B E A M

Scalable Confidential Cryptocurrency

Technology Overview

Poland, Katowice - 2019.05.14

Tomasz Waszczyk

Agenda

1. Tomek’s presentation
2. Remote call with Alex
3. Quiz with gifts- Telegram’s link: https://bit.ly/2Q4pw6X
4. How to contribute?

I strongly, strongly encourage to ask Alex as hard (technical) questions as possible! https://tlk.io/sbm

What ambasador means?

0. Meetup with CTO! ;-)
1. Closer contact with employees
2. Closer contact with community
3. Documentation
4. New experience

Company, not “project”

No ICO

Original MW implementation from scratch in C++

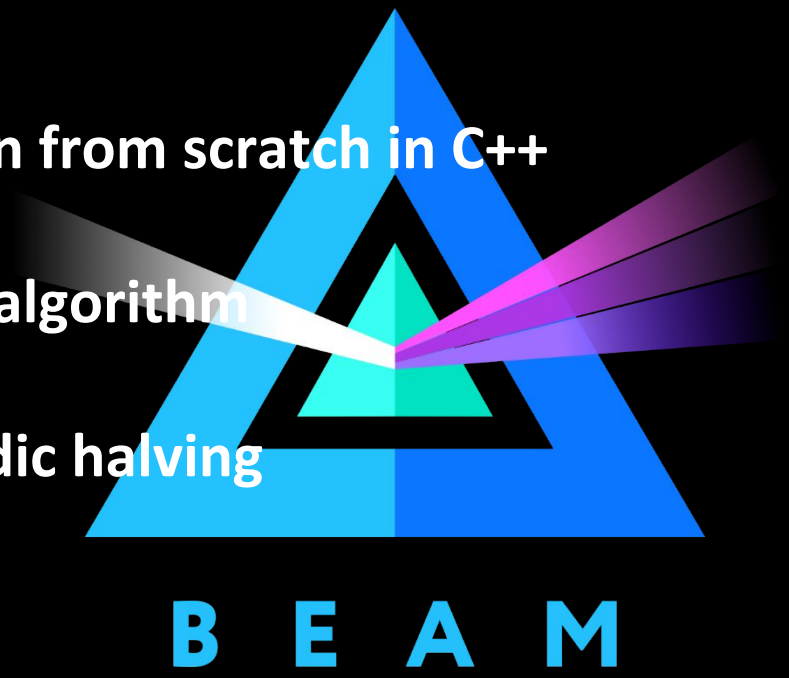
PoW mining using Equihash algorithm

Limited emission with periodic halving

Supported by Treasury

Open source

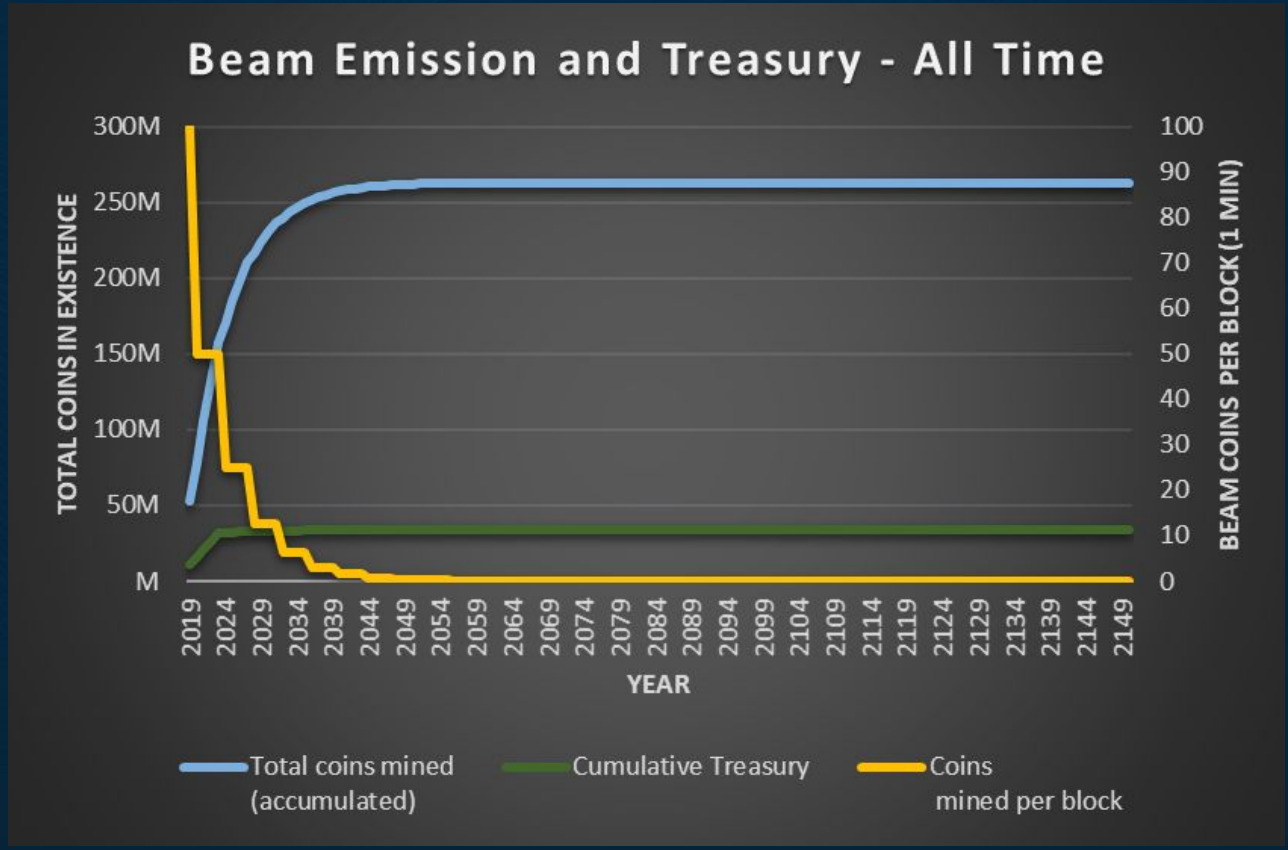
Founded by VCs, every milestone delivered



