is true without revealing the information that makes it true. For example, in Zcash when a transaction is made between two parties, the zero-knowledge proof is used to verify that the sender has enough money in their wallet to cover the total sent without revealing to the recipient, the blockchain, or anyone else the sender's wallet balance.

Imagine for a moment you are blindfolded, and you are holding two checker pieces behind your back. You don't know whether they are both the same color, or are of different colors. You hold out one and show it to your counterparty, who is not blindfolded. She tells you the color — but you don't know if she is lying. You then bring the piece behind your back again — switching the pieces, or not — and repeat the process. By doing this many times, you can start to get confident about whether the other person is lying. For example, if you bring out the same piece twice and she tells you “black” the first time, and “red” the second, you know she’s lying. If her answers are consistent with your knowledge about which piece you’re revealing, you can become quite confident about whether the other person is giving you honest information.

This kind of process can be used to shield enormous amounts of information of indefinite complexity (such as the use of recursive SNARKs to save a Merkle root of a blockchain's global state; but that's outside the scope of this book).

5.2.1 HOW DO NEW ZCASH COINS ENTER THE NETWORK?

Zcash's monetary base is a fixed supply of 21 million ZEC currency units. Every 75 seconds, a new block is mined to the Zcash blockchain and a block reward of 3.125 ZEC comes into circulation. This block reward is distributed to miners and the Zcash development fund.

The amount of the block reward reduces by half about every four years until all 21 million ZEC are in circulation. Zcash inflation almost precisely mimics that of Bitcoin. It is important to note that as new coins are created inflation goes down, and at each halvening the rate drops significantly.

5.2.2 INTRODUCTION TO ZCASH PRIVACY



Shielded Zcash addresses keep your financial information private. Transparent addresses make that information public.

Most blockchains expose all transaction and balance information publicly. That's not an embarrassing secret, that's just how they were designed. Storing and transacting with shielded Zcash gives users more control over their assets and can protect them from fraudsters and other ill-intentioned actors.

When you send Zcash from your digital wallet, you'll see that your address is a long string of numbers and letters. Your recipient will also have an address that has a long string of numbers and letters. If your address starts with a “z” and you are sending to a recipient's address that also starts with “z,” you can rest assured that the transaction information is fully private. The amount of the exchange and the addresses of each wallet are both shielded on the public blockchain. This is usually the best way of sending and receiving ZEC when privacy is required.

When you send from or receive to an address that starts with a “t,” i.e., a z-to-t or a t-to-z transaction, the privacy level is not always high, as some information will be visible on the blockchain. T-to-t transactions are fully public, just like Bitcoin transactions.

Zcash users will also encounter wallet addresses that start with “u.” These are called unified addresses, and they work like a universal travel adapter. With unified addresses, wallets can automatically move coins to the latest shielded pool. So, for example, let's say a user buys some Zcash on an exchange. That exchange may send transparent Zcash from a t-address to your unified address. If your wallet supports autoshielding though, it will automatically move those funds into private storage.

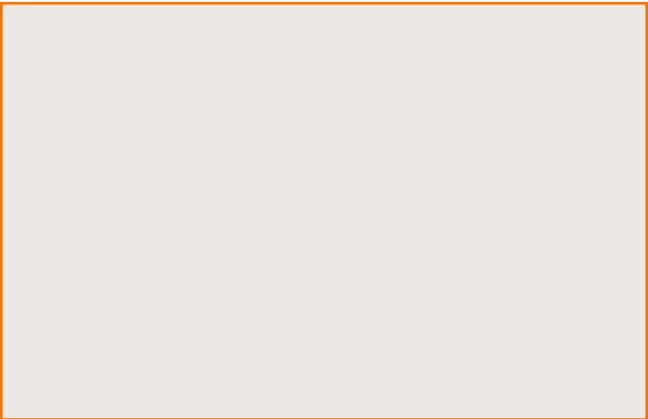


TYPES OF ZCASH ADDRESSES

Currently there are three main types of addresses in use to date. These include

TRANSPARENT

tlgoiSyw2JinFCmUnfiwwp72LEZzD42TyYu



UNIFIED ADDRESS (FULL) IMAGE PLACEHOLDER

ulckeydud0996ftppqrnpdsqyeq4e57qcyjr4raht4dc8j3nju
yj3gmm9yk7hq9k88cdkqfuusgpcpjfhwu3plm2vrd32g8du78k
zkm5un357r4vkhz4vhxd4yfl8zvszk99cm89qv4trd7jzks8
h6lukzgy25j8cv76p0g603nrrg6yt6cxsh2v8rmkasskd69ylfy
phhjyv0cxs

FOR MAXIMUM PRIVACY, ALWAYS USE Z- OR U-ADDRESSES.

5.2.3 HOW DOES THE BLOCKCHAIN KEEP TRACK OF WHO SPENDS WHICH ZCASH?

A hash tree or Merkle tree is composed of branches and leaf nodes that are labelled with the cryptographic hash of a data block. Merkle trees are an example of a cryptographic commitment scheme. The tree Root is seen as a commitment and leaf nodes proven to be part of the original commitment.

They verify data stored or transferred on P2P networks, ensuring data received from peers is unaltered. In ZcashSapling & Orchard shielded pools, the Note Commitment Tree is used to verify transactions are valid against consensus while perfectly hiding the sender, recipient & amounts consumed.



5.2.4 ARE ZCASH TRANSACTIONS SECURE?

Yes. The Zcash protocol can be considered very safe as it is among the most thoroughly documented zero-knowledge payment protocols in the world. It has been replicated by a number of other large crypto projects such as Namada and Penumbra. In addition, there have been many security audits of wallets and cryptographic components that go into products used by Zcashers.

5.2.5 WALK ME THROUGH AN ACTUAL ZCASH TRANSACTION

- Confirm that your wallet is synced to the latest blockheight.
- If fully synced, you can be assured your balance is up to date with the full spendable amount.
- Enter the unified address of your recipient into the "address" field. Either paste the address in from the clipboard or scan the QR code of your counterparty.
- Fill in the amount you wish to send; fees are automatically calculated.
- Enter a shielded memo with your transaction. Remember: Transparent addresses cannot receive memos.
- Confirm the transaction details and then click send.

Zcash block time is 75 seconds, it may take 1-2 minutes for the recipient to be notified of incoming funds. Depending on the number of confirmations required by your recipient's wallet, they may have to wait to be able to spend the Zcash.

5.2.6 EXERCISE: ZCASH TRANSACTIONS IN ACTION

To try exchanging Zcash with a friend, follow these steps:

- 1) Both of you set up a Zcash wallet.
- 2) In the "Send" option, scan the QR of your friend's address or enter their U or Z address.
- 3) Send a memo, saying: "Hi, welcome to Zcash!"

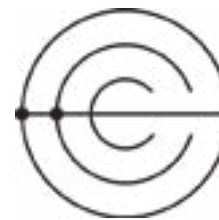
5.2.7 CAN ZCASH BE SHUT DOWN?

No. Zcash is a permissionless decentralized internet payments protocol run by individuals across the globe. Node software is free and open source. There is no central authority involved in the validation of Zcash transactions. In fact, because of Zcash's enhanced privacy, it is actually more resilient to attempts to shut down the network.

5.3

WHO'S WHO AND WHAT'S WHAT IN THE ZCASH WORLD?

There are many teams and independent developers working on Zcash, but here are a few of the key players.



Electric Coin Co. (ECC) created and launched the Zcash digital currency in 2016. Today — along with other independent teams and developers — ECC continues to support the Zcash community through product development, awareness and adoption, and various types of research. ECC is widely known to be one of the strongest cryptography teams in the world. In 2016, it was the first to successfully deploy zero-knowledge cryptography in a real-world application (Zcash), and in 2022, ECC engineers discovered Halo, a novel, recursive zero-knowledge proving mechanism that, for the first time, delivers truly trustless blockchain encryption and improved scalability. There are dozens of teams on various independent projects working to implement Halo in their own releases.



The Zcash Foundation (ZF) is a 501(c)(3) public charity that builds financial privacy infrastructure for the public good, primarily serving users of the Zcash protocol and blockchain. They, along with others, work to ensure that the Zcash protocol and the open network it powers remain decentralized and diverse. A few of ZF notable technical contributions to the ecosystem are the development of Zebra, a modern, independent Zcash node, and FROST, a threshold signature scheme. The Foundation also hosts Zcon, a yearly conference centered on privacy technology and the Zcash ecosystem, and supports grassroots, community initiatives such as Zcon Vozes, the A/V Club and various other open community calls and AMAs. Additionally, the Foundation moves Zcash forward by funding various projects in its Minor Grants program, internal and external research projects, and providing administrative support for Zcash Community Grants (ZCG).



Zcash Community Grants (ZCG) funds projects that advance the usability, security, privacy, and adoption of Zcash. ZCG is a technology advisory board that constitutes a committee of the Zcash Foundation, under its bylaws. Grants are chosen by a committee of five members who were elected by the Zcash Community Advisory Panel.

Recent projects that have been approved by the ZCG include:

Zcash Shielded Assets (ZSA) led by the QEDIT team, bringing DeFi to Zcash with a new payments protocol adding additional features to mainnet

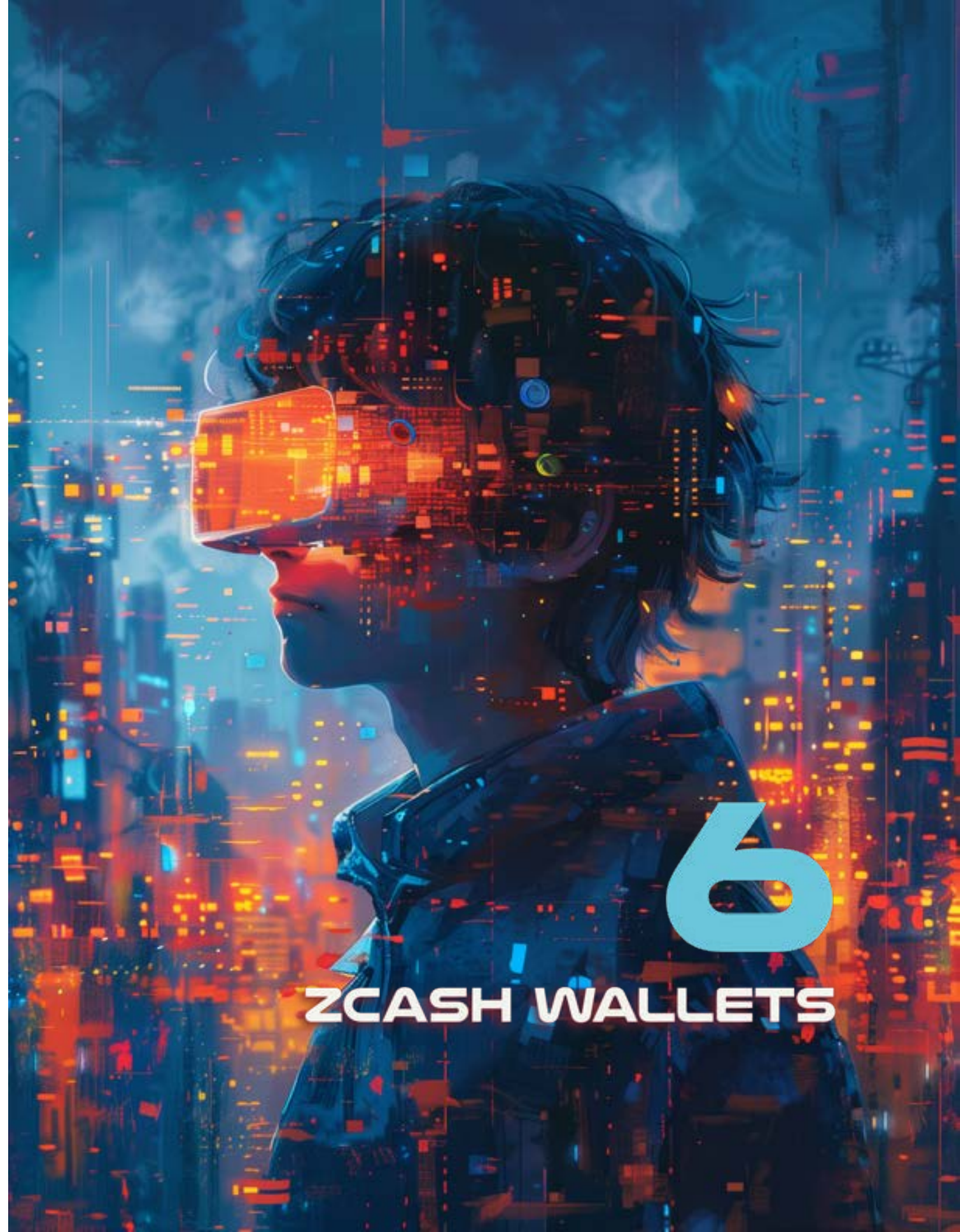
Zcash Media's short documentary featuring notable Zcashers such as Edward Snowden, Zooko Wilcox, and Deirdre Connolly

An easy one-click shielded payment and Point-of-sale system for brick and mortar shops SDK being undertaken by ZGo

The Global Ambassador program, which helps Zcash gain broader representation internationally

ZecHub is an open-source education hub centered on Zcash, featuring a global community of contributors who publish features, newsletters, blogs, tutorials, podcasts, and more.





ZCASH WALLETS

6.0

FROM NOVICE TO PRO: NAVIGATING THE WORLD OF THE ZCASH WALLET

When Zats are purchased for the first time, they will be credited to a recipient Zcash address, similar to how funds are deposited into a bank account. To receive funds into your bank account you need to provide the payer the account details so that the bank can locate and identify you in their ledger and add the corresponding credit in your favor.

The key difference is that while a bank account is centralized and subject to government regulations, a Zcash wallet is decentralized and operates on a peer-to-peer network. This means that every actor operating within the Zcash network relates to each other as peers and no one has an authority over others. Zcash has no central point of failure, but it is important to be cautious as someone's zatoshis can be in the possession of a third party, who is managing it.

This Zcash address belongs to a set of other addresses often referred to as a “wallet”. Which addresses belong or not to a specific wallet is determined by a private key. Whoever is in possession of that private key is considered the owner of the account and can have the privilege of spending the funds that are deposited in the addresses related to that private key. Similarly, like how a bank account is protected by a personal PIN or password associated with your customer identity. Just as you have control over the funds in your bank account, you can control the Zats in your wallet, and use them to make purchases or transfer them to other accounts. Just as the bank would allow anyone with your valid password and username to spend your funds, the Zcash network will consider that anyone in possession of your keys can have spend authority over the funds related to the addresses that the private key controls.

NOTE

Since there's no central authority, the peer-to-peer network can't revoke keys.

There are different kinds of private keys. Some can open just a single lock, while there are other keys that can do a lot more. Just as a locksmith can create any number of keys that can be used to open locks, there is a kind of private key that can be used to generate other private keys. The generated keys can be used to access your Zcash wallet. It is unusual to interact on a daily basis with this kind of key-generating key (or master key) as an average human person using a crypto wallet. This “master keys” are usually referred as “seed bytes”, “seed phrases” or secret recovery or backup phrase (or master private key) can be used to generate any number of private keys that can be used to spend your Zcash and to create the addresses where Zcash can be received to spend it later. You could say that a secret recovery phrase is like a locksmith, and the private keys are the keys that are created by the locksmith. Why do we emphasize the word “secret”? Because anyone that knows the secret can access and spend the funds associated with them.

An important thing to know is that there is no such thing as a “wallet” in the Zcash blockchain. The notion of a wallet is a mere abstraction that helps us to understand this relationship between cryptographic keys and the data contained in the blockchain. We can say that a wallet is a representation of the data in the blockchain from the point of view of a secret recovery phrase and its derived keys. The different wallet applications will apply this exact reasoning to show Zcash users the composition of their wallets.

They'll look at the blockchain information and will pick up all the pieces that are related to the keys the user presented as theirs and show that information in a comprehensive way.

In a self-custodial wallet (also called non-custodial wallet,) you are the only one with the keys to the wallet and you have full control over what goes in and out. On the other hand, in a custodial wallet, someone else holds the key and can access and manage the contents of the wallet on your behalf.

Self-custody is like being your own bank. Transactions are not subject to control or authority by any government or company, but it also means you bear full responsibility for keeping your Zcash secure. Self-custody ensures that third parties cannot confiscate your Zcash without your consent. Self-custody gives peace of mind in times of uncertainty, knowing your Zcash is secure.

It's important to choose the right type of wallet for each individual's needs. Sometimes people find it hard distinguish whether they are installing a custodial or a self-custodial wallet.

Wallet Type	1: Choose a Wallet	2: Install the Wallet	3: Create a new Wallet	4: Secure your Seed Phrase	5: Start using your Wallet
Self-custody wallets	Choose a self-custodial wallet provider	Follow the wallet provider's instructions	Generate recovery phrase	Store the recovery phrase in a secure location	Start using the wallet to receive and send Zcash
Custodial Wallets	Choose a custodial wallet provider	Follow the wallet provider's instructions	Create an account with the wallet provider	N/A (wallet provider holds the private keys)	Start using the wallet to receive and send Zcash

TIP

When it comes to storing your Zcash, it's not just about who has control over it - there are many other risks to consider as well. That's why it's important to find a storage solution that is both secure and convenient.

Wallet Type	Who controls my Zcash	Benefits	Risks
Self-custody wallets	The user	Complete control over funds and transactions, no approval process or account freeze, no corporate or government control, protected against arbitrary confiscation, like keeping money at home.	No recovery if recovery phrase is lost, less customer support, full responsibility falls on the user.
Custodial Wallets	The third-party provider acting as custodian	Easy recovery if access is lost, easier customer support.	Funds are always connected to the internet, more vulnerable to hacking and breaches. Custodians control and can freeze accounts.

Not all wallets have the same capabilities. It's important to know how different kinds of wallets let you access the blockchain and in what capacity. Here is a Wallet types taxonomy based on Custody of Keys and access to the blockchain.

Wallet Type	Description	Advantages	Disadvantages	Target user
Full Node Wallet	A wallet backed by a Zebra Full Node running in the same computer	It allows the user to access the blockchain with no intermediaries	It requires a lot of computing resources to run.	Someone that wants to be in control of their own infrastructure and has a computer with resources to spare that can be online most of the time.
Browser Extension Wallet	A wallet that is accessed through a web browser	Accessible from any device with an internet connection. Easy to use	Less secure. It's highly exposed to your browsing activity. It can be hacked or compromised by adversarial websites	Someone who needs to access their wallet frequently and doesn't have a lot of funds to store
Mobile Wallet	A wallet that is installed on a mobile device	Convenient. Can be accessed from anywhere	Can be lost if the device is misplaced, stolen, or hacked	Someone who needs to make transactions on the go and doesn't have a lot of funds to store. Ideal for QR initiated payments
Desktop Wallet	A wallet that is installed on a desktop computer	Can be more secure than browser extension wallets. Can be used offline	Can be hacked if the computer is infected with malware or by other users' using the same computer with other accounts	Someone who wants to store a small amount of Zcash and is comfortable with using a desktop computer
Hardware Wallet	A physical device that stores Zcash offline	Very secure, even if adversaries can get physical access to it. Can be used offline	Funds could be lost if the device and the backing recovery phrase are lost	Someone who wants to store medium to large amounts of Zcash and is willing to pay for the added security of a hardware wallet
Paper Wallet	A physical record of a Zcash wallet's private & public keys	Very secure if stored properly. Can be used offline	Not intended for daily usage. Funds can be lost or stolen if the physical record is lost or stolen	Someone who wants to store a large amount of Zcash and is willing to take the added precautions to ensure its security.

This space left intentionally blank.

TIP

Analyze the trade-offs of the wallets and know there is no ideal wallet that satisfies all needs. When choosing a Zcash wallet, there are several things you should consider:

- ➔ **Security:** Make sure the wallet has strong security measures in place, such as two-factor authentication and secure password policies.
- ➔ **Privacy:** Consider whether the wallet allows you to remain anonymous, or if it requires personal information to set up an account.
- ➔ **Ease of Use:** Choose a wallet that is easy to use and navigate, especially if you are new to Zcash .
- ➔ **Compatibility:** Make sure the wallet is compatible with your device and operating system.
- ➔ **Fees:** Compare the fees charged by different wallets to make sure you are getting the best deal.
- ➔ **Reputation:** Research the reputation of the wallet and its team to make sure it is trustworthy.
- ➔ **Control:** Some wallets give you more control over your private keys, which can be a security advantage. Consider whether you want a wallet that gives you full control, or one that is more user- friendly but may have less control.

You can always transfer your funds to a different wallet later.

6.1 THE PROCESS OF ONBOARDING AND SECURING YOUR ZCASH

Before moving any further, it's important that we learn the steps for onboarding and familiarize ourselves with the process for buying and securing Zcash safely.

