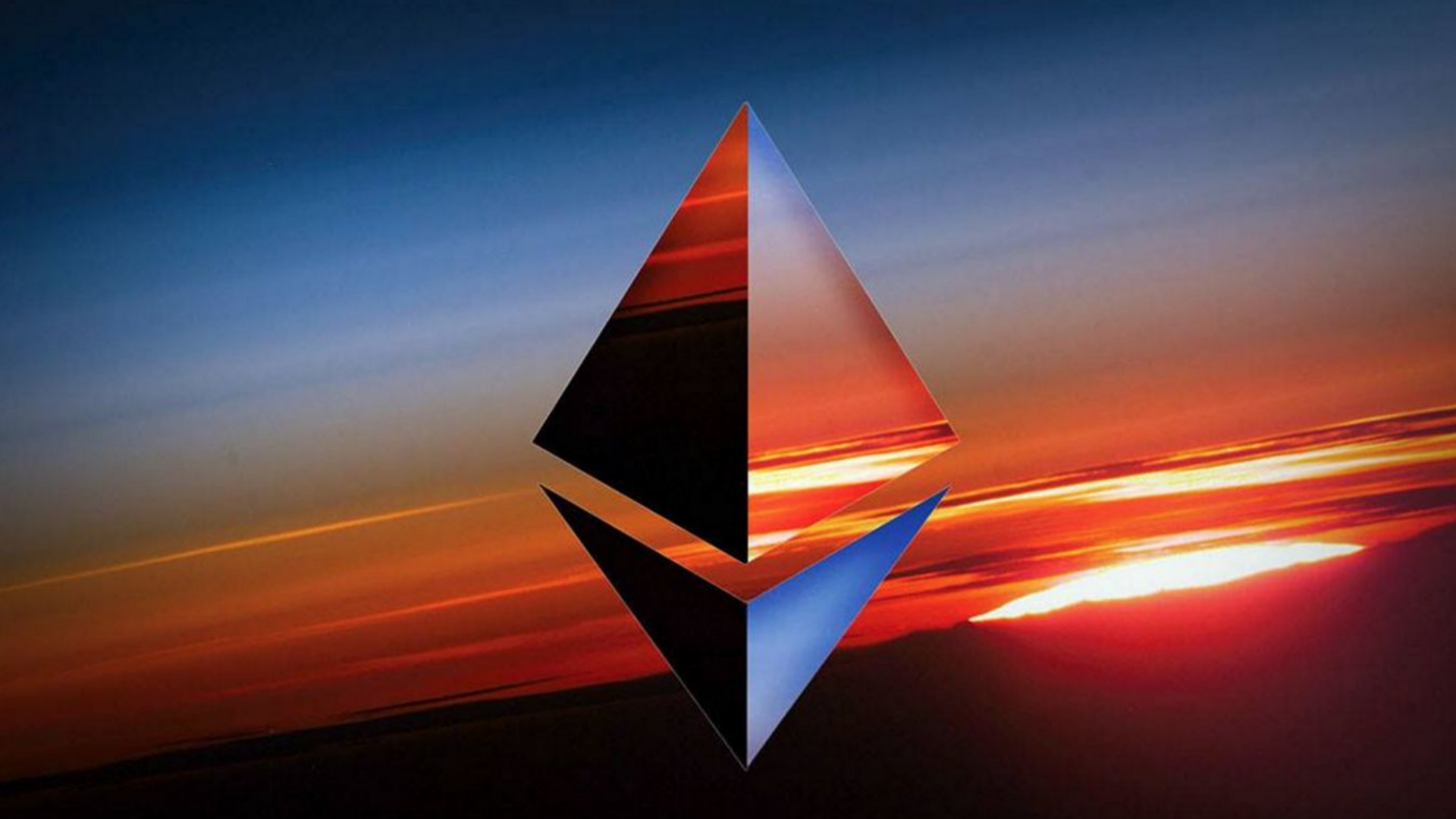


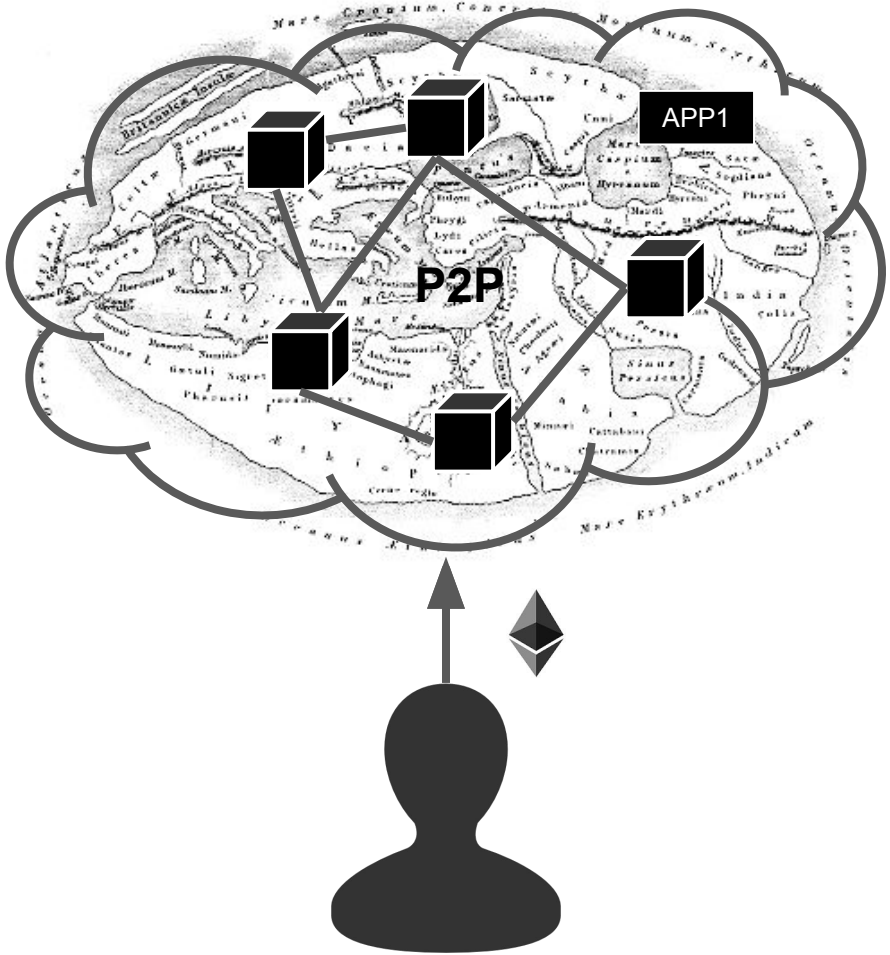
adrià massanet
computer engineering
18 y computer security
analogsynth / complex systems / nlp
founder @ bcn eth dev meetup
techdev WG @ blockchaincatalunya
4’5y freelance
twitter @codecontext
adria@codecontext.io