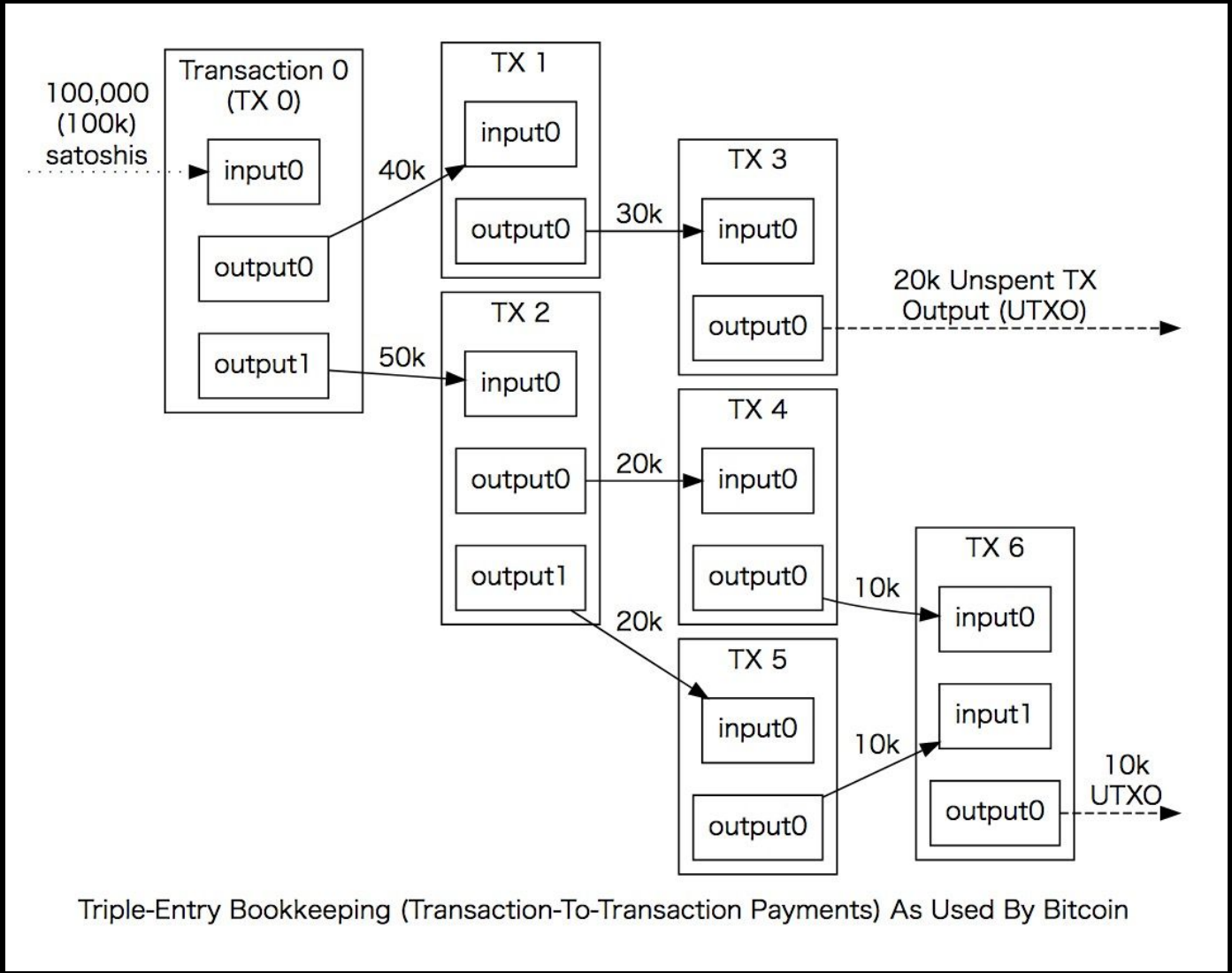
Our Investors

Coin Economics

- Capped Supply of 262, 800,000 Beam or 26,279,999,976,873,600 Groth
- First 5 years – 20% coins is emitted to Treasury
- Treasury goes to Investors, Core Team and Foundation
- Miner rewards:
  - 80 Beam in Y1
  - 40 Beam in Y2-5
  - 25 following 4 years
  - Halving until year 133



UTXO



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

f3a8b539a4ccb557c170de03836160a22f95d348eef1dd4b0e618ad26b6c8ea4

DETAILS +

#0 cabdec8fa16e250a1ceee2372bff522c7644b47e4c09f29c671e5e9f993a8ab4:1 0.02541498 BTC

#0 1EQ4FvzaPaGebFu6AmhMx7twckoA3AoGH1 0.00015364 BTC

#1 13Kx3r9V6ZVHrcxC6medhby4HGWmXeVFEm 0.024902 BTC

(RBF) 0.02505564 BTC

e966ba6e3de14fd5a26aea70d4178d22ca9c27a84f9301516c2cc508cf223dc0

DETAILS +

#0 0af55a33b608230a9f58d697d09ea24b03811943708e86c45d3fde0da8ae557d:1 4.20128152 BTC