6.1.1 THROUGH KYC EXCHANGES

1. **Choose** a Zcash exchange, or Zcash on-ramp. There are different options for buying Zcash, including traditional exchanges, peer-to-peer exchanges, and Zcash on-ramps. Choose a platform that meets your needs and is reputable. Always prioritize your privacy by choosing platforms that work with Shielded Zcash. Call to action: If your favorite platform of choice to buy ZEC does not support shielded Zcash, ask them to do so!
2. **Open** the app and receive your 12-word or 24-word recovery phrase. Write down the phrase in a safe place. The recovery phrase is used to restore access to your wallet if you lose your device or forget your password. Once you have written down the recovery phrase, you can enter it into the app to access your wallet.
3. **Connect a payment method:** Most platforms will allow you to connect a bank account, credit card, or debit card to fund your account. Follow the platform's instructions to add your payment method.
4. **Place an order:** Once your account is set up and funded, you can place an order to buy Zcash . The platform will provide you with a price quote and you can specify the amount of Zcash you to buy.
5. **Confirm the transaction:** Review the details of your transaction and confirm the purchase. The platform will process the transaction and the Zcash will be transferred to your account on the platform.
6. **Withdraw the Zcash:** If you want to transfer the Zcash to a self-custodial wallet, you will need to withdraw the Zcash from the platform and send it to your wallet. The platform will instructions for how to do this.

6.1.1.1 RISKS ASSOCIATED WITH KYC-EXCHANGES

It's important to note that when buying Zcash through a KYC-exchange, you are required to provide personal information and verify your identity. This creates a risk of identity theft and puts your personal information at risk. Additionally, KYC-exchanges hold your private keys, which means you don't have full control over your Zcash . To minimize these risks, consider using alternative options for buying Zcash, such as peer-to-peer exchanges or Zcash ATMs.

"NOT YOUR KEYS, NOT YOUR COINS"

This is a popular saying among Zcash holders. It refers to the idea that if you don't have direct control over the private keys associated with your Zcash wallet, you don't have true ownership of the coins.

The private key is a secret code that allows you to access your Zcash and spend it. When you store your Zcash with a third-party service, like an exchange or online wallet, you are relying on that service to keep your private key safe.

A lot of things can happen to an exchange service that are completely out of your control. If the service is hacked, goes out of business, or governments choose to ban it and shut it down, you will lose access to your Zcash.

So, the saying "Not your keys, not your coins" is a reminder that it's important to take control of your own private keys and store them securely. By doing this, you can ensure that you have full control over your Zcash and can access it whenever you want.

6.2.2 ONBOARD YOURSELF THROUGH EARNING ZEC.

Zcash supports its developers, creators, ambassadors and supporters through in many ways. It is possible to find projects within the Zcash community that give out ZEC in exchange for different tasks that are considered necessary for the ecosystem and the community. The Zcash Foundation, ZecHub DAO, Zcash Community Grants Committee (ZCG) and the Financial Privacy Foundation are one of the many organizations that offer grants, bounties and Request-For-Proposals that are paid in ZEC.

If you are a merchant you can set up a wallet and start receiving ZEC payments! you can get in touch with the Pay With Zcash website to list your shop in their board for Zcashers across the world to see.



6.2 EXCHANGE AND HARDWARE WALLETS

Before to begin discussing the topic fo Exchanges and Hardware wallets we would like to do a quick stop to refresh some concepts.

Zcash is widely supported across the crypto ecosystem. In previous chapters we saw that Zcash has different pools of funds. There are shielded pools and a transparent pool. When it comes to shielded pool, transactions within those pools are totally private. Senders, recipients, memos and amounts are fully encrypted and invisible to others. When it comes to the transparent Zcash pool, everything is very similar to Bitcoin. Anyone can go to a block explorer of the Zcash chain see the addresses of senders and recipients and the amount transfered (there are no memos in transparent ZEC).

TIP

Not all Exchanges and Hardware wallets support Shielded Zcash. Unfortunately, the vast majority of them only support the transparent pool of Zcash. Bear in mind which pools are supported in your exchange of choice and be vigilant of the privacy implications. Privacy First!

6.2.1 CENTRALIZED EXCHANGES

6.2.1.1 KYC'D CENTRALIZED EXCHANGES

Exchanges are financial institutions that connet the traditional finance world to the Decentralized Finance realm. The same way a Bank would offer a "Home Banking" service to their users, Centralized Cryptocurrency Exchanges (CEXs) offer their own custodial wallets that let users access with typical username and password login. CEXs are widely used to on-ramp users to crypto by exchanging crypto for fiat and viceversa (off-ramp). One of the main issues with CEXs and Privacy is that Exchanges usually require their users to go throught a Know Your Customer / Anti-Money-Laundering regulation compliance process that entails sending them an ID and other information that deanonymizes you and gives them private information they have to keep in their records and relay to authorities if they are requested or mandated to. When choosing an Exchange you should check the features of the Zcash protocol they support. There are some exchanges that support deposits and withdrawals to shielded addresses and others that are transparent ZEC only.



TIP

When you give out private information to someone, is like taking toothpaste out of the tube: you can't put it back! So be careful and consider all the implications that KYC'ing could have for you.

6.2.1.2 NON-KYC CENTRALIZED EXCHANGES

If KYC'ing to a stranger organization sounded scary to you, you are not alone! Fortunately, there are exchanges that do not require KYC/AML to their users. They don't hold assets on your behalf, you will have to use your own wallets to transfer the funds to an address they tell you to, and provide a destination address on the other asset you want to exchange so that they deposit the equivalent of the conversion rate minus their fee. They are Centralized because the exchange itself is ran by a single organization with a central structure that holds the servers and nodes of the different cryptocurrencies they work with and hold exchange pairs for. Centralization makes some things simpler because everything is one place but, have you wondered what would happen if that site is taken down or attacked? That's pretty feasible because there's a single point of failure and adversaries simply are very keen on that when choosing targets.

6.2.2 DECENTRALIZED EXCHANGES

So far we have talked about KYC and Non-KYC centralized exchanges. But here we are all rooting for a decentralized future, aren't we? Well, you are correct. There's another way! Decentralized Exchanges exist and offer similar capabilities of those Non-KYC CEXs, but with the advantage of not having a single point of failure like their centralized counterparts. DEXs run on a decentralized peer-to-peer infrastructure that executes the exchange orders and the oracles to know the exchange rates of the different asset pairings.



6.3

PRIVACY-FOCUSED WALLETS

In section 6.2 we jumped back a bit and we reviewed some concepts about the different pools that hold Zcash, them being transparent or shielded. Zcash has currently four pools. One transparent and three shielded. Within those three shielded pools Sprout, the eldest of them, is being slowly retired as no new ZEC is allowed go into to that pool. Zcashers holding funds in the Sprout are only allowed to move their funds out of the Sprout pool into others. Nowadays, shielded wallets only use two shielded pools: Sapling and Orchard.

6.3.1 TO SHIELD OR NOT TO SHIELD

Privacy is consent. With Zcash you are in control of your funds and your privacy. You are the one deciding how much information you want to share with the public sphere. For that, information is power!

When you send shielded Zcash to transparent address (transparent addresses start with the letter 't') your information as sender will be encrypted, but the amount and recipient information will be transparent.

When you send shielded Zcash to shielded address your information as sender and the recipient will be encrypted, so as the amount. There is some little exception, which is for the case that your wallet sends ZEC sitting in the Sapling pool to the Orchard Pool.

From	To	Info Revealed on Chain	Info Encrypted
transparent	transparent	Addresses, amount, fee, etc. Same as Bitcoin,	none
transparent	shielded	Sender address(es), amount, fee	recipient address(es)
shielded	transparent	recipient address(es), amount, fee	sender address(es)
shielded	shielded (same pool)	fee	sender and receiver addresses, amount, shielded memos
shielded	shielded (crossing pool)	amount, fee	sender and receiver addresses, shielded memos

TIP

Migrating Funds: Funds moving to one pool to another will reveal the amount of ZEC transferred. This allows the Zcash total supply to be auditable. This is valid for all pools, regardless of those being transparent or shielded.

NOTE

If your happen to receive transparent funds you can always shield them by sending them to your own shielded address (see section "What is Autoshielding?").

6.3.1.1 UNIFIED ADDRESSES

As Zcash has different pools, each pool has its own address type. This is an inconvenient for users since they have to understand the underpinnings of each one of them in order to manage their funds. This is not exclusive to Zcash. Other cryptocurrency protocols (like Bitcoin) have this problem too, where they release new features that need new address encodings.

Unified Addresses are like a small box that contains different addresses (we call them receivers) for wallets to use. They let users be abstracted of all that complexity by providing a single kind of address that contains other addresses. Wallets are able to look inside that small box and use the address they see most suitable for the case.

Shielded wallets know best! When sending funds to a Unified Address, the wallet will send the funds to the receiver that offers the most private transaction. Ultimately, your wallet will let your review your transaction before sending it. Wallets that prioritize shielded funds and always shield transparent funds before they can be used are called Shielded-by-Default

--- call out -- To learn more about Unified Addresses visit this article at [z.cash](#) --- call out end --

6.3.1.2 WHAT IS AUTOSHIELDING?

Zcash is widely accepted and use accross the global crypto ecosystem. Although we only recommend Zodlers and Zcashers to user Shielded Wallets, many wallets support transparent ZEC only. You can always recieve transparent funds with your shielded wallet. The best course of action when receiving transparent funds, is to shield them by moving them to a shielded pool. You can do this manually by sending the transparent ZEC to your own shielded address. Fortunately Shielded Wallets know best!. Wallets like NightHawk, Ywallet, Zashi and Zingo will detect this funds and let you know that you have transparent ZEC waiting to be shielded.

All wallets will let you shield your transparent ZEC by tapping a button. However some can actually do it automatically for you when your transparent ZEC is above a certain amount. This is what we call Autoshielding.

6.3.2 ZCASH SHIELDED WALLETS

There are many Zcash shielded wallets. Their main characteristic is that they support receiving and sending shielded ZEC and also will always prioritize sending shielded-first. All shielded wallets we are featuring are self-custody.

6.3.2.1 NIGHTHAWK WALLET

Launched mid-2020 by NightHawk Apps, Nighthawk wallet was one of the first Zcash shielded wallets available for mobile devices. Nighthawk is a Shielded-by-default light wallet for Zcash with support sending receiving shielded transactions, memo support and optional transparent addresses support with Auto-Shielding technology. Nighthawk is a wallet that has a user-friendly design and focuses heavily on first-time users facilitating access to different services that allows them to use Non-KYC CEXs to exchange ZEC or fund their wallet with fiat.



6.3.2.2 YWALLET

Originally launched as a Ycash wallet, a blockchain considered to be a friendly-fork of Zcash, Ywallet is a very feature-complete wallet multi-platform Zcash wallet. Ywallet is available for Android, iOS, Mac OS, Linux and Windows. It is designed to cover the needs of the most advanced Zcash users. Its basic mode covers a good set of functionalities that go beyond what novice users could need and its advanced mode provides high levels of customizations and tweaking in terms of funds and account management. If you are a very hands on person and curious of the inner workings of the tech you use, Ywallet has got you cover. ZEC Adventurer, procede with care!

6.3.2.3 ZASHI WALLET

Launched in March 28th 2024, Zashi is a plain, simple, shielded-by-default and straight to the point mobile wallet from Electric Coin Company. ECC is the company behind the creation of Zcash. Zashi is not the most feature complete wallet out there. It is thought to be a wallet that is all about the core principles of Zcash. It's main feature is Spend-before-sync, which allows users to detect funds fast and make them ready to spend as soon as possible.

6.3.2.4 ZINGO! WALLET

Zingo is a Shielded-by-default wallet that is developed by Zingo Labs. The folks at Zingo define themselves as "a worldly team of scrappy hackers working to build a safe community for everyone". Zingo wallet is available for both mobile (Android and iOS) and desktop computers. It features a Hacker-style aesthetic and one of its cool features is a private financial insight that will let you know how you are using your funds. ZingoLabs is a very active member of the Zcash community and contribute to many other projects across the ecosystem

6.4

HARDWARE WALLETS

The wallets mentioned in the previous section are "software wallets". This means that they are software that runs on a device that is not specifically dedicated to wallet functionality such as your mobile phone or your computer.

Although your phone may have a section of its hardware that it is dedicated to storing sensitive information securely, a smartphone was not built for that sole purpose. There are devices which only have one purpose: store cryptocurrency private keys as securely as possible. These devices are called Hardware Wallets. There are many well known Hardware Wallet manufacturers, the most renowned are Keep Key®, Ledger® and Trezor®.

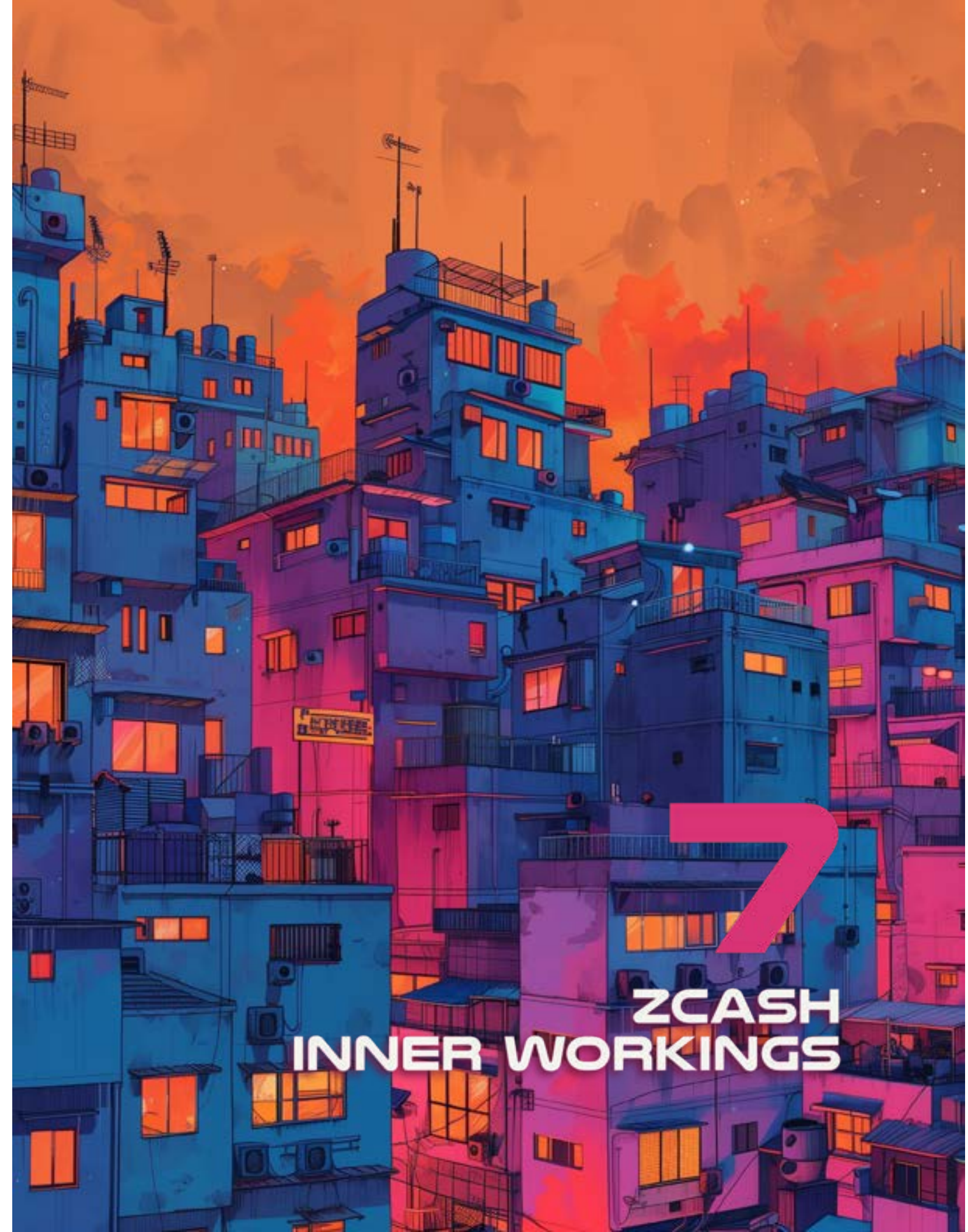
Hardware wallets let users have a device that holds their keys securely and that can resist to tampering attacks even if an adversary gets ahold of the device. Hardware wallets never expose your keys to the Internet. They usually have a companion application that connects to the Internet with your public keys to identify funds that belong to you so that you can be aware of your balance, but they will sign your transactions offline, completely disconnected from the network. Once you create a transaction with your private keys using your hardware wallet, the companion app will submit your transaction separately.

Unfortunately, to the day of writing this chapter, there is no official support for Shielded Zcash transactions. You can still use ZEC through them but you have to be aware that until Shielded ZEC is supported by those manufacturers, you will only be able to hold transparent ZEC with them. These are trade-offs to consider when holding ZEC (aka Zodling). Contents of this book will provide the needed knowledge to help you make an informed decision about what is the best way to hodl your ZEC.

[^3] Daira-Emma Hopwood, Jack Grigg, ZIP-315: Best Practices for Wallet Handling of Multiple Pools. <https://zips.z.cash/zip-0315>

1 -Thanh Bui, Siddharth Prakash Rao, Markku Antikainen, and Tuomas Aura. 2019. Pitfalls of open architecture: How friends can exploit your cryptocurrency wallet. In *Proceedings of the 12th European Workshop on Systems Security (EuroSec '19)*. Association for Computing Machinery, New York, NY, USA, Article 3, 1–6. <https://doi.org/10.1145/3301417.3312495>

2 - Francisco Gindre, Matias Urbieto, and Gustavo Rossi. 2023. Patterns for Anonymity Enhancing Cryptocurrencies Non-Custodian Mobile Wallets. In *Proceedings of the 29th Conference on Pattern Languages of Programs (PLoP '22)*. The Hillside Group, USA, Article 3, 1–29. <https://dl.acm.org/doi/abs/10.5555/3631672.3631676>



ZCASH
INNER WORKINGS

INTRODUCTION

The history of Zcash is intimately linked with Zero-Knowledge Proofs (ZKPs), particularly Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK). These mechanisms allow proving possession of certain information without revealing that information itself.

NOTE

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a specific type of ZKP that enables efficient verification of computations without disclosing the inputs and outputs involved.

The Zcash initiative combines advanced mathematics with state-of-the-art encryption, smoothly incorporated into its software architecture. Navigating through the depths of knowledge required to comprehend Zcash can be scary. However, our approach will be to unveil these concepts as we journey through them, culminating in a profound understanding of how Zcash achieves its primary objective: preserving financial privacy on an open and secure blockchain.

Throughout this journey, we will delve into the annals of history, tracing Zcash's inception, and discerning the rationale behind pivotal decisions. By the end, you will possess a robust comprehension of the myriad components that constitute Zcash today, empowering you to delve deeper into any aspect presented herein.

While a foundation in undergraduate mathematics, programming, and blockchain understanding will certainly aid your exploration, it is not a prerequisite.



Privacy is paramount in financial transactions, safeguarding sensitive information from prying eyes and potential misuse. While traditional transparent blockchains like Bitcoin offer pseudonymous transactions, Zcash strives to elevate privacy to an unprecedented level, ensuring financial confidentiality for its users.

NOTE

Understanding Zcash's genesis requires delving into the historical backdrop of cryptography and privacy-focused initiatives. By tracing its lineage, we can appreciate the evolutionary forces that have shaped Zcash into what it is today.

TRANSPARENT WORLD

In cryptocurrency, particularly in Zcash, a wallet is essentially a collection of keys. Initially, a private key is generated, from which a corresponding public key is derived. Subsequently, a hash function is applied to the public key, resulting in a payment address. This address serves as the destination for incoming funds.

