VIRTCRIME

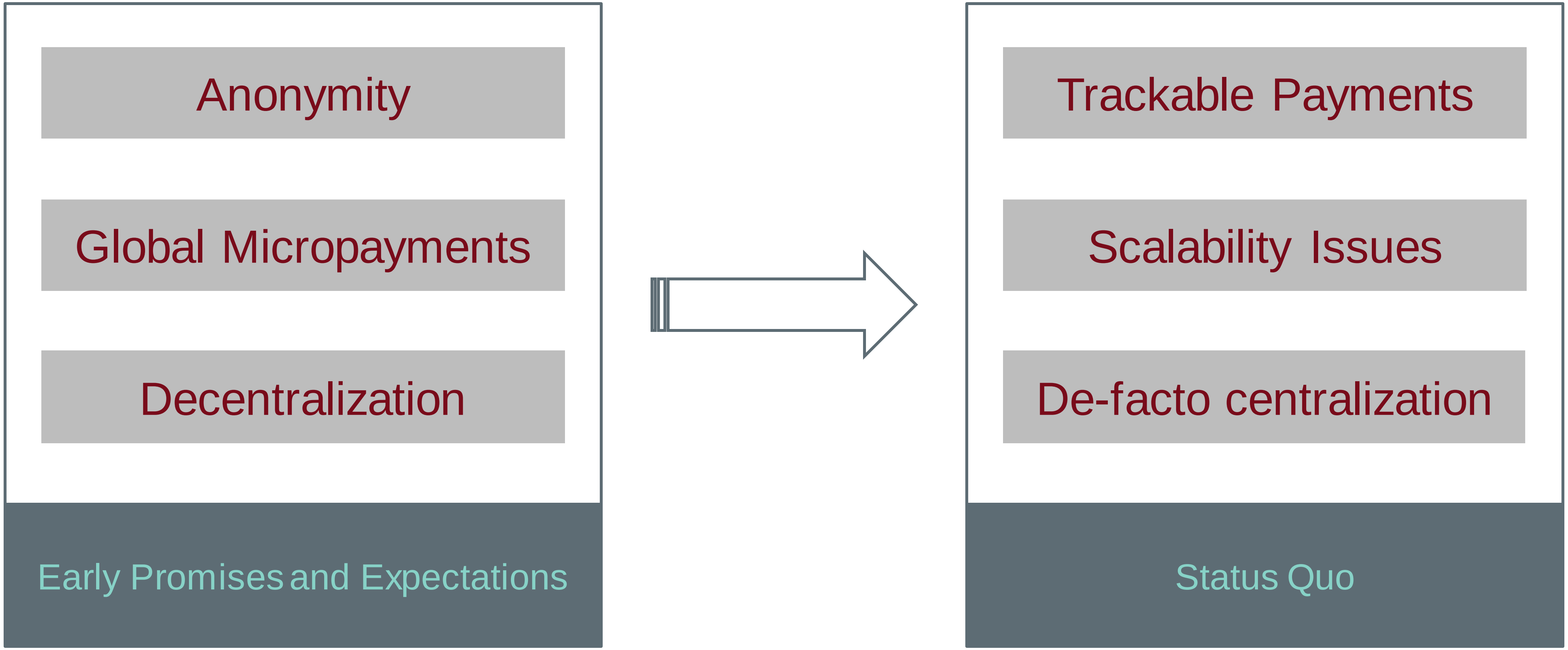
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

