
# Beam

## Best-in-class Confidential Cryptocurrency


USD Coin
$358M
TrueUSD
$243M
0x
$197M
Zilliqa
$156M
Pundi X
$155M
DigiByte
$150M
IOST
$147M
Aeternity
$144M
Aurora
$135M
Siacoin
$135M
Qtum
$302M
Nano
$239M
Paxos
$190M
Huobi Token
$135M
Steem
$116M
THETA
$102M
ThoreCoin
$102M
KuCoin Shares
$94M
Status
$94M
Waltonchain
$93M
Decred
$298M
Lisk
$236M
BitShares
$187M
Komodo
$131M
Stratis
$89M
MaidSafeCoin
$80M
aelf
$80M
Horizen
$78M
Dent
$78M
Mixin
$78M
OmiseGO
$274M
BitTorrent
$227M
Bitcoin Diamond
$186M
ABBC Coin
$129M
Cryptonex
$88M
Ardor
$77M
MonaCoin
$71M
Aion
$68M
Ark
$67M
SOLVE
$67M
Waves
$246M
Holo
$213M
ICON
$184M
Bytom
$123M
Golem
$88M
Crypto.com
$77M
WAX
$65M
Santiment
$60M
LATOKEN
$59M
Augur
$245M
Ravencoin
$202M
Verge
$178M
Insight Chain
$119M
Factom
$84M
Project Pai
$77M
GXChain
$65M
HyperCash
$57M
Zcoin
$55M
Bytecoin
$176M
Qubitica
$118M
VestChain
$81M
TrueChain
$72M
Arcblock
$63M
Loopring
$56M
Enjin Coin
$117M
Dai
$81M
DigixDAO
$71M
Clams
$61M
Metaverse ETP
$55M
Loom Network
$55M

# What was Satoshi's dream

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main

## 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

**A better version of money**

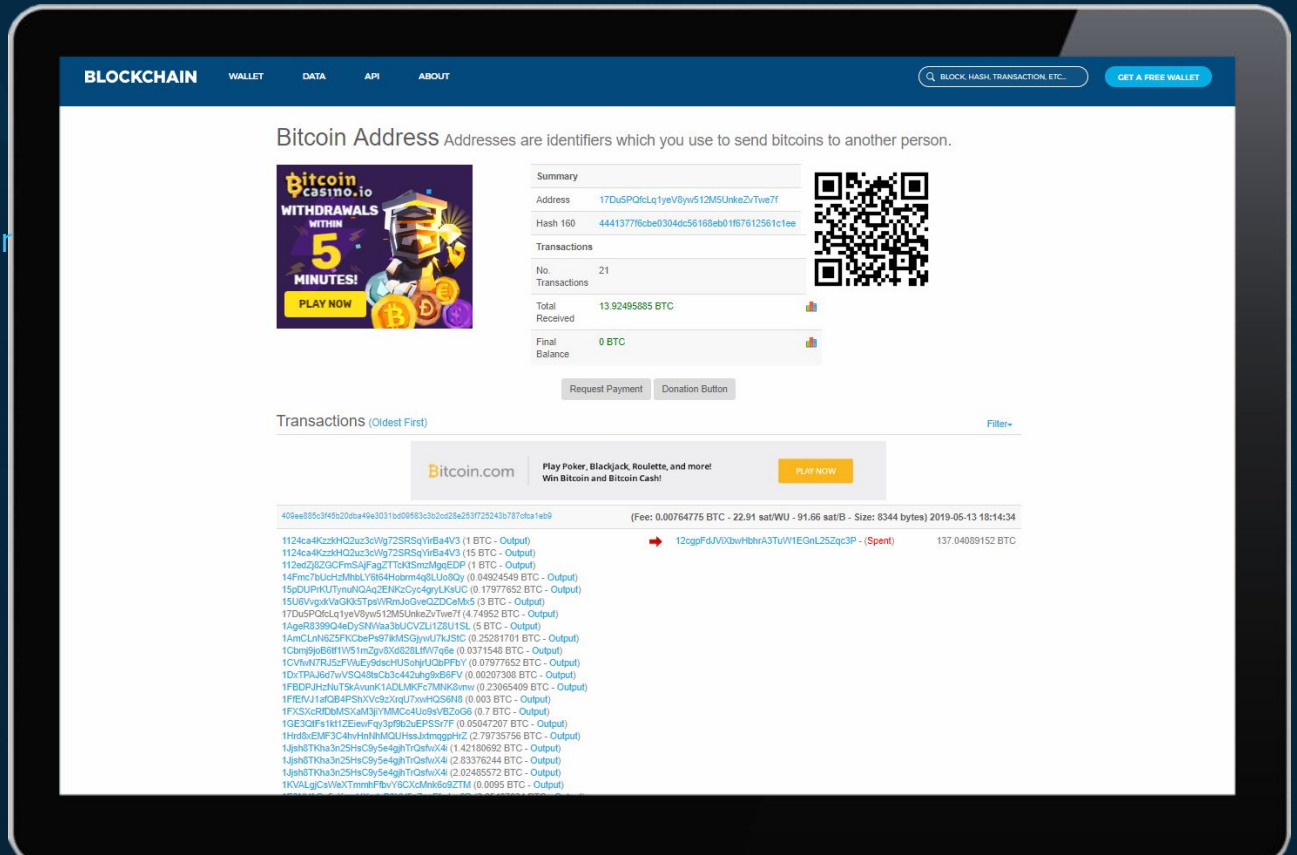
# So what's the problem?

- I want to be only with you
- So what's the problem?
- What do I do with the others?

Atkritka.com

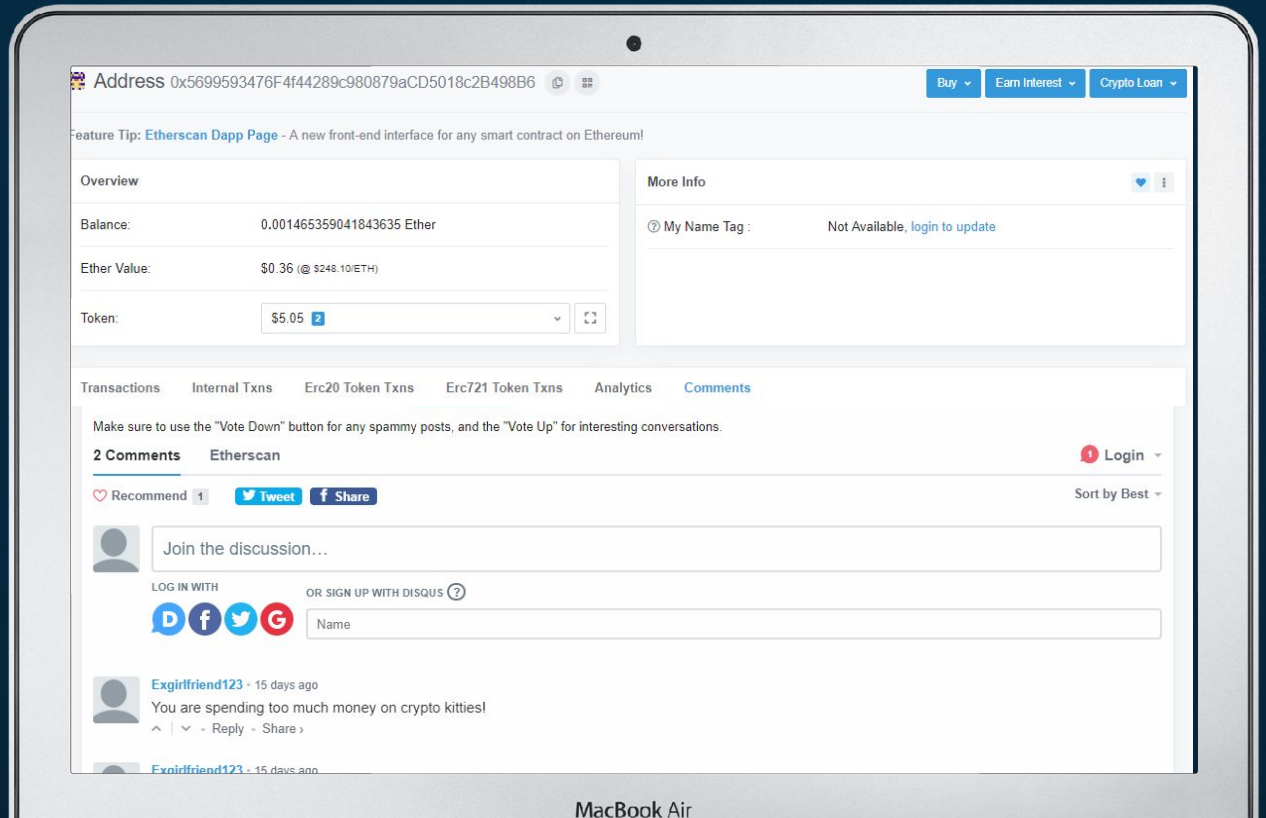
# Indeed, what do we do with the *others*