adria@codecontext.io

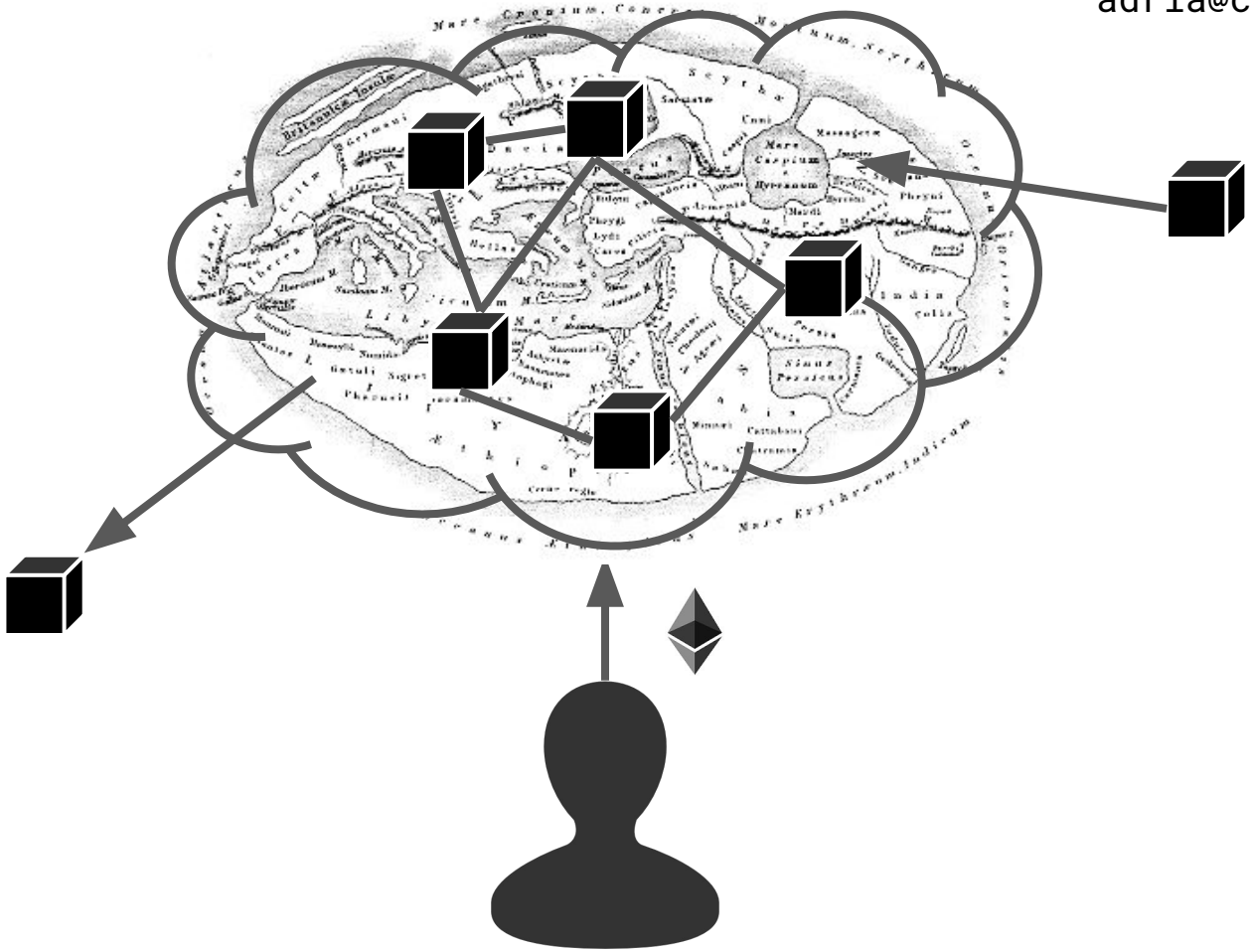
ethereum como PaaS

adria@codecontext.io

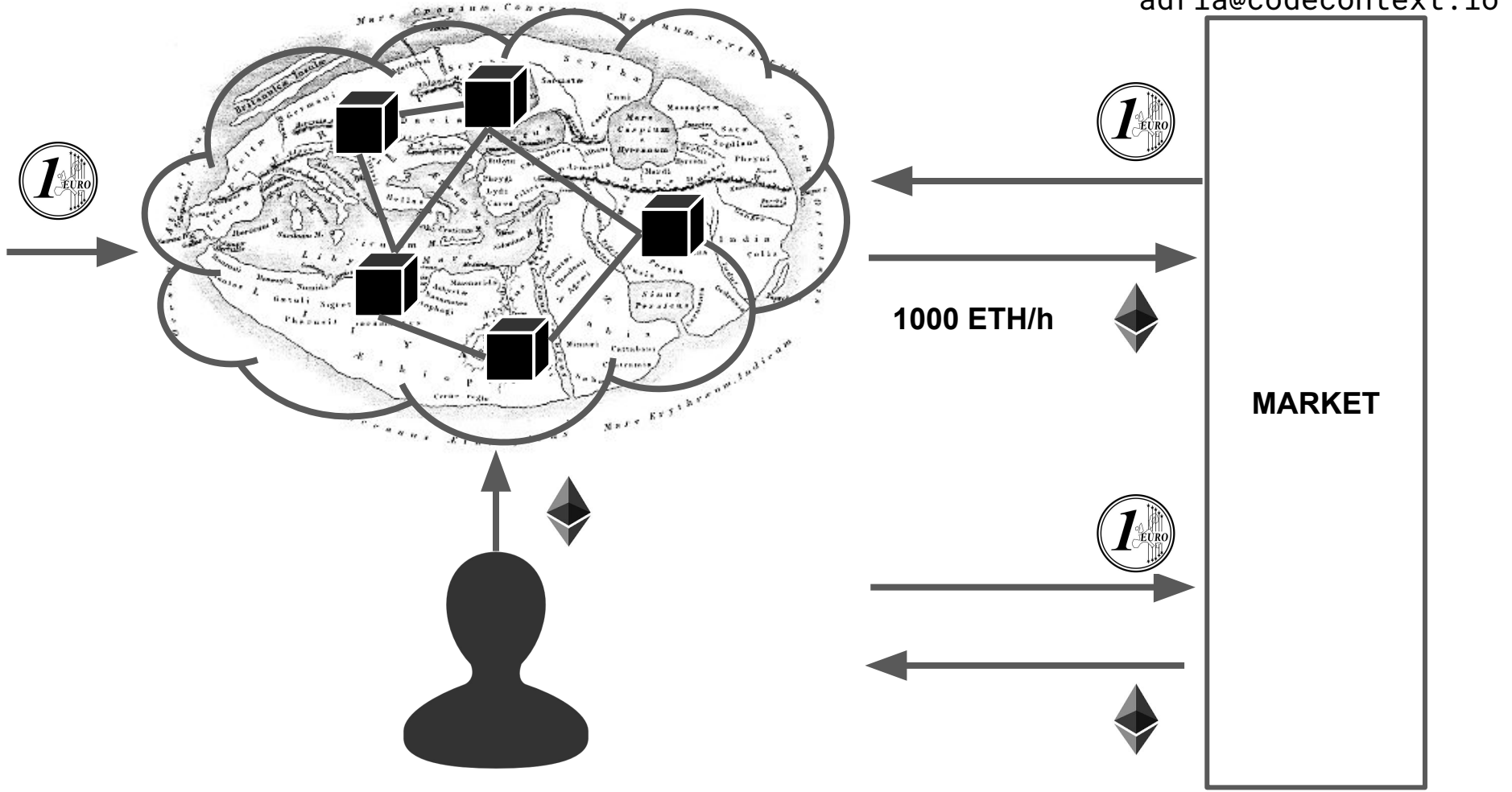
adria@codecontext.io