MONERO AND ZCASH TUTORIAL

VIRTCRIME Training Event
Innsbruck, November 8th 2019

Dr. Bernhard Haslhofer
Senior Scientist
Center for Digital Safety & Security

INSIGHTS | GENERAL OBSERVATIONS



Anonymity

Global Micropayments

Decentralization

Early Promises and Expectations

Trackable Payments

Scalability Issues

De-facto centralization

Status Quo

PRIVACY ENHANCING CRYPTOCURRENCIES

Monero

Stealth addresses
Ring signatures
Ring CTs

ZCash

Shielded transactions

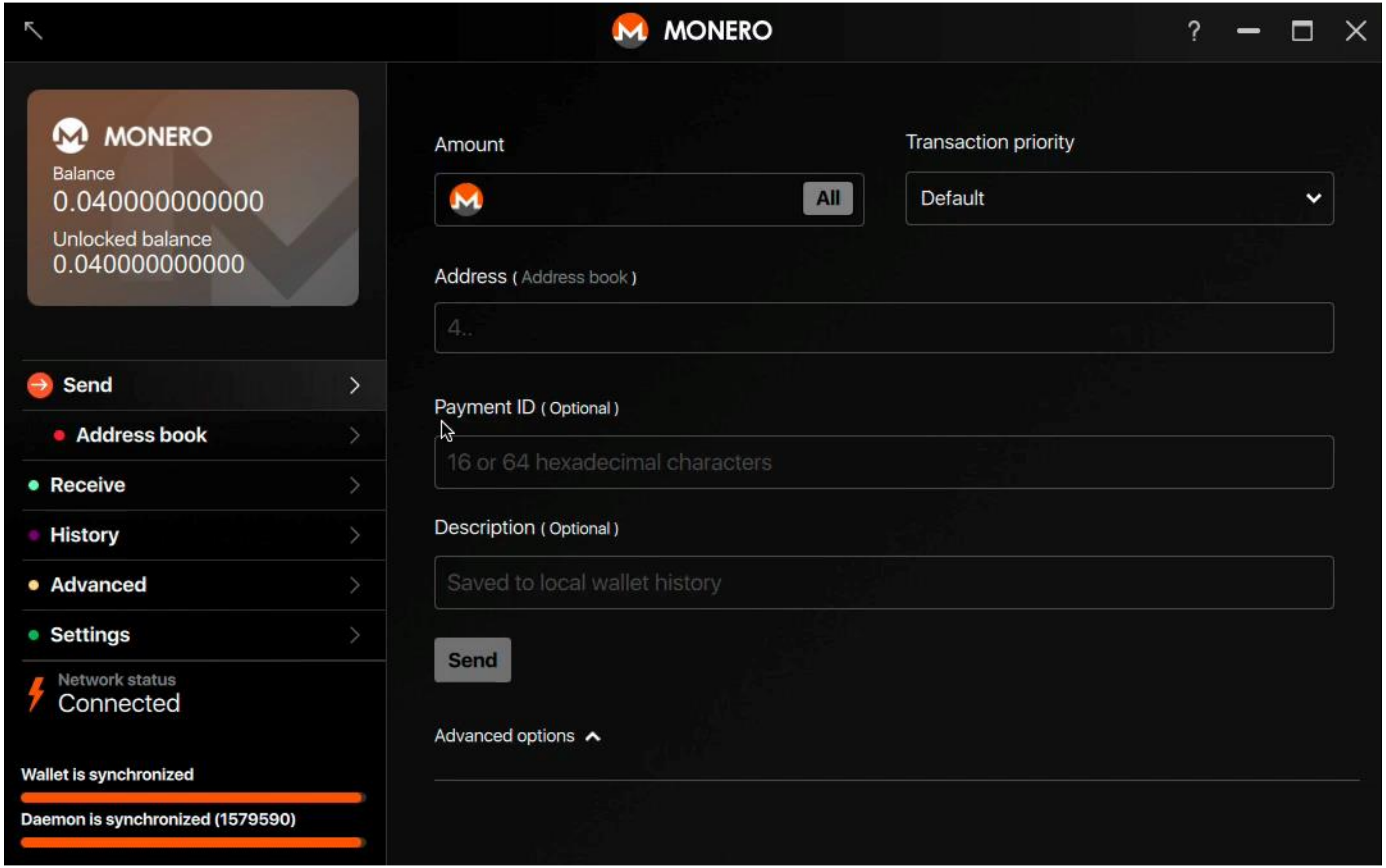
Dash

Private Send

MONERO

- One of the first and the most widely adopted CryptoNote currency
  - “An open source technology and concepts for the cryptocurrencies of the future”
  - Untraceable payments
  - Unlinkable transactions
  - Egalitarian proof of work
  - …
- https://cryptonote.org/coins

MONERO | EXAMPLE TRANSACTION



MONERO

Balance
0.040000000000

Unlocked balance
0.040000000000

Send
Address book
Receive
History
Advanced
Settings

Network status
Connected

Wallet is synchronized

Daemon is synchronized (1579590)

Amount: All

Transaction priority: Default

Address (Address book): 4..

Payment ID (Optional): 16 or 64 hexadecimal characters

Description (Optional): Saved to local wallet history

Send

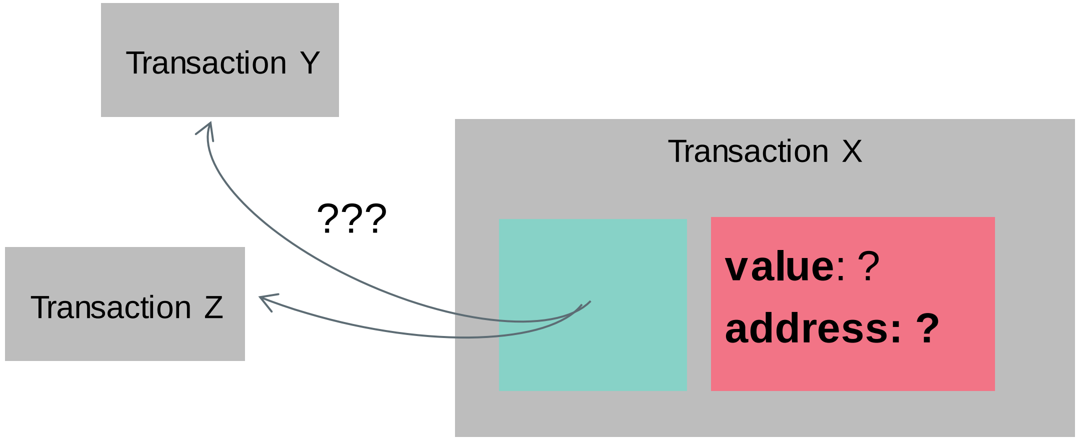
Advanced options

MONERO | SECURITY FEATURES

- Stealth addresses: outside observers do not know which addresses certain transaction outputs are assigned to

- Ring signatures: hide spent output among seemingly plausible ones

- Ring confidential transactions (Ring CTs): hide transaction amount

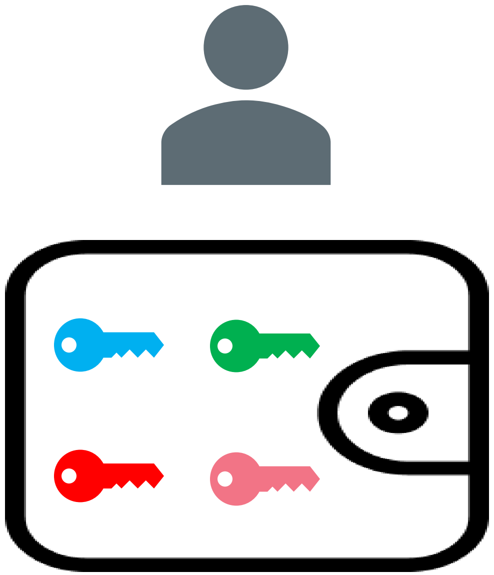


MONERO | KEYS

- Private spend key: for signing transactions and spending funds
- Private view key: view all transaction related to account (can be shared to see balance)
- Public spend key: part of Monero account address
- Public view key: part of Monero account address