Blockchain Explorer




BEAM

# Etherscan


Address 0x5699593476F4f44289c980879aCD5018c2B498B6
Buy
Earn Interest
Crypto Loan
Feature Tip: Etherscan Dapp Page - A new front-end interface for any smart contract on Ethereum!
Overview
Balance: 0.001465359041843635 Ether
Ether Value: $0.36 (@ $248.10/ETH)
Token: $5.05 2
More Info
My Name Tag : Not Available, login to update
Transactions
Internal Txns
Erc20 Token Txns
Erc721 Token Txns
Analytics
Comments
Make sure to use the "Vote Down" button for any spammy posts, and the "Vote Up" for interesting conversations.
2 Comments
Etherscan
Login
Recommend 1
Tweet
Share
Sort by Best
Join the discussion…
LOG IN WITH
OR SIGN UP WITH DISQUS
Name
ExgirlfriendI23 · 15 days ago
You are spending too much money on crypto kitties!
Reply · Share ›
MacBook Air

# Blockchain Analytics Companies





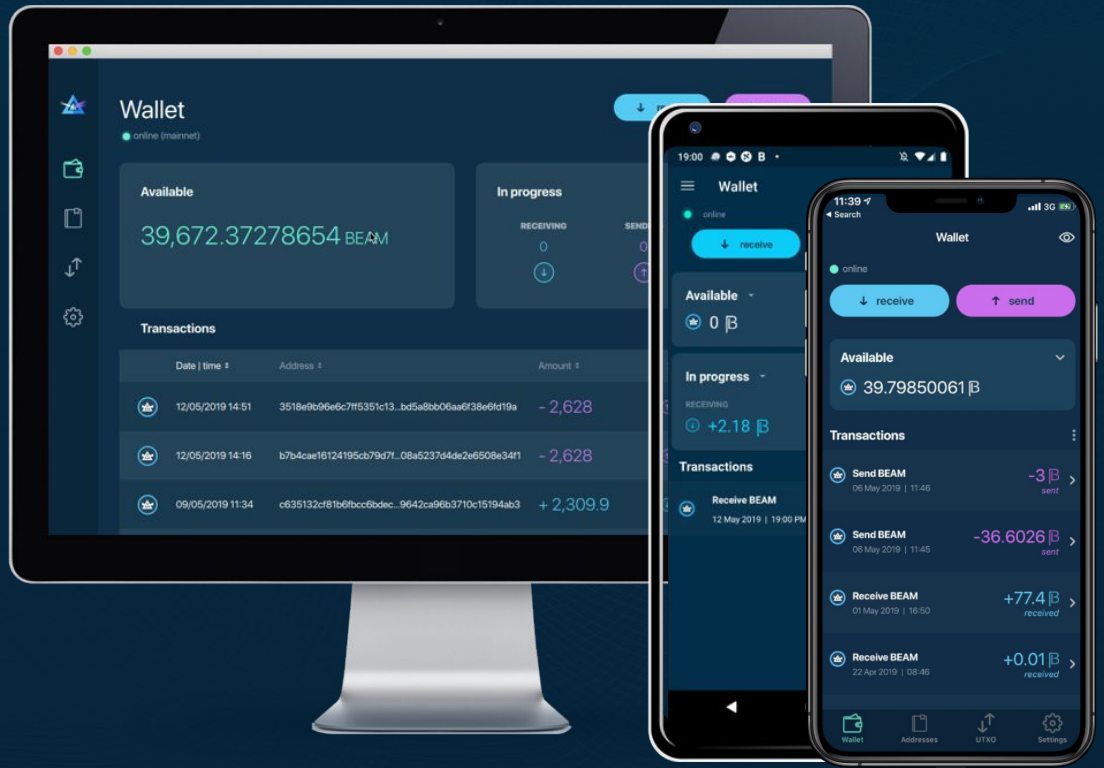

BEAM

# Now, let’s imagine it is your bank account

# Why do we need confidentiality?

# Confidential Cryptocurrencies

# Does size really matter?



# Enter Beam

A new cryptocurrency based on Mimblewimble protocol

| PoW consensus | Decentralized | Permissionless | Deflationary |
|---|---|---|---|

- Not a fork. Original work implemented from scratch in C++
- Development started in March 2018
- Mainnet launched on 01/03/2019, on the 10th anniversary of Bitcoin

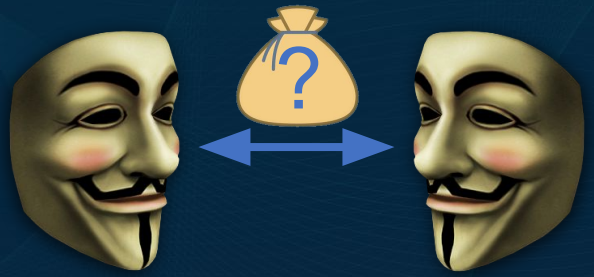
# Mimble what?