#0 3LuBj9izunG8wQyvSjsnzFYSo242jn3Ny8 0.8932 BTC

#1 18KXxoc9MabwrWuftzN4MTak51RyNM2oXn 3.30772536 BTC

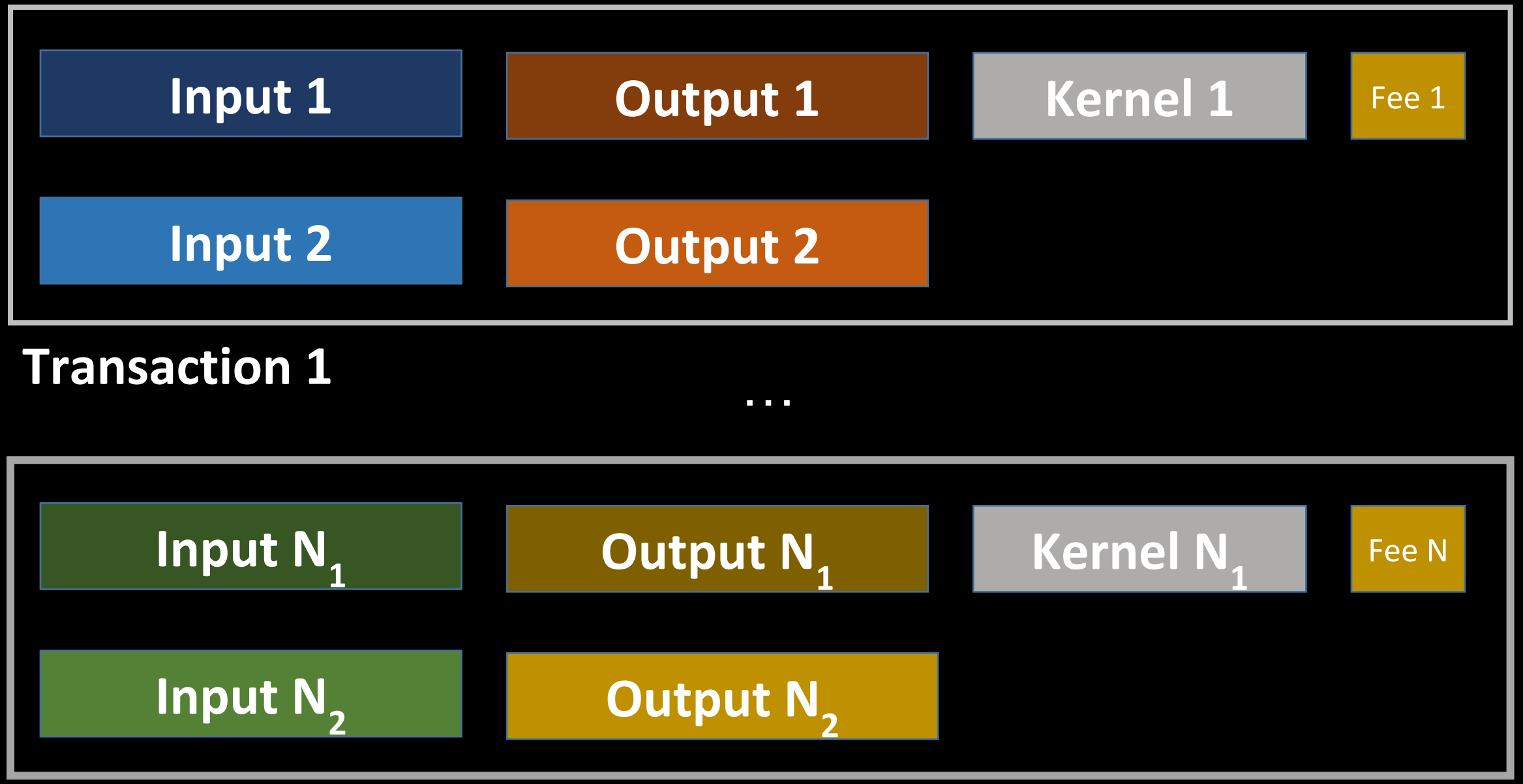
(RBF) 4.20092536 BTC

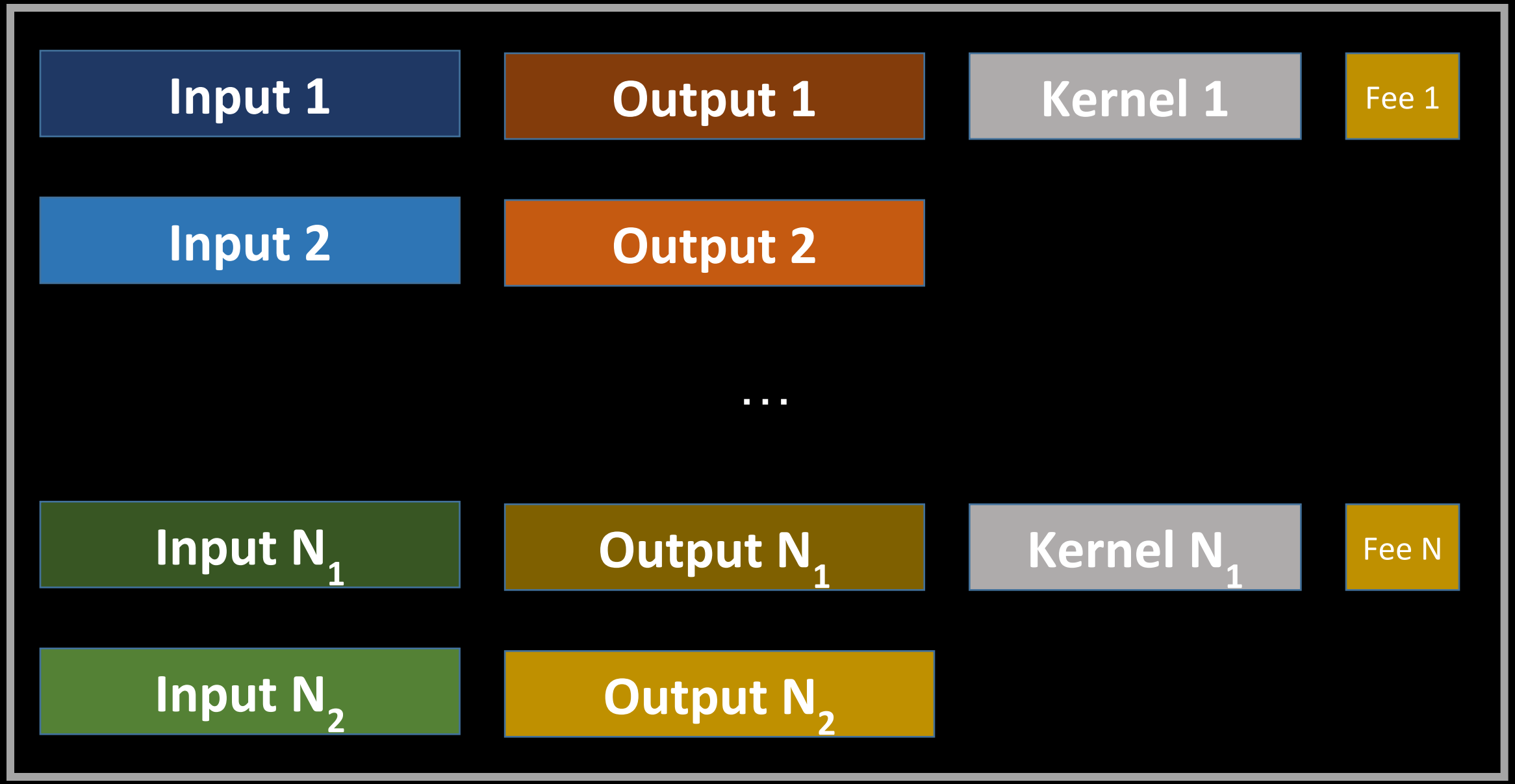
Confidential Transactions

Transaction Cut Through

Improvement

One input - one output


Input 1
Output 1
Kernel 1
Fee 1
Input 2
Output 2
Transaction 1
...
Input N_1
Output N_1
Kernel N_1
Fee N
Input N_2
Output N_2
Transaction N


Input 1
Output 1
Kernel 1
Fee 1
Input 2
Output 2
...
Input N_1
Output N_1
Kernel N_1
Fee N
Input N_2
Output N_2

Block

Beam comparison

	BEAM	BITCOIN	ZCASH	MONERO
Supply	210m	21m	21m	~18.3m (unlimited)
Pow Algorithm	Equihash	Hashcash	Equihash	Cryptonight
What is private	Everything	Not private	Everything, but only 10% of transactions are private	Sender, receiver and amount
Privacy enabled by	Confidential transactions using Pedersen commitments	None	zk-SNARKs algorithm	Ring signatures
Untraceable	No address information is stored in the blockchain	Traceable	Sender, amount and recipient data encrypted	Transactions mixed
Additional block size	None	1MB	50K (mostly public)	350K
Current size of the blockchain (greater size affects scalability)	~2-8GB	~190GB	5GB (for only 10% privacy)	~28GB
Decentralized	Yes	Yes	A trusted setup is required	No trusted setup

BEAM vs GRIN

Grin vs Beam		
Category	**Grin**	**Beam**
Programming Language	Rust	C++
Team	Anonymous (mostly)	Public
Block Time	60 s	60 s
Block Reward	60 coins	80 coins
Coin Emission	Linear	Similar to Bitcoin
Mining Algorithm	Cuckatoo	Modified Equihash
Max Supply	Infinite	262,800,000
ICO	NO	NO
Premine	NO	NO
Founders Reward	NO	YES
Funding Model	Community	Block Reward Cut
Governance Model	Community Governance	Beam Foundation