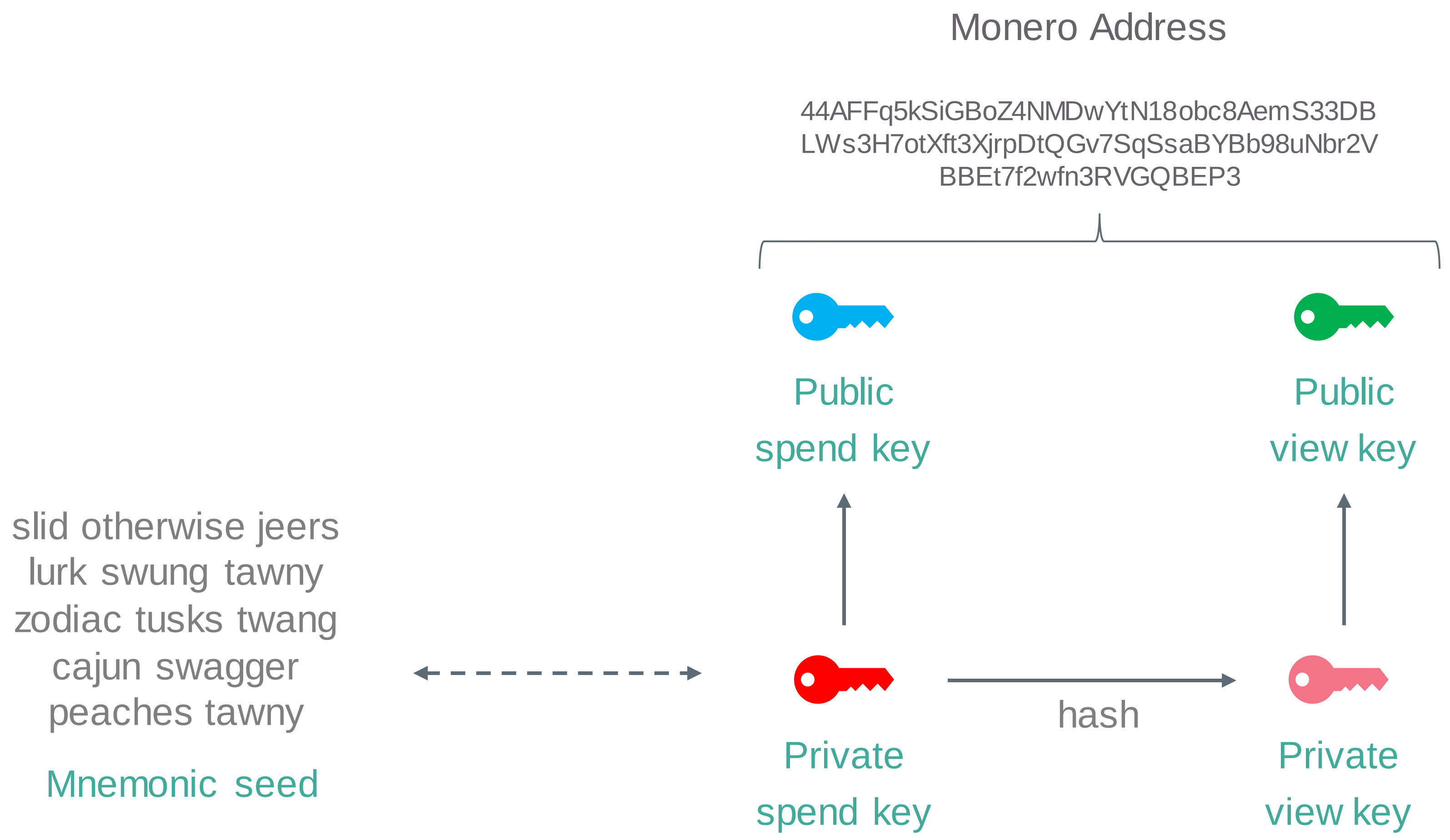
Monero Address

44AFFq5kSiGBoZ4NMDwYtN18obc8AemS33DB
LWs3H7otXft3XjrpDtQGv7SqSsaBYBb98uNbr2V
BBEt7f2wfn3RVGQBEP3



Monero Account

MONERO | KEY RELATIONSHIPS



Monero Address

44AFFq5kSiGBoZ4NMDwYtN18obc8AemS33DB
LWs3H7otXft3XjrpDtQGv7SqSsaBYBb98uNbr2V
BBEt7f2wfn3RVGQBEP3

Public spend key

Public view key

slid otherwise jeers
lurk swung tawny
zodiac tusks twang
cajun swagger
peaches tawny