adria@codecontext.io



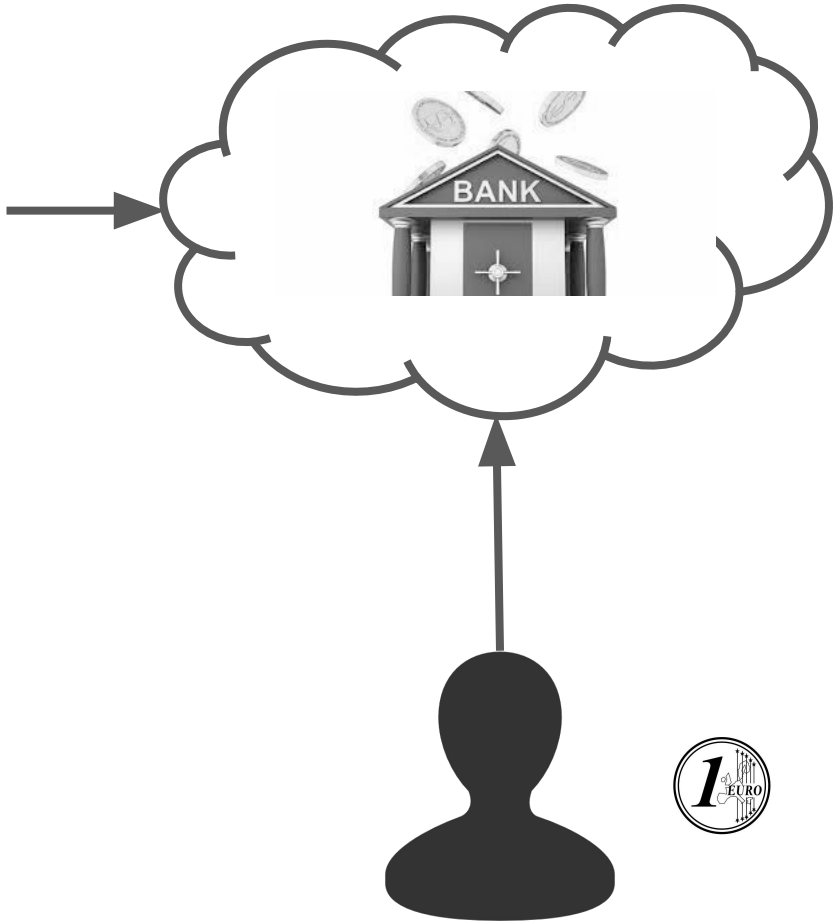
adria@codecontext.io



adria@codecontext.io

ethereum como servicio **seguro**