A new blockchain protocol

- Published in July 2016
- Author - Tom Elvis Jedusor (Voldemort)

# Mimblewimble

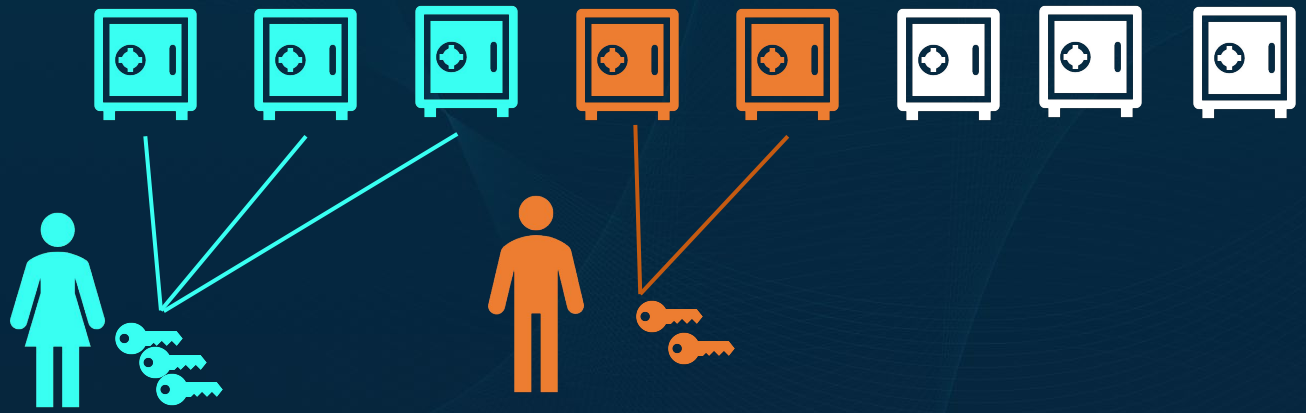
No Addresses



Sender, Receiver and Amounts are not visible

No history on blockchain

# Beam Blockchain

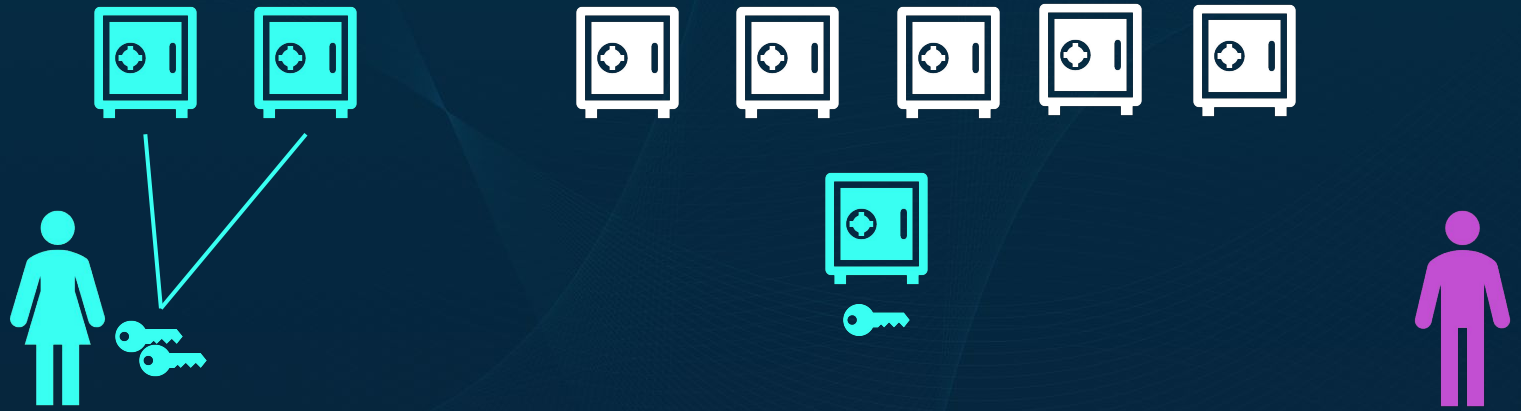


# UTXO Model

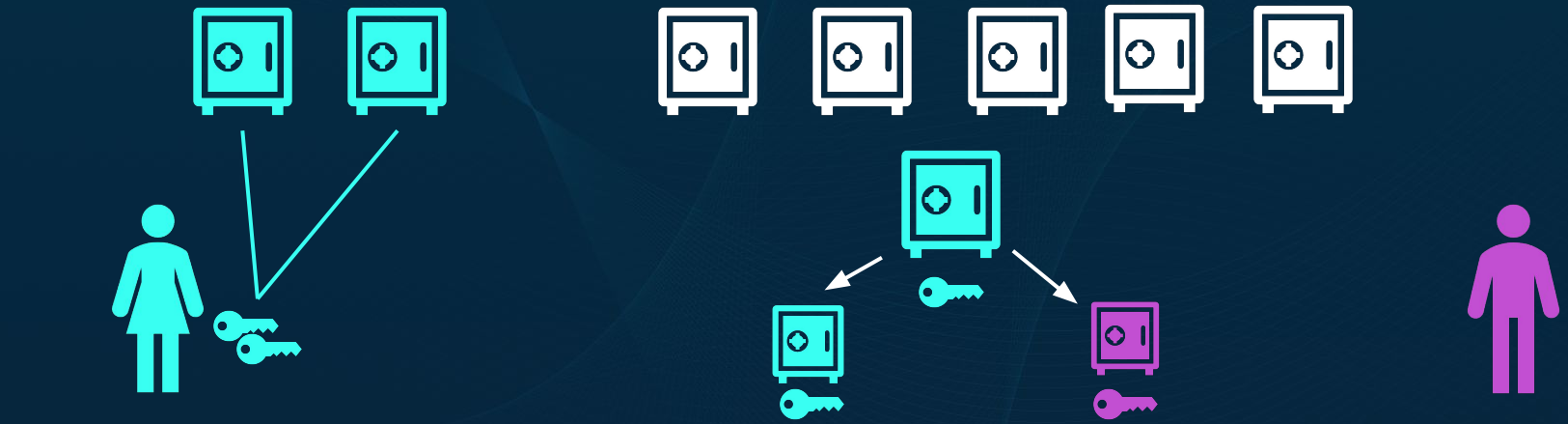


ator Points

# Creating a Transaction



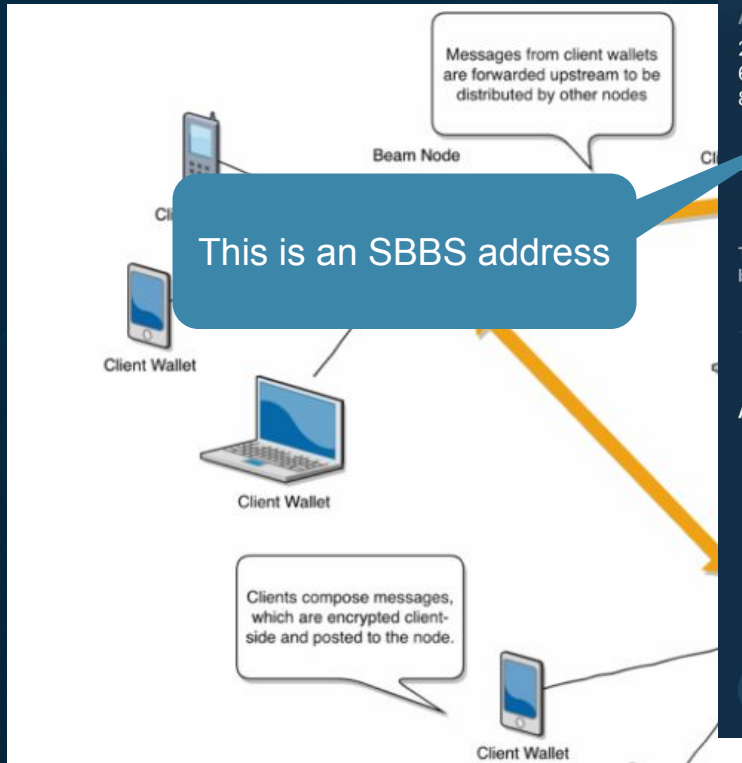