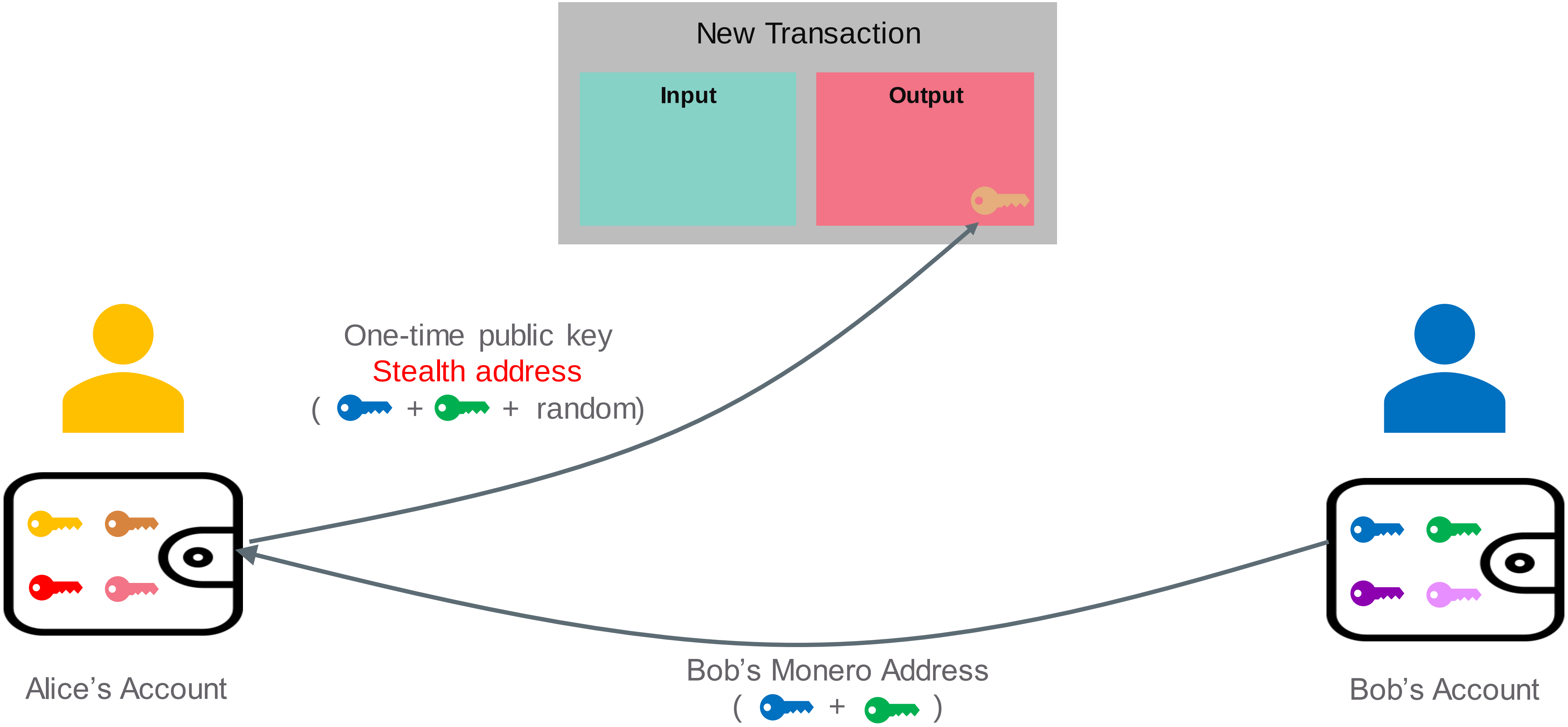
Mnemonic seed

hash

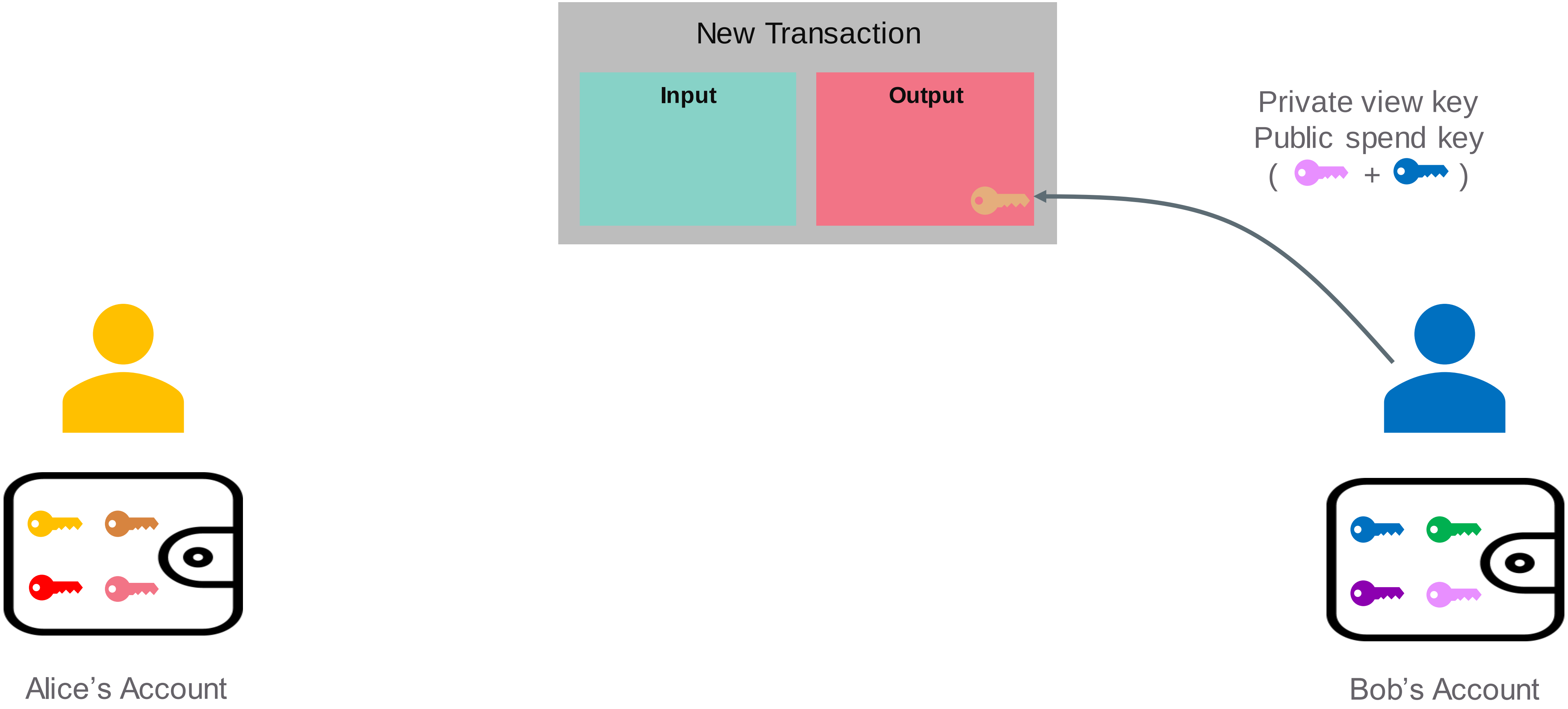
Private spend key

Private view key

MONERO | STEALTH ADDRESS



MONERO | VIEW OUTPUT(S)



