Chapter 5: Introduction 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, blockchainbased 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.

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.
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).
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 andthe 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

SAPLING
zslcpf4prtmnqpg6x2ngcrwelu9a39z9l9lquk
q9fwagnaqrkn k34a7n3szwxpjuxfjdxkuzykel53

UNIFIED ADDRESS (FULL) IMAGE PLACEHOLDER
ulckeydud0996ftppqrnpdsqyeq4e57qcyjr4raht4dc8j3nju
yj3gmm9yk7hq9k88cdkqfuqusgpcpjfhwu3plm2vrd32g8du78k
zkm5un357r4vkhz4vhxd4yfl8zvszk99cmsc89qv4trd7jzkcs8
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.