# Creating a Transaction

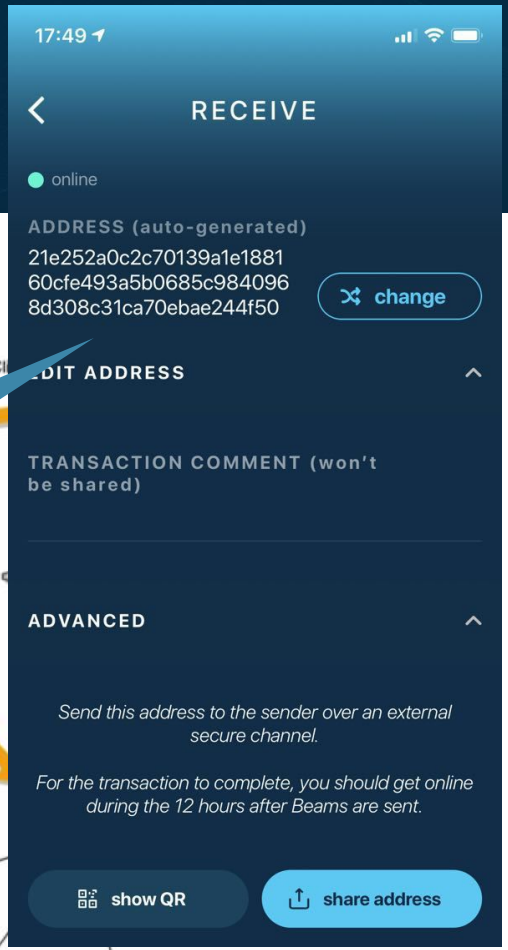


## Wait, how do the connect?

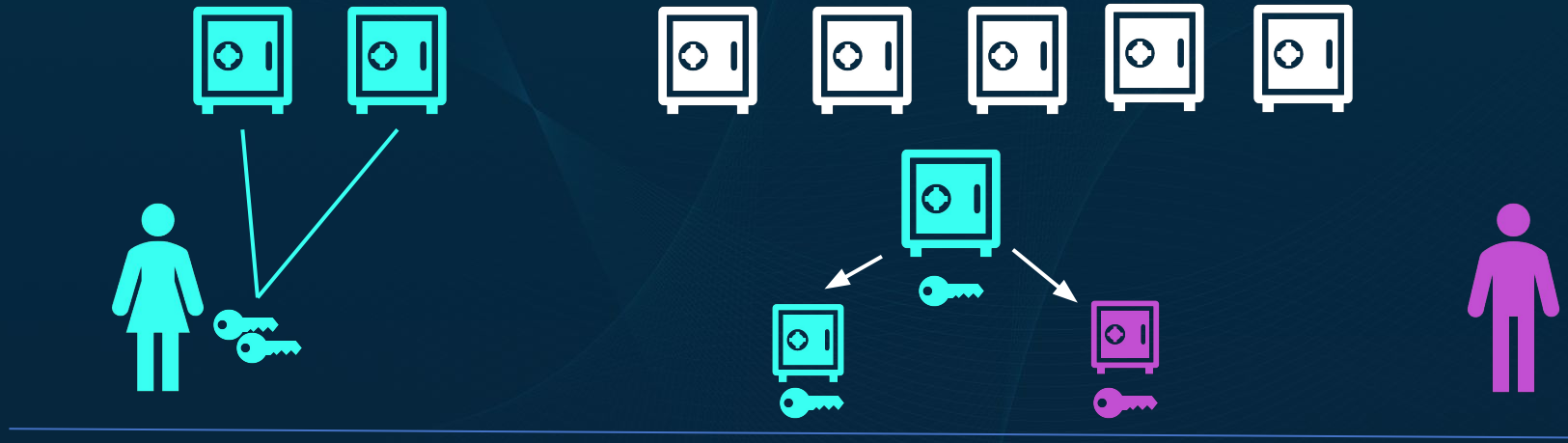
Beam SBBS – Message Board for Wallets

- Encrypted
- Distributed
- Persistent



# Creating a Transaction



# Creating a Transaction

✔ Does it sum to zero
✔ Are all the numbers positive

# Creating a transaction

- ✔ The blockchain only stores the current state
- ✔ Resulting size – 3-10 smaller than Bitcoin

