



# Compliance for Digital Assets

May 2024



**Pablo Kogan**  
Director of Engineering



**Antoine Rondelet**  
Scientific Advisor



# Abstract – Compliance for Digital Assets



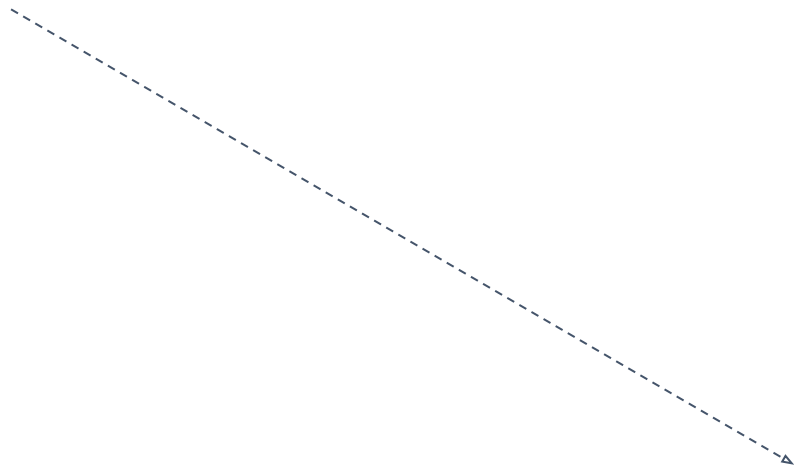
- Motivation
- Technical discussion

# Setting the scene: Cryptocurrency

*"Improved, alternative financial system"*

# Setting the scene: Cryptocurrency

*"Improved, alternative financial system"*



*Tight integration into the existing financial system*

# Setting the scene: Bitcoin auditability

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products



Chair Gary Gensler

Jan. 10, 2024

Today, the Commission approved the listing and trading of a number of spot bitcoin exchange-traded product (ETP) shares.

I have often said that the Commission acts within the law and how the courts interpret the law. Beginning under Chair Jay Clayton in 2018 and through March 2023, the Commission disapproved more than 20 exchange rule filings for spot bitcoin ETPs. One of those filings, made by Grayscale, contemplated the conversion of the Grayscale Bitcoin Trust into an ETP.

We are now faced with a new set of filings similar to those we have disapproved in the past. Circumstances, however, have changed. The U.S. Court of Appeals for the District of Columbia held that the Commission failed to adequately explain its reasoning in disapproving the listing and trading of Grayscale's proposed ETP (the Grayscale Order).<sup>[1]</sup> The court therefore vacated the Grayscale Order and remanded the matter to the Commission. Based on these circumstances and those discussed more fully in the approval order, I feel the most sustainable path forward is to approve the listing and trading of these spot bitcoin ETP shares.

The Commission evaluates any rule filing by a national securities exchange based upon whether it is consistent with the Exchange Act and regulates investors, including whether it is designed to protect investors and the public interest. The Commission is merit neutral and does not take a view on particular companies, investments, or the assets underlying an ETP. It is the issuer of a security and the listing exchange comply with the Securities Act, the Exchange Act, and the Commission's rules, that issuer must be provided the same access to our regulated markets as anyone else.

Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin. It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws. As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.<sup>[2]</sup>

Investors today can already buy and sell or otherwise gain exposure to bitcoin at a number of brokerage houses, through mutual funds, on national securities exchanges, through peer-to-peer payment apps, on non-compliant crypto trading platforms, and, of course, through the Grayscale Bitcoin Trust. Today's action will include certain protections for investors:

First, sponsors of bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products. Invested in any bitcoin ETP that is listed and traded will benefit from the disclosure included in public registration statements and required periodic filings. While these disclosures are required, it is important to note that today's action does not endorse the disclosed ETP arrangements, such as custody arrangements.

Second, these products will be listed and traded on registered national securities exchanges. Such regulated exchanges are required to have rules designed to prevent fraud and manipulation, and we will monitor them closely to ensure that they are enforcing those rules. Furthermore, the Commission will fully investigate any fraud or manipulation in the securities markets, including schemes that use social media platforms.<sup>[3]</sup> Such regulated exchanges also have rules designed to address certain conflicts of interest as well as to protect investors and the public interest.

Further, existing rules and standards of conduct will apply to the purchase and sale of the approved ETPs. This includes, for example, Regulation Best Interest when broker-dealers recommend ETPs to retail investors, as well as a fiduciary duty under the Investment Advisers Act for investment advisers. Today's action does not approve or endorse crypto trading platforms or intermediaries, which, for the most part, are non-compliant with the federal securities laws and often have conflicts of interest.

Third, Commission staff is separately completing the review of registration statements for 10 spot bitcoin ETPs simultaneously, which will help create a level playing field for issuers and promote fairness and competition, benefiting investors and the broader market.

Since 2004, this agency has had experience overseeing spot non-security commodity ETPs, such as those holding certain precious metals. That experience will be valuable in our oversight of spot bitcoin ETP trading.

Though we're merit neutral, I'd note that the underlying assets in the metals ETPs have consumer and industrial uses, while in contrast bitcoin is primarily a speculative, volatile asset that's also used for illicit activity including ransomware,<sup>[4]</sup> money laundering,<sup>[5]</sup> sanction evasion,<sup>[6]</sup> and terrorist financing.<sup>[7]</sup>

While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin. Investors should remain cautious about the myriad risks associated with bitcoin and products whose value is tied to crypto.<sup>[8]</sup>

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products

Reluctantly approved in Jan 2024

<https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023>

# Setting the scene: Bitcoin auditability

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products



Chair Gary Gensler

Jan. 10, 2024

Today, the Commission approved the listing and trading of a number of spot bitcoin exchange-traded product (ETP) shares.

I have often said that the Commission acts within the law and how the courts interpret the law. Beginning under Chair Jay Clayton in 2018 and through March 2023, the Commission disapproved more than 20 exchange rule filings for spot bitcoin ETPs. One of those filings, made by Grayscale, contemplated the conversion of the Grayscale Bitcoin Trust into an ETP.

We are now faced with a new set of filings similar to those we have disapproved in the past. Circumstances, however, have changed. The U.S. Court of Appeals for the District of Columbia held that the Commission failed to adequately explain its reasoning in disapproving the listing and trading of Grayscale's proposed ETP (the Grayscale Order).<sup>[1]</sup> The court therefore vacated the Grayscale Order and remanded the matter to the Commission. Based on these circumstances and those discussed more fully in the approval order, I feel the most sustainable path forward is to approve the listing and trading of these spot bitcoin ETP shares.

The Commission evaluates any rule filing by a national securities exchange based upon whether it is consistent with the Exchange Act and regulates themselves, including whether it is designed to protect investors and the public interest. The Commission is merit neutral and does not take a view on particular companies, investments, or the assets underlying an ETP. It is the issuer of a security and the listing exchange comply with the Securities Act, the Exchange Act, and the Commission's rules, that issuer must be provided the same access to our regulated markets as anyone else.

Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin. It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws. As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.<sup>[2]</sup>

Investors today can already buy and sell or otherwise gain exposure to bitcoin at a number of brokerage houses, through mutual funds, on national securities exchanges, through peer-to-peer payment apps, on non-compliant crypto trading platforms, and, of course, through the Grayscale Bitcoin Trust. Today's action will include certain protections for investors:

First, sponsors of bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products. Invested in any bitcoin ETP that is listed and traded will benefit from the disclosure included in public registration statements and required periodic filings. While these disclosures are required, it is important to note that today's action does not endorse the disclosed ETP arrangements, such as custody arrangements.

Second, these products will be listed and traded on registered national securities exchanges. Such regulated exchanges are required to have rules designed to prevent fraud and manipulation, and we will monitor them closely to ensure that they are enforcing those rules. Furthermore, the Commission will fully investigate any fraud or manipulation in the securities markets, including schemes that use social media platforms.<sup>[3]</sup> Such regulated exchanges also have rules designed to address certain conflicts of interest as well as to protect investors and the public interest.

Further, existing rules and standards of conduct will apply to the purchase and sale of the approved ETPs. This includes, for example, Regulation Best Interest when broker-dealers recommend ETPs to retail investors, as well as a fiduciary duty under the Investment Advisers Act for investment advisers. Today's action does not approve or endorse crypto trading platforms or intermediaries, which, for the most part, are non-compliant with the federal securities laws and often have conflicts of interest.

Third, Commission staff is separately completing the review of registration statements for 10 spot bitcoin ETPs simultaneously, which will help create a level playing field for issuers and promote fairness and competition, benefiting investors and the broader market.

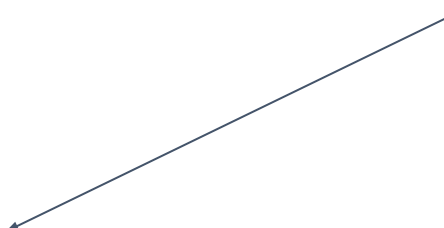
Since 2004, this agency has had experience overseeing spot non-security commodity ETPs, such as those holding certain precious metals. That experience will be valuable in our oversight of spot bitcoin ETP trading.