Grin

Using Mimblewimble protocol

Implemented in Rust

PoW mining using Cuckoo Cycle algorithm

Unlimited emission

Open Source

Supported by Community

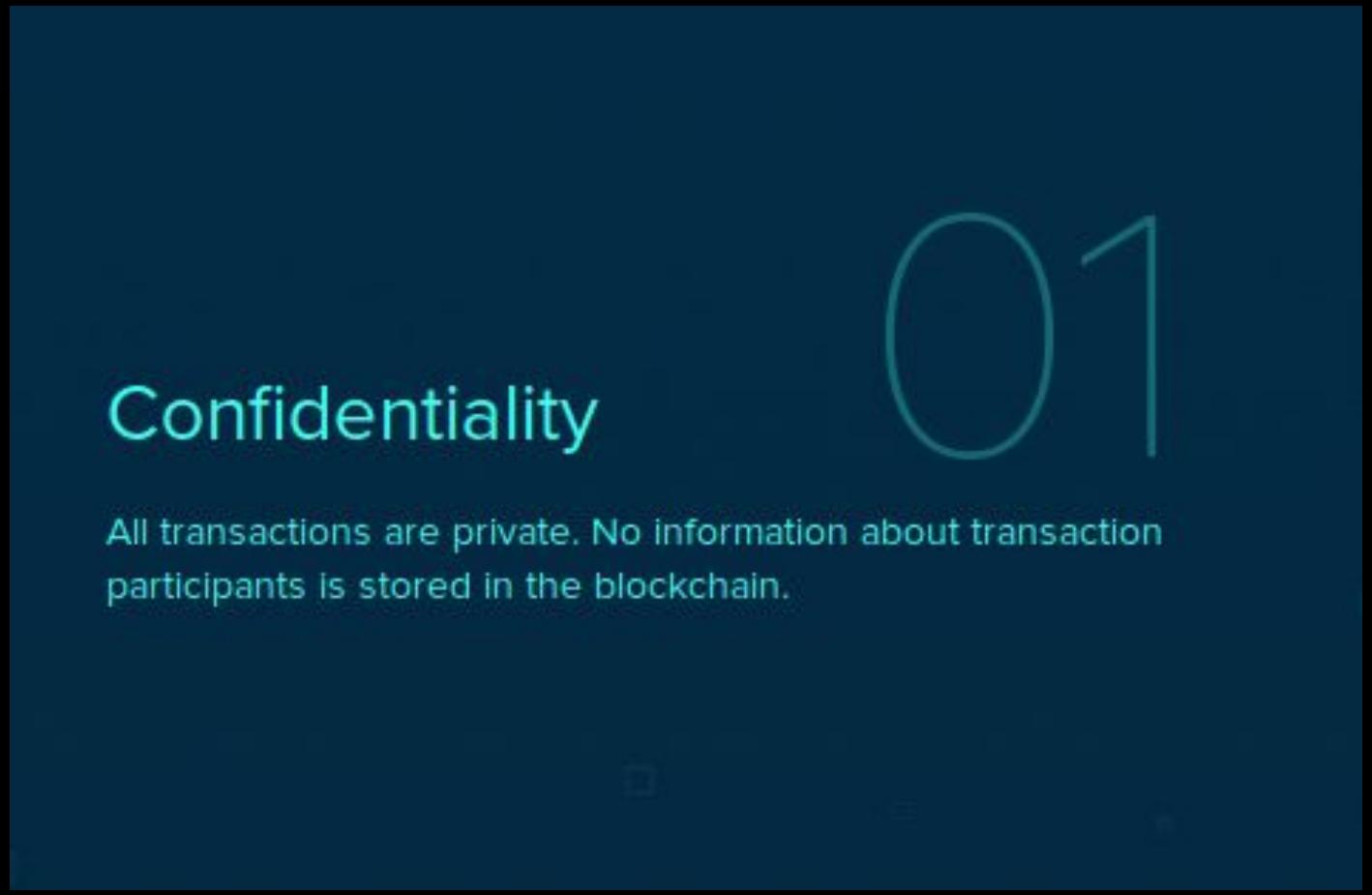
Podałeś/aś dalej

hashmap @hashmap · 7 maj

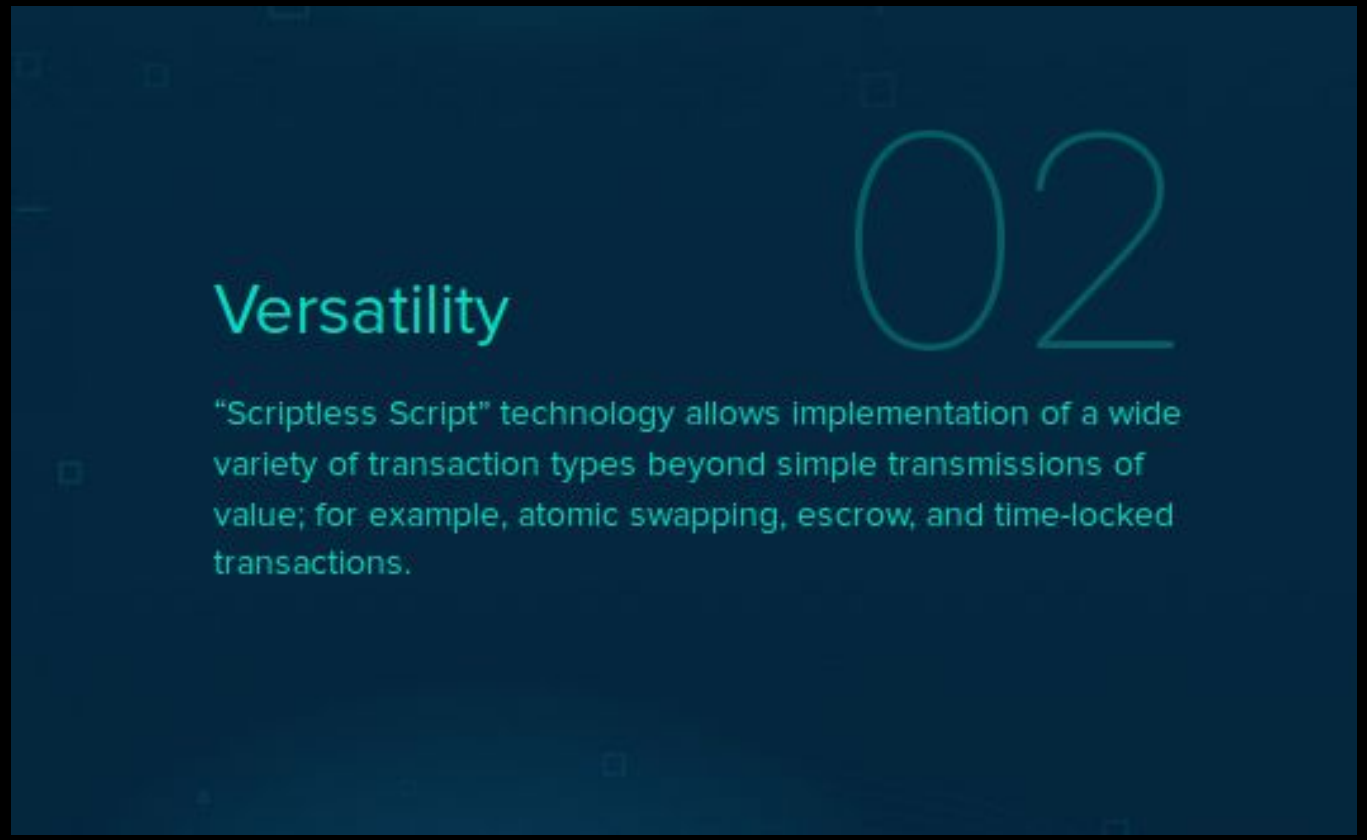
Grin received a 50 BTC donation, a very special one, a coinbase from block 93709,
mined on2010-11-25 08:16. This is insane by so many reasons. Thanks a lot!