New Transaction

Input

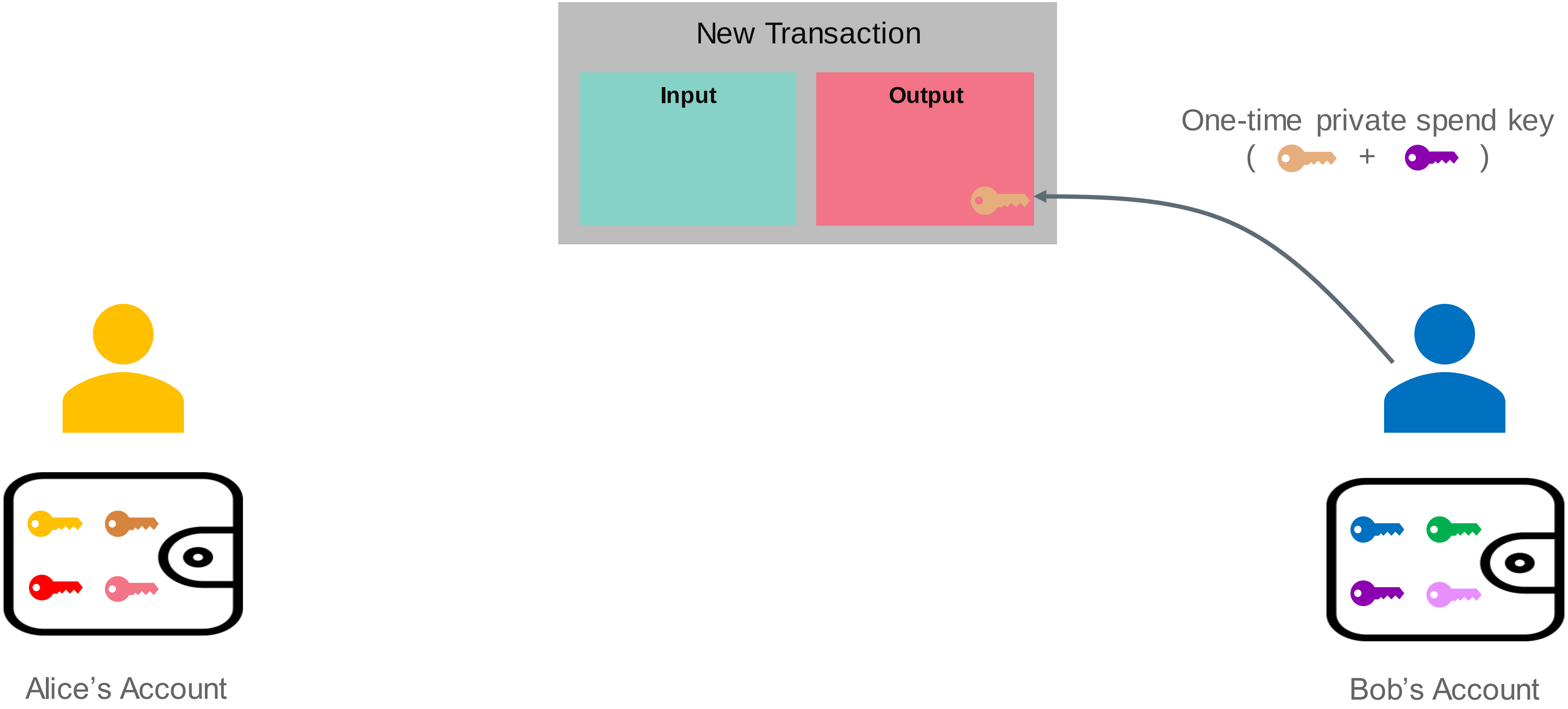
Output

Private view key
Public spend key
(+)

Alice’s Account

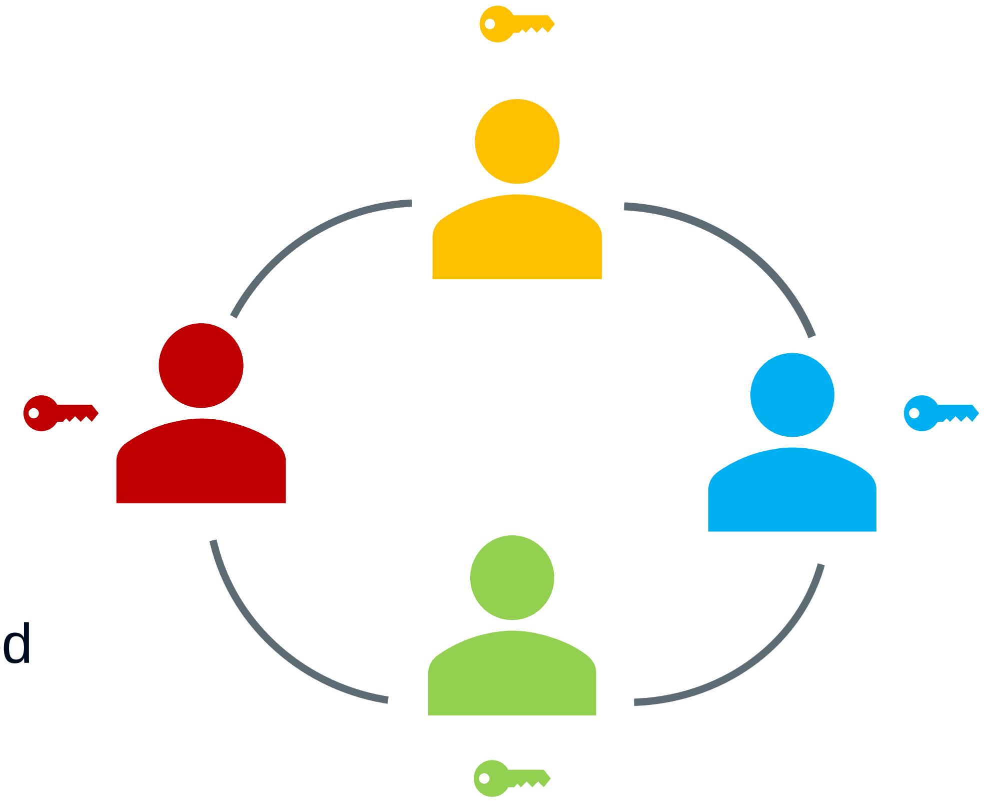
Bob’s Account

MONERO | SPEND OUTPUT(S)