Though we're merit neutral, I'd note that the underlying assets in the metals ETPs have consumer and industrial uses, while in contrast bitcoin is primarily a speculative, volatile asset that's also used for illicit activity including ransomware,<sup>[4]</sup> money laundering,<sup>[5]</sup> sanction evasion,<sup>[6]</sup> and terrorist financing.<sup>[7]</sup>

While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin. Investors should remain cautious about the myriad risks associated with bitcoin and products whose value is tied to crypto.<sup>[8]</sup>

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products

... Non security commodity ...



<https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023>

# Setting the scene: Bitcoin auditability

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products



Chair Gary Gensler

Jan. 10, 2024

Today, the Commission approved the listing and trading of a number of spot bitcoin exchange-traded product (ETP) shares.

I have often said that the Commission acts within the law and how the courts interpret the law. Beginning under Chair Jay Clayton in 2018 and through March 2023, the Commission disapproved more than 20 exchange rule filings for spot bitcoin ETPs. One of those filings, made by Grayscale, contemplated the conversion of the Grayscale Bitcoin Trust into an ETP.

We are now faced with a new set of filings similar to those we have disapproved in the past. Circumstances, however, have changed. The U.S. Court of Appeals for the District of Columbia held that the Commission failed to adequately explain its reasoning in disapproving the listing and trading of Grayscale's proposed ETP (the Grayscale Order).<sup>(1)</sup> The court therefore vacated the Grayscale Order and remanded the matter to the Commission. Based on these circumstances and those discussed more fully in the approval order, I feel the most sustainable path forward is to approve the listing and trading of these spot bitcoin ETP shares.

The Commission evaluates any rule filing by a national securities exchange based upon whether it is consistent with the Exchange Act and regulations thereunder, including whether it is designed to protect investors and the public interest. The Commission is merit neutral and does not take a view on particular companies, investments, or the assets underlying an ETP. It is the issuer of a security and the listing exchange comply with the Securities Act, the Exchange Act, and the Commission's rules, that issuer must be provided the same access to our regulated markets as anyone else.

Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin. It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws. As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.<sup>(2)</sup>

Investors today can already buy and sell or otherwise gain exposure to bitcoin at a number of brokerage houses, through mutual funds, on national securities exchanges, through peer-to-peer payment apps, on non-compliant crypto trading platforms, and, of course, through the Grayscale Bitcoin Trust. Today's action will include certain protections for investors:

First, sponsors of bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products. Investors in any bitcoin ETP that is listed and traded will benefit from the disclosure included in public registration statements and required periodic filings. While these disclosures are required, it is important to note that today's action does not endorse the disclosed ETP arrangements, such as custody arrangements.

Second, these products will be listed and traded on registered national securities exchanges. Such regulated exchanges are required to have rules designed to prevent fraud and manipulation, and we will monitor them closely to ensure that they are enforcing those rules. Furthermore, the Commission will fully investigate any fraud or manipulation in the securities markets, including schemes that use social media platforms.<sup>(3)</sup> Such regulated exchanges also have rules designed to address certain conflicts of interest as well as to protect investors and the public interest.

Further, existing rules and standards of conduct will apply to the purchase and sale of the approved ETPs. This includes, for example, Regulation Best Interest when broker-dealers recommend ETPs to retail investors, as well as a fiduciary duty under the Investment Advisers Act for investment advisers. Today's action does not approve or endorse crypto trading platforms or intermediaries, which, for the most part, are non-compliant with the federal securities laws and often have conflicts of interest.

Third, Commission staff is separately completing the review of registration statements for 10 spot bitcoin ETPs simultaneously, which will help create a level playing field for issuers and promote fairness and competition, benefiting investors and the broader market.

Since 2004, this agency has had experience overseeing spot non-security commodity ETPs, such as those holding certain precious metals. That experience will be valuable in our oversight of spot bitcoin ETP trading.

Though we're merit neutral, I'd note that the underlying assets in the metals ETPs have consumer and industrial uses, while in contrast bitcoin is primarily a speculative, volatile asset that's also used for illicit activity including ransomware,<sup>(4)</sup> money laundering,<sup>(5)</sup> sanction evasion,<sup>(6)</sup> and terrorist financing.<sup>(7)</sup>

While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin. Investors should remain cautious about the myriad risks associated with bitcoin and products whose value is tied to crypto.<sup>(8)</sup>

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products

### Footnote [5]

[5] See Basel Institute on Governance, "Quick Guide 1: Cryptocurrencies and Money Laundering Investigations" (August 2023), available at <https://baselgovernance.org/publications/quick-guide-1-cryptocurrencies-and-money-laundering-investigations>. See also Chainalysis, "Crypto Money Laundering: Four Exchange Deposit Addresses Received Over \$1 Billion in Illicit Funds in 2022" (Jan. 26, 2023), available at <https://www.chainalysis.com/blog/crypto-money-laundering-2022/>.

### Relay on Bitcoin graph analysis

<https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023>

# Setting the scene: Bitcoin auditability

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products



Chair Gary Gensler

Jan. 10, 2024

Today, the Commission approved the listing and trading of a number of spot bitcoin exchange-traded product (ETP) shares.

I have often said that the Commission acts within the law and how the courts interpret the law. Beginning under Chair Jay Clayton in 2018 and through March 2023, the Commission disapproved more than 20 exchange rule filings for spot bitcoin ETPs. One of those filings, made by Grayscale, contemplated the conversion of the Grayscale Bitcoin Trust into an ETP.

We are now faced with a new set of filings similar to those we have disapproved in the past. Circumstances, however, have changed. The U.S. Court of Appeals for the District of Columbia held that the Commission failed to adequately explain its reasoning in disapproving the listing and trading of Grayscale's proposed ETP (the Grayscale Order).<sup>[1]</sup> The court therefore vacated the Grayscale Order and remanded the matter to the Commission. Based on these circumstances and those discussed more fully in the approval order, I feel the most sustainable path forward is to approve the listing and trading of these spot bitcoin ETP shares.

The Commission evaluates any rule filing by a national securities exchange based upon whether it is consistent with the Exchange Act and regulations thereunder, including whether it is designed to protect investors and the public interest. The Commission is merit neutral and does not take a view on particular companies, investments, or the assets underlying an ETP. It is the issuer of a security and the listing exchange comply with the Securities Act, the Exchange Act, and the Commission's rules, that issuer must be provided the same access to our regulated markets as anyone else.

Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin. It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws. As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.<sup>[2]</sup>

Investors today can already buy and sell or otherwise gain exposure to bitcoin at a number of brokerage houses, through mutual funds, on national securities exchanges, through peer-to-peer payment apps, on non-compliant crypto trading platforms, and, of course, through the Grayscale Bitcoin Trust. Today's action will include certain protections for investors:

First, sponsors of bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products. Investors in any bitcoin ETP that is listed and traded will benefit from the disclosure included in public registration statements and required periodic filings. While these disclosures are required, it is important to note that today's action does not endorse the disclosed ETP arrangements, such as custody arrangements.

Second, these products will be listed and traded on registered national securities exchanges. Such regulated exchanges are required to have rules designed to prevent fraud and manipulation, and we will monitor them closely to ensure that they are enforcing those rules. Furthermore, the Commission will fully investigate any fraud or manipulation in the securities markets, including schemes that use social media platforms.<sup>[3]</sup> Such regulated exchanges also have rules designed to address certain conflicts of interest as well as to protect investors and the public interest.

Further, existing rules and standards of conduct will apply to the purchase and sale of the approved ETPs. This includes, for example, Regulation Best Interest when broker-dealers recommend ETPs to retail investors, as well as a fiduciary duty under the Investment Advisers Act for investment advisers. Today's action does not approve or endorse crypto trading platforms or intermediaries, which, for the most part, are non-compliant with the federal securities laws and often have conflicts of interest.

Third, Commission staff is separately completing the review of registration statements for 10 spot bitcoin ETPs simultaneously, which will help create a level playing field for issuers and promote fairness and competition, benefiting investors and the broader market.

Since 2004, this agency has had experience overseeing spot non-security commodity ETPs, such as those holding certain precious metals. That experience will be valuable in our oversight of spot bitcoin ETP trading.

Though we're merit neutral, I'd note that the underlying assets in the metals ETPs have consumer and industrial uses, while in contrast bitcoin is primarily a speculative, volatile asset that's also used for illicit activity including ransomware,<sup>[4]</sup> money laundering,<sup>[5]</sup> sanction evasion,<sup>[6]</sup> and terrorist financing.<sup>[7]</sup>

While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin. Investors should remain cautious about the myriad risks associated with bitcoin and products whose value is tied to crypto.<sup>[8]</sup>

## Statement on the Approval of Spot Bitcoin Exchange-Traded Products

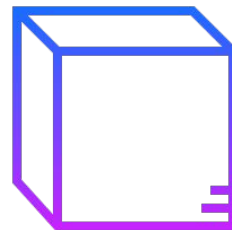
Tightly integrated into the existing financial system

<https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023>



# Setting the scene: Crypto Mixers and compliance

Fully Opaque  
mechanism



# Setting the scene: Crypto Mixers and compliance

## Feds Blacklist Tornado Cash, Ban Ethereum Mixing Tool in US

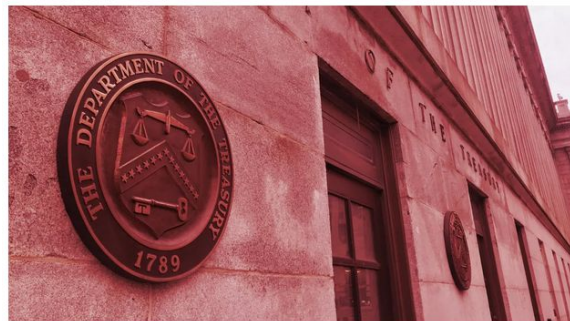
The U.S. Treasury Department put the Ethereum mixing service on the Specially Designated Nationals list today.