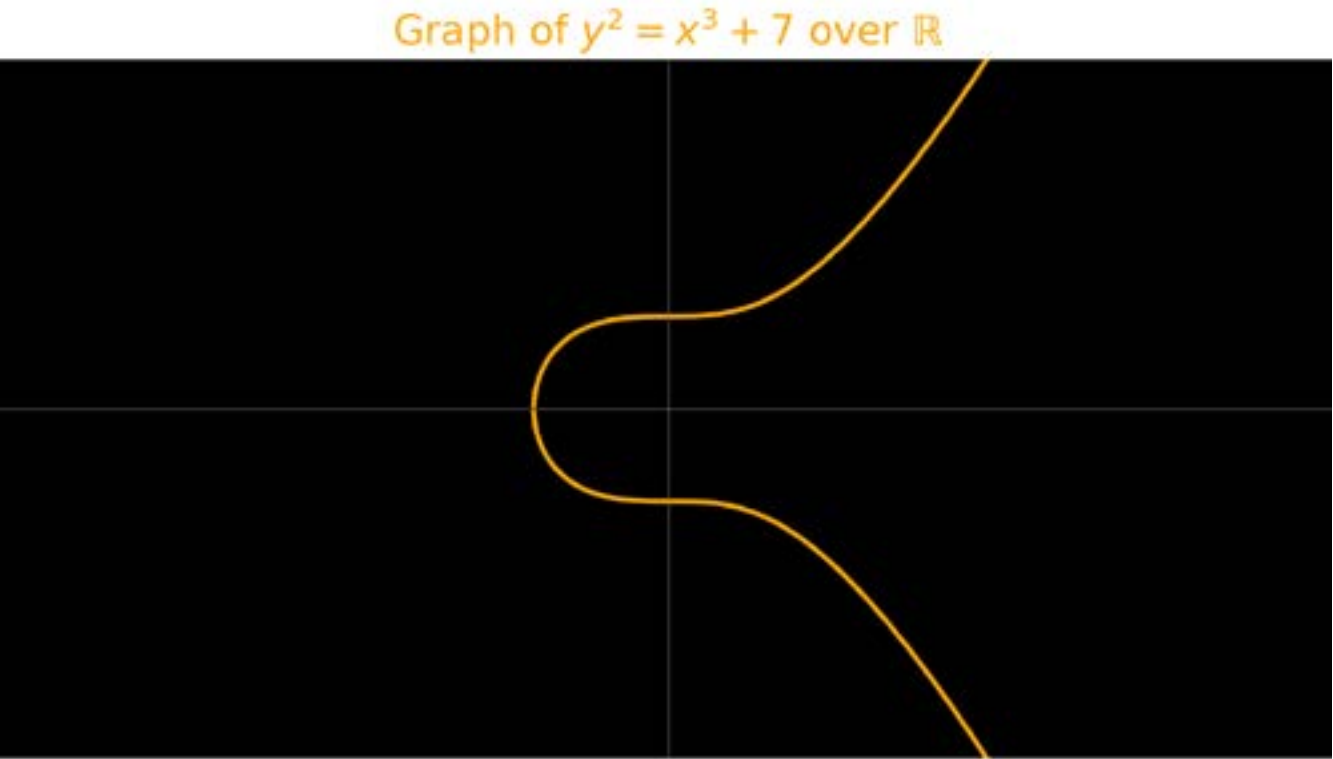
7.1.1 GENERATING PRIVATE KEYS

Private and public keys are numerical representations, specifically generated by solving elliptic curve equations. The elliptic curve utilized for Zcash’s transparent addresses is *secp256k1*, the same curve employed in the Bitcoin protocol:

$$y^2 = x^3 + 7$$

This curve operates over a finite field \mathbb{F}_p , where p is an exceedingly large prime number. In practical terms, this means that the curve’s function operates within a finite subset of numbers, rather than over all possible numbers. The use of a finite field ensures that computations on the curve remain efficient and manageable, even with large prime numbers.

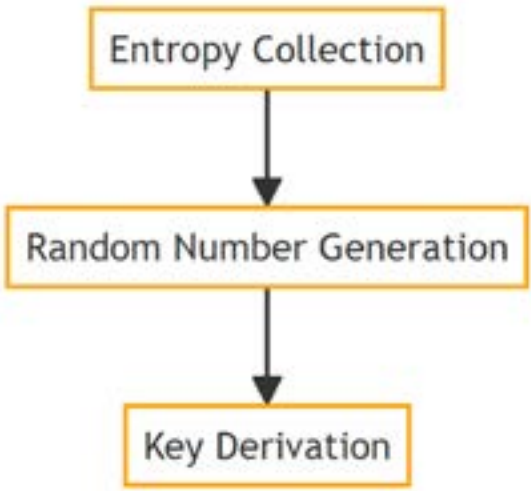
Here is a visualization of the *secp256k1* curve with the Real numbers as the domain of the function. It’s important to note that while this visualization helps in understanding the curve’s shape, the actual domain used in cryptographic operations is not the real numbers, but rather the finite field



In Zcash, cryptographic keys can be generated through various methods, each offering unique advantages in terms of security and usability. Here, we explore three common approaches:

➤ RANDOM NUMBER GENERATOR (RNG):

One method for generating keys involves using a Random Number Generator (RNG) to produce a random seed, which is then used as input for key derivation. RNGs are algorithms or hardware devices designed to generate unpredictable and statistically random numbers, ensuring cryptographic strength.



ADVANTAGES:

- Cryptographic Strength: Random seeds provide strong cryptographic security.
- Unpredictability: RNG-generated keys are highly unpredictable and resistant to attacks.
- Scalability: RNG-based key generation can easily scale to generate large numbers of keys.

EXAMPLE:

➤ Random Seed (Decimal):

68123456789012345678901234567890123456789012345678901234567890123

➤ Random Seed (Hexadecimal):

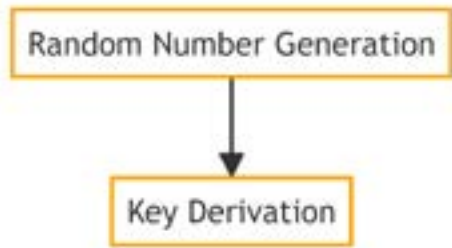
0x3B9ACA0057BE5C5E3A44F5B17E2FC1DAA17F1E15398A4C9A5B6A0A6FD73F13CB

EXPLANATION

The example illustrates a random seed generated by an RNG. This seed serves as the basis for deriving cryptographic keys.

➔ **RANDOM NUMBER AS SEED:**

Another approach involves generating a random number directly, which serves as the seed for key derivation. This method offers simplicity and efficiency, as it eliminates the need for additional entropy collection steps.



ADVANTAGES:

- ➔ Simplicity: Directly using a random number simplifies the key generation process.
- ➔ Efficiency: Eliminates the need for additional entropy collection steps.

EXAMPLE:

- ➔ Random Number (Decimal):

6724321098765432109876543210987654321098765432109876543

- ➔ Random Number (Hexadecimal):

0x3B9ACA0057BE5C5E3A44F5B17E2FC1DAA17F1E15398A4C9A5B6A0A6FD73F13CB

EXPLANATION

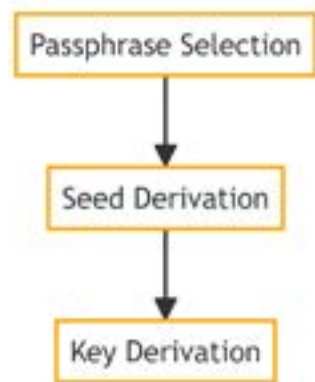
In this example, a random number is generated directly and used as the seed for key derivation, bypassing the need for entropy collection.

➔ **PASSPHRASE-BASED KEY GENERATION (RECOMMENDED):**

The recommended approach involves generating keys based on a memorable passphrase. This method leverages a passphrase as input to derive a seed, which is then used for key derivation. Passphrase-based key generation offers usability and accessibility advantages, as users can easily remember their passphrase.

ADVANTAGES:

- ➔ Usability: Passphrase-based key generation is user-friendly and easy to remember.
- ➔ Accessibility: Users can access their keys using a passphrase, enhancing usability.



EXAMPLE:

- ➔ Passphrase: "MySecretPassphrase123!"

EXPLANATION

In this example, a passphrase "MySecretPassphrase123!" is chosen. A key derivation function is applied to convert the passphrase into a seed, which is then used to derive cryptographic keys. Passphrase-based key generation offers the advantage of usability and accessibility, as users can easily remember their passphrase and derive keys from it.



WARNING

It's essential to understand the following security considerations regarding cryptographic keys in Zcash:

Private Key Loss: If you lose your private key, there is typically **no way to recover it**. Therefore, it's crucial to securely store your private keys and create backups to prevent loss.

Ownership and Access: Anyone in possession of your private key can access and spend the associated coins. Thus, it's paramount to safeguard your private keys from unauthorized access.

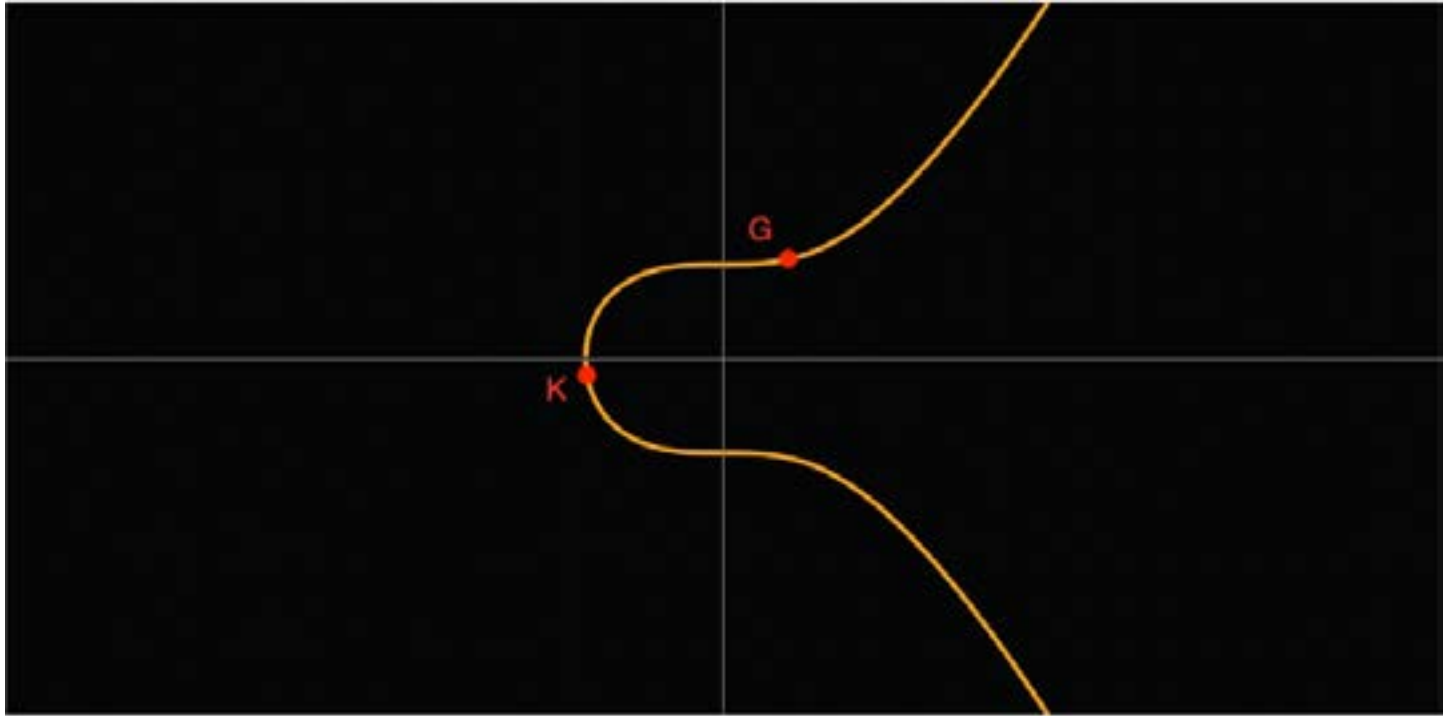
Taking proactive measures to protect your private keys is fundamental to ensuring the security of your Zcash holdings. By maintaining strict control over your private keys and adhering to best practices in key management, you can mitigate the risks associated with key loss and unauthorized access.

7.1.2 TRANSPARENT PUBLIC KEYS AND ADDRESSES

In the previous section, we discussed how to generate a private key which is then used to generate a public key, which in turn is used to generate a Zcash transparent address where funds can be received.

You can think of the private key as the password to your bank account, which should be kept secret, whereas the public key is equivalent to your account number, which you can share with others in order to receive money.

In this case however, the two values are linked so that, in order to generate a public key and therefore a resulting Zcash address, the private key is multiplied with a constant number, G aka the Generator point, which is a point that exists on the secp256k1 curve and is defined in the curve parameters.



$$K \text{ (Public Key)} = k \text{ (Private Key)} \times G \text{ (Generator Point)}$$

This will give us an X and Y coordinate pair representing another valid point on the curve, K, which will this is for our purposes the derived public key.

Now that we have our public key, we can use this to generate a public address by applying 2 hash functions to it in order to make it a smaller, fixed length (40 characters as opposed to up to 79 chars.)

7.2 SHIELDED WORLD

Building on our understanding of the Zcash's transparent world, let's explore into the more private side of Zcash with shielded addresses and transactions, the features that truly set Zcash apart in the blockchain space.

7.2.1 VALUE POOLS

The Zcash blockchain is structured around various value pools, each corresponding to a different type of address or stage of the network's evolution. These pools include:

- Transparent Pool: Contains all funds in transparent addresses, similar to Bitcoin's transaction model.
- Sprout Pool: The initial shielded pool, to be deprecated, representing the first implementation of private transactions.
- Sapling Pool: Represents the next evolution, introducing improved efficiency and privacy.
- Orchard Pool: The latest advancement in Zcash's privacy technology.

The total of these pools equates to the sum of ZEC in circulation. The `getblockchaininfo` RPC method allows users to check the total value in each pool, providing transparency into the distribution of ZEC across different address types.

7.2.2 EVOLUTION OF SHIELDED TECHNOLOGY

The evolution of shielded technology in Zcash shows its pioneering journey towards privacy within the blockchain space.

SPROUT: THE FOUNDATION OF PRIVACY

Sprout, introduced at Zcash's launch on October 28, 2016, marked the first implementation of shielded transactions using zk-SNARKs. This was a groundbreaking technology designed to enable transaction verification without revealing sensitive information.

SAPLING: BOOSTING EFFICIENCY AND ADOPTION

The Sapling network upgrade, activated on October 29, 2018, significantly improved the efficiency and usability of shielded transactions. It introduced new shielded addresses with improved transaction speed and memory usage. This upgrade facilitated mobile apps, exchanges, and vendor adoption of Zcash by making private transactions more practical for everyday use. One of the key features of Sapling was the decoupling of the spending authority from the ability to see transactions with the introduction of the viewing keys.

ORCHARD: ADVANCING PRIVACY WITH HALO 2

Orchard, part of the Network Upgrade 5 (NU5) activated in May 2022, represented the latest advancement in Zcash's privacy technology. It incorporates the Halo 2 proving system, eliminating the need for a trusted setup previously required for generating zk-SNARKs. This upgrade also introduced the concept of Unified Addresses, simplifying the user experience by supporting both shielded and transparent transactions within a single address format.

The evolution of shielded technology in Zcash shows its pioneering journey towards privacy within the blockchain space.

➔ **SPROUT: THE FOUNDATION OF PRIVACY**

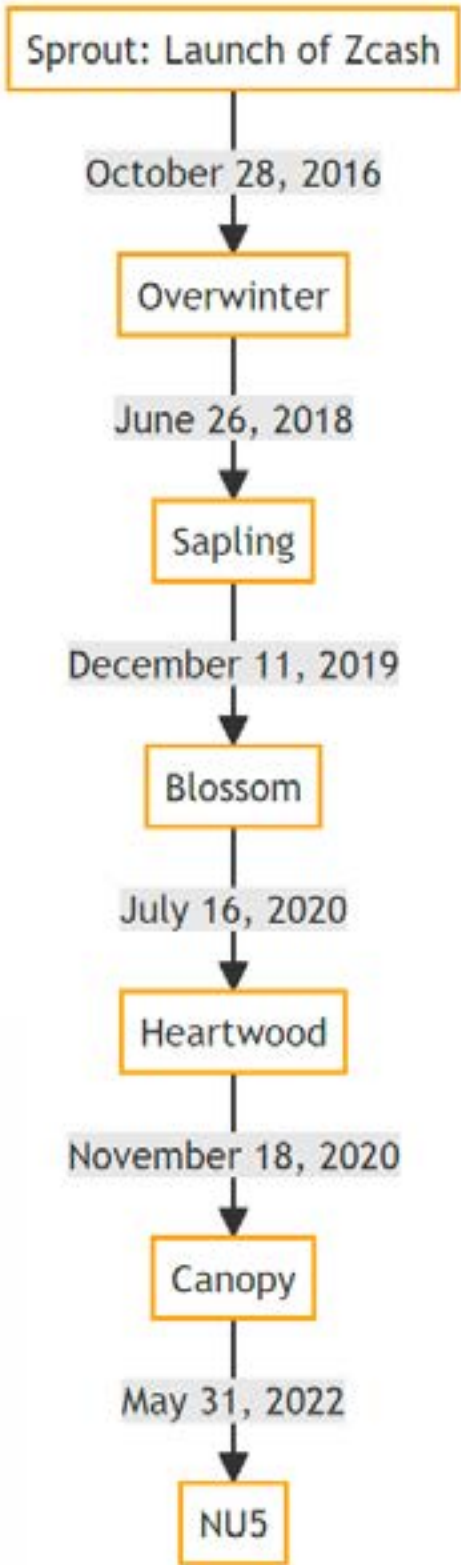
Sprout, introduced at Zcash’s launch on October 28, 2016, marked the first implementation of shielded transactions using zk-SNARKs. This was a groundbreaking technology designed to enable transaction verification without revealing sensitive information.

➔ **SAPLING: BOOSTING EFFICIENCY AND ADOPTION**

The Sapling network upgrade, activated on October 29, 2018, significantly improved the efficiency and usability of shielded transactions. It introduced new shielded addresses with improved transaction speed and memory usage. This upgrade facilitated mobile apps, exchanges, and vendor adoption of Zcash by making private transactions more practical for everyday use. One of the key features of Sapling was the decoupling of the spending authority from the ability to see transactions with the introduction of the viewing keys.

➔ **ORCHARD: ADVANCING PRIVACY WITH HALO 2**

Orchard, part of the Network Upgrade 5 (NU5) activated in May 2022, represented the latest advancement in Zcash’s privacy technology. It incorporates the Halo 2 proving system, eliminating the need for a trusted setup previously required for generating zk-SNARKs. This upgrade also introduced the concept of Unified Addresses, simplifying the user experience by supporting both shielded and transparent transactions within a single address format.



7.2.3 SHIELDED ADDRESSES AND KEYS

In this section, we’ll give a brief overview of how the various different keys and addresses are generated, starting from an initial private key within the Zcash protocol’s shielded ecosystem.

We will discuss the three types of shielded addresses supported by Zcash: Sprout, Sapling, and Orchard, explaining their significance and how they’re generated.

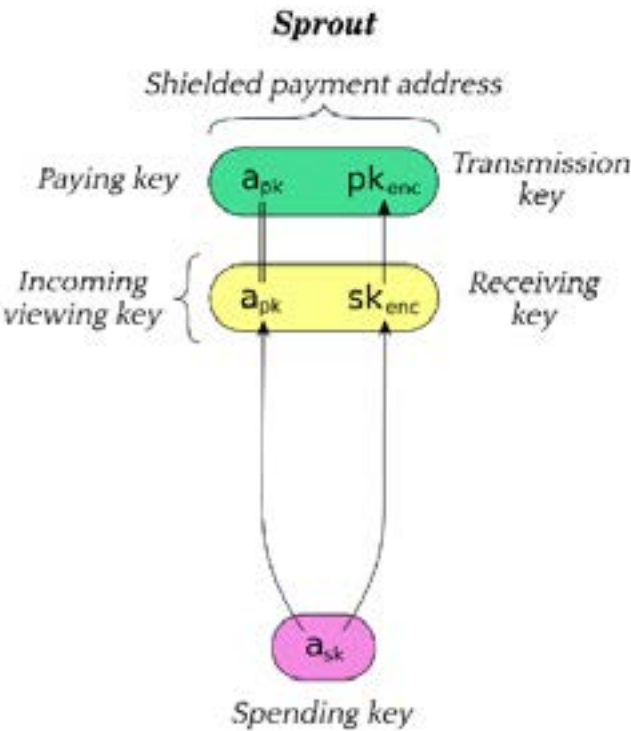
Upcoming sections will cover shielded transactions, bridging our understanding of Zcash’s protocol and its main features.

7.2.3.1 SPROUT SHIELDED ADDRESSES AND KEYS

Sprout addresses, although legacy, remain an integral part of the Zcash protocol, holding value within the sprout shielded pool. Despite the absence of a way to create new Sprout addresses, understanding their mechanics is important not only due to their historical significance within Zcash but also because it lays the foundational knowledge necessary for comprehending the advancements and distinctions of later shielding technologies, such as Sapling and Orchard.

As with transparent addresses, and indeed all other shielded address types, in order to generate a Sprout address, we start with a private key which is a random number in the Sprout case selected from a specific finite set of numbers. We then apply a number of transformations on this private key to generate:

- ➔ a spending key
- ➔ a viewing key, and
- ➔ the Sprout shielded address.



7.2.3.2 SAPLING SHIELDED ADDRESSES AND KEYS

Sapling addresses and functionality represent an evolution within the Zcash protocol, offering enhanced efficiency and features compared to their Sprout predecessors.