34 151 912

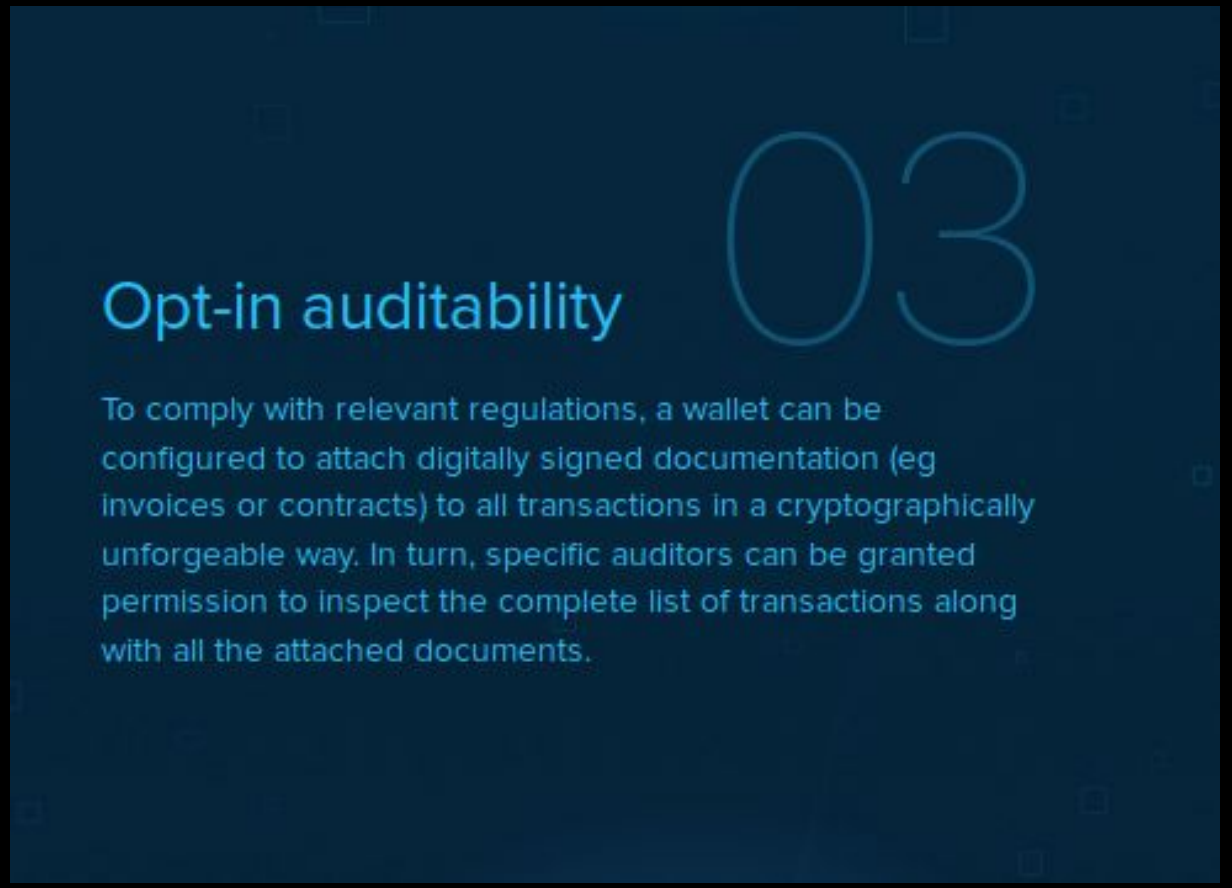
Features


01
Confidentiality
All transactions are private. No information about transaction participants is stored in the blockchain.

Features


02
Versatility
“Scriptless Script” technology allows implementation of a wide variety of transaction types beyond simple transmissions of value; for example, atomic swapping, escrow, and time-locked transactions.

Features


03
Opt-in auditability
To comply with relevant regulations, a wallet can be configured to attach digitally signed documentation (eg invoices or contracts) to all transactions in a cryptographically unforgeable way. In turn, specific auditors can be granted permission to inspect the complete list of transactions along with all the attached documents.

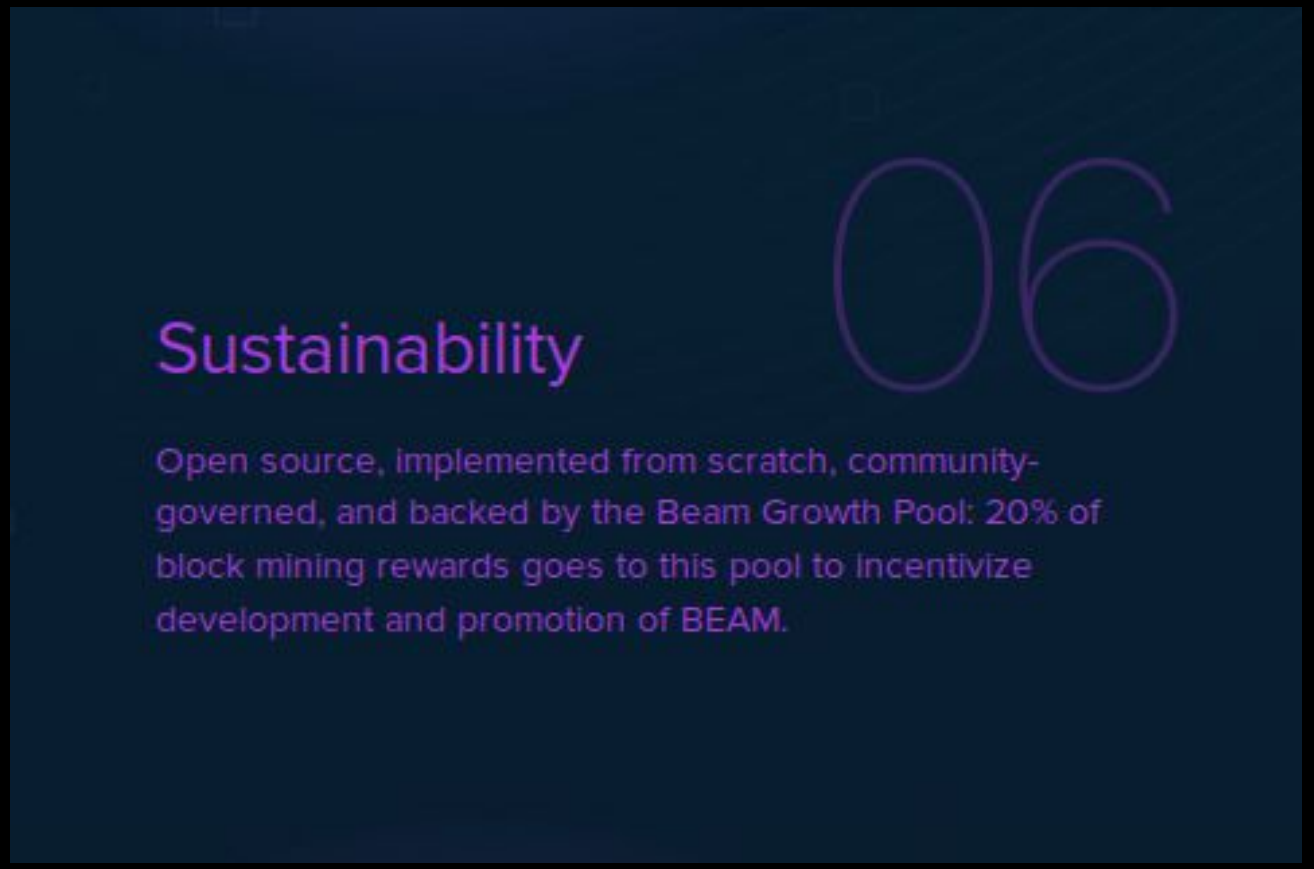
Features


04
Confidential assets
Multiple asset types (eg real estate tokens, corporate debts and simply new currencies) can be created and exchanged via BEAM confidential transactions mechanisms.