By [Mat Di Salvo](#)

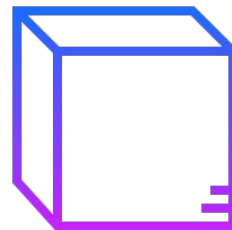
Aug 8, 2022

2 min read



The Office of Foreign Assets Control is a department within the U.S. Treasury. Image: Shutterstock

## Fully Opaque mechanism



# Setting the scene: Crypto Mixers and compliance

## Feds Blacklist Tornado Cash, Ban Ethereum Mixing Tool in US

The U.S. Treasury Department put the Ethereum mixing service on the Specially Designated Nationals list today.



By [Mat Di Salvo](#)

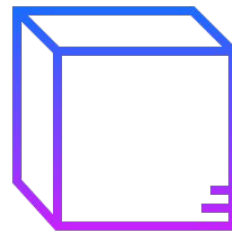
Aug 8, 2022

2 min read



The Office of Foreign Assets Control is a department within the U.S. Treasury. Image: Shutterstock

## Fully Opaque mechanism



Interesting fact: No blockchain actions were done to ban the service

# Setting the scene: Crypto Mixers and compliance

## Feds Blacklist Tornado Cash, Ban Ethereum Mixing Tool in US

The U.S. Treasury Department put the Ethereum mixing service on the Specially Designated Nationals list today.



By [Mat Di Salvo](#)

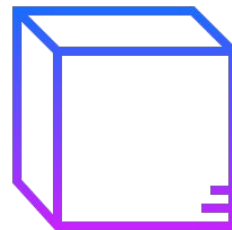
Aug 8, 2022

2 min read



The Office of Foreign Assets Control is a department within the U.S. Treasury. Image: Shutterstock

Fully Opaque mechanism

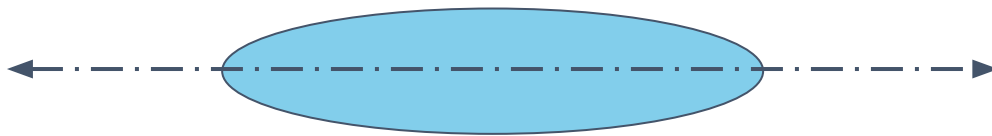
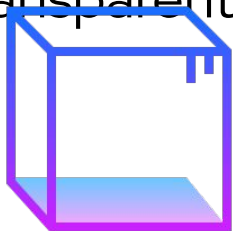


Interesting fact 2: Some major actors “over complied”

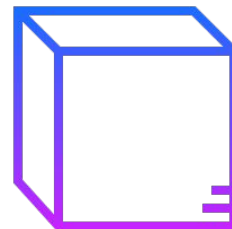
# Setting the scene

## ■ The axis of privacy

Fully  
Transparent



Fully Opaque

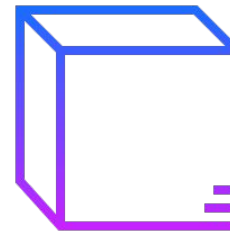


→  
Add privacy

←  
Add Compliance

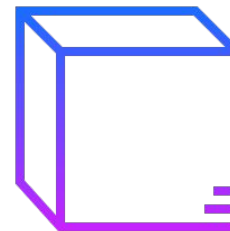
# Public blockchain usage for B2B

- Currently not being used
- Requires privacy



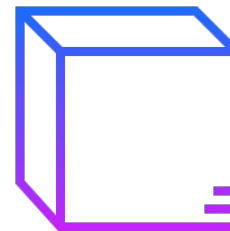
# Public blockchain usage for B2B

- Currently not being used
- Requires privacy
- Requires compliance / auditability



# Public blockchain usage for B2B

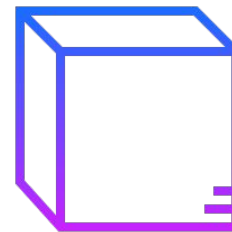
- Currently not being used
- Requires privacy
- Requires compliance / auditability
- No such system exists





# Public blockchain usage for B2B

- Currently not being used
- Requires privacy
- Requires compliance / auditability
- No such system exists



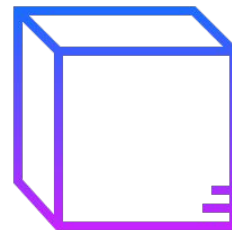
Motivation



# Approaches for compliance / auditability

- Enhanced viewing keys
- Blacklist / Whitelist enforcement
- Asset traceability
- Privacy budget
- Other

Opaque

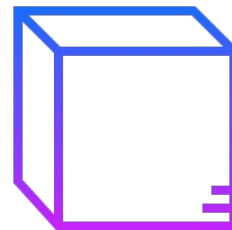


← Add Compliance

# Approaches for compliance / auditability

- **Enhanced viewing keys**
- Blacklist / Whitelist enforcement
- Asset traceability
- Privacy budget
- Other

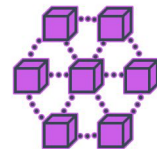
Opaque



←  
Add Compliance

Example: Zcash/Orchard – a fully opaque blockchain protocol

- Privacy achieved using homomorphic commitments, encryption, re-randomized signature scheme and a ZK proof system

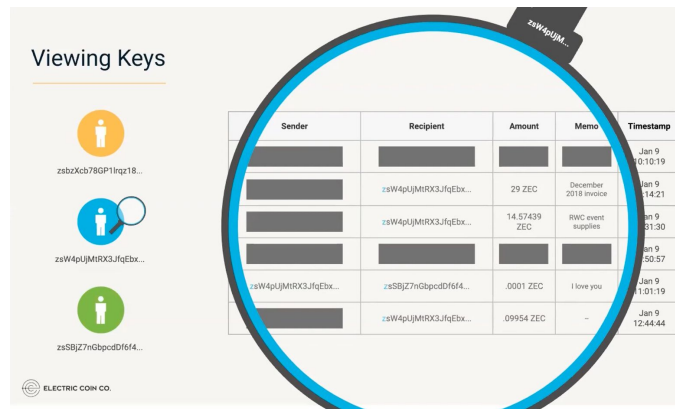


# Viewing Keys

Example: Zcash/Orchard viewing keys

- Provide the ability to disclose transaction history
- Viewing key is separate from the spending key

Viewing Keys



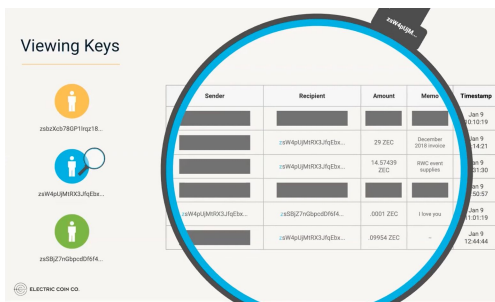
Sender	Recipient	Amount	Memo	Timestamp
				Jan 9 10:10:19
	zsW4pUjMRX3Jf9Ebx...	29 ZEC	December 2018 invoice	Jan 9 14:21
	zsW4pUjMRX3Jf9Ebx...	14.57439 ZEC	RWC event supplies	Jan 9 11:30
				Jan 9 10:57
zsW4pUjMRX3Jf9Ebx...	zsSBjZ7nGbpcdf6f4...	.0001 ZEC	I love you	Jan 9 11:01:19
	zsW4pUjMRX3Jf9Ebx...	.09954 ZEC	-	Jan 9 12:44:44

ELECTRIC COIN CO.

# Viewing Keys

Example: Zcash/Orchard viewing keys

- The viewing key will reveal the entire history

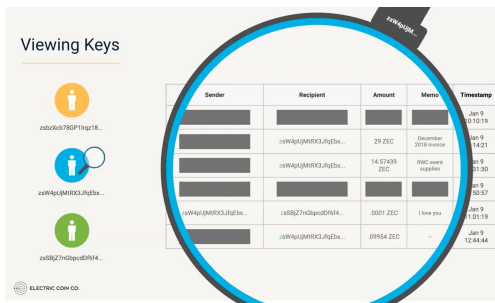


# Viewing Keys

Example: Zcash/Orchard viewing keys

- The viewing key will reveal the entire history
- The revealed in/out addresses are re-randomized

Viewing Keys



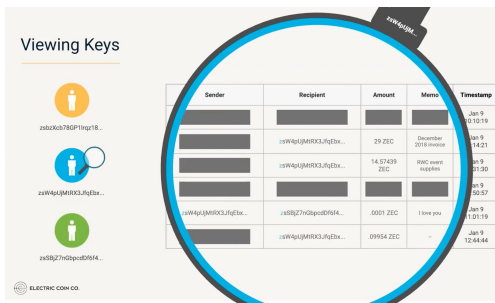
Sender	Recipient	Amount	Memo	Timestamp
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Jan 9 0:10:19
[REDACTED]	[REDACTED]	29 ZEC	December 2018 invoice	Jan 9 14:21
[REDACTED]	[REDACTED]	14.57428 ZEC	2018 month invoice	Jan 9 15:30
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Jan 9 16:57
[REDACTED]	[REDACTED]	0001 ZEC	I love you	Jan 9 1:01:19
[REDACTED]	[REDACTED]	0954 ZEC	-	Jan 9 12:44:44

QEDIT.COM ID

# Viewing Keys

Example: Zcash/Orchard viewing keys

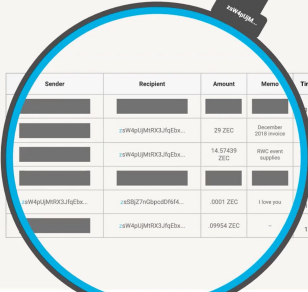
- The viewing key will reveal the entire history
- The revealed in/out addresses are re-randomized
- Currently, decryption using the viewing keys is not guaranteed by the consensus.