Garantías: regulación auditorias

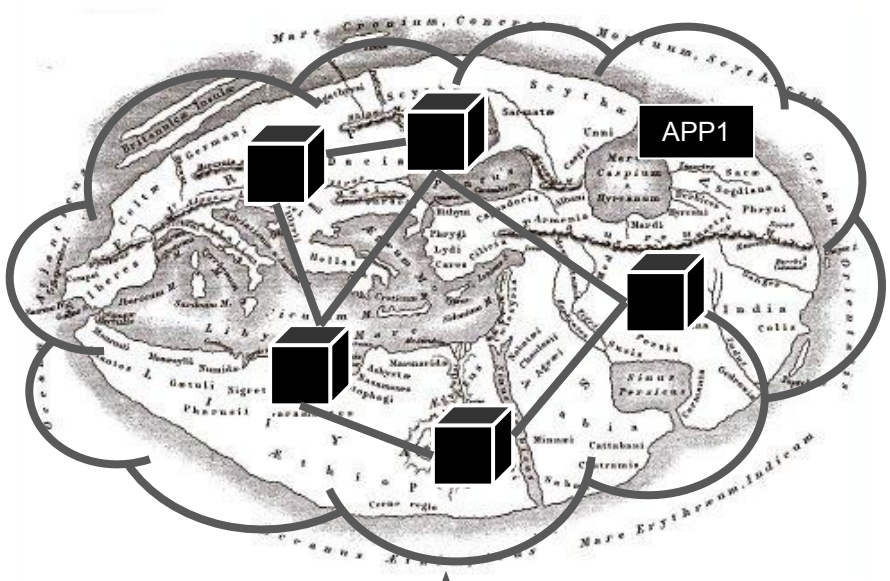


Banco es autoridad “Solo tu puedes acceder a las aplicaciones que gestionan tu dinero”*