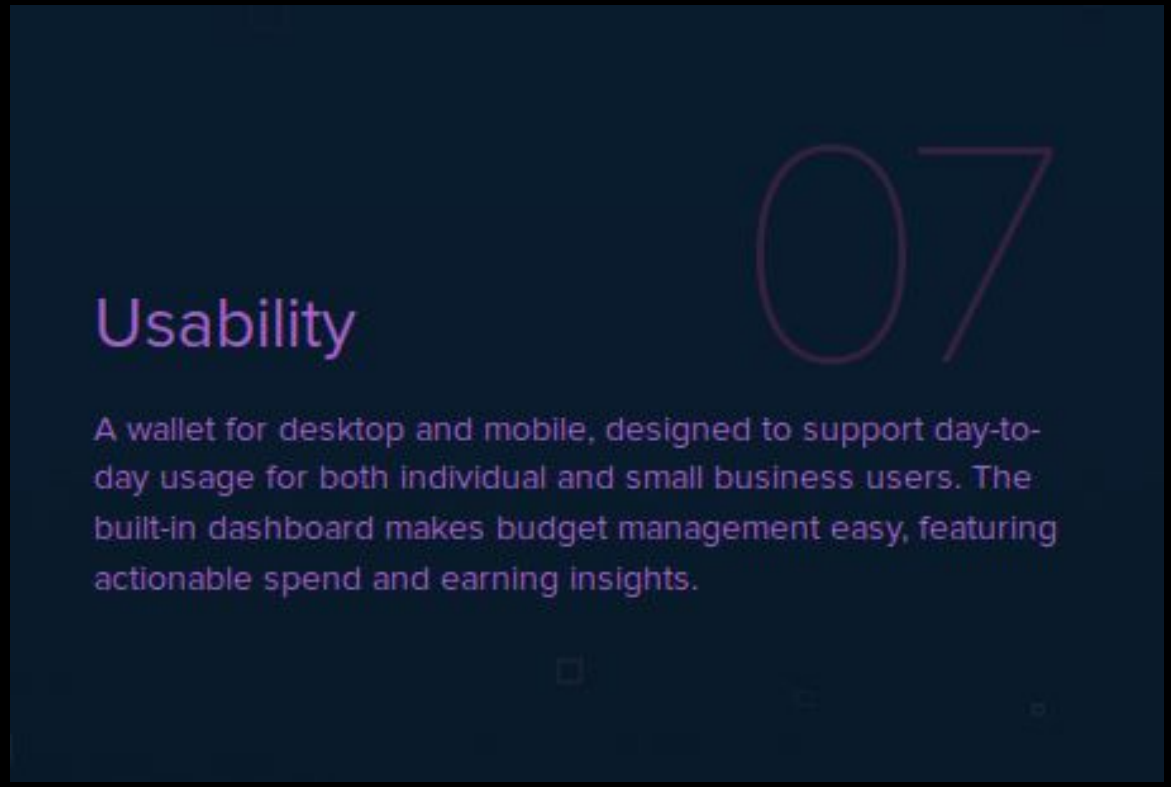
Features


05
Scalability
The “cut-through” feature of Mimblewimble helps to avoid excessive computational overhead, making the BEAM blockchain orders of magnitude smaller than any other blockchain implementation.

Features


06
Sustainability
Open source, implemented from scratch, community-governed, and backed by the Beam Growth Pool: 20% of block mining rewards goes to this pool to incentivize development and promotion of BEAM.

Features


07
Usability
A wallet for desktop and mobile, designed to support day-to-day usage for both individual and small business users. The built-in dashboard makes budget management easy, featuring actionable spend and earning insights.

Features


08
Compatibility
An industry-proven Equihash algorithm was selected to ensure broad adoption by existing GPU miners. BEAM comes with an extensive set of tools for running and managing mining nodes.

BEAM’s strategic goals

- payment proof
- atomic swap
- BTC
- ETH

Scriptless Scripts

Timelocked Transactions

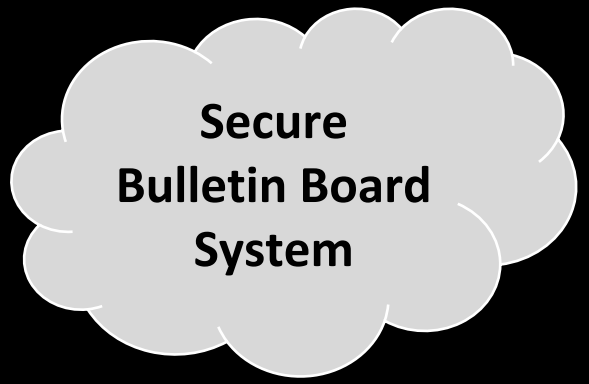
Escrow Transactions

Atomic Swaps

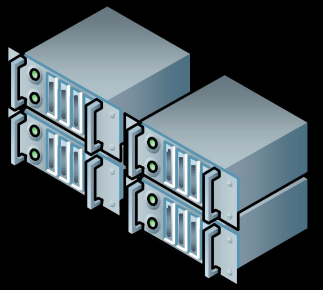
Auditable Transactions

Sender

Receiver



1. Receiver wallet generates random identifier
2. Identifier is sent to the Sender via external channel
3. Sender initiates a transaction via Secure BBS
4. Once transaction is created, it is sent to the node



Node

No addresses are sent to nodes or recorded in the blockchain

Both wallets have to participate in transaction creation

Wallet has to store both transaction value and blinding factor

Faucet to try BEAM

https://bitmate.ch/

2019 ROADMAP

Jan-Feb 2019

Agile Atom

- Payment and Exchange API
- Mining Pool API
- Lightning Position Paper

March 2019

Bright Boson

- Beam<>BTC Atomic Swap
- Hardware Wallet Integration
- Android and iOS Wallets
- Payment Platforms Integration
- Fast Node sync
- Payment Confirmation

June 2019

Clear Cathode

- PoW Algorithm Change
- One-sided Payments
- Lightning POC
- Multisig Support
- Bulletin Board for Swaps