Work in  
progress

Viewing Keys

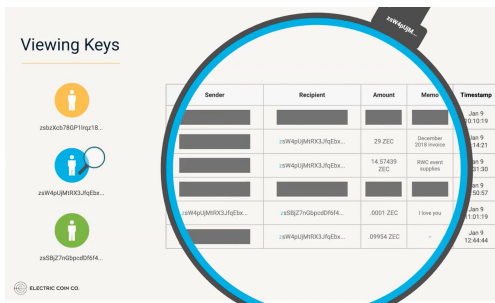


Sender	Recipient	Amount	Message	Timestamp
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Jan 9 13:10:19
[REDACTED]	[REDACTED]	29 ZEC	December 2018 invoice	Jan 9 14:21
[REDACTED]	[REDACTED]	14.57429 ZEC	2018 month invoice	Jan 9 15:30
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Jan 9 16:57
uW4y4j9W9KXUj9f3k...	zxB9jZ7nQ2pud8f6A...	0001 ZEC	I love you	Jan 9 13:15:19
[REDACTED]	[REDACTED]	0954 ZEC	-	Jan 9 12:44:44

ELECTRIC COIN CO

# Enhanced viewing keys on top of OrchardZSA

- ZSA is an extension of the Orchard protocol to allow permissionless issuance and transfer of user defined assets.



# Enhanced viewing keys on top of OrchardZSA

- ZSA is an extension of the Orchard protocol to allow permissionless issuance and transfer of user defined assets.

$\text{NoteCommit}_{\text{rcm}}^{\text{OrchardZSA}}(g_d^*, pk_d^*, v, \rho, \psi, \text{AssetBase}^{\text{Orchard}})$

Viewing Keys

Sender	Recipient	Amount	Memo	Timestamp
[redacted]	[redacted]	[redacted]	[redacted]	Jan 9 13:10:19
[redacted]	[redacted]	29 ZEC	December 2018 invoice	Jan 9 14:21
[redacted]	[redacted]	14.57429 ZEC	[redacted]	Jan 9 15:30
[redacted]	[redacted]	[redacted]	[redacted]	Jan 9 16:57
[redacted]	[redacted]	0.001 ZEC	I love you	Jan 9 13:15:19
[redacted]	[redacted]	0.0954 ZEC	[redacted]	Jan 9 12:44:44

# Enhanced viewing keys on top of OrchardZSA

- ZSA is an extension of the Orchard protocol to allow permissionless issuance and transfer of user defined assets.

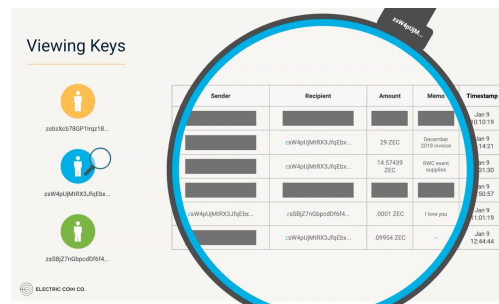
$\text{NoteCommit}_{\text{rcm}}^{\text{OrchardZSA}}(g_d^*, pk_d^*, v, \rho, \psi, \text{AssetBase}^{\text{Orchard}})$

$\text{assetDigest} \leftarrow \text{Blake2b512}(\dots ||ik|| \text{asset\_desc})$

“Issuer public key”

Description

Viewing Keys



Tender	Recipient	Amount	Memo	Timestamp
████████████████████	████████████████████	████████	████████	Jan 9 13:19
████████████████████	████████████████████	29 ZEC	December 2018 invoice	Jan 9 14:21
████████████████████	████████████████████	14.57429 ZEC	████████	Jan 9 15:30
████████████████████	████████████████████	0001 ZEC	I love you	Jan 9 15:57
████████████████████	████████████████████	0954 ZEC	████████	Jan 9 15:19
████████████████████	████████████████████	████████	████████	Jan 9 12:44:44

# Enhanced viewing keys on top of OrchardZSA

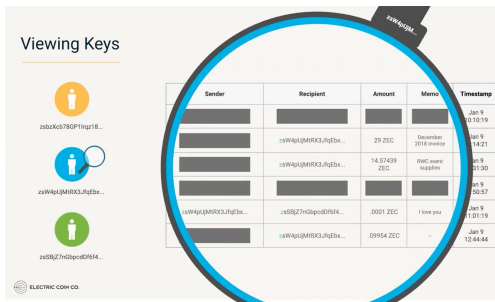
- ZSA is an extension of the Orchard protocol to allow permissionless issuance and transfer of user defined assets.

$\text{NoteCommit}_{\text{rcm}}^{\text{OrchardZSA}}(g_d^*, pk_d^*, v, \rho, \psi, \text{AssetBase}^{\text{Orchard}})$

$\text{assetDigest} \leftarrow \text{Blake2b512}(\dots ||ik|| \text{asset\_desc})$

$\text{assetBase} \leftarrow \text{GroupHash}(\text{assetDigest})$

Viewing Keys

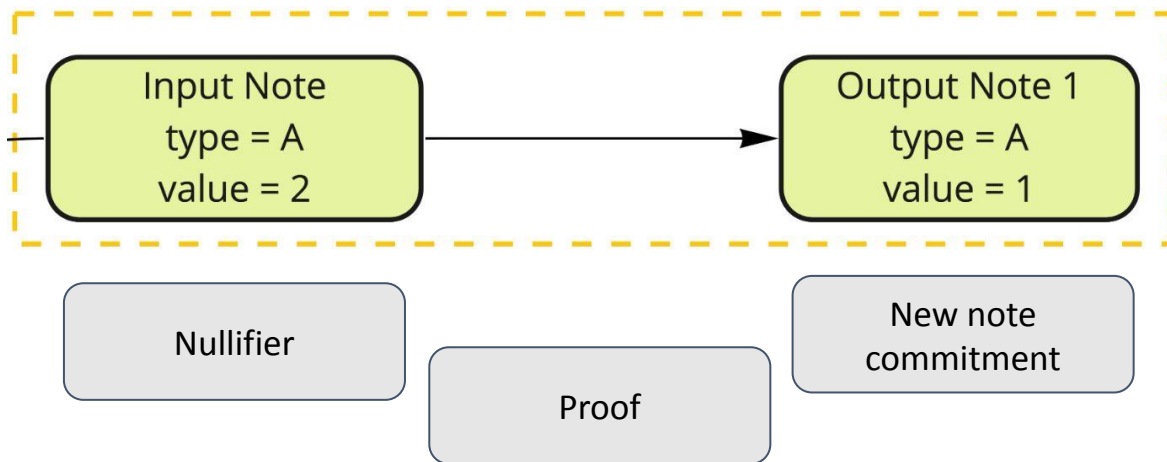


Tender	Recipient	Amount	Memo	Timestamp
				Jan 9 13:10:19
		29 ZEC	December 2018 invoice	Jan 9 14:21
		14.57429 ZEC	2018 month invoice	Jan 9 15:30
				Jan 9 16:57
		0001 ZEC	I love you	Jan 9 18:19
		0954 ZEC		Jan 9 12:44:44

ELECTRIC COIN CO

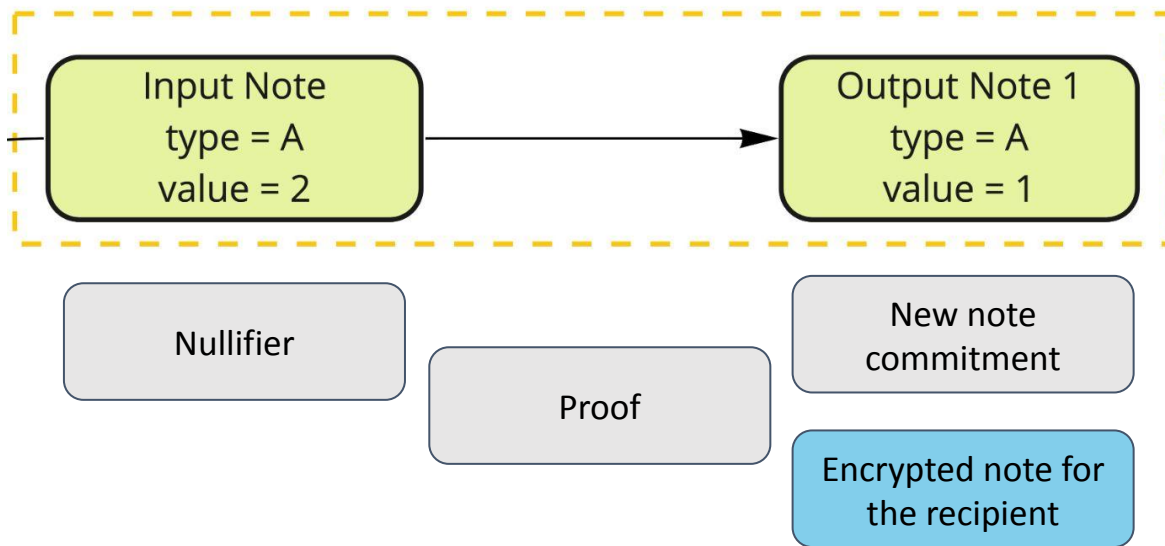
# Enhanced viewing keys on top of OrchardZSA