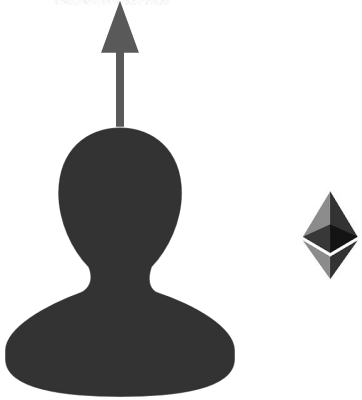
Código de acceso a Banca Online

adria@codecontext.io

Garantías: criptografia



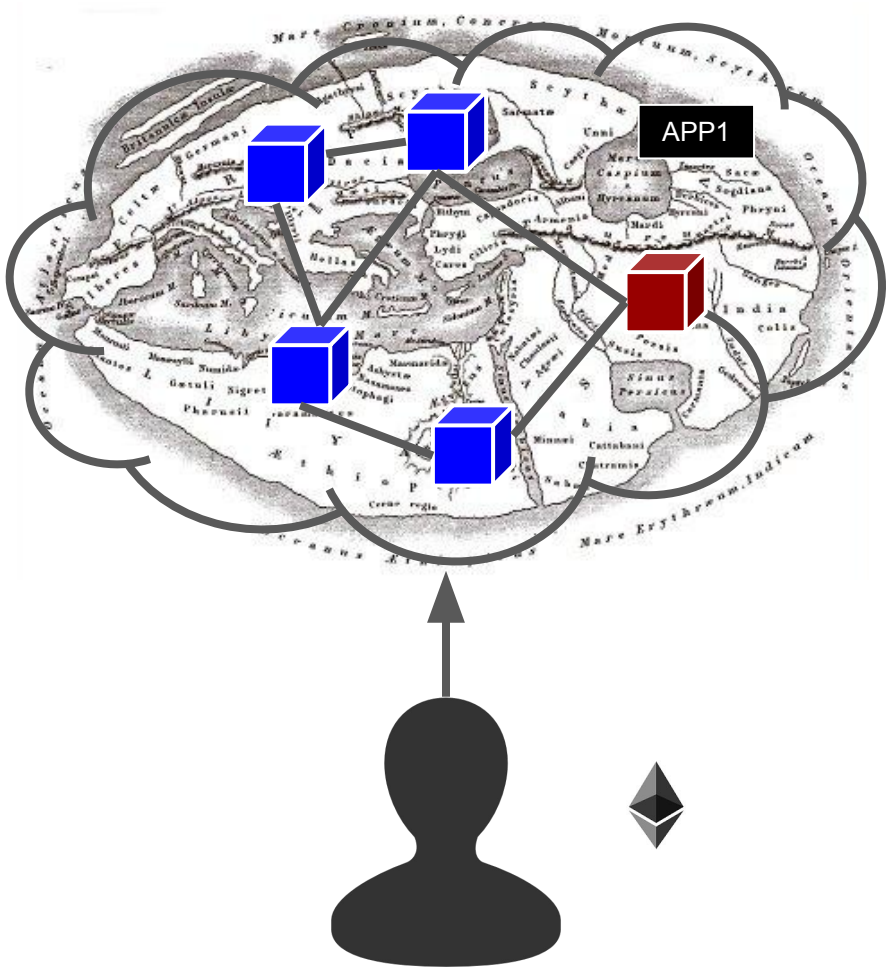
Ethereum es autoridad “Solo tu puedes acceder a las aplicaciones que gestionan tu dinero”*