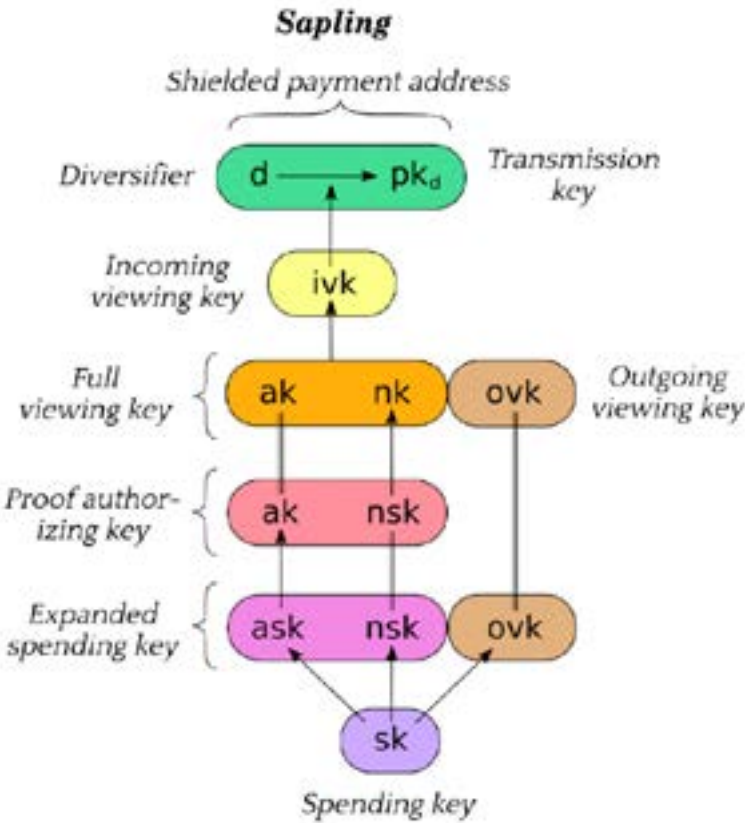
SAPLING MASTER KEYS

In the Zcash Sapling protocol, whether you start with a spending key or a master key, several components can be derived, each serving distinct roles in various cryptographic processes. The main ones to be aware of are as follows:

- Spend Authorizing key: Used to authorize spending operations.
- Proof Authorizing key: Utilized in generating zero-knowledge proofs for transactions, ensuring the spender has the right to spend.
- Outgoing Viewing key: Allows the holder to view outgoing transaction details without revealing the transaction's value to others.
- Diversifier key: Used to generate diversified addresses, allowing users to use multiple addresses derived from the same key.

From these components, standard keys are derived for transaction processes:

- Authorizing key: Derived from the Spend Authorizing Key, used in the transaction signing process to prove ownership of the funds being spent.
- Nullifier key: Derived from the Proof Authorizing Key, used to mark spent notes and prevent double-spending.
- Incoming Viewing key: Derived from the Authorizing Key and Nullifier Key, allows the holder to view incoming transactions to the addresses derived from the corresponding Diversifier Key.



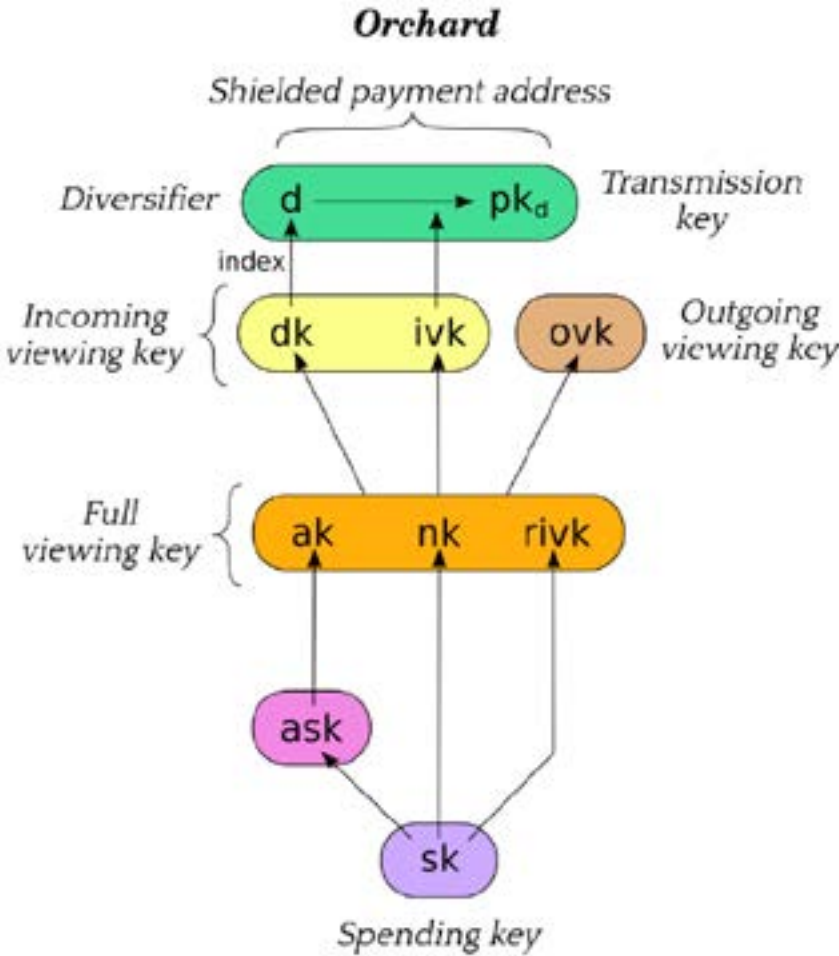
The derivation of Sapling child keys allows for the creation of multiple, distinct addresses from a single master key. This process follows a hierarchical deterministic (HD) structure, enabling efficient management and recovery of addresses.

Each child key can further derive its own child keys, creating a tree-like structure of keys. This is especially useful for organizing addresses into categories (e.g., for receiving, change, or different purposes).

This hierarchical structure enables a single seed to recover an entire wallet of multiple addresses.

7.2.3.3 ORCHARD SHIELDED ADDRESSES AND KEYS

Orchard keys and payment addresses are structurally similar to Sapling and take advantage of lessons learned during Sapling development to simplify the components derived from the spending key.



7.2.3.4 UNIFIED ADDRESSES

Zcash’s introduction of Unified Addresses marks a significant advancement, simplifying user interaction with different address types. Unified Addresses encapsulate information for multiple types of addresses (transparent, Sapling, and Orchard) within a single, user-friendly identifier. This innovation facilitates transactions between different pools and address types, streamlining the user experience while preserving privacy and interoperability within the Zcash ecosystem.

DERIVATION OF UNIFIED ADDRESSES

Unified Addresses in Zcash are designed to bundle various types of addresses, including transparent (P2PKH), Sapling, and Orchard addresses, into a single construct.

COMPONENTS OF A UNIFIED ADDRESS:

- Transparent Component: Derived from the traditional P2PKH address format used in Bitcoin, this component allows for interoperability with systems that require transparent transactions.
- Sapling Component: Utilizes zk-SNARKs for privacy-preserving transactions. Each Sapling address is associated with a unique viewing key and spending key.
- Orchard Component: The latest addition to Zcash’s privacy protocol, using Halo 2 proofs to enable efficient and private transactions without trusted setup.

Unified Addresses enable users and services to interact with multiple Zcash address types through a single identifier, simplifying transactions and enhancing privacy. When a user sends Zcash to a Unified Address, their wallet software automatically determines the most appropriate address type to use, based on the transaction’s requirements and the capabilities of the sender’s and receiver’s wallets.

7.2.4 SHIELDED ADDRESSES AND KEYS

Now that we have a very good understanding of shielded addresses and keys, it is time to see them in action and understand how they fit inside transactions that protect the privacy of Zcash users.

At the moment, the Zcash protocol supports two versions of transactions that are encoded inside blocks. These currently supported transaction versions are version 4 and version 5. The main difference between them is that version 4 allows for both Sprout and Sapling transactions, while version 5 supports Sapling and Orchard transactions.

The recommended transaction version for new software to use is, of course, version 5, while version 4 is there to support legacy Sprout transactions. Let’s define the components of each transaction type.

Before actually going into how each protocol version (Sprout, Sapling, Orchard) handles shielded transactions, there are some general concepts that we should learn:

NOTES

A note represents the amount of Zcash (ZEC) that is being transferred in a shielded transaction. It contains information about the value being transferred and the recipient’s address but does not reveal this information on the blockchain. Notes are part of the encrypted data that only the recipient can decrypt using their private viewing key.

NOTE COMMITMENT

A note commitment is a cryptographic commitment to the contents of a note, including the amount and the recipient’s shielded address. When a note is created in a transaction, its commitment is publicly recorded on the blockchain. However, the commitment is designed such that it’s computationally infeasible to derive the note’s contents from it, ensuring the privacy of the transaction.

NOTE COMMITMENT TREE

The Note Commitment Tree is a type of computational structure known as a Merkle tree that aggregates all the note commitments created from transactions into a single structure. Each time a note commitment is created, it is appended to the tree. The root of this tree (the Merkle root) is updated and included in the blockchain’s block header. This structure allows for efficient verification of the existence of a note commitment within the tree without revealing its position or the details of other notes, contributing to the privacy and integrity of shielded transactions.

NULLIFIERS

A nullifier is derived from a shielded note and is used to prevent double-spending. When a note is spent in a transaction, its nullifier is revealed and recorded on the blockchain. This nullifier is a unique identifier for the note but does not disclose any information about the note itself. Network participants can check the list of nullifiers to ensure that a note has not been spent twice without knowing anything about the note’s value or recipient.

7.2.4.1 SPROUT TRANSACTIONS

The main component of Sprout transactions is the notion of JoinSplits. JoinSplits are specific to the Sprout phase of Zcash and serve as the cornerstone of Zcash's privacy features in this phase. They enable the transaction to hide the sender, receiver, and amount transferred, providing privacy and interchangeability to Zcash transactions.

JOINTSPLIT TRANSACTIONS

JoinSplit transactions conceal the transaction details from everyone except the sender and receiver. This includes hiding the identities of the sender and receiver and the amount being transferred, using zk-SNARKs to ensure that transactions are valid without revealing these details.

Each JoinSplit transaction involves the combination of inputs (funds) from multiple sources (joining) and allocation to multiple outputs (splitting), within a single transaction. This process obscures the flow of funds, adding an additional layer of privacy. This combination of components is known as joinsplit descriptions.

A JoinSplit description includes encrypted transaction details, a zk-SNARK proof to validate the transaction's integrity and privacy, and, when applicable, any transparent inputs or outputs. These components ensure that while the transaction is verifiable by the network, the privacy of the transaction participants is maintained.

A JoinSplit transfer is an individual shielded value transfer.

7.2.4.2 SAPLING TRANSACTIONS

The introduction of Sapling in Zcash transactions marked a significant evolution in the protocol's approach to privacy and efficiency.

At its core, a Zcash transaction may include a mix of transparent and shielded transfers. The process begins with the a Sapling value balance, a number that reflects the net value transfer between the transparent and shielded pools within a transaction. This balance adjustment ensures that the transaction's total input value matches its total output value, maintaining the principle of conservation of value across the Zcash network.

SAPLING SPENDS

Sapling spends allow users to consume existing shielded notes. For each spend, a zero-knowledge proof (`zkproof`) validates the right to spend without revealing the note's value or the spender's identity. The `nullifier` associated with each spent note prevents double-spending, while the `spendAuthSig` confirms the spender's authorization.

SAPLING OUTPUTS

Sapling outputs are the transaction's destinations for new shielded notes. These outputs encrypt details about the value and recipient, making the information accessible only to intended recipients. This encryption, facilitated by an ephemeral key, secures the transfer of value while preserving the privacy of the transaction details.

Benefits Over Sprout

Compared to its predecessor, Sprout, Sapling introduces several key improvements:

- ➔ **Efficiency:** Sapling reduces the time and memory required to construct shielded transactions. This efficiency gain is primarily due to the optimized zero-knowledge proving system (Groth16), which offers smaller proof sizes and faster verification times.
- ➔ **Privacy:** Sapling strengthens privacy through improved key management. The protocol allows users to view incoming transactions without revealing their private spending keys, thanks to the introduction of viewing keys and diversified addresses.
- ➔ **User Experience:** The enhancements in efficiency significantly improve the user experience by making transactions faster and less resource-intensive. This improvement makes shielded transactions more accessible to a broader range of users and devices, potentially increasing the adoption of privacy features.
- ➔ **Delegation Capabilities:** Sapling's viewing keys enable the delegation of transaction viewing capabilities without compromising the security of the funds. This feature allows for more flexible privacy controls and the potential for third-party auditing in a privacy-preserving manner.

In summary, the integration of Sapling components into Zcash v4 transactions represents a significant leap forward in the pursuit of a more private, efficient, and user-friendly digital currency. By addressing the limitations of the Sprout protocol, Sapling sets a new standard for privacy-preserving transactions in the blockchain space.

7.2.4.3 ORCHARD TRANSACTIONS

Orchard transactions are encapsulated in the Zcash transaction version 5 (v5), which also accommodates transparent and Sapling data. Orchard introduces new mechanisms for shielded transactions, leveraging the latest advancements in zero-knowledge proofs to enhance privacy and efficiency.

The heart of an Orchard transaction lies in the Orchard Actions, which encapsulate the movement of ZEC within the Orchard shielded pool. Each action is a detailed record that includes the input (if spending), the output (if creating new ZEC), and all the necessary cryptographic proofs to validate the transaction without compromising privacy.

An Orchard Action includes value commitments, nullifiers for spent notes, and the new commitments for any created notes, alongside the necessary zk-SNARK proofs to verify these elements without revealing underlying data.

- Privacy and Security Features: Powered by the novel Halo 2 proving system, Orchard actions do not require a trusted setup, mitigating potential security risks associated with initial parameter generation. This improvement significantly reduces the blockchain’s exposure to vulnerabilities related to the setup phase.
- Efficient Verification and Compact Proofs: The recursive proof composition enabled by Halo 2 allows Orchard transactions to be verified quickly and efficiently, contributing to a scalable blockchain ecosystem that can handle higher volumes of transactions without compromising speed or security.

ORCHARD BENEFITS OVER SAPLING AND SPROUT

Elimination of Trusted Setup

Orchard, through its use of the Halo 2 proving system, eliminates the need for a trusted setup.

Improved Scalability and Efficiency

Thanks to the recursive nature of Halo 2 proofs, Orchard transactions are more scalable and efficient. The proofs are both smaller in size and faster to verify compared to those used in Sapling and Sprout, leading to quicker transaction processing times and lower costs, even as the network grows.

Enhanced Privacy

Orchard builds on the privacy features of Sapling but with additional improvements. The use of Halo 2 allows for more sophisticated encryption techniques and the possibility for future privacy features without sacrificing efficiency or requiring a trusted setup.

Greater Flexibility

The architecture of Orchard, coupled with the Halo 2 proving system, lays the groundwork for more complex and flexible transaction types.

TIP!

In Zcash, the “trusted setup” is a foundational step required for the secure implementation of zk-SNARKs, the cryptographic method enabling privacy in transactions. This process involves generating a set of public parameters (often referred to as “toxic waste”) essential for constructing zero-knowledge proofs. The integrity of this setup is crucial; any compromise could potentially allow the creation of counterfeit coins. To mitigate this risk, Zcash’s initial setups for the Sprout and Sapling upgrades involved elaborate ceremonies with multiple participants, designed to ensure that as long as one party securely destroyed their portion of the toxic waste, the network would remain secure.

However, acknowledging the inherent risk and trust involved in such setups, Zcash moved towards an “untrusted setup” with the introduction of the Halo 2 proving system in the Orchard network upgrade. Halo 2 eliminates the need for a trusted setup by using recursive zk-SNARKs that don’t require a setup phase vulnerable to the toxic waste dilemma. This advancement significantly reduces the trust required in the setup process, enhancing the security and decentralization of the network by removing the potential for a single point of failure in the creation of zk-SNARK parameters. This shift marks a significant milestone in Zcash’s evolution, offering robust privacy without the need for a trusted setup ceremony.

NOTE

A **viewing key** has the necessary information to view information about payments to an Address, or (in the case of a Full Viewing Key) from an Address. An Incoming Viewing Key can be derived from a Full Viewing Key, and an Address can be derived from an Incoming Viewing Key.

7.3

CONCLUSION

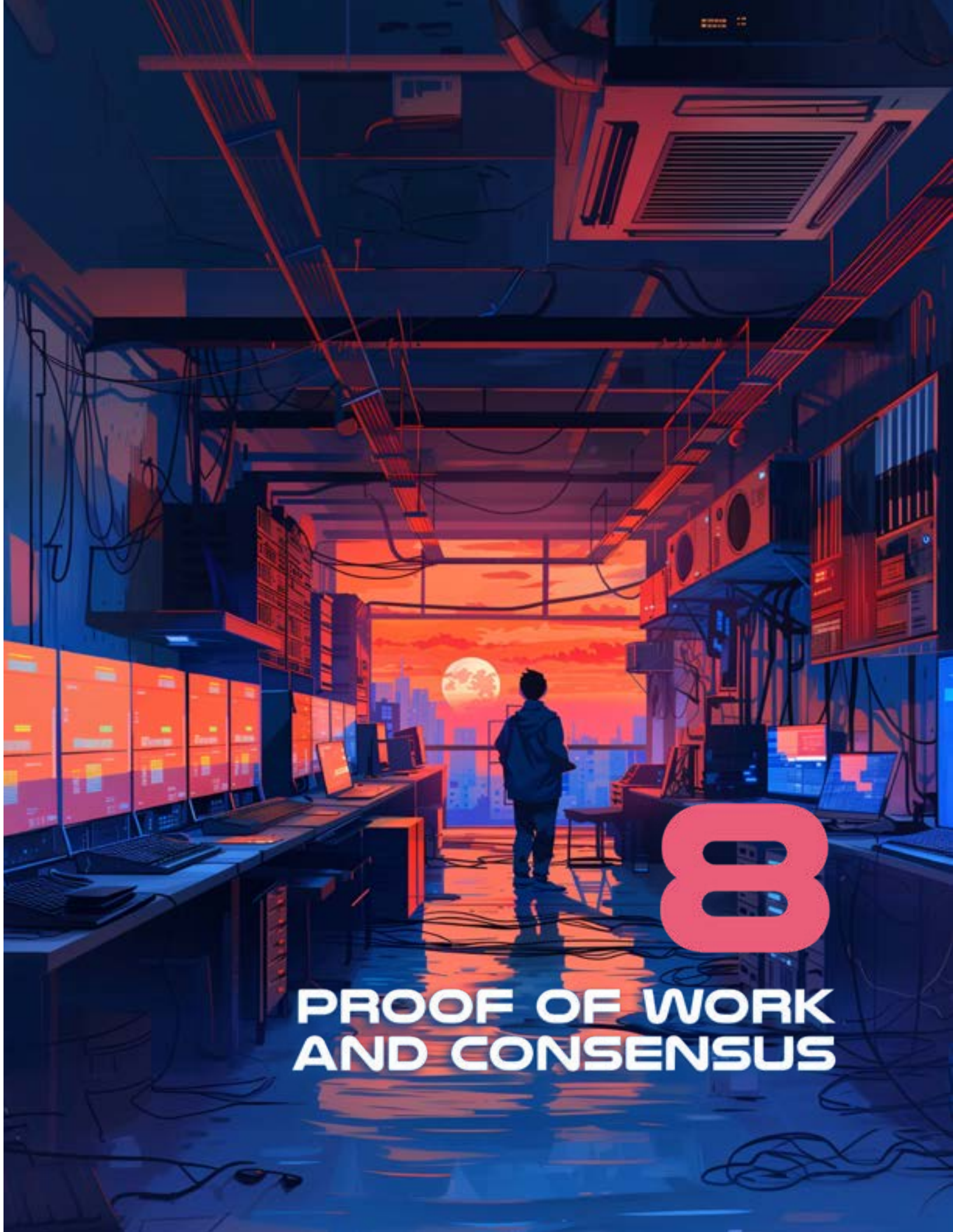
“The vast expanse of cryptography, mathematics, and engineering that constitutes the foundation of Zcash is both immense and intricate, continuously evolving in complexity. To encapsulate the entirety of this technology within a single book chapter is an endeavor that borders on the overly ambitious. The primary objective of this writing is not to exhaustively dissect each facet of the Zcash protocol with rigorous detail but to illuminate some of its most pivotal aspects. This exploration is designed to demystify the protocol, encouraging readers to delve deeper into its workings without intimidation.

The Zcash protocol specification presents a formidable challenge in terms of comprehension. It is my hope that this chapter serves as a beacon, guiding both developers and enthusiasts through the labyrinthine intricacies of Zcash, regardless of their prior exposure to its underlying mechanisms.

Embarking on this literary journey necessitated extensive research on my part, revealing new layers of complexity even to someone entrenched within Zcash development. Despite my intimate involvement with Zcash, attaining a comprehensive grasp of certain mechanisms remains a challenge. The process of compiling this chapter has been as much an educational journey for me as it is intended to be for you, the reader.

In sharing this knowledge, my aspiration is to sow the seeds of curiosity and understanding within those who have invested their time in engaging with this chapter.” - Oxarbitrage





8

**PROOF OF WORK
AND CONSENSUS**

You’ve probably heard that cryptocurrencies such as Zcash are “decentralized.” The usual quick explanation is that there is no “central authority” you need to trust when you use a particular cryptocurrency, as opposed to regular fiat systems. This claim raises a fundamental question: If no authoritative entity gets to decide what is right and wrong, what mechanism brings trust to the whole system? Our goal in this chapter will be to answer this question. Along the way, we will cover some other interesting topics such as how new ZEC enters circulation and what decentralization even means. We will also build intuition around some technical topics, such as how the Zcash blockchain works, and why miners need to prove their work.