- OrchardZSA Action:



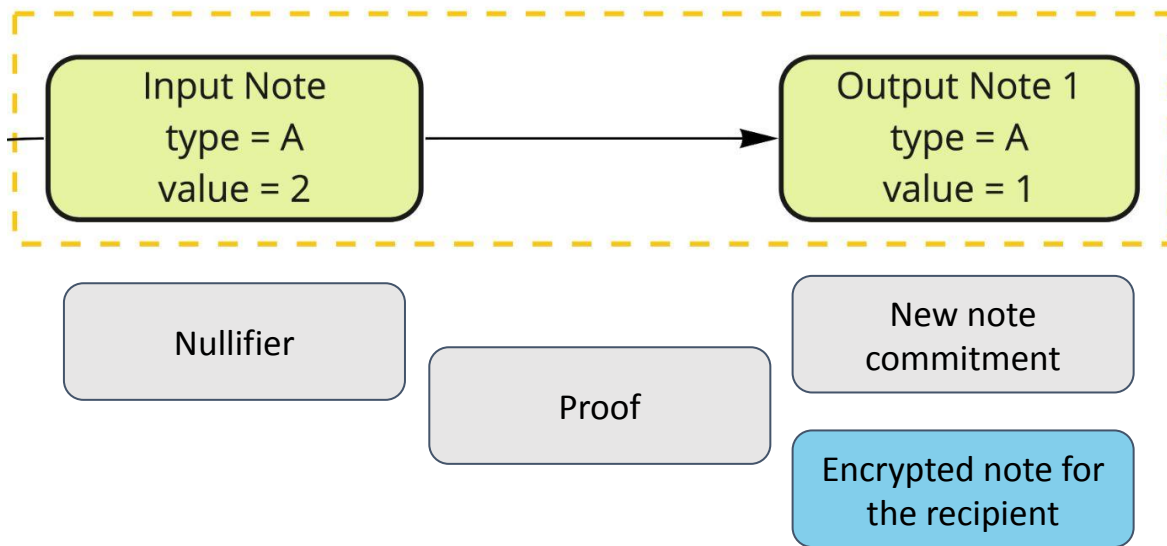
# Enhanced viewing keys on top of OrchardZSA

- OrchardZSA Action:



# Enhanced viewing keys on top of OrchardZSA

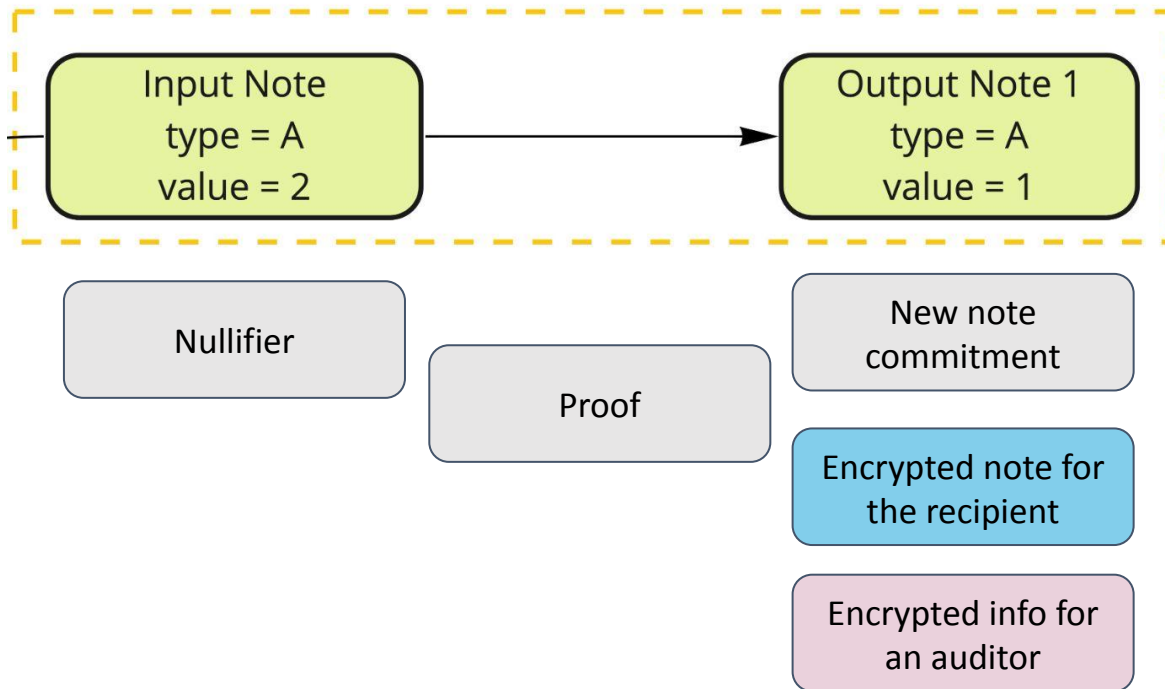
- OrchardZSA Action:





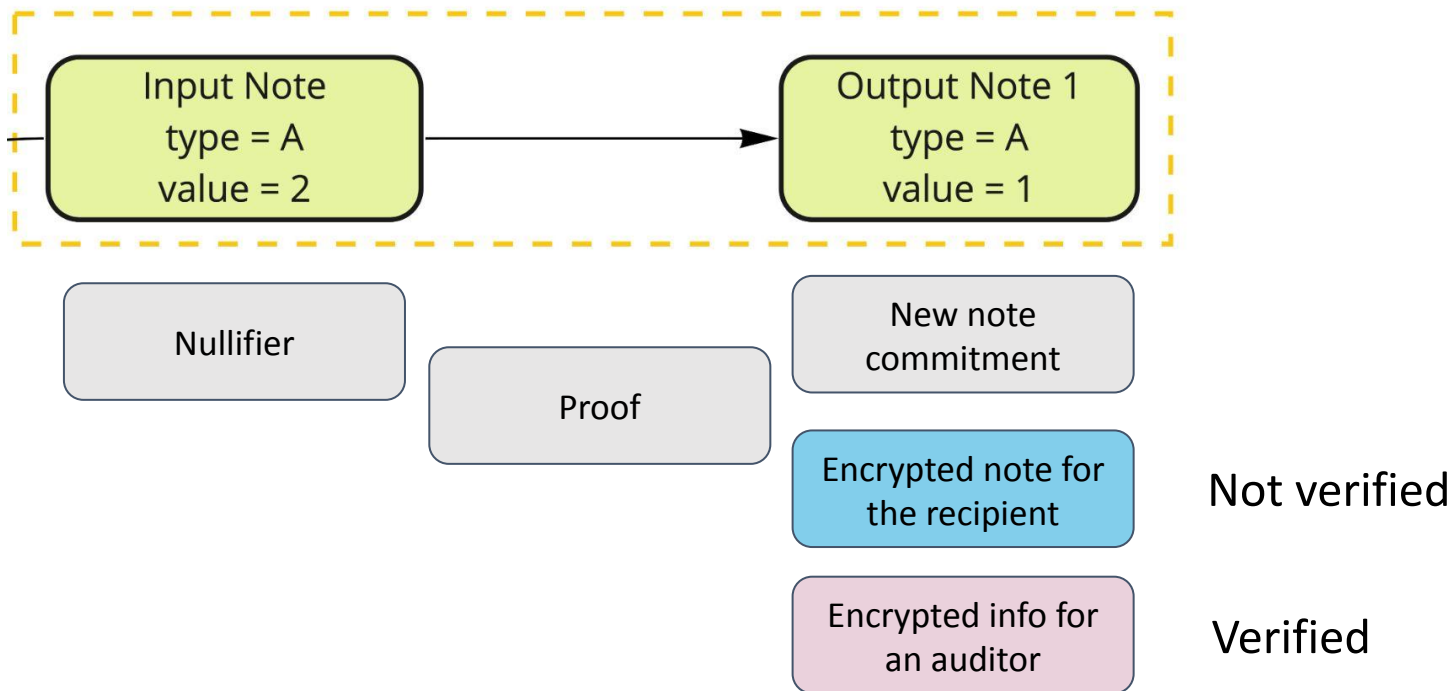
# Enhanced viewing keys on top of OrchardZSA

- OrchardZSA Action with auditability:



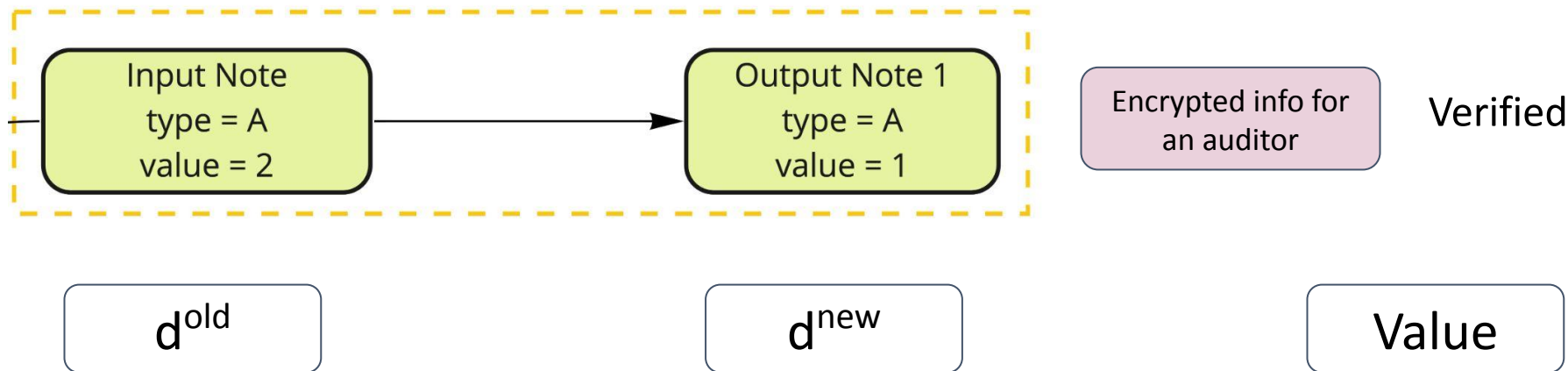
# Enhanced viewing keys on top of OrchardZSA

- OrchardZSA Action with auditability:



# Enhanced viewing keys on top of OrchardZSA

- Plaintext for the auditor info:



# Enhanced viewing keys on top of OrchardZSA

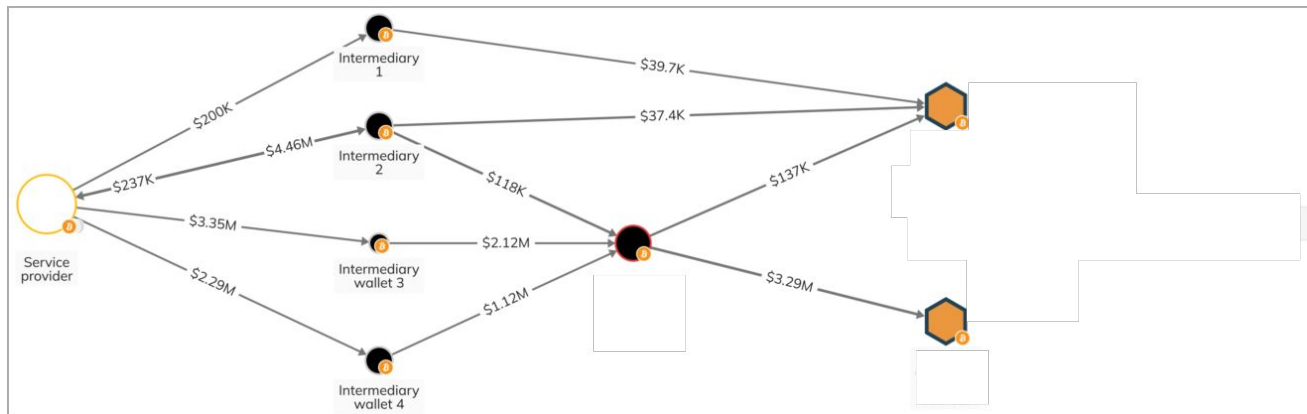
- Plaintext for the auditor info

$d^{\text{old}}$

$d^{\text{new}}$

Value

- Will allow the auditor “bitcoin style graph-analysis” **only for this assetBase**



# Enhanced viewing keys on top of OrchardZSA



Encrypted info for  
an auditor

**Verified**

The plaintext is constructed correctly

# Enhanced viewing keys on top of OrchardZSA



Encrypted info for  
an auditor

**Verified**

The plaintext is constructed correctly

- $d^{\text{old}} \leftrightarrow (\text{nf}, \text{nk}, \rho, \psi, \text{cmx}^{\text{old}}, \dots)$

Instance

Witness

# Enhanced viewing keys on top of OrchardZSA



The plaintext is constructed correctly

- $d^{\text{old}} \leftrightarrow (\text{nf}, \dots)$
- $d^{\text{new}} \leftrightarrow (\text{cmx}, \dots)$

# Enhanced viewing keys on top of OrchardZSA



Encrypted info for  
an auditor

**Verified**

The plaintext is constructed correctly

- $d^{\text{old}} \leftrightarrow (\text{nf}, \dots)$
- $d^{\text{new}} \leftrightarrow (\text{cmx}, \dots)$
- $v \leftrightarrow (\text{cmx}, \dots)$



# Enhanced viewing keys on top of OrchardZSA



The plaintext is constructed correctly

- $d^{\text{old}} \leftrightarrow (\text{nf}, \dots)$
- $d^{\text{new}} \leftrightarrow (\text{cmx}, \dots)$
- $v \leftrightarrow (\text{cmx}, \dots)$

OR  $m^{\text{audit}} := d^{\text{old}} \mid d^{\text{new}} \mid v \leftrightarrow (\text{nf}, \text{cmx}, \dots)$

# Enhanced viewing keys on top of OrchardZSA

The ciphertext is constructed correctly

C

Verified

$$C = \text{Enc}_k(m^{\text{audit}})$$

- $P = m^{\text{audit}}$

# Enhanced viewing keys on top of OrchardZSA

The ciphertext is constructed correctly

C

Verified

$$C = \text{Enc}_k(m^{\text{audit}})$$

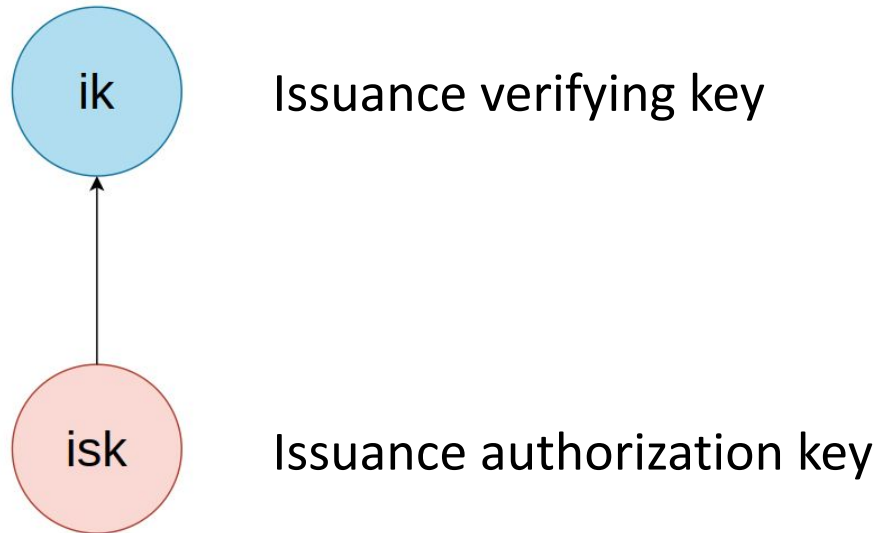
- $P = m^{\text{audit}}$
- Encrypted to the “*correct auditor*” using the “*correct key*”

# The ciphertext is constructed correctly

- OrchardZSA issuance keys

Encrypted info for  
an auditor

**Verified**

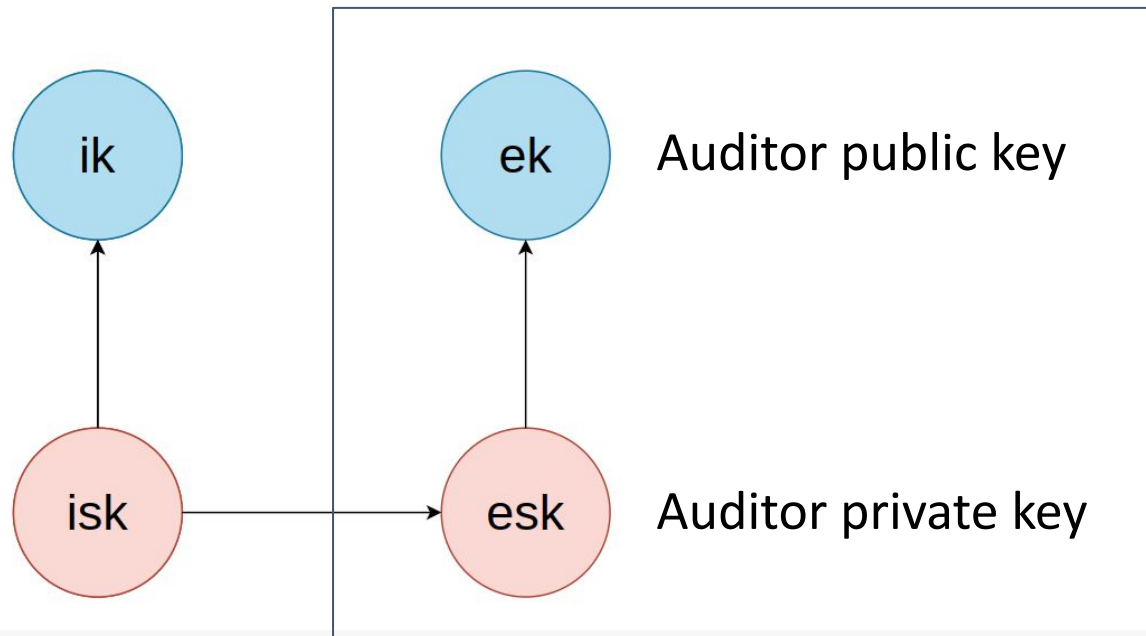


# The ciphertext is constructed correctly

- Auditor key derivation

Encrypted info for  
an auditor

**Verified**

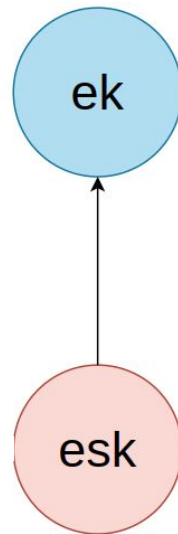
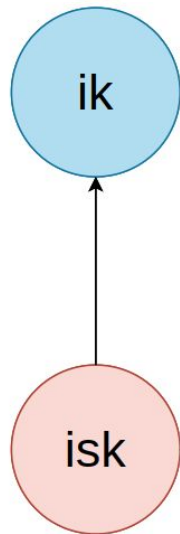