BEAM

# Transaction Cut-through

**Alice** **Bob**

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

$P_O = r_2 \cdot G + v \cdot H$

$(r_2 - r_1) \cdot G$

$P_I = r_2 \cdot G + v \cdot H$

$P_O = r_3 \cdot G + v \cdot H$

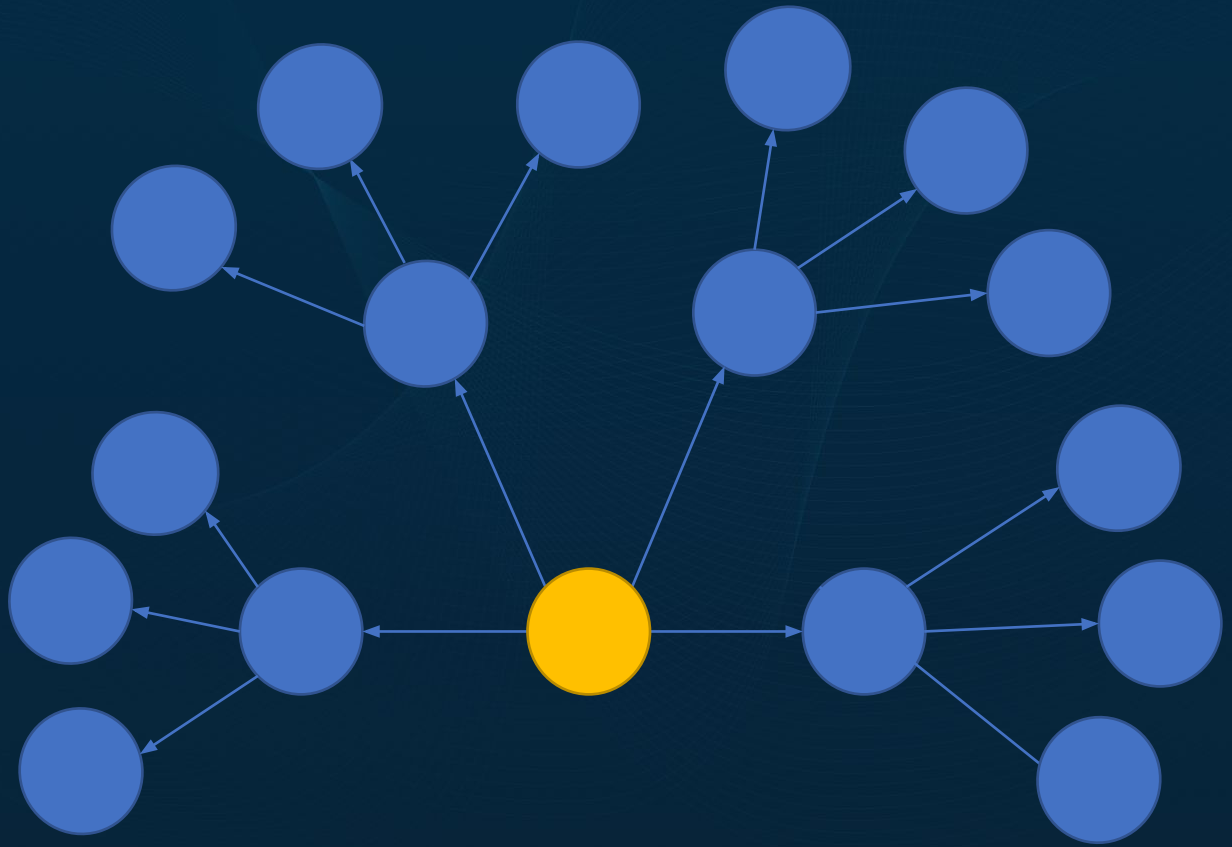
$(r_3 - r_2) \cdot G$

**Bob** **Carol**

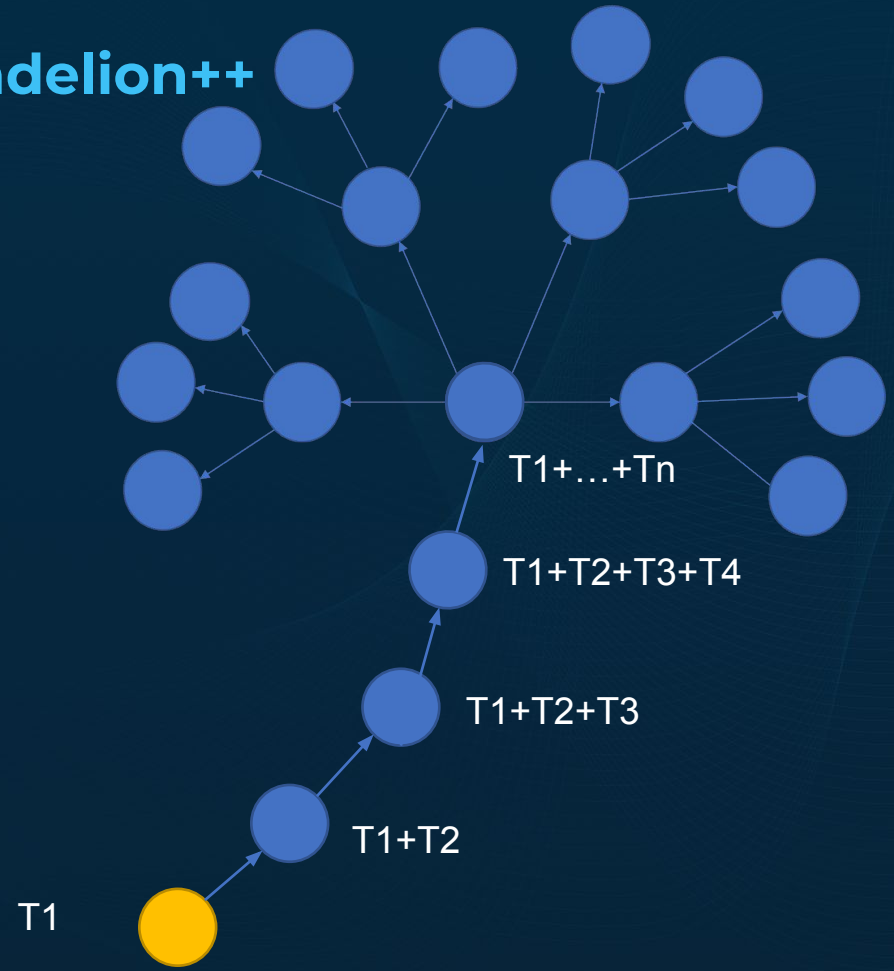
- Same repeated for all the blockchain
- Intermediary states removed –keep just current state of UTXOs
- Result – 3-10 times smaller than Bitcoin

BEAM

# Network-level Anonymization

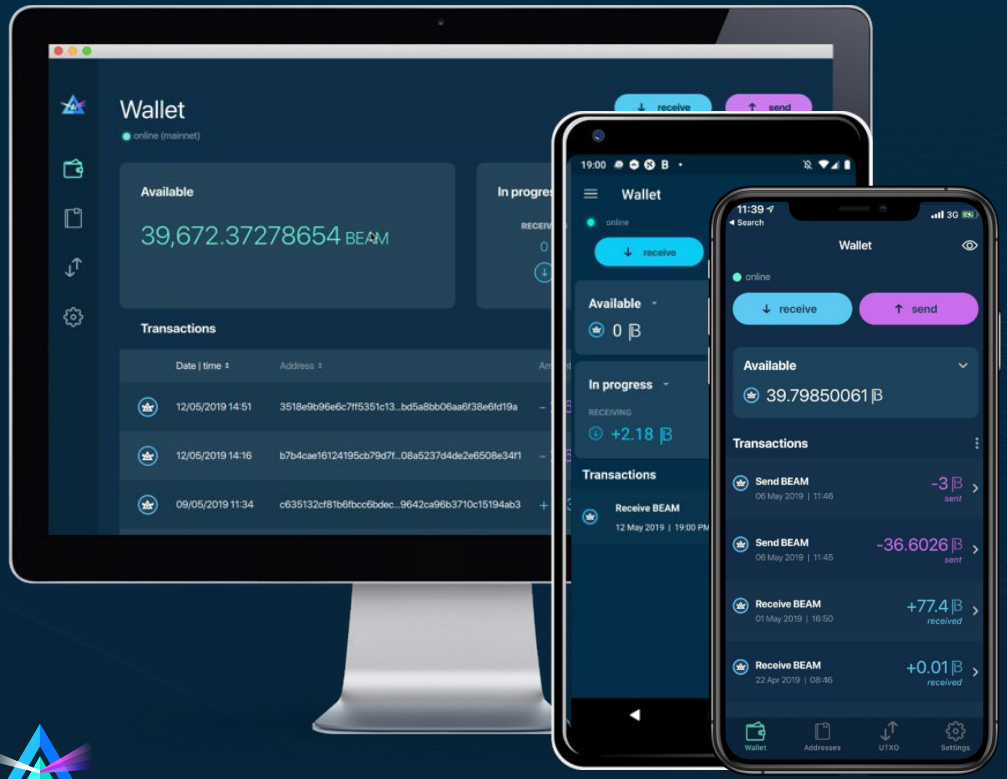


# Dandelion++




- Probabilistic Forwarding
- Decoy outputs for best privacy

# Current status




- Over 1.4M transactions
- 400K(?) GPUs
- Accepted in dozens of online stores
- Beautiful and usable wallets for all platforms
- Atomic Swaps
- In the works:
  - Hardware wallets
  - Lightning
  - One-sided Transactions

BEAM

# Some Highlights

One-sided payments

- No need to be online
- Recipient creates a set of UTXOs with *compensatory kernel*
- Sender can create transaction without Receiver participation