8.0

A PRELUDE ON HASH FUNCTIONS

Before we can start discussing the decentralized consensus in Zcash, we need to briefly introduce hash functions. Intuitively, a **hash function** is a function that can take any number of bits and produce a bit string of a fixed size. If you use two equal inputs, you’ll naturally get two equal outputs, but the most important property of these functions is that changing any bit on the input makes the function produce a completely different output. We call the output of a hash function a **hash**.

Hash functions are an elementary building block in cryptography, and we call them a cryptographic primitive. Cryptocurrencies generally rely on many different cryptographic primitives and concepts from cryptography, which is why people started calling them cryptocurrencies.



8.0.1 INTEGRITY CHECKS

If you download an app to your phone from the internet, your phone will run it through a hash function and compare the result to a hash provided by the server. If the hashes match, your phone can be sure every bit in the downloaded app is correct, and your phone knows nobody injected anything malicious into the app during the transmission. We call this an **integrity check** and use it everywhere, even in cryptocurrencies. On the other hand, if there’s even a single bit off, you’ll get a completely different hash. The hash functions we use in practice are so good that you’ll get about half the output bits randomly flipped if you flip a single bit on the input.

8.0.2 HASH FUNCTIONS ARE IRREVERSIBILITY

Another important property is that if you have only the output, there’s no way for you to reconstruct the input. We say that hash functions are **irreversible**, meaning that the output doesn’t tell you anything about the input. And yet, reversing a hash function is exactly what miners do when they mine Zcash. Reversing an irreversible hash function might seem weird, and we’ll discuss it further in the section on proof of work where we hopefully build confidence in what miners really do. For now, let’s take at least a high level overview.

You might have heard that miners solve hard mathematical puzzles. Saying it this way makes the whole mining business unnecessarily more mysterious than it is because all miners do is that they repeatedly create and try ridiculous amounts of inputs as fast as they can until they hit a hash the network needs. This is essentially the most naive way of obtaining the correct input, and this approach is called **brute force**. If brute-forcing a problem is the only way to get the solution, we call the problem **computationally hard**. Since hash functions are irreversible, reversing them is computationally hard.

Note that the emphasis is on the “computational” hardness, not “mathematical” hardness.

Also, note that we’re using the term “reverse,” meaning a change in direction, instead of “revert,” meaning a return to a previous state. You can think of hash functions as “one-way” functions in the sense that if your friend gives you an input, you will be able to compute its hash easily, but if they give you a hash and ask for an input that produces the hash, you won’t be able to give them an answer.

8.0.3 COLLISION RESISTANCE

Since hash functions take arbitrary inputs and produce fixed-size outputs, they map an infinite set to a finite one. This means we must have lied when we said that each input leads to a unique output a couple of paragraphs above. In reality, there is an infinite amount of inputs that lead to the same output for each hash function! Although this fact is theoretically true, we may neglect it in practice and pretend that no two inputs lead to the same output, or at least that it’s impossible to find such two inputs. We call such hash functions **collision-resistant**.

The reason why we can afford collision resistance is the size of the set of possible hash values. We typically use no less than 256 bits for the output.

There are 2256 ways to arrange the 256 zeroes and ones in such an output, so we get 2256 distinct hash values. If you’ve never thought of how unbelievably big this number is, you might be surprised. For intuition, there are only around one thousand times more atoms in the visible universe. Using such a laughably big amount of possible outputs makes finding two colliding inputs out of practical reach, even though we know it’s a bit of a lie. Notice that the same lie applies to your private keys.



8.0.4 OTHER PROPERTIES

The last two properties that we will care about are that you can’t predict what the output will look like unless you run the function, and running the function is fast. These properties mean that if you want to get a hash of your data, the only way to get it is to run it through the function, and you’ll get the result in under a millisecond.

8.1 THE ZCASH NETWORK AND BLOCKCHAIN

We have hash functions under our belt now, and our intention for the rest of the chapter is to build intuition around how reversing a collision-resistant hash function, also called **mining**, leads to **Byzantine fault tolerance**, which brings **decentralized consensus** to Zcash. Along the way, we’ll also cover Zcash issuance, but we’ll gulp that down only as a side dish compared to the mystical decentralized Byzantine thing. However, before we do that, let us briefly discuss the Zcash network and blockchain so we can digest the fancy Byzantine lingo more easily later on.

8.1.1 NOBODY CAN TELL YOU WHAT YOU OUGHT TO DO

We can see Zcash as a peer-to-peer (P2P) network of cooperating participants. P2P is a term from computer networking that denotes a network where all participants have equal privileges and voluntarily share information with each other without any central authority or coordination. Every participant is a client and a server for all other participants at the same time, and no participant is able to boss others around. We’ll refer to the participants as **nodes** in the network.

Zcash has currently two node implementations: **zcashd** and **zebrad**. The former originates from the Bitcoin codebase and was used to launch Zcash. Its software is outdated by modern standards and that’s the reason why Zcash engineers decided to implement the latter node from scratch using modern technology. The current plan is to eventually fully transition from zcashd to zebrad and stop using zcashd.

You might be wondering what the peculiar “d” means at the end of the node names. It stands for a “daemon”. Computer daemons are programs that are meant to run as a background process in the operating system without user interaction. It became a common practice in the industry to add the “d” at the end of the name of such programs.

Running your own node means you get full access to the network, and you don’t need to rely on or trust anyone else in the network. The only authority for you is your node. It will download all past transactions and verify them, and you can freely exchange value with your peers over the Internet. And since individual transactions are encrypted to the secret key of the recipient, nobody can watch over your shoulder when you transact. A ZK proof, the validity of which can anyone verify, will prove that the opaque ciphertext contains a valid transaction. Moreover, also thanks to ZK proofs, the encrypted transactions don’t even contain information about where the funds come from, so recipients can’t track you. You can indeed add tags to your transactions via the memo field, so recipients can identify incoming payments. If you don’t, then the recipient will only see the amount of ZEC show up in their account, and nothing else.



8.1.2 THE ZCASH BLOCKCHAIN

If we squint at the Zcash Protocol, to the point where we essentially close our eyes, we will see the following steps emerge:

1. Wallets broadcast new transactions.
2. Some nodes gather incoming transactions into a block and start finding a so-called proof of work (PoW) for this block. Let’s call these nodes **miners**. Note that blocks are just bundles of transactions.
3. Once a miner finds a **PoW** for the block, they broadcast it to the network.
4. All other nodes verify the block and accept it only if all transactions in it are valid and not already spent.
5. Miners express their acceptance of the received block by starting to create another block on top of the received one. They do so by inserting the hash of the received block into the one currently being created.
6. The cycle repeats.

Notice that each block contains a hash of the block directly preceding it. This implies you can backtrack the blocks up to the initial one, called the **genesis block**. By following the steps in the list above, miners in the network build a chain of blocks containing users’ transactions, starting with the genesis block. Let’s call this chain the Zcash **blockchain**.

8.2

PROOF OF WORK

Imagine you receive way too many unsolicited e-mails, and you want them to stop. You'll publicly announce: "I'll read an incoming e-mail only if its hash will start with at least ten zero bits." When you receive an e-mail, you hash it, and you look at the bits in the hash. If the first ten are not all zero, you'll straight up delete the e-mail. You can do such a check very quickly since hash functions are fast. Also, you don't need to do any of this personally—you can implement it in your e-mail client, or perhaps you could even bake it into the e-mail protocol itself.

It's important to note that the sender is not able to check if the hash of their e-mail starts with ten zeroes when they are composing it. This is because whenever they change anything in the e-mail, they'll get a different hash, so they need to hash the final version of the e-mail only. But what if the hash doesn't meet the criterion? We'll solve that by adding an extra field to the metadata of the e-mail. Let's call it a *nonce*.

Since the sender can't predict what the hash will look like with any particular nonce, their only option is to keep trying different nonces until they get a hash that has at least ten leading zeroes. This essentially means they're trying to reverse the hash function—the sender knows what the output should look like, and they're trying to come up with an appropriate input. Since the hash function is irreversible, brute force is the sender's only option. Once they get an e-mail the hash of which starts with at least ten zeroes, they can send it because they know that only then you won't consider it spam. We'll refer to the hash of the e-mail as the *proof of work (PoW)* for the e-mail. Notice that there's no need to explicitly attach the PoW to the e-mail since you, as the verifier, will always quickly check the validity of the PoW by hashing the e-mail yourself anyway. In other words, the PoW is an implicit proof that the verifier checks by deriving it from the data, and there's no explicit proof to "trust". Also, observe the asymmetry between producing the proof and verifying it—generating the proof is a computationally hard problem, but checking it takes only one application of the hash function.

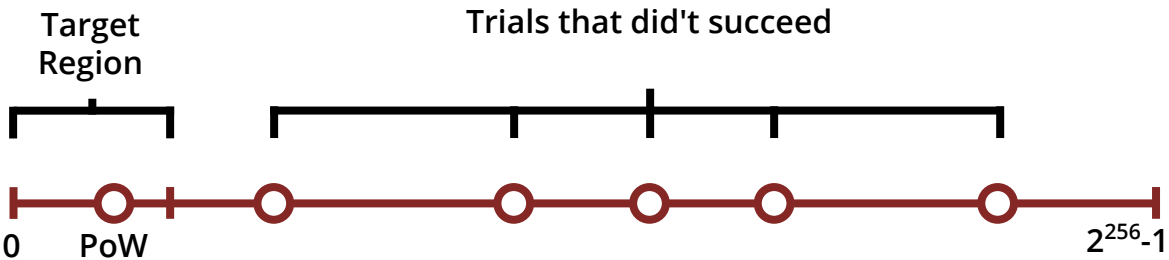
How many nonces, on average, does the sender need to go through until they get the PoW? Since we can't predict anything about the output, all hash values are equally likely, and we can describe the output as a random variable with uniform distribution. Having ten zero bits in a row should then take $2^{10} = 1024$ trials on average, so anyone who wants you to read their e-mail must go through the work of trying around a thousand hashes. Indeed, some senders might be lucky and get the PoW with the first nonce, but that will not work on average.

8.2.1 PROOF OF WORK IN ZCASH

Similarly to the e-mail PoW system we outlined above, Zcash nodes also expect a PoW for each block. When a node receives a new block, it checks that all the transactions and the block's metadata are valid. Among these checks, there is the PoW check: the node hashes the block and checks that the hash starts with enough zero bits. However, this time, the number of required leading zero bits is dynamic. Let's call this number the *threshold*. A higher threshold means that it is harder to mine the block because its hash needs to start with more zeroes, and vice versa for a lower threshold.

This is because the more leading zeroes in a hash we need, the more hashes, on average, we need to try before we hit the right one.

The image below illustrates the process of finding a valid PoW. Let's say that we're using a hash function that outputs 256-bit hashes, and let's put all the outputs on an imaginary line segment. We order them according to the integer values their bits represent: we start with the hash with all bits set to zero—the zero hash—on the left, and we end with the hash with all bits set to one on the right, ordering all the other hash values in between. The threshold determines a specific hash on the imaginary line segment which we'll call the *target*. The region between the zero hash and the target is where a valid PoW needs to land because all hashes in this region have enough leading zero bits and all hashes above the target don't. Since miners can't predict what hash value their block will generate, their only option is to keep blindly shooting at the line segment until they generate a block with a hash that lands under the target. In reality, the target is extremely close to the zero hash, so it takes a lot of work to generate a block with such a hash. The dots on the line segment depict individual hashes.



Each node keeps track of time and sets the expected threshold for the next block so that it should take 75 seconds to mine it. If a node receives a block with a PoW that doesn't meet the expected threshold, it discards the block as invalid. Miners know this, so they don't even try to fool the nodes, and keep hashing until they get a block with a valid PoW, and only then broadcast it to the nodes.

Note that even though each node sets the expected threshold on its own, they all follow the same formula baked into their source code. This implies that all nodes in the network have the same expectations for the next block in a synchronized way, and indeed, miners use the same formula as well. Ultimately, miners are also nodes in the network with the difference that they are trying to extend the blockchain with a new block. If a node receives a new block with a valid PoW and sees that it took less than 75 seconds to mine it, the node increases the threshold so that miners need to work harder to produce the next one. On the other hand, if it takes more than 75 seconds to mine a block, each node lowers the threshold so that miners have an easier job. This balancing keeps the average time between blocks at 75 seconds when the global hashing power of the network fluctuates.

8.2.2 WHY DO MINERS EVEN BOTHER?

When a miner starts mining a new block, they create a so-called *coinbase transaction*, and place it as the first transaction in the block. This transaction contains a *block reward*, which is currently two-fold: it is a sum of the *block subsidy* and *transaction fees*. Since the miner is the author of the coinbase transaction, they can send the block reward to any address they wish, but they typically send it to themselves. Collecting the reward is the motivation for miners to keep producing new blocks.

The block subsidy is a mechanism through which new ZEC enters circulation—it contains fresh ZEC which didn't exist before. We'll cover the details in a forthcoming section on ZEC issuance. The transaction fees motivate miners to include users' transactions in the block. Miners collect them by summing up the fees of all transactions in the block and adding the result to the reward. The fees also help prevent potential spam transactions. If transactions had no cost, a malicious entity could keep publishing an enormous amount of them by sending the ZEC back to themselves. All blocks have a limited size, and since miners would have no means to distinguish such transactions from legitimate ones, the spam would occupy a significant portion of the block space, leading to a denial-of-service attack.



Let's call the global hashing power of all miners in the network the *hash rate* of the network. Notice that since nodes always adjust the threshold so that it takes 75 seconds to get the next block, the higher the network's hash rate, the less likely it is for an individual miner to generate a block, and vice versa for a lower hash rate. This means that miners compete with each other for the reward, and the more hashing power an individual miner has, the more likely they are to win the competition. By hashing power, we mean how many hashes they can come up with in, say, one second. Miners nowadays use so-called ASICs (Application-Specific Integrated Circuits) which is hardware that has the hash function baked directly into the sand of the chips of the hardware.

EXERCISE

Imagine you are a Zcash miner trying to generate a block with a valid PoW, and the expected threshold is 42, so the hash of the block needs to start with at least 42 zero bits. If you take only a single shot, meaning you try only one nonce, what is the probability that you succeed? Incidentally, the Zcash network requires a similar number of leading zero bits for a valid PoW at the time of writing this book.

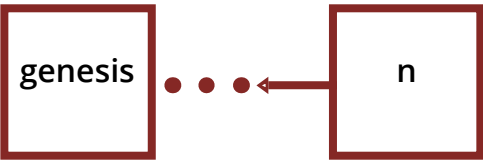
SOLUTION

Since we can describe the output from a hash function as a random variable with a uniform probability distribution, the probability of getting a hash with 42 leading zero bits is one in 2^{42} , which is approximately one in four trillion. This implies that on average, Zcash miners currently need to try around four trillion nonces for each block before they manage to append it to the blockchain.

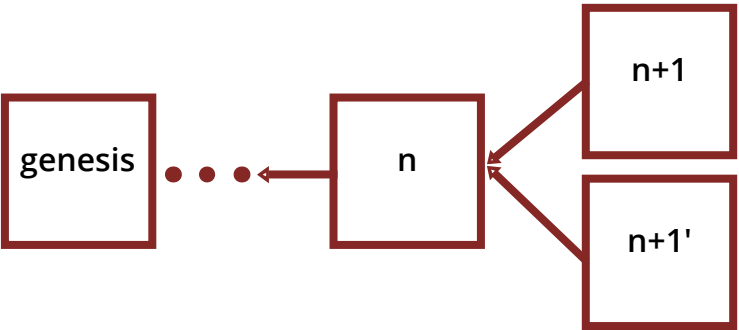
8.3

DESCENTRALIZED CONSENSUS

We've built our intuition for PoW, and we're ready to understand why the Zcash network doesn't need any central entity in charge. Consider the blockchain depicted below. It starts with the genesis block and ends with block n . Let's say that block n is the most recent block, or in other words, the current *tip* of the Zcash blockchain.



Let's now consider a scenario where a miner publishes a block, let's call it $n + 1$, and almost at the same time, another miner publishes another block, $n + 1'$. Since both miners had the same tip n , both new blocks now reference n as their parent block, leading to a *chain split*. This situation is depicted below.

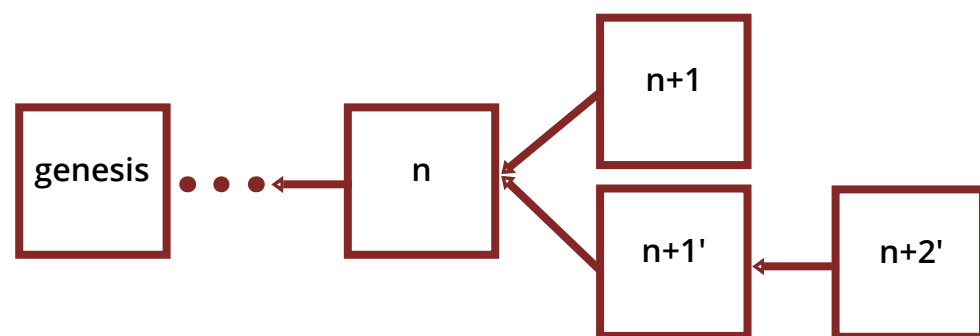


It is crucial to note that blocks $n + 1$ and $n + 1'$ can contain conflicting transactions: block $n + 1'$ can contain a transaction that spends the same funds as a transaction contained in block $n + 1$. We'll refer to an attempt to spend the same funds twice as *double-spending*. To rule out the possibility of double-spending, all nodes in the network now need to reach a decentralized consensus and collectively agree on which block to keep, and which one to abandon. We'll call abandoned blocks *orphans*. Note that individual nodes don't obey anyone but themselves, and yet they have to reach a collective agreement. This problem was known a long time ago and was first solved in practice by Satoshi Nakamoto when they implemented Bitcoin.

EXERCISE

You might have heard that PoW is the secret sauce that cryptocurrencies use to solve the double-spending problem in a decentralized way. We have covered PoW quite thoroughly in the previous section, so can you guess how the nodes do it? The truth is that PoW is only a part of the special recipe, and we need one more ingredient, although a simple one. Try to pause and ponder what the solution could be before hopping on to the paragraph below. For example, try adding new blocks to each of the possible chain paths, and maybe you'll come up with the same solution as Satoshi Nakamoto! Remember, the end goal is to eventually end up with a single chain that all nodes agree on. Resolving this problem was the key component that brought the advent of decentralized cryptocurrencies.

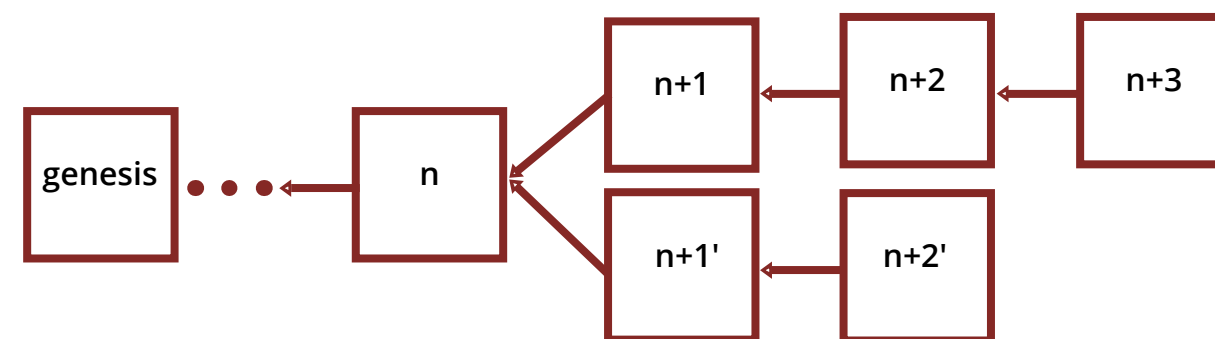
The solution the nodes use when resolving a situation like this is to, well, wait. And see what happens. More precisely, each node always prefers the longest chain and ignores the rest. This is a bit more nuanced in reality because Zcash nodes resolve chain splits by always considering the chain with the “most PoW put in” to be the main one, but we can abstract that away and replace it with “the longest chain”. Let’s see what happens when a miner appends a new block to $n + 1'$, as depicted below.



Nodes in the network can see that the new block $n + 2'$ extends the chain that used to end with block $n + 1'$, so block $n + 1$ becomes an orphan, and its transactions are discarded. All nodes follow this logic because each node knows what others will prefer, and that is the longest chain. Another way to see it is that the motivation for nodes to follow this rule carefully is a fear of being ignored by others. A node is free to adhere to any rules it wants, but if it starts following a chain other than what others consider the main chain, then the node will be ignored by others, which means a loss of funds. One could draw a loose parallel between the motivation for the nodes to behave this way in the network, and the motivation for humans to behave a certain way in society since certain behaviors lead to being ignored, which also induces a fear of loss.