# The ciphertext is constructed correctly

- Auditor key derivation

Encrypted info for  
an auditor

**Verified**



Auditor public key

Auditor private key

# The ciphertext is constructed correctly

- OrchardZSA AssetBase derivation

Encrypted info for  
an auditor

**Verified**

$$assetDigest \leftarrow \text{Blake2b512}(\dots ||ik||asset\_desc)$$
$$assetBase \leftarrow \text{GroupHash}(assetDigest)$$

# The ciphertext is constructed correctly

- OrchardZSA with compliance

Encrypted info for  
an auditor

**Verified**

AssetBase derivation

$$assetDigest \leftarrow \text{Blake2b512}(\dots || ik || asset\_desc)$$
$$assetBase \leftarrow \text{GroupHash}(assetDigest) + \text{GroupHash}(ek)$$

Auditor public key





# Enhanced viewing keys on top of OrchardZSA

The ciphertext is constructed correctly

C

Verified

$$C = \text{Enc}_k(m^{\text{audit}})$$

- $P = m^{\text{audit}}$
- Encrypted to the “*correct auditor*” using the “*correct key*”

# Enhanced viewing keys on top of OrchardZSA

The ciphertext is constructed correctly

C

Verified

$$C = \text{Enc}_{ek}(m^{\text{audit}})$$

- $P = m^{\text{audit}}$

Instance

Witness

- $\text{Enc}_{ek}(m^{\text{audit}}) \leftrightarrow (\text{cmx}, \dots, \text{assetBase}, ek, \dots)$

# Enhanced viewing keys on top of OrchardZSA

The ciphertext is constructed correctly

C

Verified

$$C = \text{Enc}_{ek}(m^{\text{audit}})$$

Asymmetric encryption can be replaced with symmetric encryption (at a cost)

- $P = m^{\text{audit}}$

Instance

Witness

- $\text{Enc}_{ek}(m^{\text{audit}}) \leftrightarrow (\text{cmx}, \dots, \text{assetBase}, ek, \dots)$

# Enhanced viewing keys on top of OrchardZSA

Challenge :

Encrypted info for  
an auditor

**Verified**

- The encryption scheme should be quantum secure (QS privacy)

# Enhanced viewing keys on top of OrchardZSA

Challenge :

Encrypted info for  
an auditor

**Verified**

- Model the selected encryption scheme as a ZK proof system circuit

# Enhanced viewing keys on top of OrchardZSA

Challenge :

Encrypted info for  
an auditor

**Verified**

- Model the selected encryption scheme as a ZK proof system circuit

Pilot: [Verifiable encryption using Halo2 \(link\)](#)

# Enhanced viewing keys on top of OrchardZSA

Open question :

Encrypted info for  
an auditor

**Verified**

- What is the *proof size* and *proof generation time* ?

# Enhanced viewing keys on top of OrchardZSA

Open question :

Encrypted info for  
an auditor

**Verified**

- Do we extend the existing Orchard circuit with the new logic (*efficiency gain*, cmx) or separate into a new circuit (*modularity*) ?



# Enhanced viewing keys on top of OrchardZSA

Open question :

Encrypted info for  
an auditor

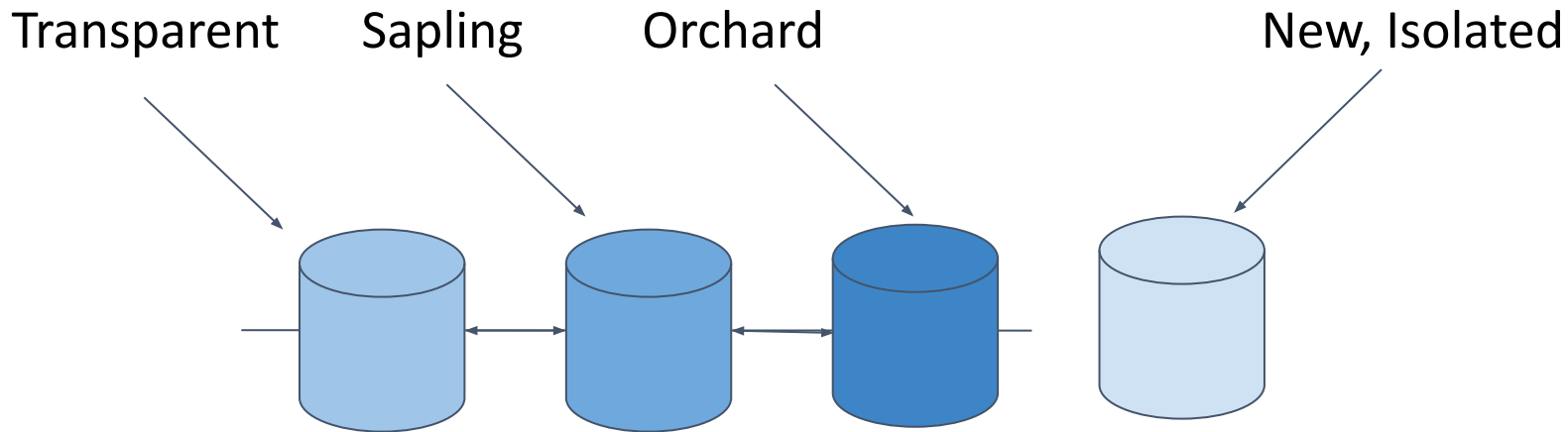
**Verified**

- Do we require indistinguishability from a regular transfer  
(at a significant cost)?

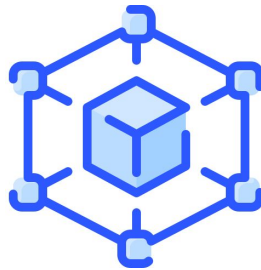
# Enhanced viewing keys on top of OrchardZSA

Open question :

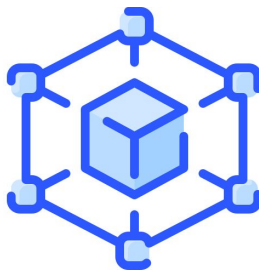
- If not, do we create a separate pool for “compliant assets”?



# Questions ?



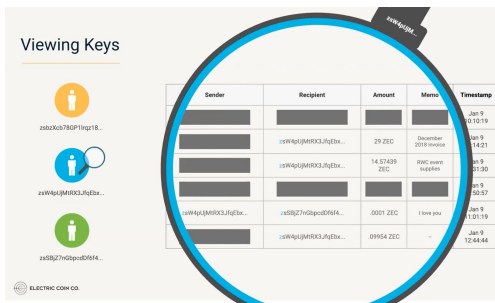
Thank you



# Viewing Keys

Example: Zcash/Orchard viewing keys, **Potential improvements**

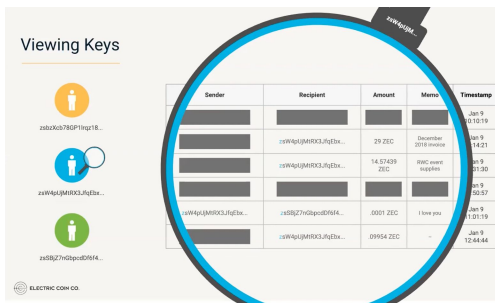
- Enforcement by the protocol
  - Need to ensure properties of the plaintext



# Viewing Keys

Example: Zcash/Orchard viewing keys, **Potential improvements**

- Enforcement by the protocol
  - Need to ensure properties of the plaintext
  - ZK or Verifiable encryption