Trezor T

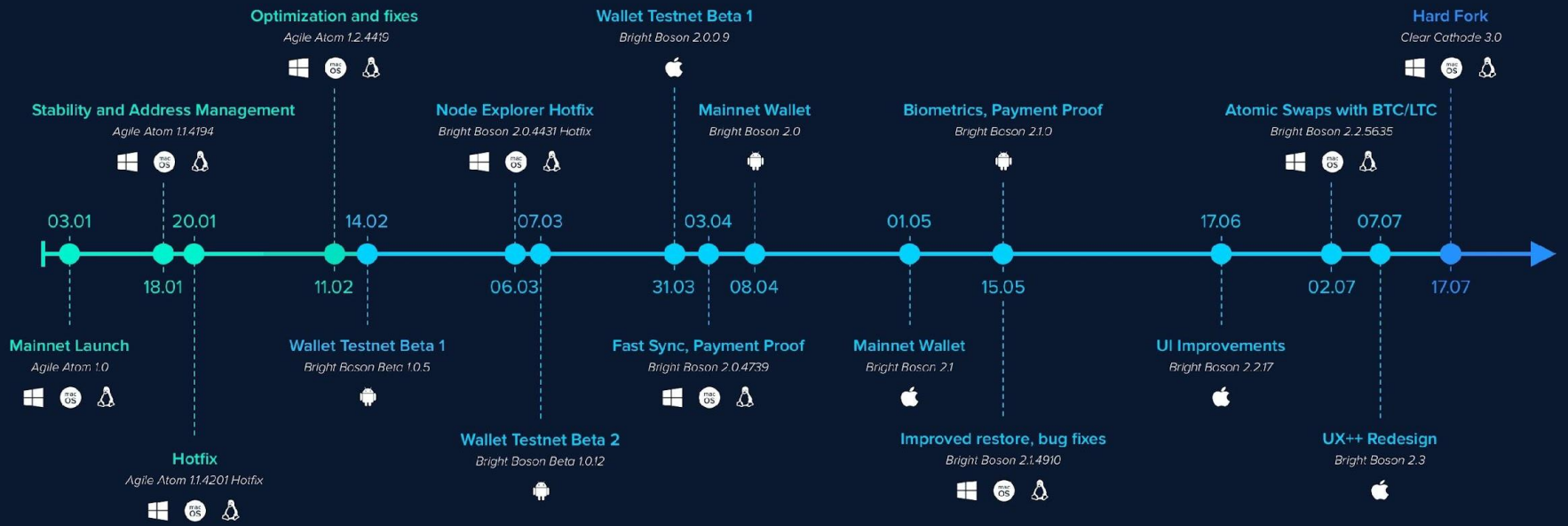

Pull request submitted

Laser Beam

- Lightning-like payment channels
- Fast payment, no fees
- Routing – at a later stage

BEAM

# Beam Releases in 2019



# Beam Hard Fork – August 15 2019

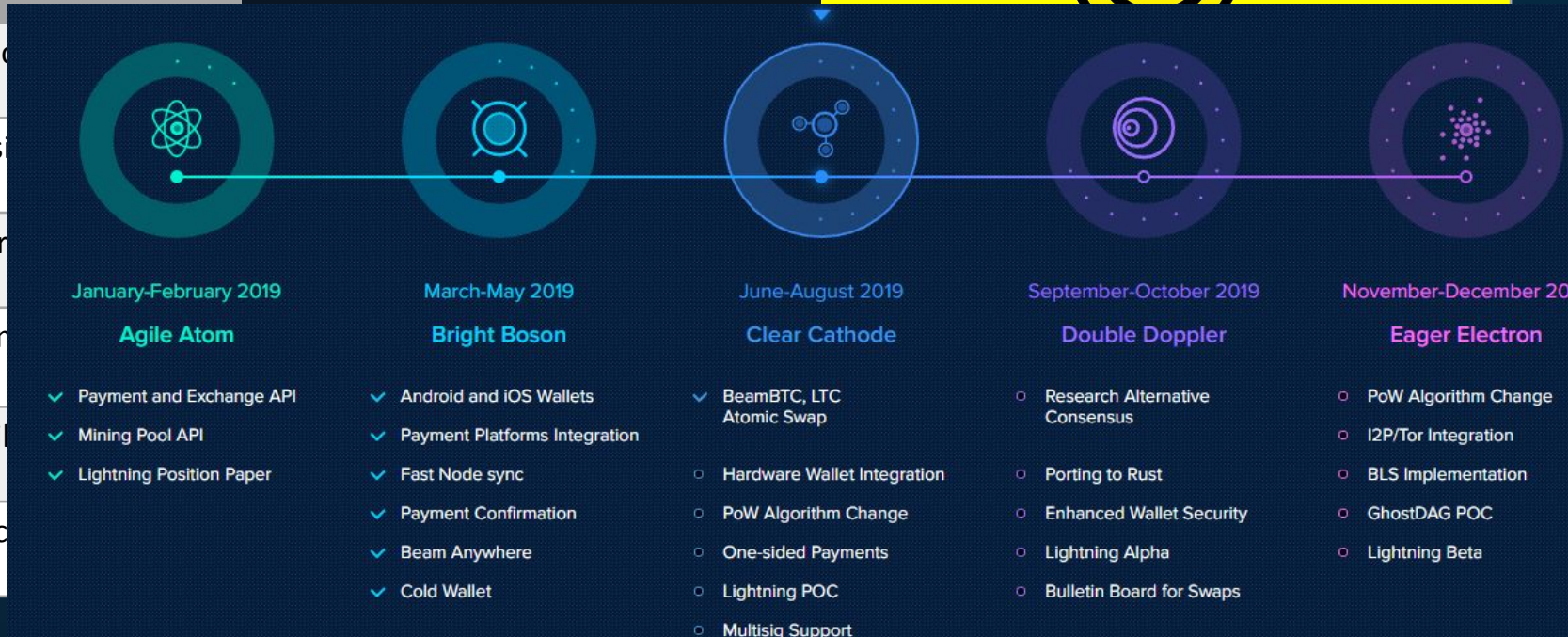
- Beam Hash I -> Beam Hash II
- Based on EquihashR - modified Equihash n=150, k=5
- Memory Requirement: approx. 3.2Gb, same as Beam Hash I
- Better Energy Efficiency, more sols/sec

| | BeamHash | | BeamHash II | |
|---|---|---|---|---|
| | Perf | Watts | Perf | Watts |
| AMD Radeon 7 | 17.5 sol/s | 206 W | 23.6 sol/s | 175 W |
| Nvidia GTX 1080 | 8.5 sol/s | 132 W | 11.3 sol/s | 118 W |

- MAKE SURE TO UPGRADE ALL THE SOFTWARE BEFORE Aug 15

# Beam and Grin

| | BEAM | MW |
|---|---|---|
| Protoc | | |
| Emissi | | |
| Gover | | |
| Roadr | | |
| Usabil | | |
| Privac | | |