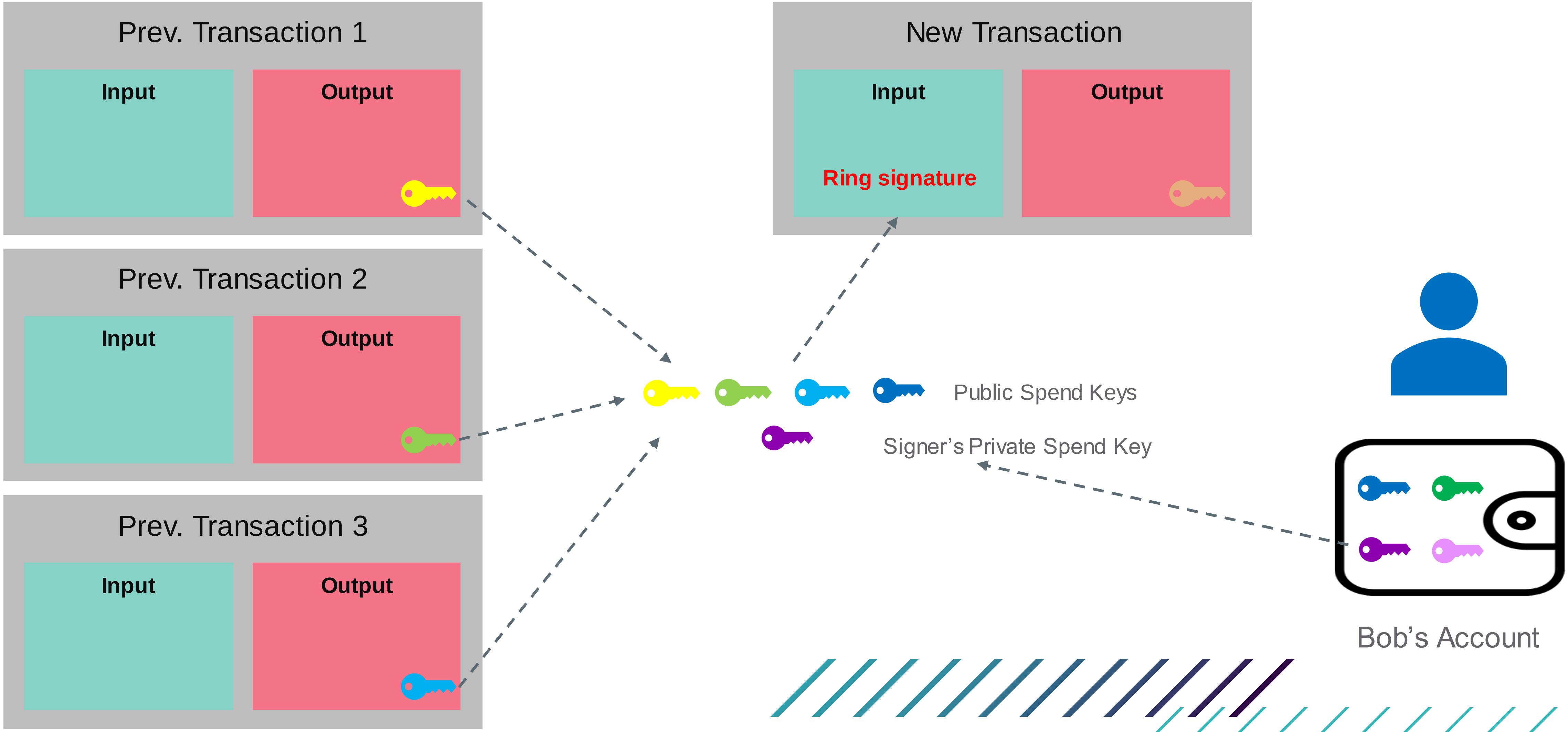


MONERO | RING SIGNATURES

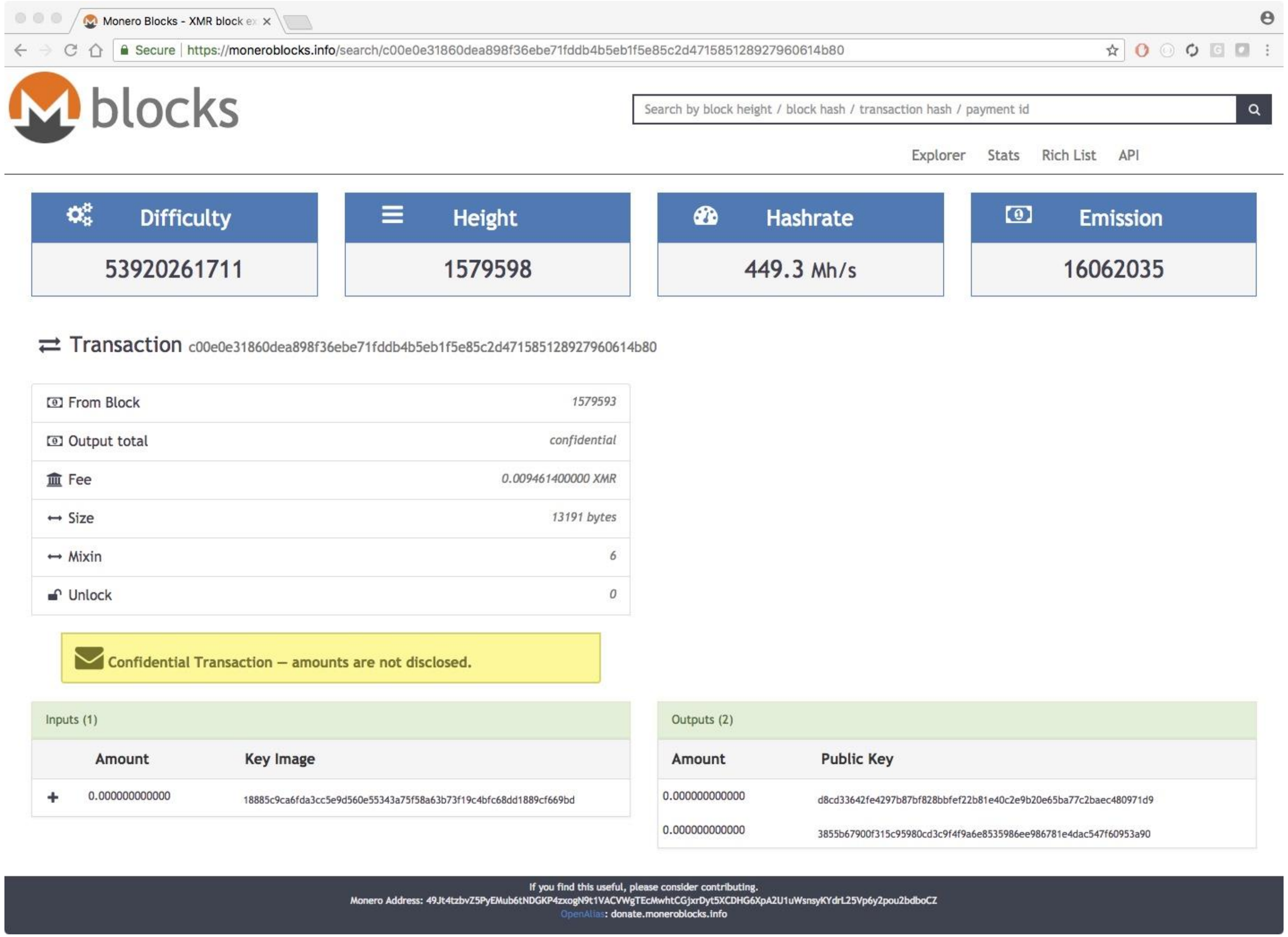
- A type of signature that can be performed by any member of a group
- Each user has private / public key pairs
- Signature is created from a number of public keys
- Message signed with ring signature is endorsed by someone in a particular group of people
- Not possible to compute which of the group members’ keys as used to produce signature



MONERO | RING SIGNATURES



MONERO | INSPECT EXAMPLE TRANSACTION


Monero Blocks - XMR block ex
Secure
https://moneroblocks.info/search/c00e0e31860dea898f36ebe71fddb4b5eb1f5e85c2d471585128927960614b80
blocks
Search by block height / block hash / transaction hash / payment id
Explorer
Stats
Rich List
API

Difficulty	Height	Hashrate	Emission
53920261711	1579598	449.3 Mh/s	16062035

Transaction c00e0e31860dea898f36ebe71fddb4b5eb1f5e85c2d471585128927960614b80

From Block	*1579593*
Output total	*confidential*
Fee	*0.009461400000 XMR*
Size	*13191 bytes*
Mixin	*6*
Unlock	*0*

Confidential Transaction — amounts are not disclosed.