Sept 2019

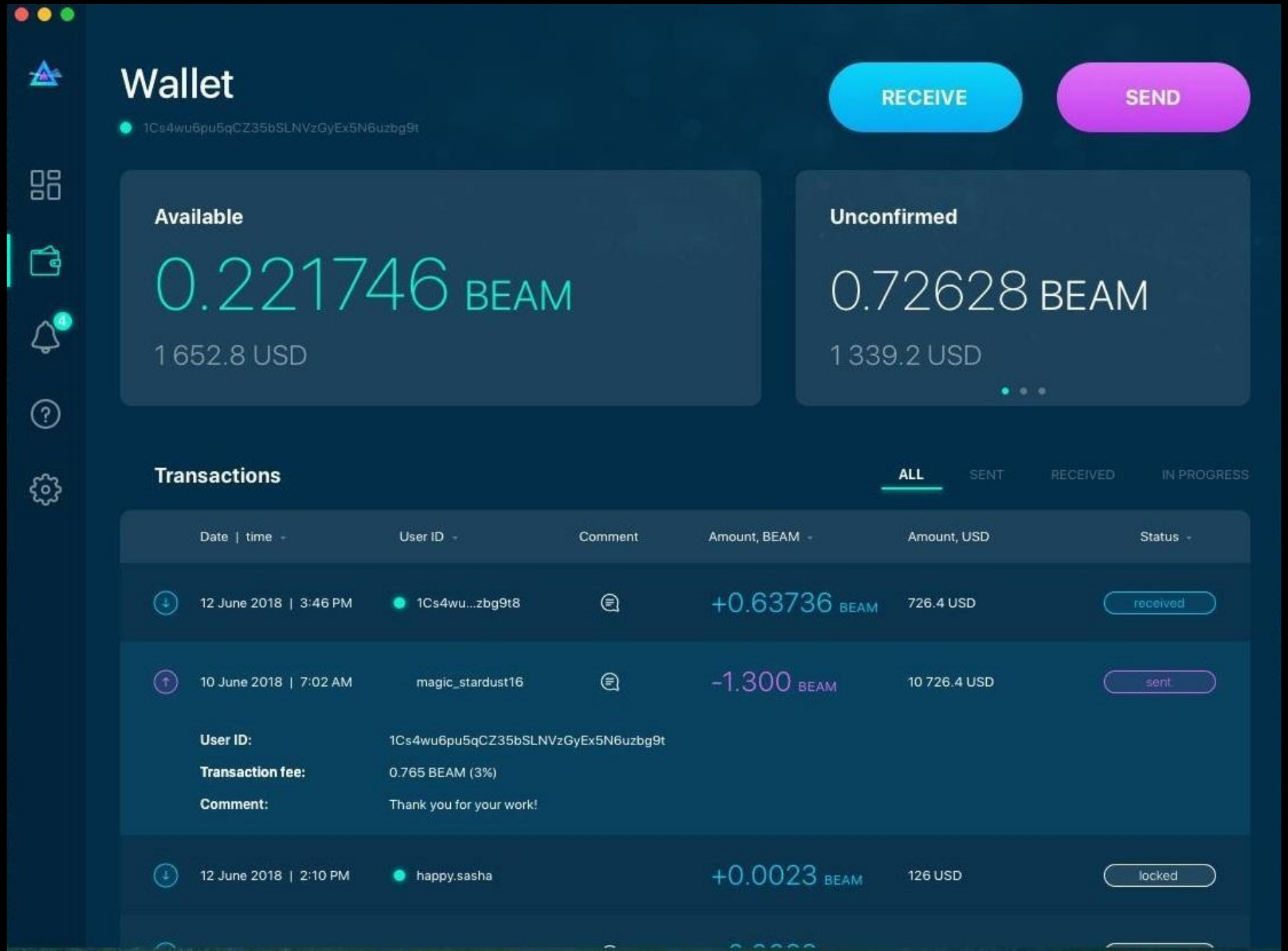
Double Doppler

- Research Alternative Consensus
- Porting to Rust
- Enhanced Wallet Security
- Lightning Alpha

Dec 2019

Eager Electron

- PoW Algorithm Change
- I2P/Tor Integration
- BLS Implementation
- GhostDAG POC
- Lightning Beta


Wallet
1Cs4wu6pu5qCZ35bSLNVzGyEx5N6uzbg9t
RECEIVE
SEND
Available
0.221746 BEAM
1 652.8 USD
Unconfirmed
0.72628 BEAM
1 339.2 USD
Transactions
ALL
SENT
RECEIVED
IN PROGRESS
Date | time
User ID
Comment
Amount, BEAM
Amount, USD
Status
12 June 2018 | 3:46 PM
1Cs4wu...zbg9t8
+0.63736 BEAM
726.4 USD
received
10 June 2018 | 7:02 AM
magic_stardust16
-1.300 BEAM
10 726.4 USD
sent
User ID:
1Cs4wu6pu5qCZ35bSLNVzGyEx5N6uzbg9t
Transaction fee:
0.765 BEAM (3%)
Comment:
Thank you for your work!
12 June 2018 | 2:10 PM
happy.sasha
+0.0023 BEAM
126 USD
locked

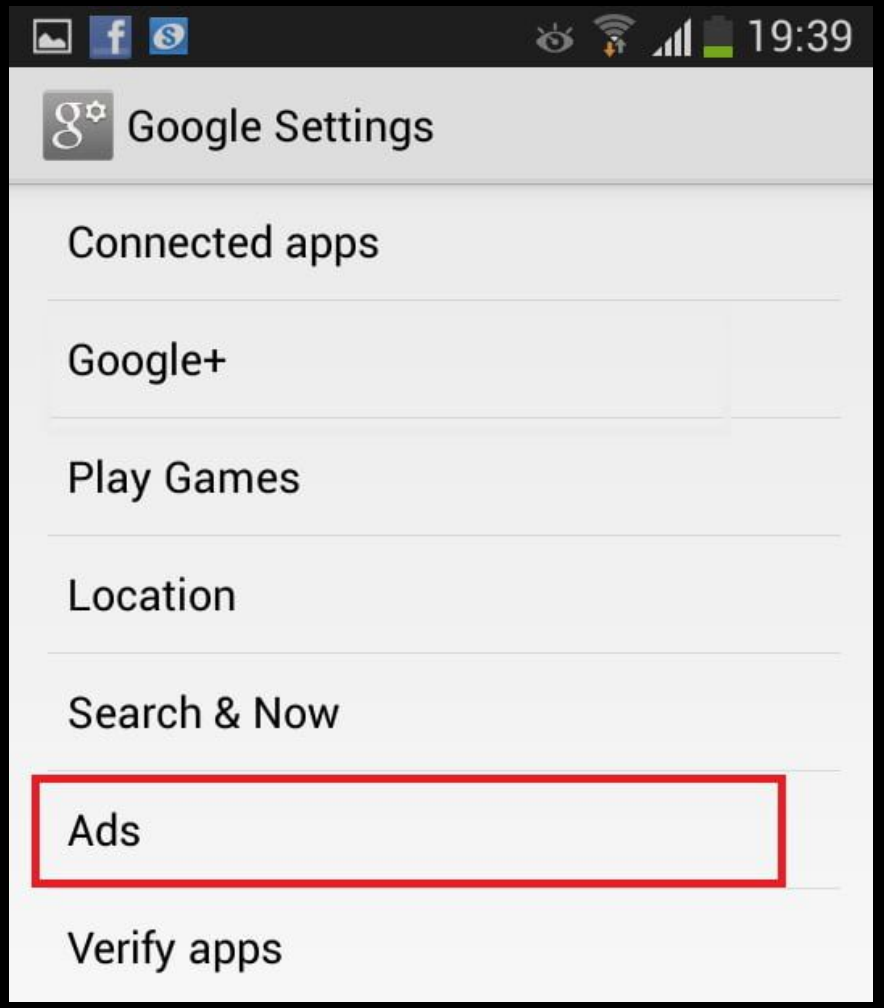
Future plans

Mobile wallet

Confidential Assets

Smart Contracts

Pro Tip - Android and advertising ID

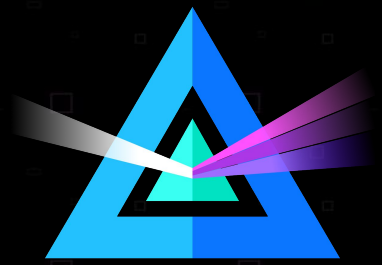


Wsparcie Silesia Blockchain Meetup

- “Like it” i/lub “Share” w social media
- Zadawać pytania
- Powiedzieć co robić lepiej, konstruktywnie doradzić
- Pomóc przy stolikach
- “Star” na Github
- #zaproponujsam #pomyśl #think!