BEAM

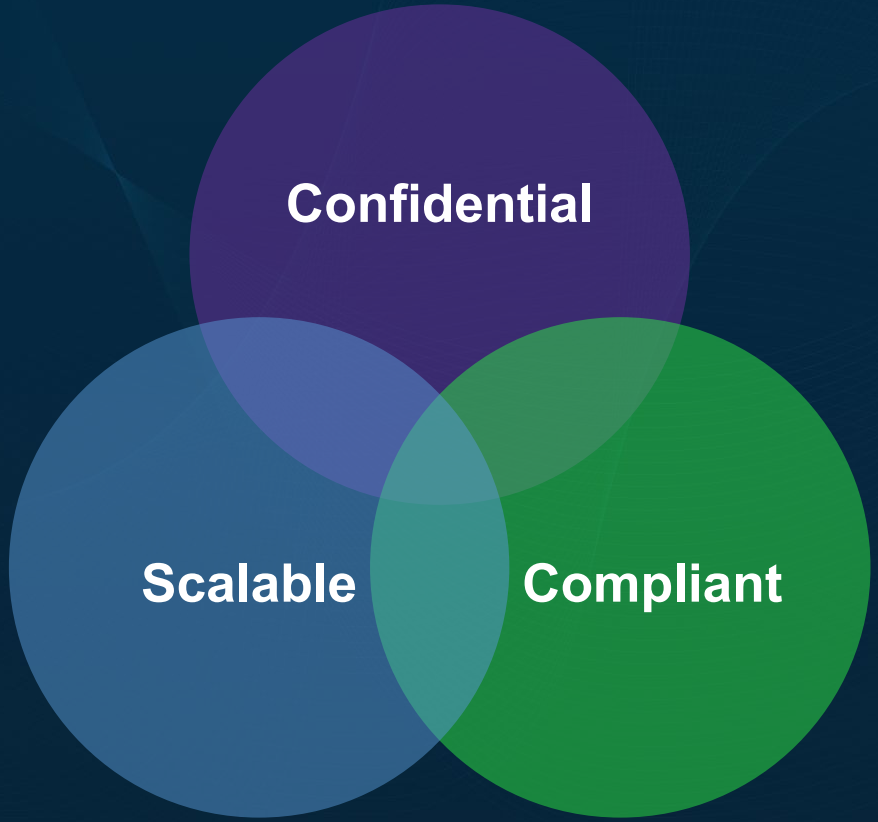
## Problem solve

Confidenti


ability

# Our reality

# A digital currency must be

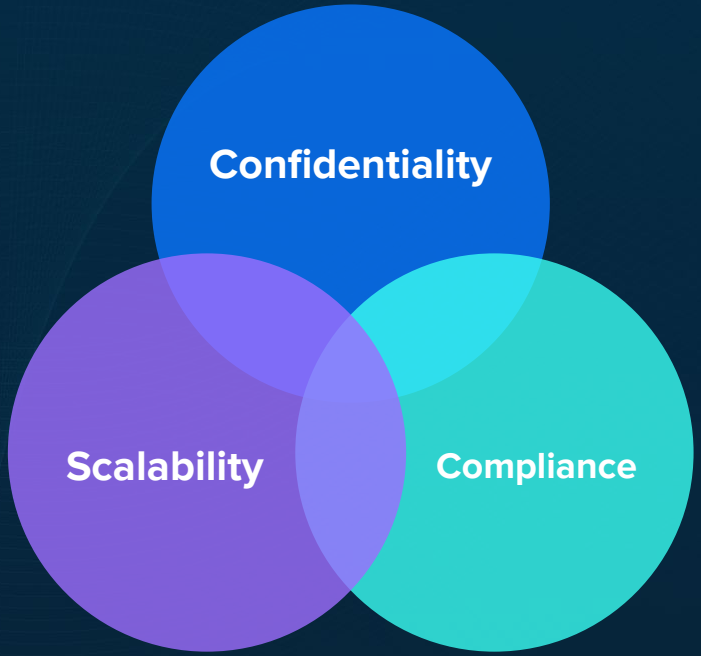



BEAM

# And not just currency

- Permissionless Digital Cash
- Stablecoins
- Security Tokens
- Derivatives
- State-owned Digital Cash
- Enterprise Use Cases
- And more..

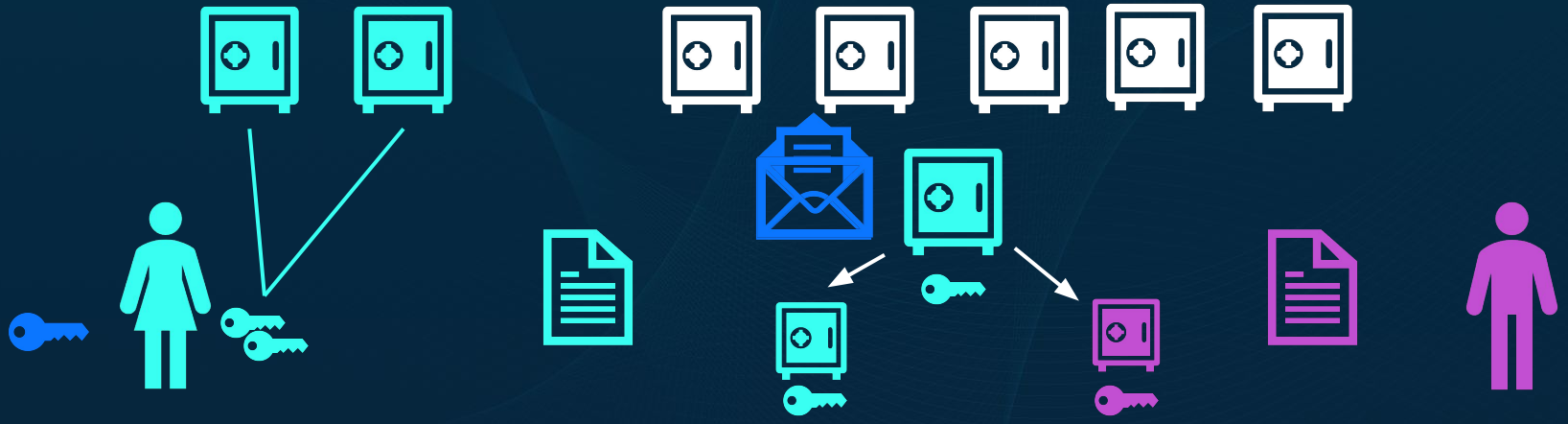
All require

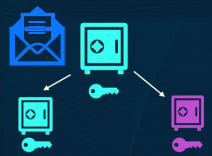



**Today: Pick Any One**

BEAM

# Opt-in Compliance in Beam





# What next?


To Innovation Av
CONTINUE STRAIGHT
North
Shaw Road
EXIT HERE

# Why and What

We want a world where crypto coexists with legacy financial ecosystem and makes operations **cheaper**, **faster** and **better**

We are building a platform for transfer of diverse kinds of value that is **confidential**, **scalable** and optionally **compliant**