Inputs (1)

	Amount	Key Image
+	0.000000000000	18885c9ca6fda3cc5e9d560e55343a75f58a63b73f19c4bfc68dd1889cf669bd

Outputs (2)

Amount	Public Key
0.000000000000	d8cd33642fe4297b87bf828bbfef22b81e40c2e9b20e65ba77c2baec480971d9
0.000000000000	3855b67900f315c95980cd3c9f4f9a6e8535986ee986781e4dac547f60953a90

If you find this useful, please consider contributing.
Monero Address: 49Jt4tzbvZ5PyEMub6tNDGKP4zxogN9t1VACVWgTEcMwhtCGjxrDyt5XCDHG6XpA2U1uWsnsyKYdrL25Vp6y2pou2bdboCZ
OpenAlias: donate.moneroblocks.info

ZCASH

- Bitcoin fork with optional anonymity
- Two transaction types
  - Transparent transactions (as in Bitcoin)
  - Shielded transactions (encrypted)
- Shielded transactions hide the sender, recipient, and the value on the blockchain
- Backed by highly regarded research

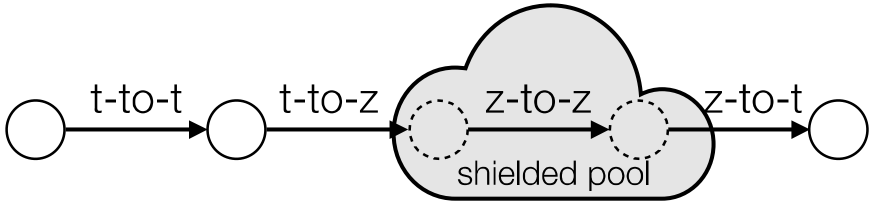
ZCASH | TRANSACTION TYPES

- t-to-t: visible quantities of ZEC move between visible t addresses

- t-to-z: a visible amount of ZEC moves from a visible t address to a hidden z address within the shielded pool

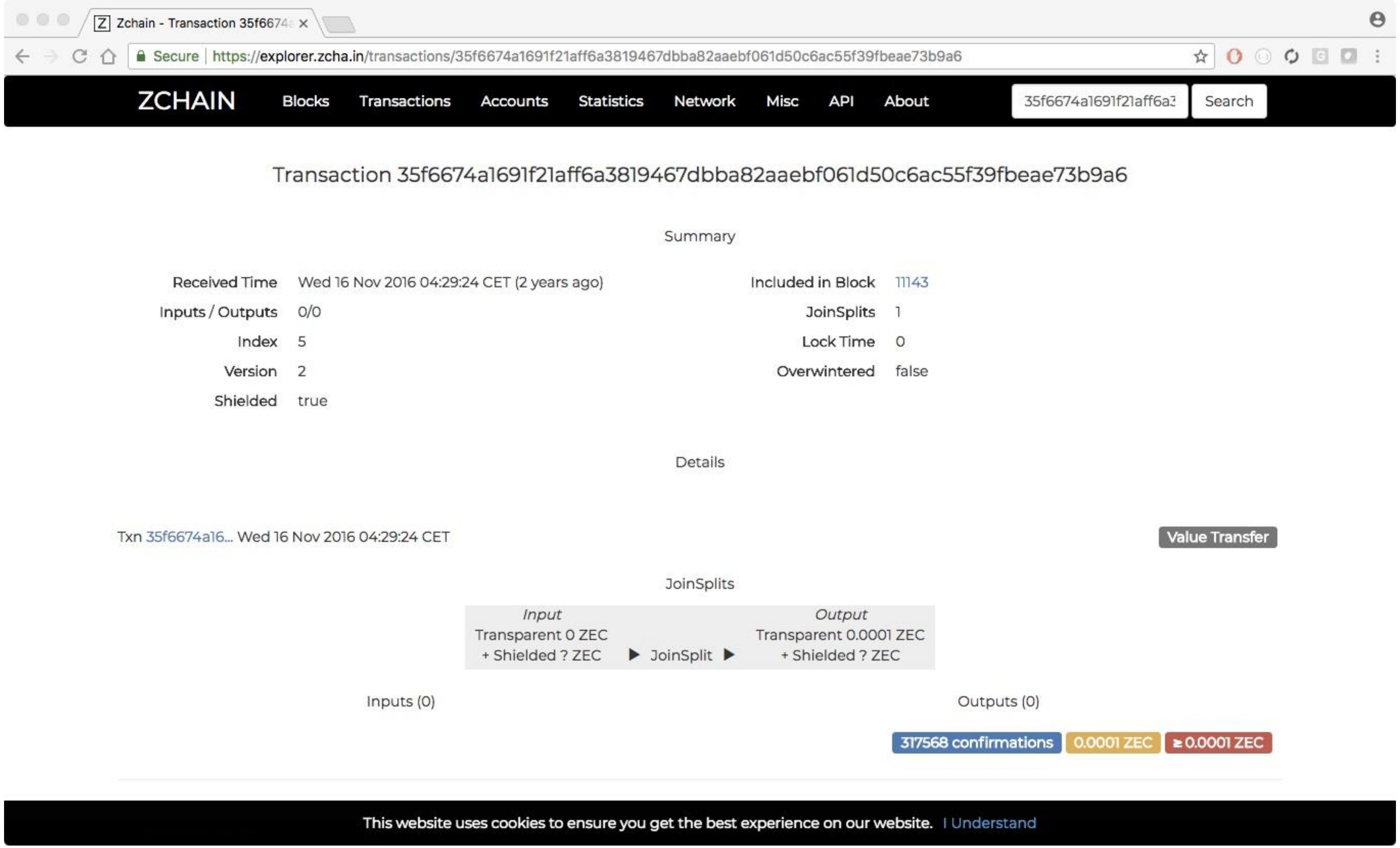
- z-to-z: a hidden quantity of ZEC moves between hidden z-addresses

- z-to-t: a hidden quantity of ZEC moves from a hidden z address out of the shielded pool to a visible t address



[Kappos et al. 2018]