Imagine you are selling your computer for 1 ZEC, your friend is sending you the money from their phone, and the current tip of the blockchain is again at block n . The wallet in the phone generates a transaction and sends it to the wallet’s preferred node. This node stores the transaction in its **mempool**, which is a place in the node’s volatile memory where it stores **unconfirmed** transactions, or in other words, transactions that are waiting for inclusion in the blockchain. Nodes share the contents of their mempools with each other, so the node will broadcast the transaction to its peers, and these peers will broadcast the transaction to their peers until every node has the transaction. This is how new transactions are propagated in the Zcash network.

Let’s now say that a miner has included the transaction in block $n + 1'$, and your node has just received the block, but you’ve also received block $n + 1$, published by another miner, who didn’t include the transaction in their block. You know that there is a chain split, and you have to wait because if block $n + 1'$ becomes an orphan, all Zcash nodes will act as if the transaction never happened. After about a minute, you see block $n + 2'$ on top of $n + 1'$, so you hand the computer over to your friend because $n + 1'$ became a part of the longest chain and $n + 1$ became an orphan. You now know you will be able to spend the funds contained in the transaction you’ve received in $n + 1'$. However, consider now the scenario depicted below where block $n + 1$ gets suddenly extended by two blocks $n + 2$ and $n + 3$.



This scenario could happen because the miner who has previously produced block $n + 1$ could ignore or not receive block $n + 2'$, and then get very lucky by mining two blocks in a row, namely $n + 2$ and $n + 3$. Zcash nodes can now see that the longest chain is the one ending with $n + 3$, and perform a so-called **rollback**, which is a switch from the chain ending with $n + 2'$ to $n + 3$. This rollback makes blocks $n + 1'$ and $n + 2'$ orphaned, and the transaction of your interest gets ignored. This means that your friend can now spend the 1 ZEC they just sent you on something else, essentially leading to double-spending since you’ve already given them your computer. Note that no money was made out of thin air and the overall amount of ZEC wasn’t inflated—only you’ve lost your money, and your friend got it back right after the purchase. How do we solve this? Isn’t it a fatal flaw?

The important observation is that rollbacks won’t happen indefinitely in practice. It is possible to show that the probability of a rollback drops exponentially with each new block appended to the blockchain. The intuitive reasoning is that each new block makes any particular chain exponentially more difficult to “re-hash”, and come up with an even longer, alternative chain. This observation leads to the conclusion that the deeper a block is in the chain, the more immutable its data is, and the more we can trust the data. So the solution to the problem described in the previous paragraph is to wait until a transaction we are interested in gets buried under a few blocks, and only then hand over the goods. Zcash nodes will perform rollbacks for up to 100 blocks from their current tip, and if there’s an attempt to roll the longest chain back even further, the nodes will refuse it.

8.3.1 SYBIL RESISTANCE

At this point, we have covered how the Zcash network forms decentralized consensus. Note that PoW is not the mechanism that directly determines what data constitutes the agreed-upon transaction history—it is the chain selection mechanism. We could even say that the authority that ultimately determines the transaction history is the entity that has the ability to come up with the longest chain, and that is the majority of the mining nodes. This claim might make PoW seem not that important. However, PoW still plays a crucial role because the network uses it to rate-limit block creation in a **Sibyl-resistant** way.



Sibyl attacks are attacks where a single attacker spawns many fake identities and uses them to influence the attacked system the way they desire. For example, we could naively base mining, and in particular, chain split resolution, on voting where miners would vote on the right block using their IP address. Certain miners would then be able to easily gain an unfair advantage over others by having easy access to many IP addresses at no cost while others wouldn’t have this benefit.

On the contrary, PoW brings in Sibyl resistance because it constrains miners with real-world assets that are not effortlessly obtainable. These assets are the energy and hardware that a miner has to use to come up with the right hash. If a miner wants to scale their operations, they must invest their resources in these assets, just to be able to hash faster. Notice that the key to the Sibyl resistance of mining is the irreversibility, or “one-wayness”, of the hash function.

Earlier in this chapter, we mentioned Byzantine fault tolerance (BFT) and said that Zcash is a BFT system.

We promised we would conquer this fancy lingo, and we are ready to do so now. A **Byzantine fault** is a condition in a decentralized system that can present different symptoms to different peers in the system. For example, some nodes might act maliciously and send deceiving messages to their peers, or send different messages to different peers, or some nodes might not receive certain information due to network conditions, or even disappear from the network and show up later with an outdated state. Many such Byzantine faults make different nodes have a different view of the whole network's state, so some nodes might perform rollbacks while others don't. However, as long as the “honest” nodes stay in the majority, they will recover from all these faults and reach a consensus. It is worth noting that the consensus does not hold with absolute certainty but with “high probability”, which is sufficient for real-world use. The reason is the probabilistic nature of any particular node having “the best chain” since there's always a probability of some other node showing up with an even “better chain”, but in real life, this probability becomes exponentially negligible with the number of blocks that would differ between these two chains.

8.3.2 MODIFYING THE CONSENSUS RULES

We mentioned that when a node receives a block, it performs a lot of checks to make sure the block is valid, and if there's anything wrong, the node discards the block as invalid. Let's call these checks the **consensus rules**. Zcash is an evolving cryptocurrency, so let's now think about how we can modify the set of the consensus rules and what implications those modifications might have.

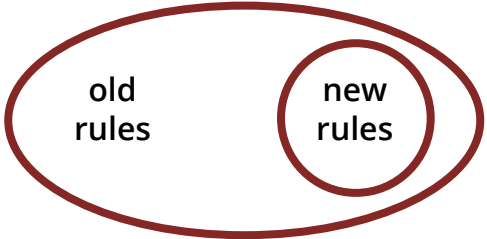
Whenever we modify the set of consensus rules, we introduce either a so-called soft or a hard **fork**.

Such changes are always introduced in a new version of a Zcash node. Note that nobody can force anyone to run any particular version of a node, so all changes in the network require consent from node operators. If there's a change in the consensus rules, and some nodes decide to adopt it, while others don't, there will be a permanent chain split at the height where the change came into effect, and both groups will end up with their own branch of the original blockchain. Most likely, each group will give their chain a different name, and there will be two different cryptocurrencies, sharing a common part of the blockchain created before the split.

Let's now discuss soft forks and hard forks in more detail.

8.3.2.1 SOFT FORKS

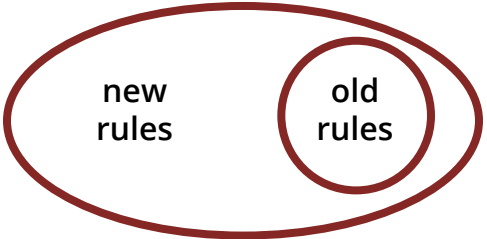
A soft fork restricts the consensus rules, so the updated set of the consensus rules becomes a strict subset of the original set. This means that soft forks are backward compatible since the original nodes will keep accepting all blocks accepted by the updated nodes. The diagram below depicts the relationship between the old and new sets of consensus rules.



In the case of a soft fork, if the majority of the mining nodes adopt it, the whole network will keep reaching consensus, and blocks created by the original nodes that fall out of the scope of the updated rules will keep becoming orphaned. The reason is that the updated mining nodes won't accept such blocks, and will keep replacing them with blocks that comply with the updated rules. The soft fork is effective in this scenario, even without non-mining nodes switching to it. However, if the updated mining nodes stay in the minority, the original and updated nodes in the network will each end up with their own chain. This is because the old mining nodes will keep building their original chain, but since it will contain blocks that the updated nodes won't accept, the updated mining nodes will start creating their own chain.

8.3.2.2 HARD FORKS

A hard fork relaxes the consensus rules, so the updated set of the consensus rules becomes a strict superset of the original set. The diagram below depicts the relationship between the new and old sets of consensus rules:



In the case of a hard fork, if the original mining nodes stay in the majority, the blocks created by the updated nodes that fall out of the scope of the original rules will keep becoming orphaned. The hard fork is not effective in this scenario. On the other hand, if the updated nodes become the mining majority, there will be a chain split unless all nodes, including the non-mining ones, switch to the new, broader set of consensus rules. The reason why the non-mining nodes also need to do the switch is so that they can accept blocks complying with the new set of consensus rules.

8.3.2.3 NETWORK UPGRADES

The main difference between hard and soft forks is that in order to avoid a chain split, a hard fork requires every node in the network to adopt it, while a soft fork requires adoption only from the majority of the mining nodes.



We call hard forks and soft forks **network upgrades** in Zcash. So far, there have been six network upgrades and each was adopted by the whole network:

OVERWINTER - Was the first network upgrade for Zcash. It included versioning, replay protection for network upgrades, performance improvements for transparent transactions, a new feature of transaction expiry, and more.

SAPLING - Was the second network upgrade. It introduced significant efficiency improvements for shielded transactions. Since Sapling, users can create shielded transactions on their phones in only a few seconds, using only 40 MB of memory. Sapling also introduced the so-called full viewing keys, which give owners of shielded addresses the ability to view incoming and outgoing transaction details without exposing their private spending keys. The upgrade also allowed the hardware that constructs the zero-knowledge proof to be independent of the hardware that signs the transaction.



BLOSSOM - Was the third network upgrade. It reduced the expected time between blocks from 150 to 75 seconds. Increasing the block frequency allowed faster transaction resolution and increased the overall transaction throughput of the network. The emission rate and halving schedule remained unchanged, so the halved block times also required that the per-block reward be halved.



HEARTWOOD - Was the fourth Zcash network upgrade. It modified the consensus rules to enable coinbase funds to be mined to shielded Sapling addresses. The upgrade also enabled efficient proofs of work for light clients.



CANOPY - Was the fifth network upgrade for Zcash, coinciding with the first Zcash halving. It established a new development fund for the next four years, which we will discuss in the following section.



NU5 - Was the sixth network upgrade. It enabled full support for the Orchard shielded protocol and Unified Addresses. NU5 moved Zcash to the Halo proving system, removing the need for the trusted setup and upgrading the protocol's underlying cryptography. Naming conventions for this and future Zcash network upgrades have shifted from a theme-based alias, like Canopy and Sapling, to a simple number system. This was meant to provide clarity and consistency moving forward.

8.3.3 DECENTRALIZATION IS A SPECTRUM

We mentioned that for an individual Zcasher, their node is their authority because they don't need to rely on anyone else or any other node. We also mentioned that from the perspective of the whole Zcash network, the authority that determines the contents of the agreed-upon transaction history is the entity that has the ability to come up with the longest chain, and that is the majority of the mining nodes. We can see that we can consider various types of authorities, depending on where we position ourselves when we think about Zcash.

After discussing authorities, we discussed how Zcash forms consensus in a decentralized way. However, we haven't covered one important question yet: Are we sure the network won't have a tendency to head toward centralization over time? For example, could the majority of the mining nodes converge to a single mining node? Having multiple types of authorities and questions like these leads us to the conclusion that it's better to look at decentralization not as a binary property, but rather as a multi-dimensional spectrum. Let's look at this spectrum closer by answering the questions we asked in this paragraph. But before we can do that, we need to introduce mining pools.

8.3.3.1 MINING POOLS

Zcash miners unite forces and form so-called **mining pools**. A mining pool is a single Zcash node that prepares new blocks that are ready for inclusion in the blockchain but miss a PoW. The pool then sends these blocks to individual miners, who don't run their node and don't create blocks, but only run their hashing hardware to find a nonce that leads to a PoW for the block they get. Once such a miner finds such a nonce, it sends the complete block back to the mining pool which then broadcasts it to its peers. The pool then distributes the block reward to the individual miners who participated in the hashing process, and even miners who didn't manage to find the PoW get paid based on how much hash rate they provided. Notice that the pool can easily measure the hash rate of an individual miner by checking how close they were able to get to the target region, even if the miner didn't manage to go below the target and get the PoW. In fact, the pool continuously measures the hash rate of each miner by periodically asking them to submit the block they're working on. The closer the miner can get to the target region, the higher the hash rate they have.



The motivation for miners to join a pool is pragmatic since it lets them get paid for their work on a frequent and regular basis. Intuitively, the probability that a miner manages to mine the next block is equal to the proportion of the miner's hash rate to the hash rate of the whole Zcash network. Non-industrial miners can afford only a negligible fraction of the network's hash rate, so if they decided to mine on their own, they would need to wait for weeks or even years before they mine a block. On the other hand, if they join a mining pool that manages to mine at least one block per day, they can get paid daily by the pool.

8.3.3.2 51% ATTACKS

Let's now bring our attention back to the questions we asked at the beginning of this section, and given our knowledge of mining pools, let's ask a slightly more accurate question: What could happen if the whole network's hash rate was dominated by a single mining pool? The answer is that such a pool would be able to perform rollbacks of arbitrary depth, also known as 51% attacks. We call those rollbacks as such because having at least half of the network's hash rate is a sufficient condition for being able to perform them. Note that the pool would not be able to create new ZEC out of thin air with a 51% attack. It would only be able to perform double-spending by altering the best chain at its will. To restrict the impact of an attempted 51% attack in practice, Zcash nodes limit the number of blocks they are willing to roll back to 100 when switching to a different chain.

An important topic that merits discussion is the asymmetry between the motivation to perform a 51% attack and the motivation not to do it. The motivation to perform the attack is straightforward—the pool can manipulate the recent transaction history to its advantage and benefit from double-spending. However, the attack will likely bring the price of Zcash down, effectively reducing the value of the pool's loot. Another consequence is that miners who mine with the pool are likely to leave and start mining with a competing pool because they also don't want to see the value of Zcash decrease. A loss of mining hash rate for the pool then means less future earnings since pools profit from keeping part of the block reward from the blocks they mine. As a result of this asymmetry between the motivation to perform and not to perform the attack, pools are better off making a profit from playing an honest game instead of trying to be malicious. In other words, a successful 51% attack means sawing off the branch the pool is sitting on. Individual miners also don't want to undermine their business, which is an incentive for them not to concentrate all in a single pool and keep the hash rate spread among multiple pools instead.

Another scale where mining centralization can occur is the production of mining hardware. Since the hardware is highly specialized, there are currently only a few companies that produce it, and they keep the design for themselves. However, similarly to mining pools, the profit model also motivates hardware producers to keep building a positive reputation instead of behaving maliciously.

EXERCISE

Imagine you are a miner in a pool, and you manage to find a nonce that leads to a valid PoW. You know that when you send the completed block back to the pool, the reward will go to the pool because the coinbase transaction in the block references the pool's address. Instead of sending the block back to the pool, can you change the reward address to an address you control, and publish the block on your own? This way, you could keep the reward for yourself.

SOLUTION

If the answer was a “yes”, then the pool would make no money because each miner could easily send the reward to themselves once they find a valid nonce. This is impossible because whenever you flip even a single bit in the block data, you'll get a completely different hash of the block, and you have to start searching for the PoW again from scratch.

8.4

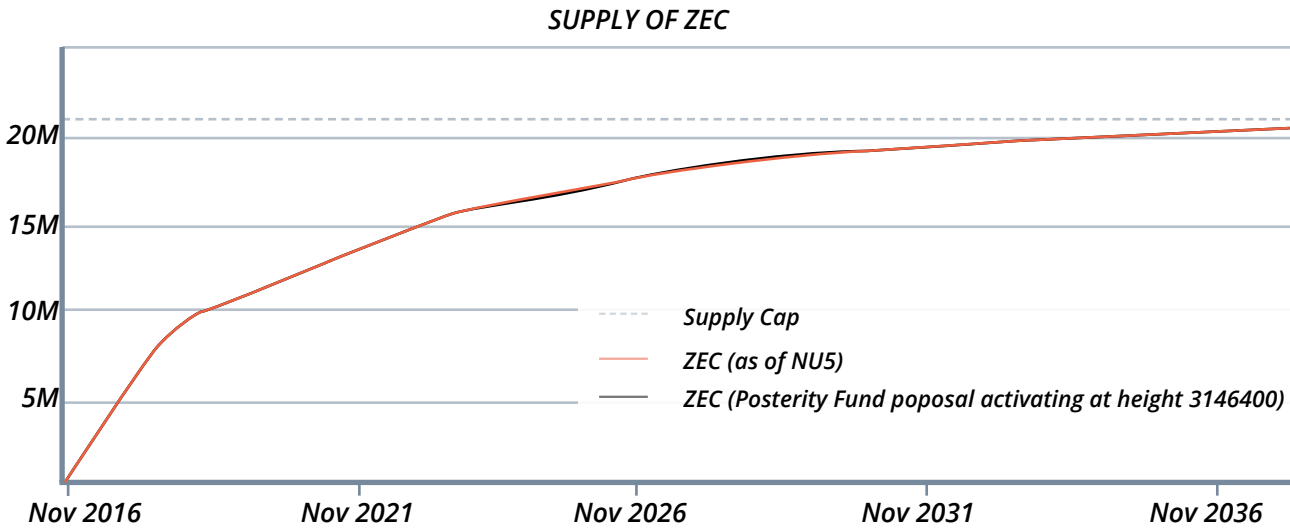
ZEC ISSUANCE

As we have already mentioned, the way new ZEC enters circulation is the **block reward**: the first transaction of each block, called the coinbase transaction, is created by the block's miner and contains fresh ZEC which the miner sends to themselves. The Zcash protocol is currently designed so that the block reward halves every four years, and there will be 30 **halvings** in total. The last halving will make the block reward drop to zero. These properties have the following consequences:

- 1. Transaction fees will be the only motivation for miners to keep mining after the 30th halving since there will be no block reward.
- 2. The total supply of ZEC is limited. We can mathematically model the reward as a finite geometric sequence. If we sum up the sequence, we get a number very close to 21 million ZEC. The total supply will reach this limit when the 30th halving occurs.
- 3. Half of the total supply was emitted before the first halving. More specifically, miners created 10.5 million ZEC in the first four years following Zcash's launch in November 2016.

4. The circulating supply of ZEC will reach 99% of the total supply in the mining **epoch** between the seventh and eighth halving, which is the epoch between the years 2040 and 2044.

The figure below depicts the supply of ZEC in the first 20 years of Zcash's existence, and also illustrates the last three points from the list above.



8.4.1 THE FOUNDERS' REWARD AND DEV FUND

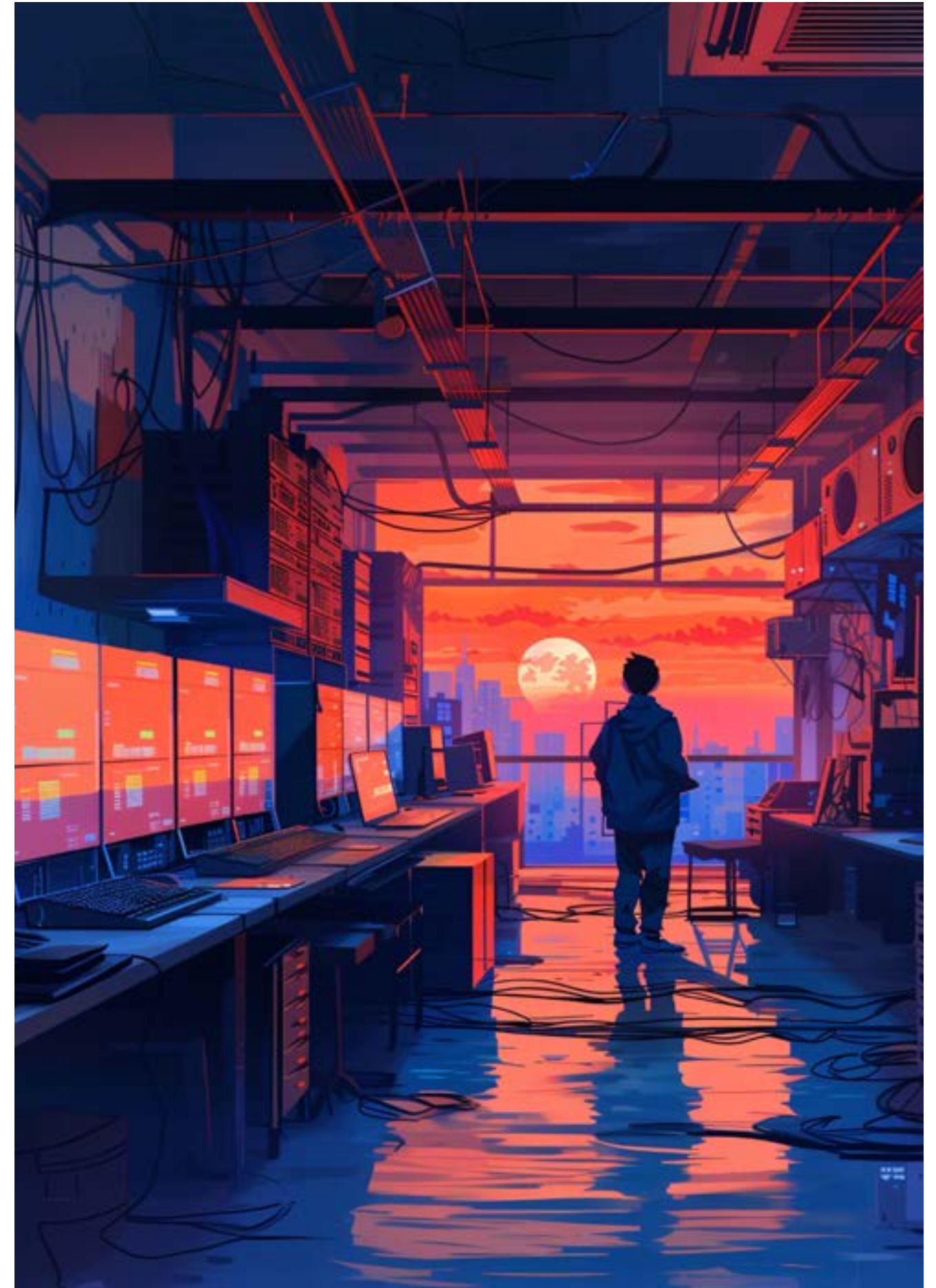
Not all of the reward goes to the miners. When they create the coinbase transaction, they need to send a part of the newly issued ZEC to a set of addresses determined by the Zcash protocol specification. The specification contains consensus rules that define what addresses the miners need to use and how much they need to send. If they don't do so, other nodes will discard the block as invalid since it won't pass the consensus rules validation. Let's now look at this part of the reward in more detail. In the initial four years of Zcash's existence, 20% of the newly created ZEC was allocated to its founders, initial investors, employees, and advisors. This part of the reward was referred to as the Founder's Reward. When the first halving came, the Founders' Reward ended and was replaced by a so-called Dev Fund, defined in ZIP 1014. The Dev Fund also lasts for four years, consists of 20% of the block subsidies, and is split into the following three slices:

- 35% for the Electric Coin Company;
- 25% for the Zcash Foundation; and
- 40% for the Zcash Community Grants. At the time of writing this book, the second halving is around the corner, and the Zcash community is currently deciding how to fund the development of Zcash further.