Thank You

Q & A

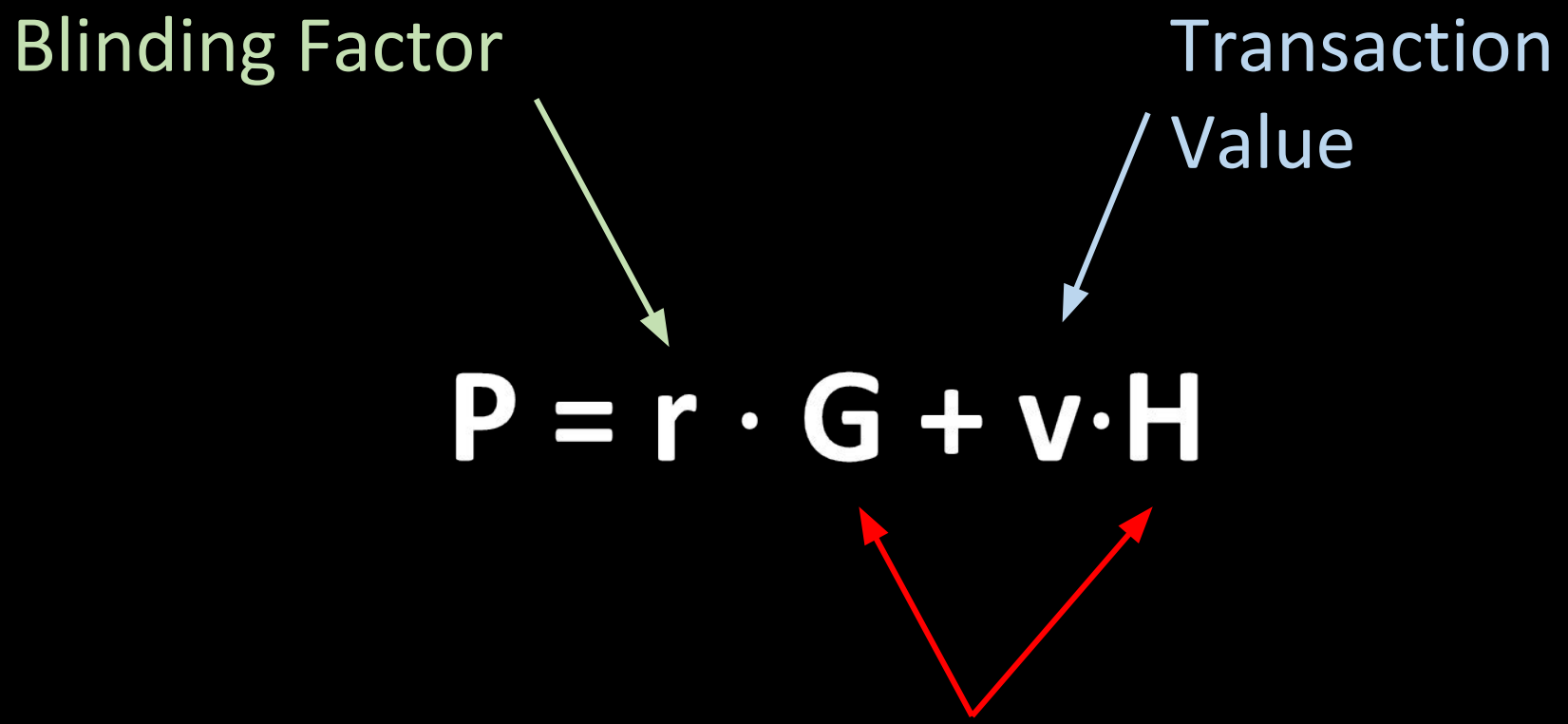


https://www.beam-mw.com

https://t.me/BeamPrivacy

https://medium.com/beam-mw

UTXO


Blinding Factor
Transaction Value
P = r · G + v·H
Generator Points

Simple Transaction

Alice

Bob

$P_i = r_1 \cdot G + v \cdot H$

$P_O = r_1 \cdot G + v \cdot H$

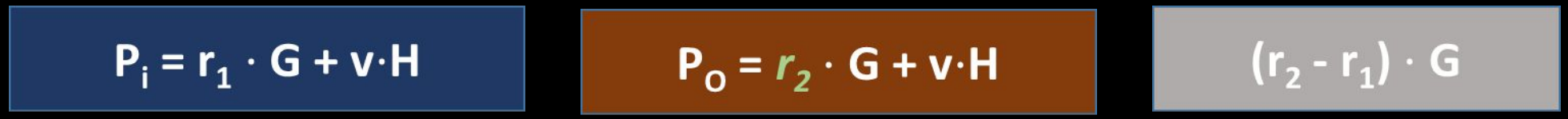
Inputs

Outputs

$\sum = 0$

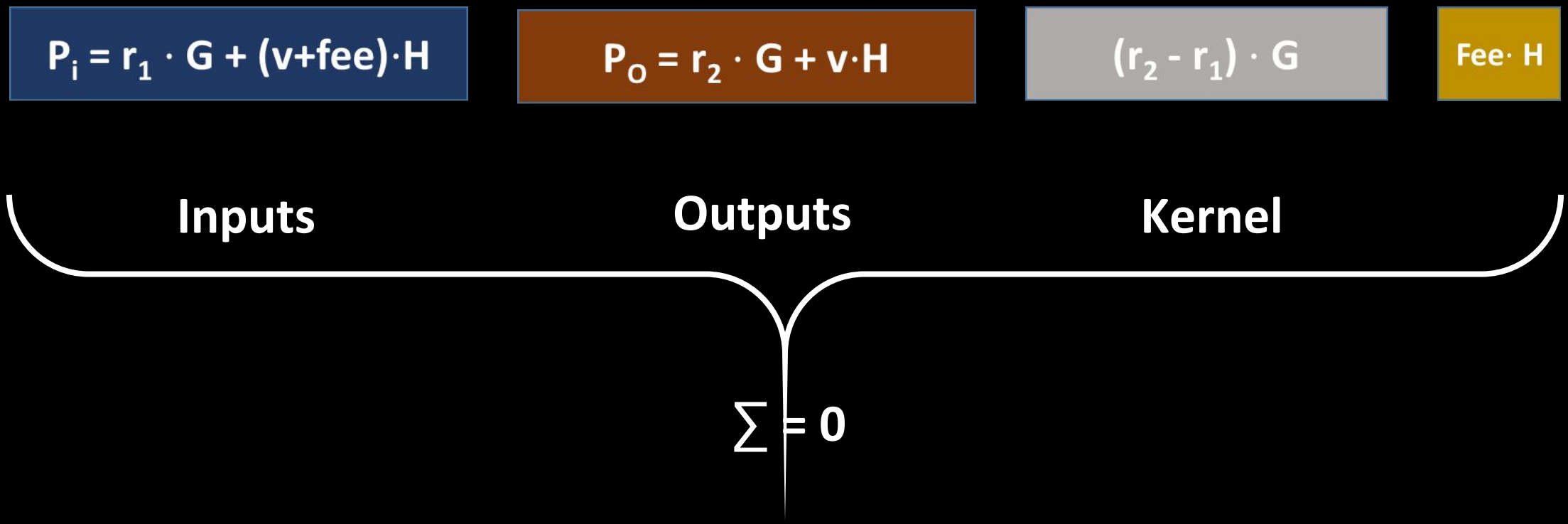
Simple Transaction

Alice **Bob**



Inputs **Outputs** **Kernel**

Simple Transaction



Simple Transaction

Bulletproofs

Benedikt Bünz , Jonathan Bootle , Dan Boneh , Andrew Poelstra , Pieter Wuille , and Greg Maxwell

Each output should contain proof that value is positive and does not overflow

Bulletproofs is a non interactive zero knowledge range proof protocol with very short proofs and no trusted setup

Transaction Cut Through

Alice	Bob	
$P_i = r_1 \cdot G + v \cdot H$	$P_O = r_2 \cdot G + v \cdot H$	$(r_2 - r_1) \cdot G$
$P_I = r_2 \cdot G + v \cdot H$	$P_O = r_3 \cdot G + v \cdot H$	$(r_3 - r_2) \cdot G$
Bob	Carol	

The structure of a block resembles that of a transaction

All elements in the block are sorted to obscure the original order

Cut through can happen both within a block and across blocks