ZCASH | SHIELDED TRANSACTION



Zchain - Transaction 35f6674a
Secure | https://explorer.zcha.in/transactions/35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbeae73b9a6
ZCHAIN
Blocks
Transactions
Accounts
Statistics
Network
Misc
API
About
35f6674a1691f21aff6a3
Search

Transaction 35f6674a1691f21aff6a3819467dbba82aaebf061d50c6ac55f39fbeae73b9a6

Summary

Received Time	Wed 16 Nov 2016 04:29:24 CET (2 years ago)	Included in Block	11143
Inputs / Outputs	0/0	JoinSplits	1
Index	5	Lock Time	0
Version	2	Overwintered	false
Shielded	true		

Details

Txn 35f6674a16... Wed 16 Nov 2016 04:29:24 CET

Value Transfer

JoinSplits

Input		*Output*
Transparent 0 ZEC + Shielded ? ZEC	▶ JoinSplit ▶	Transparent 0.0001 ZEC + Shielded ? ZEC

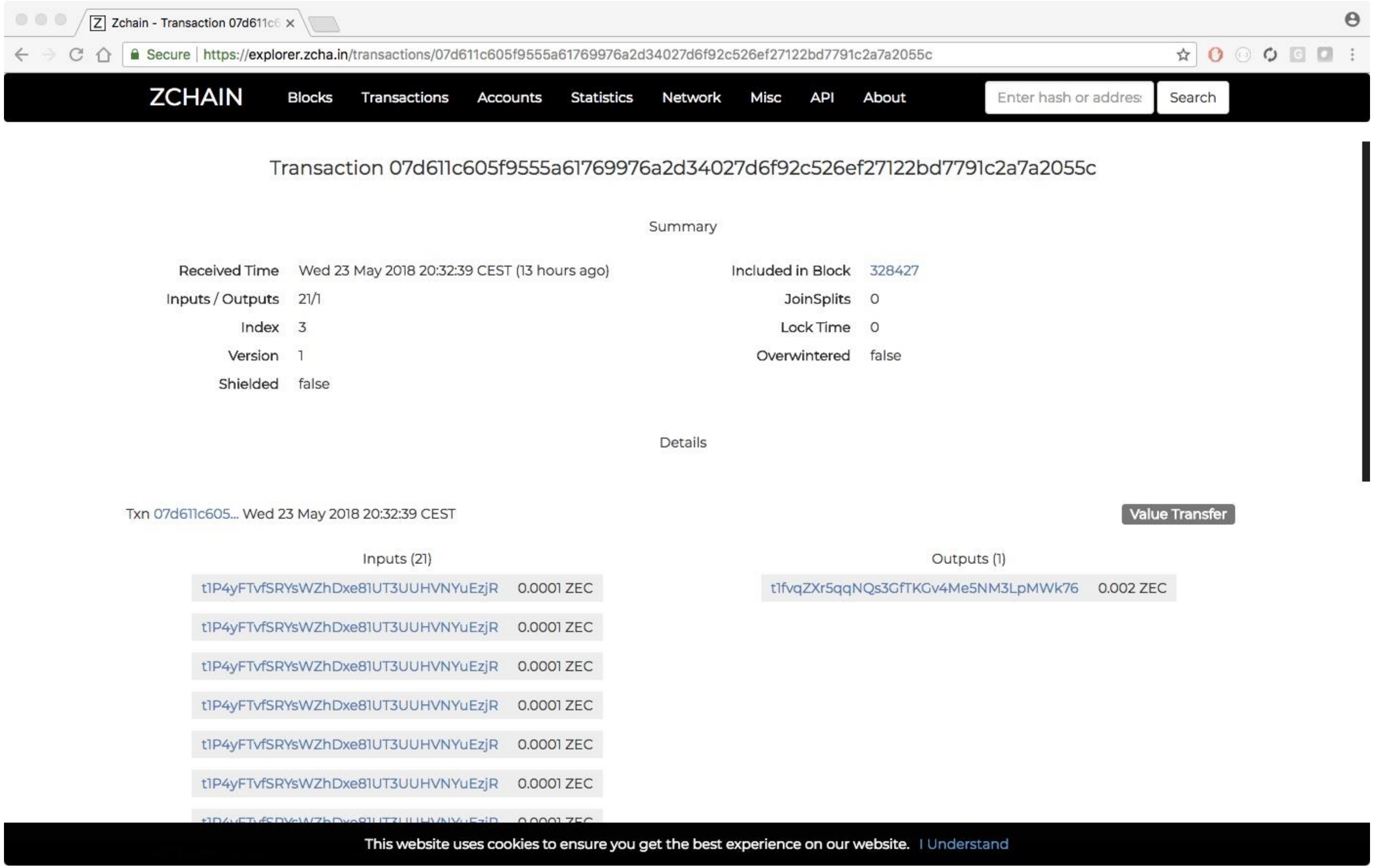
Inputs (0)

Outputs (0)

317568 confirmations 0.0001 ZEC ≥ 0.0001 ZEC

This website uses cookies to ensure you get the best experience on our website. I Understand

ZCASH | TRANSPARENT TRANSACTION



Zchain - Transaction 07d611c6
Secure | https://explorer.zcha.in/transactions/07d611c605f9555a61769976a2d34027d6f92c526ef27122bd7791c2a7a2055c
ZCHAIN
Blocks
Transactions
Accounts
Statistics
Network
Misc
API
About
Enter hash or addres
Search

Transaction 07d611c605f9555a61769976a2d34027d6f92c526ef27122bd7791c2a7a2055c

Summary

Received Time	Wed 23 May 2018 20:32:39 CEST (13 hours ago)	Included in Block	328427
Inputs / Outputs	21/1	JoinSplits	0
Index	3	Lock Time	0
Version	1	Overwintered	false
Shielded	false		

Details

Txn 07d611c605... Wed 23 May 2018 20:32:39 CEST

Value Transfer

Inputs (21)		Outputs (1)	
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC	t1fvqZXr5qqNQs3GfTKGv4Me5NM3LpMWk76	0.002 ZEC
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC		
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC		
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC		
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC		
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC		
t1P4yFTvfSRYsWZhDxe81UT3UUHVNYuEzjR	0.0001 ZEC		

This website uses cookies to ensure you get the best experience on our website. I Understand titanium-project.info

virtcrime-project.info

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

bernhard.haslhofer@ait.ac.at

https://graphsense.info

KIRAS Sicherheitsforschung

FFG Promoting Innovation.