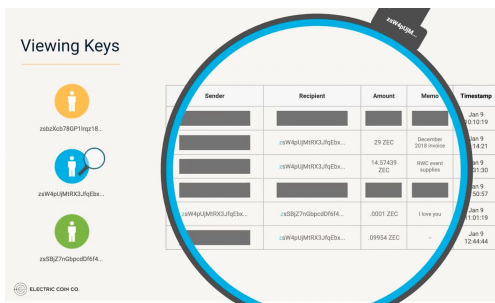


# Viewing Keys

Example: Zcash/Orchard viewing keys, **Potential improvements**

- (Provable) Granularity

Viewing Keys



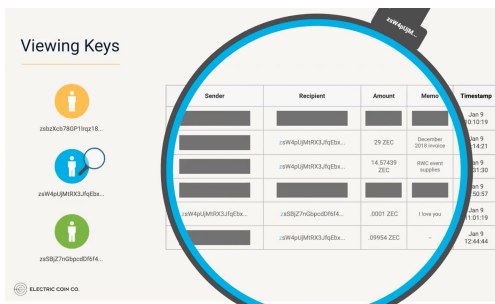
Sender	Recipient	Amount	Message	Timestamp
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Jan 9 13:10:19
[REDACTED]	z58kqjg9h9KXUj9f3Bx...	29 ZEC	December 2018 invoice	Jan 9 14:21
[REDACTED]	z58kqjg9h9KXUj9f3Bx...	14.57429 ZEC	2018 month invoice	Jan 9 15:30
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Jan 9 16:57
uW4y4jM9KXUj9f3Bx...	z58BjZ7nQ2p0d8f6A...	0001 ZEC	I love you	Jan 9 13:15:19
[REDACTED]	z58kqjg9h9KXUj9f3Bx...	0954 ZEC	-	Jan 9 12:44:44

ELASTIC COIN CO

# Viewing Keys

Example: Zcash/Orchard viewing keys, **Potential improvements**

- Disable address re-randomization (On per-asset basis)

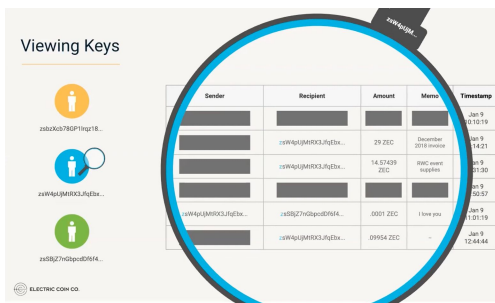




# Viewing Keys

Example: Zcash/Orchard viewing keys, **Potential improvements**

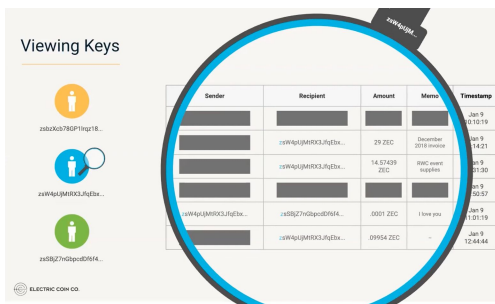
- Global viewing key (On per-asset basis)



# Viewing Keys

Example: Zcash/Orchard viewing keys, **Potential improvements**

- Global viewing key (On per-asset basis)
- Potentially split between multiple parties (SS)
  - I.E. The regulator and the issuer



Viewing Keys

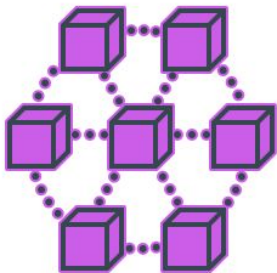
Sender	Recipient	Amount	Message	Timestamp
[Redacted]	[Redacted]	[Redacted]	[Redacted]	Jan 9 13:10:19
[Redacted]	[Redacted]	29 ZEC	December 2018 invoice	Jan 9 14:21
[Redacted]	[Redacted]	14.57429 ZEC	2018, current invoice	Jan 9 15:30
[Redacted]	[Redacted]	[Redacted]	[Redacted]	Jan 9 16:57
[Redacted]	[Redacted]	0001 ZEC	I love you	Jan 9 17:19
[Redacted]	[Redacted]	0954 ZEC	[Redacted]	Jan 9 17:44:44

ELECTRIC COIN CO.

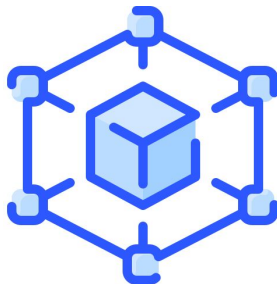
# Setting the scene

- Three types of systems

Public blockchain



Payment service



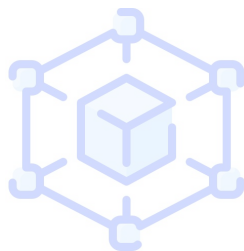
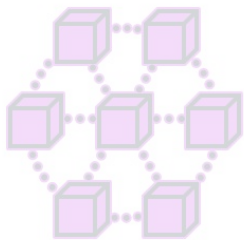
CBDC



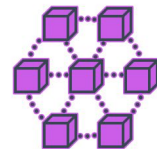
# Privacy budget – applicability

In the context of a **CBDC**

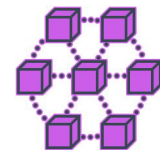
- A well-defined central authority to assign the privacy tokens
- A well-defined set of approved users on the receiving end



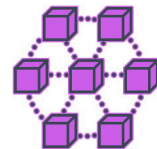
# Methodology for real world testing



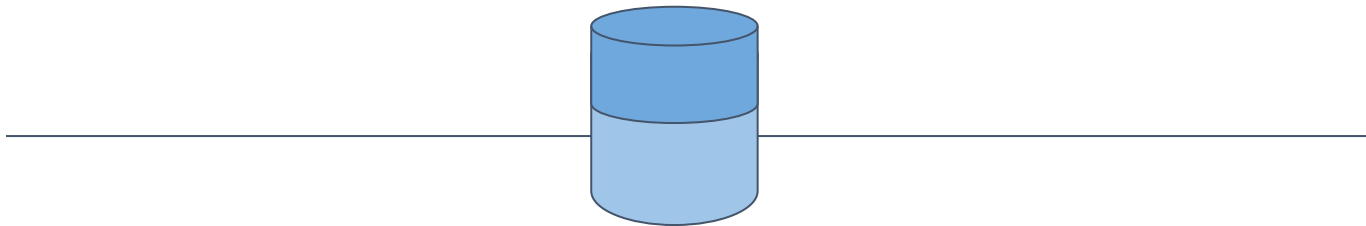
- No one-size fits-all solution



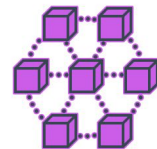
- Host multiple assets with different privacy/compliance guarantees on a single blockchain



- Host multiple assets with different privacy/compliance guarantees on a single blockchain



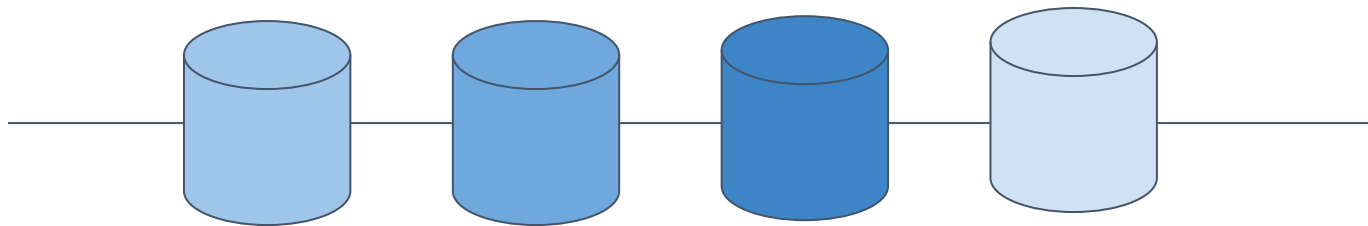
Control compliance feature using issuance flags



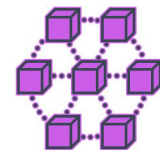


# Methodology for real world testing

- Host multiple assets with different privacy/compliance guarantees on a single blockchain

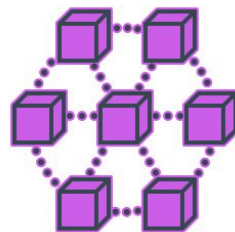
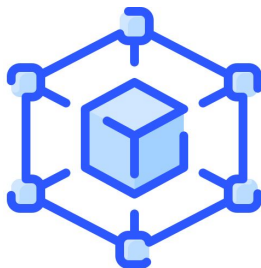


Same blockchain, multiple shielded pools



# Conclusion

- We have the cryptographic building blocks to balance compliance and privacy.



■ Thank you!

Compliance feature: Blacklist enforcement

Desired properties:

- Ability to freeze funds for a suspicious address
- Unfreeze if suspicion was removed



Potential approach assuming cryptographic accumulators

- An authority commits the **updated** accumulator digest to the chain

Potential approach assuming cryptographic accumulators

- An authority commits the **updated** accumulator digest to the chain
- Sender produces a non-membership proof for
  - The canonical address
  - And / Or
  - The re-randomized address

Potential approach assuming cryptographic accumulators

- An authority commits the **updated** accumulator digest to the chain
- Sender produces a non-membership proof for

- The canonical address

And / Or

- The re-randomized address

Guarantee: Sender is not blacklisted at the time of the transfer.



## Advantages

- Privacy preserving (verifier learns nothing except non-inclusion)
- User friendly (if legit, can be removed from the blacklist)

## Advantages

- Privacy preserving
- User friendly

## Disadvantages

- Who controls the blacklist? (consider a committee or a per-asset authority)
- Blacklisting re-randomized addresses might not be effective and there is a difficulty deduce the canonical address (consider removing re-randomization)

Direct applicability for a shielded Public blockchain