8.5

A CLOSING NOTE

Even though it is a remarkable achievement that humans have figured out a way to build a system that forms consensus without relying on a trusted party, it is important to keep in mind that it is not necessary to understand all of its internals to be able to use it. It is also important to keep in mind that the purpose of the system is to serve people and help them achieve great things in their lives. We don't need to go far to find examples that illustrate this. Think of something simple you use every day; for example, even a microwave oven. It is not necessary to know all the fascinating physics and engineering that humans had to come up with to know that it's something that lets you throw your food in, quickly heat it over the air, and carry on with your day, doing things that matter to you. And similarly for Zcash, it is not necessary to know all the beautiful mathematics and engineering that humans had to come up with to know that it's something that lets you freely exchange value with your peers, and carry on with your day, knowing that you're in control of your finances.





9

APPENDIX

Bringing Zcash to High Schools

@Frostbyte11211

OVERVIEW

Privacy is an essential asset that Zcash aims to secure. It ensures safety, control, and the right to grant access. Creating a Zcash club in your high school can help members understand in more detail that Zcash is the most trusted digital currency. Some valuable benefits of privacy that are relevant to high school students include independence, protection against identity theft, and online safety. Privacy provides freedom, which is everything.

Where to Begin

1. Get it approved by your high school!
 - To become school-approved, most high schools require talking with a faculty member or filling out a form. This step is crucial! The club can't happen without the school's approval.
 - Talk to an administrator at your school to learn how to register the club appropriately.
2. Find a fun teacher to help
 - Selecting an advisor who is supportive of online privacy and cryptocurrencies, as well as a fun person could be beneficial. If they are knowledgeable about digital currencies they may be able to provide guidance and resources to help expand the club's opportunities, and if they're a fun teacher it can bring in an audience for meetings.
3. Find a time and place to hold a first meeting
 - Consider finding a spacious and comfortable space to talk with the group.
4. Get the word out!
 - There are various ways to spread the word such as posting flyers around the school, talking with friends about the club, or advertising in the school announcements/newsletter.
 - You could reach a bigger part of your school community by promoting the club virtually as well. This can be through creating social media accounts, advertising in online newsletters, or finding different ways to connect with the school community online.
 - Strive to create an inviting and inclusive environment that welcomes members regardless of their knowledge surrounding cryptocurrency. More members the better!

Getting the Club Meetings Started

Plan to host monthly club meetings overviewing a chapter every meeting

At the first meeting, the members can introduce themselves and discuss their backgrounds around cryptocurrency. You can also have an icebreaker activity where you take turns asking questions to make the environment more relaxed and inclusive for everyone.

Choose someone to lead the class exercises and discussion. The class exercises are a good time to break and discuss further as a group any comments or questions that arise while reading.

Decide if you want to elect officers to help lead the exercises/discussions. People may want to join if they know there is an opportunity to be a leader within the club.

End of Year Celebration

As the last meeting of your class approaches, it marks a memorable occasion to celebrate all the hard work you have put in and the knowledge you have gained throughout the course. This meeting is especially significant as you will also be celebrating receiving your first Zcash! To make the most of this momentous day, the meeting should be a reflection of your accomplishments and a time to enjoy some well-deserved celebration. You can plan the event with games, food, music, or any other activities that you find enjoyable and fitting for the occasion. So, let your creativity flow and make this last class meeting a memorable one!

Conclusion

Maintaining privacy is crucial, and Zcash provides a secure way to protect your financial information digitally. By introducing Zcash to high schools, we can educate students on the significance of financial privacy while making it a fun experience. The club can serve as a platform to learn about digital currencies and provide an exciting opportunity to earn Zcash.



GLOSSARY

51% Attack: A type of attack on a blockchain network in which a single entity or group controls a majority of the network's computing power, allowing them to manipulate transactions and potentially disrupt the network.

Acceptability: The quality of being tolerated, allowed or accepted.: "money derives its purchasing power entirely from its acceptability as a medium of exchange"

Actions: In the Orchard protocol, instead of creating several individual proofs for each Spend and Output, they are merged into a single concept called "Actions."

A.I. Artificial Intelligence: The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

Address Reuse: The practice of using the same Bitcoin address for multiple transactions.

Aggregate Proof: A combined proof that confirms the authenticity of multiple individual proofs.

Altcoin Season: A period of time when alternative cryptocurrencies experience significant price increases, often due to increased investor interest and adoption.

Altcoins: Digital currencies excluding Bitcoin.

Anti-inflationary: Of or relating to measures to counteract or combat inflation.

AML (Anti-Money Laundering): A term used for combating money laundering and financial crimes, includes all financial policies, regulations, and laws.

Arborist Call: Bi-monthly meetings discussing protocol and research development updates. These calls provide an opportunity for community members and stakeholders to engage with the development process. You can register for the Arborist Call at the specified times. Notes from these calls are typically shared afterward.

Asset Pairing: Assets that can be traded for each other on an Exchange.

ATM (Automatic Teller Machine): A computerized electronic machine that performs basic banking functions.

Atomic Swap: A peer-to-peer exchange of one cryptocurrency for another without the need for a centralized exchange or intermediary.

Auction: A process by which goods or assets are sold to the highest bidder.

Auto-shielding: Enables users (more specifically their wallets) to automatically move funds from a transparent address to the latest shielded ZEC pool.

Balance: The amount of money held in an account or address.

Bartering: The exchange of goods and services without the use of money.

Basket of Goods: A collection of goods or services used to measure changes in the cost of living.

Benchmarking: The process of gathering and comparing performance metrics against some defined standard.

Bit: A unit of information expressed as either a 0 or 1 in binary notation.

Bitcoin: A digital currency system that allows people to transact digital value without the need for a centralized payment intermediary.

Block: A record in a blockchain that contains a set of transactions.

Blockchain: A system in which a record of transactions, especially those made in a cryptocurrency, is maintained across computers that are linked in a peer-to-peer network.

Block Explorer: A tool used to view and explore blockchain data, allowing users to view individual blocks, transparent transaction components, and publicly visible wallet addresses.

Block Reward: The amount awarded to the miner for mining a block. This amount is included in the block that was mined.

Block Size: The largest quantity of data that a single block can accommodate in a blockchain.

Block Subsidy: The amount of newly minted coins that are emitted in every new block.

Blockchain: A public record of all transactions that have taken place for the given network.

Blockchain Analysis: The process of inspecting, identifying, clustering, modeling and visually representing data on a blockchain.

Blockheight: A measure used to determine the number of blocks before a specific block on the blockchain.

Blossom: The 3rd major network upgrade for the Zcash protocol, included reducing block times, adjusting block rewards, and improving transaction efficiency.

Bootstrap: A 501c3 charity that directly owns and funds the Electric Coin Company via the Zcash Development Fund.

Browser-extension Wallet: A cryptocurrency wallet that saves a private key on an internet browser, considered user-friendly but also the least secure.

BTC: The ticker symbol and unit measure used for Bitcoin.

Brute Force: A cryptographic attack that attempts to break a code with repeated trial decryption attempts.

Budget: An estimate of income and expenditure for a set period of time.

Byte: A group of binary digits or bits, usually 8.

Byzantine Fault Tolerance (BFT): A system that is able to resist the class of failures derived from the Byzantine Generals' Problem. This means that a BFT system is able to continue operating even if some of the nodes fail or act maliciously.

Canopy: The 5th major network upgrade for the Zcash protocol, introduced various improvements and optimizations, enhancing security, scalability, and usability.

Capital Controls: Restrictions on the movement of money across borders.

Cash: Money in coins or notes, as distinct from checks, money orders, or credit.

Cashless: A term characterized by the exchange of funds by check, debit or credit card, or various electronic methods rather than the use of cash.: "the cashless society".

Censorship-resistant: The characteristic of being unable to be suppressed or prohibited.

Central Authority: An agency or organization that is designated a facilitating role in the implementation and operation of an international treaty in public and private international law.

Central Bank Digital Currencies (CBDCs): A fiat currency that exists in a digital form.

Central Bank: A financial Institution that oversees the commercial banking system of a state or an economic union of nations and manages the monetary policy.

Centralization: The concentration of power or control in a single entity.

Centralized System: A system in which power or control is concentrated in a single entity.

Chaintip: Referring to the latest block that is appended to the blockchain.

Chain Split: A situation where miners submit different blocks for the same Parent block, resulting in an Orphan block by the Longest-chain Rule.

Child Key: Distinct keys for HD (Hierarchical Derivation) addresses derived from a single master key.

Ciphertext: The encrypted form of plaintext after applying a cipher to secure the message.

Coinbase Transaction: The initial Block Subsidy transaction in a single block within the blockchain.

Cold storage: A method of storing spending keys offline, away from the risk of hackers or other online threats.

Collision Resistant: A desired property of cryptographic hash functions where it is difficult to find two different input values that result in the same hash value outputs.

Commodity: A raw material that can be bought or sold.

Commodity money: Objects that have value in and of themselves and are used as a medium of exchange, such as gold or silver.

Computationally Hard: The hypothesis that a particular problem cannot be solved efficiently.

Confirmation: The process of a transaction being processed (mined) by the network. Every subsequent block generated adds one more confirmation to the transaction.

Compatibility: A state in which two things are able to exist or occur together without problems or conflict

Consensus mechanism: A method of an implementation of Rules used in blockchain technology to validate transactions and ensure the integrity of the blockchain.

Consensus: An agreement reached between all participants.

Consent: Permission given for something to happen or agreement to do something.

Counterparty: The other party that participates in a financial transaction.

Cryptocurrency: A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

Cryptocurrency Exchange: A platform where users can buy, sell, and trade cryptocurrencies for other assets such as fiat currency or other cryptocurrencies.

Cryptocurrency wallet: A software program that stores private keys and allows users to send, receive, and manage their cryptocurrency.

Cryptographic-Commitment-Scheme: A cryptographic protocol that allows a sender to commit a chosen value (or statement) while keeping it hidden to the Receiver, and the Receiver has the ability to reveal the committed value later.

Cryptography: A branch of mathematics that helps create secure systems.

Cypherpunk: An activist movement that originated in the late 1980s. It advocates for personal privacy and freedom through the use of cryptography.

Cypherpunk Zero: A creative universe and collaborative effort between ECC, illustrator Stranger Wolf, Mighty Jaxx, and select ecosystem partners. It consists of a forthcoming series of webcomics, NFTs, and physical collectibles. The project explores the relationship between privacy, self-sovereignty, and creative freedom.

DApp: A decentralized application that is distributed, open source software application that runs on a peer-to-peer (P2P) blockchain network rather than on a single computer.

Debasement: The reduction in the value of a currency, often by reducing the amount of precious metal in a coin.

Debt: Something that is owed to someone else.

Decentralization: The distribution of power and control across a network, rather than having a central authority.

Decentralized Autonomous Organization (DAO): An organization or network governed by smart contracts and run on a blockchain, without a central authority or management structure.

Daemon: A background process that handles requests for services without requiring direct user interaction.

Decentralized Consensus: The concept of achieving consensus through decentralized or independent means.

Decentralized Exchange (Dex): A peer-to-peer crypto trading platform that functions without any involvement of a third party.

Decentralized Finance (DeFi): A movement within the cryptocurrency industry to create decentralized financial products and services that operate on a blockchain.

Decentralized System: A system in which power or control is distributed among multiple entities.

Delegation: The process of distributing and entrusting work to another person.

Deshielding: Refers to a transaction from a shielded address to a transparent address. The origin of the transaction is not visible, however the funds enter a publicly visible value pool.

Difficulty (mining): Determined by the nonce threshold, it dictates how time-consuming it should be to locate the right hash for every block, based on the actual and target block times.

Digital Asset: A digital representation of value that can be traded or used as a store of value.

Desktop Wallet: a wallet that is designed to be run on a computer operating system e.g. Ubuntu.

Distributed Ledger: A database that is spread across a network of computers, rather than being stored in a central location.

Disclosure: The act of making something known.

Diversifier Key: The key used to determine the generation of Diversified (Snap) addresses from a Private Spending Key.

Divisibility: The capacity of being divided into smaller quantities.

Domain (function): The set of input values for which the function is defined.

Domain Name System: A hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks.

Double coincidence of wants: The phenomenon where two parties in a barter economy both have what the other party wants and wants what the other party has.

Double Spend: An instance of a malformed transaction that attempts to spend a UTXO that has already been spent. Spending a UTXO will produce an associated nullifier included in the block that prevents it being spent twice.

Delegated Proof of Stake (DPoS): A popular evolution of the PoS concept, whereby users of the network vote and elect delegates to validate the next block. Delegates are also called witnesses or block producers.

Dust Transaction: A transaction that sends an amount that is too small to be economically viable.

Ease of Use: The concept that describes how easily users can use a product.

Electric Coin Company (ECC): Created and launched the Zcash digital currency in 2016. Currently the primary maintainers of the initial Zcash node, zcashd. Developers of Halo, Blake3 and every major Zcash network upgrade.

ECDSA (Elliptic Curve Digital Signature Algorithm): A cryptographically secure digital signature scheme.

Electronic (Digital) Currency: Any means of payment that exists in a purely electronic form.

Elliptic curve: An algebraic curve over a field whose solutions are confined to a region of space that is topologically equivalent to a torus.

Encoding: The process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format, usually for transmission.

Encrypted Memos: An additional field for text allowed in fully shielded transactions, visible only to the sender and recipient.

Entropy: The lack of order or predictability.

Ephemeral Key: The Cryptographic Key used to encrypt the Memo Field.

Exchange Rate: The value of one currency in relation to another.

Equihash: The memory-oriented proof-of-work mining algorithm used on Zcash.

Faucet: A faucet is an application that dispenses micro-quantities cryptocurrency usually for testing.

FATF (Financial Action Task Force): also known by its French name, Groupe d'action financière (GAFI), is an intergovernmental organization founded in 1989 on the initiative of the G7 to develop policies to combat money laundering and to maintain certain interest.

Fiat (money): Currency that is not backed by a commodity, such as gold or silver.

Fiat-Shamir: A technique for creating a digital signature based on an interactive proof of knowledge.

Field (Transaction): Refers to information given by the user that goes into a transaction .e.g amount and memo.

Finite Field: A group of related numbers that amount to a finite number of elements, commonly to the order of a Prime number.

Financial Institution: A business entity that provides service as an intermediary for different types of financial monetary transactions.

Financial System: A system that allows the exchange of funds between financial market participants.

Fixed-supply: Refers to an invariable productive capacity for a given good or service.

FOMO: Fear of missing out, a term used to describe the feeling of anxiety or regret that one may miss out on a profitable opportunity.

Fork: A fork occurs when a blockchain splits into two competing paths. The cause of forks can vary between the unintentional creation of competing blocks, resulting in a temporary split, and intentional upgrades to the rules that govern how new blocks are created.

Founders' Reward: Represents 20% of the total block reward, deducted from every block's value for the first four years. Transparently distributed to drive protocol development and growth.

Free2z: A social website for anonymous content and private donations powered by Zcash.

FROST: Flexible Round-Optimised Schnorr Threshold signature scheme. Designed to reduce the interaction between participants who jointly own an individual private signing key and wish to use this private key to collectively sign a message. In Zcash, FROST will sign transactions from joint owners of a signing key share that could not be signed without a certain threshold number of participants.

FUD: Fear, uncertainty, and doubt, a term used to describe negative rumors or information that can cause market panic or decline.

Fully Shielded: Refers to a Zcash shielded transaction where the notes are spent into the same shielded pool as where they came from.

Full Node: A node that is able to download the entire blockchain history to observe and enforce its predetermined rules.

Full Node Wallet: A wallet that is integrated into a Full Node.

Full Viewing Key: A cryptographic key that allows for a holder to view the complete history of a given Zcash Shielded address without the ability to spend any balance it holds.

Fungibility: The property of a good or a commodity whose individual units are essentially interchangeable.

GDP: Gross domestic product, the total value of goods and services produced in a country in a given period of time.

Genesis Block: The initial (first) block of data computed in the history of a blockchain network.

Groth16: An algorithm that enables a quadratic arithmetic program to be computed by a prover over elliptic curve points derived in a trusted setup, and quickly checked by a verifier. It uses auxiliary elliptic curve points from the trusted setup to prevent forged proofs.

Halo: Halo: A proof system that modifies the zk-SNARK model to enable the creation of recursive proofs (multiple proofs condensed into one). The Halo zero-knowledge proving system was implemented in Zcash to remove reliance on setup ceremonies, and Halo recursion, a scalability solution, is under development. The current implementation is called Halo2.

Hard Fork: A change to a blockchain protocol that creates a new version of the blockchain, which is not compatible with the previous version.

Hardware Wallet: A physical device used for storing private keys and managing cryptocurrency, providing enhanced security over software wallets.

Hash Function: A mathematical function that takes input data of any size and outputs a fixed-size string of characters, commonly used in cryptography and blockchain technology.

Hash Rate: A generalized measure of the theoretical total amount of hashes produced by miners of a given network for a given timespan, typically measured in seconds, also known as a solution rate.

HD (Hierarchical Deterministic) Wallet: A method that generates a series of key pairs from one seed, providing convenience and manageability as well as high-level security. Zcash wallets enable several

shielded public keys to be created from the root private key within a wallet.

HODL: A term used in the cryptocurrency community to describe holding onto cryptocurrency long-term, rather than selling or trading it.

Honest Node: A Full Node that correctly maintains the consensus mechanism it supports.

Hot Wallet: A cryptocurrency wallet that holds custody of a user's spending keys. Hot is an acronym for Hosted.

Imports: The goods and services produced in another country and sold in the domestic market.

Index (Market): Displays a measure of performance for a traded asset(s) against predetermined metrics and methods.

Infinite Field: A group of related numbers that amount to an infinite number of elements.

Inflation: An increase in the general price level of goods and services in an economy.

Integrity Check: Examines stored files or network packets to determine if they have been altered or changed.

Interactive Proof System: An abstract machine that models computation as the exchange of messages between two parties: a Prover and a Verifier.

Intermediary: A person or organization that makes business or financial arrangements between companies or organizations that do not deal with each other directly.

Initial Coin Offering (ICO): A fundraising method in which a new cryptocurrency is sold to investors prior to the project's launch. Traditionally known as an IPO.

Inputs (transaction): The notes or UTXO's that are put into a transaction plan and result in a spend.

Investing: Expending money, time or effort with the expectation of achieving a profit or advantageous result.

Immutability: The quality of being resistant to any alterations or change.

IP Address: A numerical label that is assigned to a device connected to a computer network that uses the

Internet Protocol for communication.

Irreversibility: The quality of being impossible to change back to a previous condition or state.

Joinsplit: The method used in Zcash Sprout transactions which involves the combination of inputs (funds) from multiple sources (joining) and allocation to multiple outputs (splitting), within a single transaction.

JubJub: An elliptic curve designed for efficient implementation in zk-SNARK circuits.

Know Your Customer (KYC): References a set of guidelines that financial institutions follow to verify the identity and risks of a customer.

Layer-1 Protocol: Refers to a base network and its underlying infrastructure. Layer-1 blockchains can validate and finalize transactions without relying on another network.

Layer-2 Protocol: A secondary layer built on top of a Layer-1 blockchain network, often used to enhance scalability, speed, and functionality that is absent from Layer-1.

Leaf Node: A data object that represents the edge of a path along the branches of a Merkle Tree.

ledger: A record, often associated with financial transactions.

Ledger Hardware Wallet: A wallet system that utilizes a secure device for storing keys and signing transactions offline.