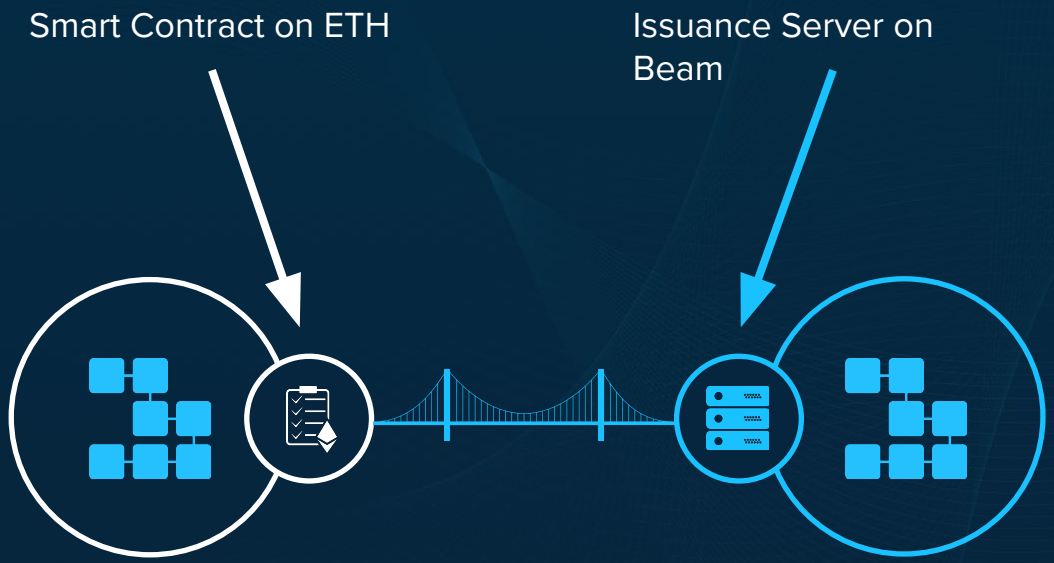
# Confidential Assets

- An Asset on Beam is represented by a Pedersen Commitment:
  - P = v*H + r*G
  - H and G are EC points known to everyone, v is Value, r is the secret key
- Confidential Assets are issued by choosing a new H
- Transactions are processed similarly to the Native token
- New Assets can be issued by anyone for a small network fee

**Confidential Asset Metadata:**

- ✔ Name
- ✔ Description
- ✔ Total supply
- ✔ Emission schedule
- ✔ Certificate of the Issuer
- ✔ Issuer's public key
- ✔ Address of Contract server
- ✔ Authorization Signature

# Bridges

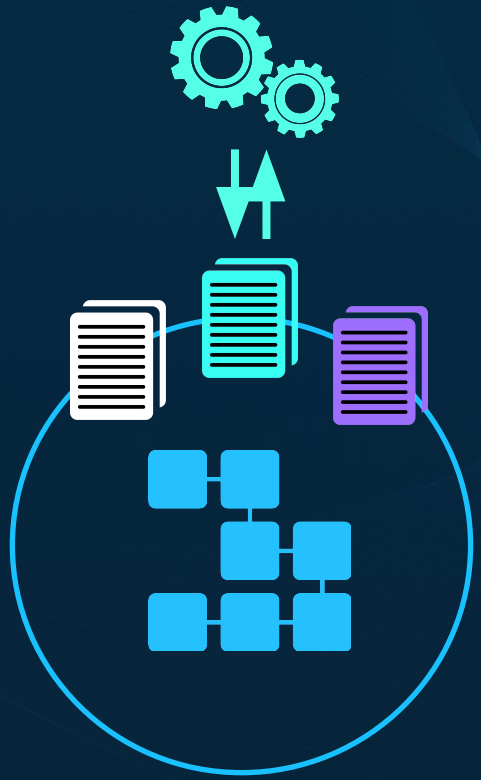



Use cases: stablecoins, utility tokens, NFT

**The process**

1. Assets are locked in a smart contract on foreign network
2. The Bridge issues matching assets on Beam
3. Asset is freely and confidentially traded
4. Holder of the asset can send it to Bridge and burn it, releasing the foreign asset

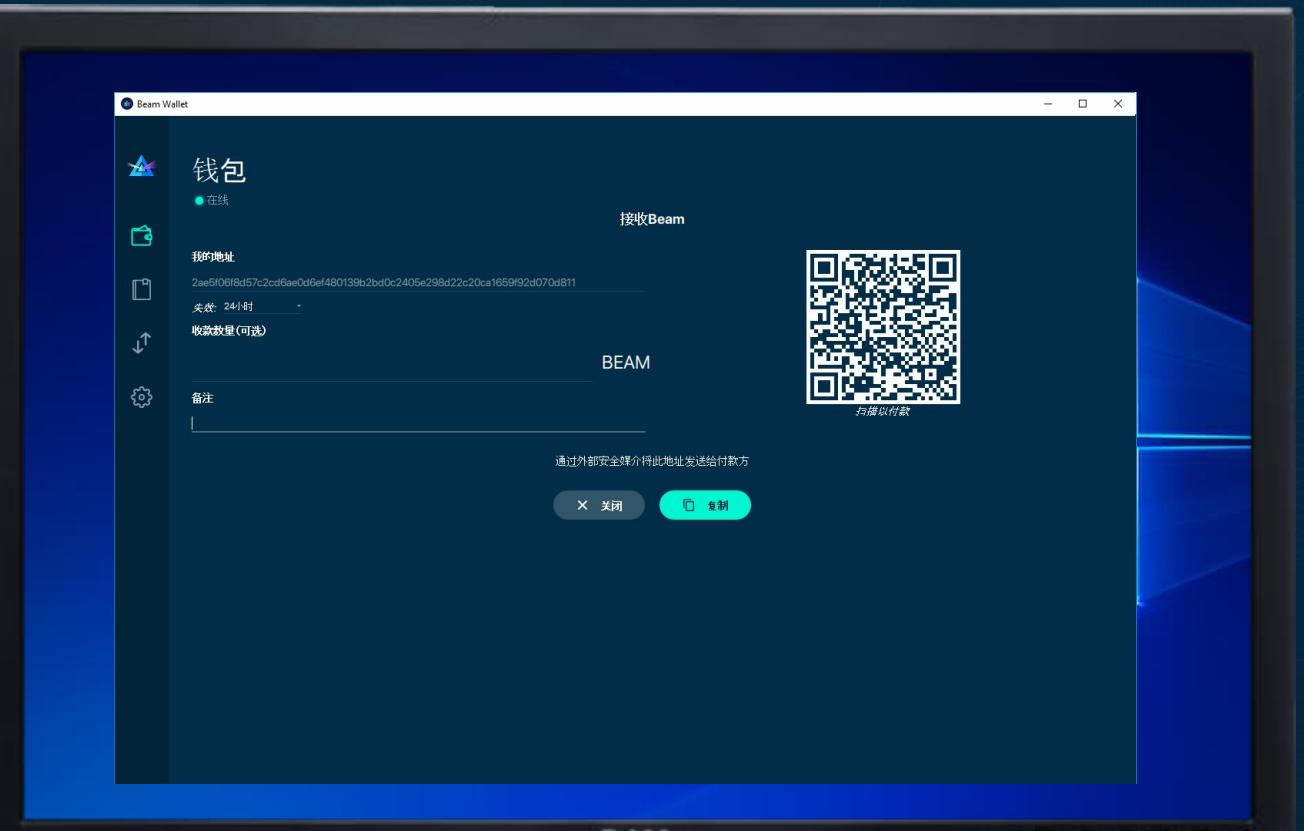
# Oracle-based Smart Contracts for STOs and more



**The process**

1. Issuer registers a new Confidential Asset class
2. To trade the asset, A and B create a transaction
3. They attach relevant info (contract, KYC, etc.) and send to Issuer
4. If approved, the Issuer produces signs the transaction with its private key
5. Nodes validate the transaction and presence of the Authorization Signature

# And, one more thing




# Get Beam Wallets Now

Get your Beam coins:

- In Beam Wallet, click “receive”
- Copy your address
- Connect to @beambbot on Telegram
- Type /faucet <your address>

# Thank you!

BEAM

https://www.beam.mw

https://t.me/BeamPrivacy

https://medium.com/beam-mw

QQ GROUP: 909677190

BEAM