Librustzcash: A Rust workspace containing all crates and dependencies for working with Zcash.

Lightning Network: A layer-2 payment protocol that enables faster and cheaper Bitcoin transactions by using off-chain channels for smaller transactions.

Light client: A term used to describe any wallet that makes use of LightwalletD as its primary source of information.

LightwalletD: A stateless server that serves light clients (light wallets) with blockchain information that it fetches from a Zcash full node. This information is pre-fetched during a syncing period and updated with every new block.

Lightweight Node: A Bitcoin client that only stores a limited amount of data from the blockchain, rather than the full chain. The Zcash equivalent is referred to as a Pruned Node.

Loan: A thing that is borrowed, especially a sum of money that is expected to be paid back with interest.

Longest-chain Rule: States that the valid chain with the most accumulated computational work is considered the longest and most secure.

Machine Learning: The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyze and draw inferences from patterns in data.

Malicious Node: A node seeking to deny service to other nodes in the network it serves.

Mainnet: The primary network where transactions take place on a specific distributed ledger.

Malware: Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Master Key: A set of bytes, usually referred to as a seed phrase, that is responsible for deriving Private Spending Keys for restoring a wallet.

Mediums of exchange: Objects or systems that are widely accepted in exchange for goods and services.

Mempool: A mechanism for network nodes to store the information about all unconfirmed transactions.

Memo Field: A feature of Zcash Shielded transactions, it is a transaction field that can be used to incorporate encrypted text information in the transaction.

Metadata: Data generated alongside a user's transaction, including block height (timestamp), transaction version (note types), total inputs/ outputs and transaction fee.

Metaverse: A decentralized network of virtual worlds that are connected by a shared set of protocols and standards.

Merkle Proof: The process of traversing a Merkle tree from a leaf to the root, hashing each level with the previous to produce a unique hash for the structure of the tree. Providing the final hash allows other actors to determine if the data in a Merkle tree is the same as their own.

Merkle Tree: A tree-like data structure used in the Bitcoin-like blockchains to efficiently verify the integrity of large sets of data.

Miner (blockchain): an entity engaged in the process of validating the information in a blockchain block by generating a cryptographic solution that matches specific criteria e.g. difficulty.

Mining Pool: An organization that provides access to a mining stratum, which is a method of aggregating the work needed to mine a block and provides a way to earn rewards through mining without having to directly mine a block.

Mining (Data): The process where nodes compete in solving complex mathematical calculations to find solutions to blocks of transaction data. Miners are typically rewarded with both the transaction fees of

the transactions they confirm and block rewards.

Mnemonic Phrase: An alternative way of referring to a Secret Recovery Phrase, also known as a '*seed phrase*' and '*recovery phrase*': a series of words that correspond to a very long cryptographic key, used

to generate addresses of a cryptocurrency wallet.

Mobile SDK: Mobile protocols for implementing specific wallets on mobile devices e.g. Android, ios.

Mobile Wallet: An online payment tool or software application that serves is designed to be used on a mobile device e.g. Android.

Monetary and Fiscal Policy: The policies of a central bank and government, respectively, that influence the money supply and interest rates in an economy.

Monetary Supply: The total amount of money in circulation in an economy.

Money: A current medium of exchange.

Multi-Signature (Multisig) Wallet: A wallet that requires multiple signatures or approvals before a transaction can be executed, providing additional security depth.

Multisignature (Address): An address requiring multiple private key signatures to spend funds. Zcash supports legacy-Transparent multisig address and Orchard shielded Frost multisig address functionality.

Network: A group of interconnected entities.

Nighthawk: An independent, Zcash Community Grants funded mobile wallet that supports Shielded Zcash.

Node Network: A network of separate, interconnected computers or devices that support and maintain a computer protocol.

Node: A computer or device that is connected to a node network and participates in the verification and transmission of information.

Non-Fungible Token (NFT): A type of digital asset that represents a unique or one-of-a-kind item, often used to represent art, collectibles, or other unique objects.

Non-Monetary Payment: The exchange of goods or services without actual money changing hands.

Nonce: A random number that is added to a block header to create a hash that meets the difficulty target.

Notes (Transaction): A term used to describe UTXO's, they are the individual data objects that correlate to specific received transactions

Note Commitment: A cryptographic commitment to a valid Leaf Node that binds the value of a note.

Note Commitment Tree: A Merkle tree defined over every note, of which are hashed and inserted into this Merkle tree so proofs can use it to prove note authenticity.

NU5: The 6th major network upgrade for the Zcash protocol which introduced Halo, the Orchard value pool and Unified Address types which also marked the initial deprecation of Legacy Transparent and

Sapling addresses.

Nullifier: A unique identifier for a spent note but does not disclose any information about the note itself.

Nullifier Key: A Cryptographic Key used to derive a nullifier for proving the validity of a spent note.

NYDFS (New York State Department of Financial Services): The department of the New York state government responsible for regulating financial services and products.

One-way Function: A function that is easy to compute on every input, but Computationally Hard to invert.

On/Off-ramp: Services that allow cryptocurrencies to be converted from or back to fiat currency.

Open-source: Software for which the original source code is made freely available and may be redistributed and modified.

Oracles: Services that are outsourced from the client to accelerate normally expensive computations. With cryptocurrencies, they are often the result of Trusted-Setsups.

Orchard Shielded Pool: The third shielded pool for Zcash which itself uses Unified type address receivers with the prefix U.

Orchard Actions: Term used to describe the inputs, outputs and cryptographic material associated with an Orchard transaction.

Orphan Block: A block that is not included in the main chain of the blockchain due to being invalidated by a longer competing chain.

Outgoing Viewing Key: A Cryptographic Key that allows the holder to view outgoing transaction details without revealing the transaction's value to others.

Output: A new Note or UTXO that is a product resulting from a spend.

Overwinter: The 1st Network Upgrade for Zcash, introduced various performance improvements and features including transaction expiry.

P2PKH: The address format used in Bitcoin.

Paper Wallet: A printed copy of a user's private and public keys used for storing and managing cryptocurrency offline.

Partially Shielded: A Zcash Shielded transaction which involves sending notes from one shielded pool to another which reveals the amounts that cross pools.

Password: A string of words that must be used to gain access to a computer system or service.

Peer-to-Peer Network: A communications network consisting of relay channels for the direct transfer of information between two network participants (peers).

Peg: A fixed exchange rate between two currencies, where one is compared to the value of another.

PIN (Personal Identification Number): An identifying number allocated to an individual by a bank or other organization and used for validating electronic transactions.

Permissionless: The quality of not requiring authorization.

Plaintext: Any data in a form that can be viewed or used without requiring a key or other decryption device.

Point of sale (POS): The place at which goods are retailed.

Portability: The ability to be easily carried or moved.

Prime Number: A whole number that cannot be exactly divided by any whole number other than itself and 1.

Privacy: The state or condition of being free from being observed or disturbed by other people.

Private Blockchain: A blockchain that is controlled by a single organization rather than a network of public nodes.

Private Key: A secret piece of data that enables a person to generate a valid cryptographic signature, encrypt or decrypt some data..

Privilege: A special right, advantage, or immunity granted or available only to a particular person or group.

Proof: A small piece of data that certifies the truth of a statement without revealing any additional information.

Proof Authorizing Key: A Cryptographic Key used to prove that possession of the associated Private Spending Key when spending a note.

Proof-of-Liquidity: A cryptographically signed assertion by a trusted third-party auditor that an actor holds the declared number of resources. Proof-of-Liquidity is used for cryptocurrencies that are pegged to a real-world security or commodity.

Proof-of-Stake (PoS): A consensus mechanism by which validating-participants stake cryptocurrency to validate transactions and earn a reward. The return is based on the amount staked.

Proof of Work: A consensus mechanism by which miners execute trial computations to solve a hash function that resolves to a block. The return is based on overall hashing capacity and speed.

Proof Verification: The process of checking the validity of a proof, typically done by a “verifier”.

Protocol (Computer): A set of rules governing the exchange or transmission of data between devices.

Prover: The entity that generates a proof in a zero-knowledge proof system, attesting to the truth of a statement without revealing any additional information.

Public Blockchain: A blockchain that is freely accessible to anyone to participate in and verify transactions.

Public Key: A unique identifier used for receiving cryptocurrency, derived from a user’s private key through a mathematical process.

Public Ledger: A decentralized database that keeps a public record of all information on the network.

Purchasing Power: The ability of money to buy goods and services.

QEDIT: The development team working to build and integrate the Zcash Shielded Assets protocol.

QR code: A machine-readable code consisting of an array of black and white squares, typically used for storing URLs or other information for reading by the camera on a smartphone.

Random Number Generation: Process by which, often by means of a random number generator (RNG), a sequence of numbers or symbols that cannot be reasonably predicted better than by random chance is generated.

Receivers (Unified Address): The individual destination addresses that are encoded into a Unified Address.

Recovery: The action or process of regaining possession or control of something stolen or lost.

Recursive Proofs: A proof that verifies the correctness of another instance of itself, allowing any amount of computational effort and data to produce a short proof that can be checked quickly. This compression technique enables handling unlimited amounts of computation.

Regulations: A rule or directive made and maintained by an authority.

Representative Money: Money, which represents a claim on a physical commodity.

Remittance: A sum of money sent in payment for goods or services or as a gift.

Reserve Ratio: The proportion of deposits that a bank must hold as reserves. Reserve Banking

Restrictive banking: Restrictions or limitations on banking services or access to banking services.

Rollback: Occurs when a blockchain is rewound to a previous state, and a set of the most recent blocks and the transactions they contain are discarded. Zcash has a rollback limit of 100 blocks.

RPC (Remote Procedure Call): A protocol allowing a client to execute functions on a remote server.

Rug Pull: A scam in which the creators of a product or service facilitate increased reliance on a given free product or service for a customer base and begin charging for the service, typically leaving the customer with little recourse.

Sanctions: A threatened penalty for disobeying a law or rule.

Sapling: The second major Zcash network upgrade that introduced the Sapling value pool, vastly improved efficiency for shielded transactions. It was activated at block height 419200.

Satoshi Nakamoto: The pseudonym used by the anonymous creator(s) of Bitcoin.

Satoshi: The smallest unit BTC, equal to 0.00000001 of a Bitcoin. It is named after the pseudonym of the creator of Bitcoin, Satoshi Nakamoto.

Satoshis per byte (sat/b): A unit used to measure the amount of bitcoin transaction fee paid per byte of transaction data.

Scarcity: The state of being scarce or in short supply.

Secp256k1: The name of the elliptic curve used by Bitcoin to implement its public key cryptography.

Secret Key: A piece of information or a framework that is used to decrypt and encrypt messages.

Security: Procedures followed or measures taken to ensure the safety of a state or organization.

Securities (Investing): A financial instrument as an investment of money made into a business with the expectation of a profit to come through the efforts of someone other than the investor.

SegWit (Segregated Witness): A Bitcoin protocol upgrade that changes the way data is stored on the blockchain, allowing for increased capacity and lower transaction fees.

Selective Disclosure: A feature of Shielded Addresses where the owner can disclose shielded transaction data by sharing a viewing key or payment disclosure with a third party.

Self-custody: A means of holding assets by which only you have access to them.

Sensimilla: A collision-resistant hash function and commitment scheme designed for efficiency in algebraic circuit models.

Shielded Labs: The first Zcash organization formed outside the United States, supporting protocol development and Zcash adoption.

Shielded Transaction: A transaction exclusively between shielded addresses. The addresses and optional memo are encrypted. Values that stay in the same pool are encrypted as well but any value inputs that cross value pools are revealed.

Shielding (Transaction): A Zcash transaction that sends Transparent funds into a Shielded Pool.

Sidechain: A blockchain that is connected to another blockchain, allowing for the transfer of assets or information between the two chains.

Signature: A mathematical mechanism that allows someone to prove ownership.

Single Point of Failure: A part of a system that, if it fails, will stop the entire system from working.

Smart Contract: A self-executing contract with the terms of the agreement written into code.

SNARKS (Succinct Non-Interactive Argument of Knowledge): SNARKs are a kind of zero-knowledge proof system that are short and quick to verify. SNARKs are characterized by their use of the KZG (Kate, Zaverucha, and Goldberg) commitment scheme which uses elliptic curve cryptography.

Society: The community of people living in a particular country or region and having shared customs, laws, and organizations.

Soft Fork: A change to a blockchain protocol that is backward-compatible with older versions of the software.

Sol/s (Solutions Per Second): A measure of the rate at which Equihash solutions are found during mining. Each solution is tested against the current target after being added to the block header and hashed.

Sound-Unsound Money: The quality of a currency to the extent that it is, or is not, liable to sudden appreciation or depreciation in value.

Spam Transactions: Transactions which create an undesirable extra load on the network due to not following Transaction best practices.

Spend Authority: The quality of having in possession the Private Spending Key for a given address.

Spend Authorizing Key: A Cryptographic Key that proves a senders ability to spend i.e. Private Spending Key.

Sprout: The initial version of Zcash, launched on October 28, 2016.

Stablecoin: A type of cryptocurrency designed to maintain a stable value, often by being pegged to a fiat currency or other asset.

Standard of Living: The level of income, comforts and services available, generally applied to a society or location.

Supply and Demand: The economic principle that the price of a good or service is determined by the interaction of the quantity of the good or service that is supplied and the quantity that is demanded.

Surveillance: A close observation, often carried out in secret.

Sybil-resistance: The measure of a network's ability to withstand Sybil attacks, when an attacker creates numerous identities on a network and uses them to gain influence over other Nodes.

Syncing: The process of establishing consistency between source and target data stores.

Testnet: An instance of a blockchain powered by the same or a newer version of the underlying software, to be used for testing.

Third Party: Of or relating to a person or group besides the two primarily involved in a situation.

Time Value of Money: The principle that money is worth more in the present than in the future.

Time Preference: Is the current relative valuation placed on receiving a good or some cash at an earlier date compared with receiving it at a later date.

Testnet: An alternative blockchain that mimics the main network for testing purposes. Testnet coins have no value and allow developers and users to experiment without using actual currency. It is also used to test network upgrades before implementing them on the main network.

Token: A unit of value often used to represent a specific asset or utility within a particular ecosystem.

Tokenization: The process of creating a digital representation of an asset or asset class, allowing for fractional ownership and transferability.

Trade and Commerce: A term that for the

broader way people have transactions and communicate with each other.

Trading Pair: A set of two currencies or assets that can be traded against each other on a cryptocurrency exchange.

Traditional Finance: the mainstream financial system and the conventional institutions such as retail, investment, and commercial banks, insurance companies, and other regulated entities that operate within it.

Transaction: an exchange or interaction between entities.

Transaction Expiry: enforces that a transaction expires if it remains unconfirmed in the mempool for too long. Expired transactions can be resubmitted or replaced with new ones. The default expiry in Zcash is 20 blocks.

Transaction Fee: An additional value added to incentivize miners to include a transaction in a block. For Zcash, zip317 dictates the default base fee is 0.0001 and 0.00005 for each additional input and output, past the first two "grace actions".

Transaction ID: An alphanumeric Hash string that resolves to a particular transaction included in a blockchain.

Transaction: The transfer of value from one address to another.

Transparent Transaction: Involves sending or receiving transactions where the address and associated value are publicly visible on a blockchain.

Transparent Address: a P2PKH Zcash address that has the same intrinsic qualities of a Bitcoin address.

Trial Decryption: the process of attempting to transform encrypted information into its original format.

Trusted Setup: The process of generating cryptographic parameters for the network using secure multi-party computation.

Trustless: A system that does not require trust, or a trusted setup, in any third party or intermediary.

Two-Factor Authentication (2FA): A security measure that requires two methods of authentication, typically a password and a separate code or device, to access an account or complete a function.

Unbanked: Individuals or communities without access to traditional banking services.

Unconfirmed: the state of a transaction that has been broadcast to the network but has yet to be included in a block.

Underbanked: refers to individuals or families who have a bank account but often rely on alternative financial services to manage their finances.

Uniform Probability Distribution: a type of probability distribution in which all outcomes are equally likely.

Unit of Account: A standard unit of measurement used to express the value of goods and services.

Unified Addresses: A Zcash address format that can encode one or multiple Zcash address types (Transparent, Sapling, and Orchard).

Units: The unit of account for Zcash coins is 'ZEC'. The smallest unit is 0.00000001 or 1 Satoshi/Zat.

Upgrade Activation: A specific block height that triggers a network upgrade. The success or failure of the upgrade depends on whether a majority of the node participants run the upgraded software.

User-Defined Assets: An extension of the Orchard Protocol enabling native shielded assets (ZSAs).

UTXO (Unspent Transaction Output): The result of a transaction that a user receives and can spend in the future. Each UTXO can only be spent once, which differs from account-based systems.

UX (User Experience): how a user interacts with and experiences a product, system or service.

v# Transaction: Refers to the transaction type implemented with the associated network upgrade e.g. NU5 Network Upgrade v5 specification.

Value: the regard that something is held to

deserve; the importance, worth, or usefulness of something.

Verifier: The Verifier receives a proof, checks to make sure the proof is valid, and then updates the state root.

Viewing Key: Owners of shielded addresses can share transaction details with trusted third parties using a view key. The view key grants read and transaction construction access but not spend authority over the address.

Virtual Machine: A computer operating system that is running within another operating system. Virtual machines can simulate a unique computer on a subset of the resources of a larger machine.

Volatility: The degree of variation in the price of an asset over time.

Wallet Address: A unique identifier used to send and receive value, typically represented as a string of letters and numbers.

Wallet Backup: A copy of the wallet database including transaction history, private keys and recovery phrase/seed keywords, can be used to restore access to the wallet in case the original is compromised.

Wallet (Cryptocurrency): A virtual container for an electronic value instrument, similar to a physical wallet, that contains private key(s) that allow spend authority to the value allocated to it.

Whale (Cryptocurrency): An individual or organization that holds a significant amount of cryptocurrency, capable of influencing market prices through large trades.

White Hat Hacker: An hacker who uses their skills to identify and fix vulnerabilities in computer systems and networks.

Whitepaper: A report that explains the problem and solution that a project or cryptocurrency is trying to address.

XBT: Alternative abbreviation for bitcoin.

Ywallet: An independent, Zcash Community Grants funded mobile wallet that supports Shielded Zcash.

Zashi Wallet: the Electric Coin Company developed wallet that supports Shielded Zcash.

Zatoshi (Zat): the smallest unit ZEC, equal to 0.00000001 of a Zcash. It is named after the pseudonym of the creator of Bitcoin, Satoshi Nakamoto.

Zero-Knowledge Proofs: Cryptographic techniques that allow one party to prove the truth of a statement without revealing any additional information.

Zcash: is a privacy-focused, decentralized cryptocurrency which is based on Bitcoin's codebase that facilitates both privately and publicly visible transactions.

Zcash Community Grants (ZCG): A community-elected grants committee that funds projects advancing Zcash usability, security, privacy, and adoption.

Zcashd: The original Zcash network full node. Developed and maintained by the ECC, it (though not limited to) enforces network consensus of the Zcash blockchain, enforces network rules, and validates and relays transaction mempool data. Zcashd deprecation, in favor of Zebrad.

Zcash Foundation: The Zcash Foundation is a 501(c)(3) public charity that builds financial privacy infrastructure for the public good, primarily serving users of the Zcash protocol and blockchain. The Zcash Foundation are the primary developers and maintainers of the Zebrad and Frost repositories, facilitate the Zcash Community Grants Committee as well as the Arborist call.

Zcon: Presented by the Zcash Foundation, it is a conference focusing on the Zcash ecosystem, can be in-person or virtual as well as regional and global variety.

Zebrad: An independent full node implementation of the Zcash protocol, developed by the Zcash Foundation. Written in the Rust Programming Language, Zebrad has been designated to be the future main Zcash full node.

ZecHub: An open-source education hub for Zcash, driven by the community. Funded by the Zcash Community Grants Committee, it produces content on privacy technologies, including Zcash.

ZecPages: A censorship-resistant, Zcash Viewing Key powered social media platform. It includes a directory of Zcash users and an anonymous message board.

Zerocash: the original name for the Zcash protocol that is built on top of the Bitcoin codebase.

Zero-Knowledge Proof (ZKP): a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, while avoiding conveying to the verifier any information beyond the mere fact of the statement's truth.

ZF A/V Club: Empowers local Zcash communities globally by creating a network of content creators who share fresh news about Zcash and online privacy.

Zingo Wallet: An independent, Zcash Community Grants funded mobile wallet that supports Shielded Zcash.

ZIP (Zcash Improvement Proposal): A method for developing community proposals regarding new features, implementation details, and design decisions for the Zcash cryptocurrency, primarily with Github.

Zingo Wallet: A Zcash Community Grants Committee funded mobile wallet that supports Unified Addresses and Orchard. It is maintained by Zingo Labs.

zk-SNARK (Zero-knowledge Succinct Argument of Knowledge): A proof used in the Zcash protocol, allowing Shielded Addresses to validate associated transactions without revealing the address or value transacted.

Zodler: from "hodler", it refers to an individual who holds onto their Zcash for the long term, regardless of market volatility.