Clave privada criptográfica personal

adria@codecontext.io

Garantías: criptografia

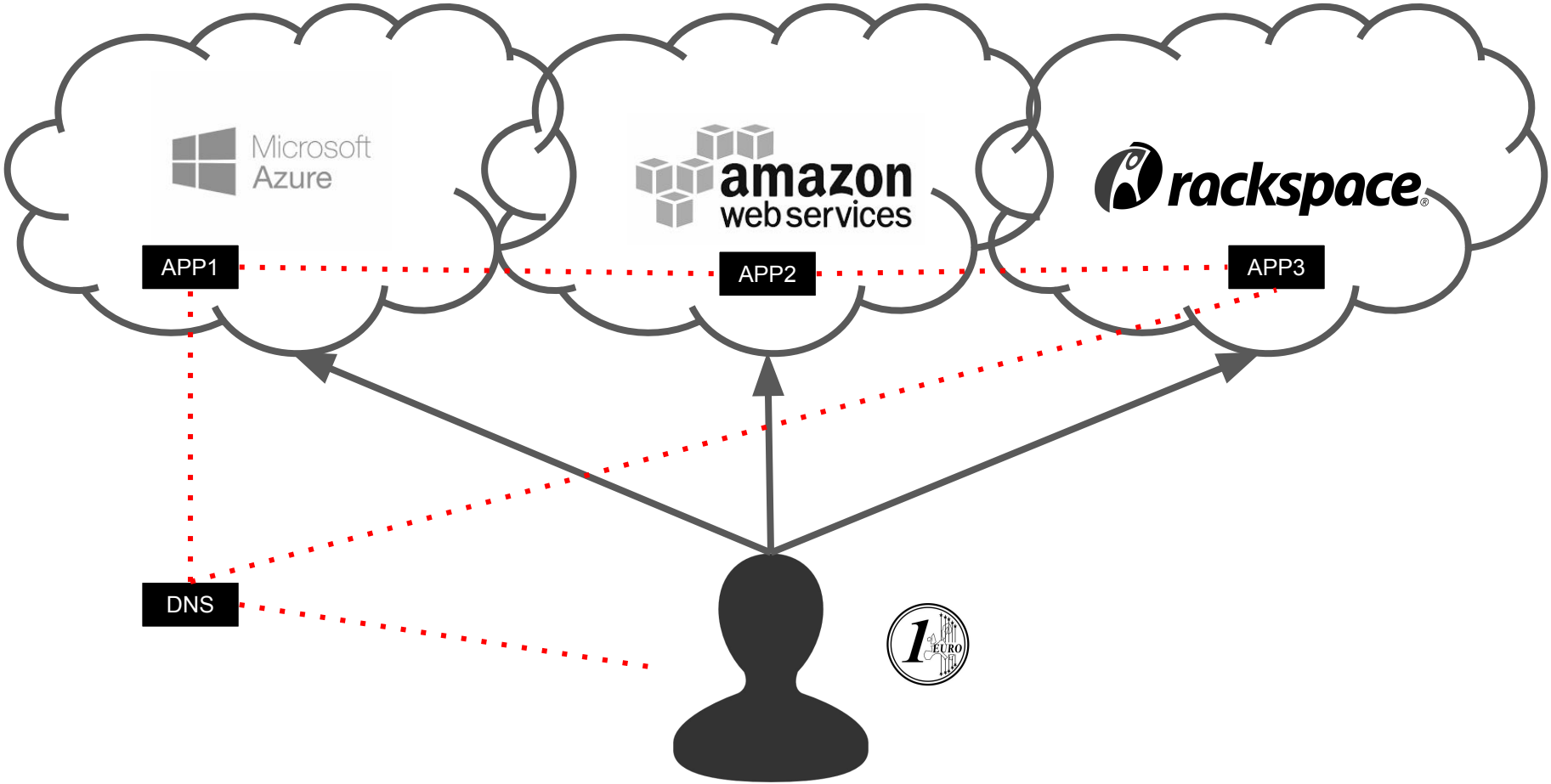


Ethereum es autoridad “Solo tu puedes acceder a las aplicaciones que gestionan tu dinero”*

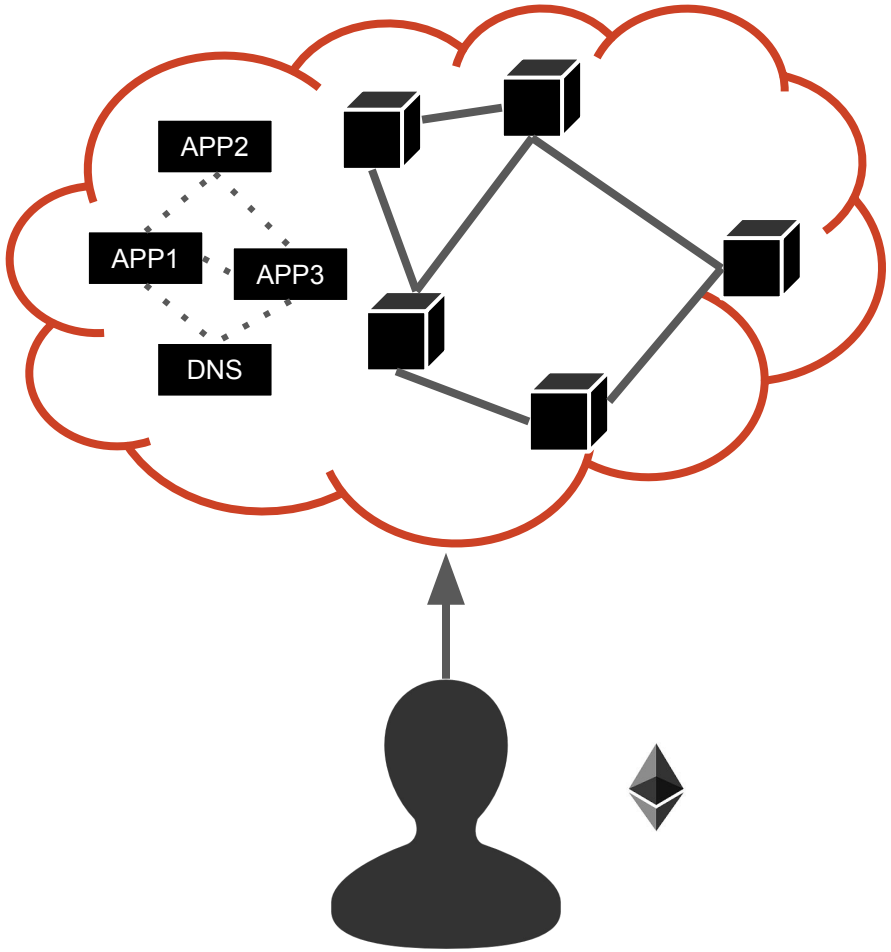
Clave privada criptográfica personal

adria@codecontext.io

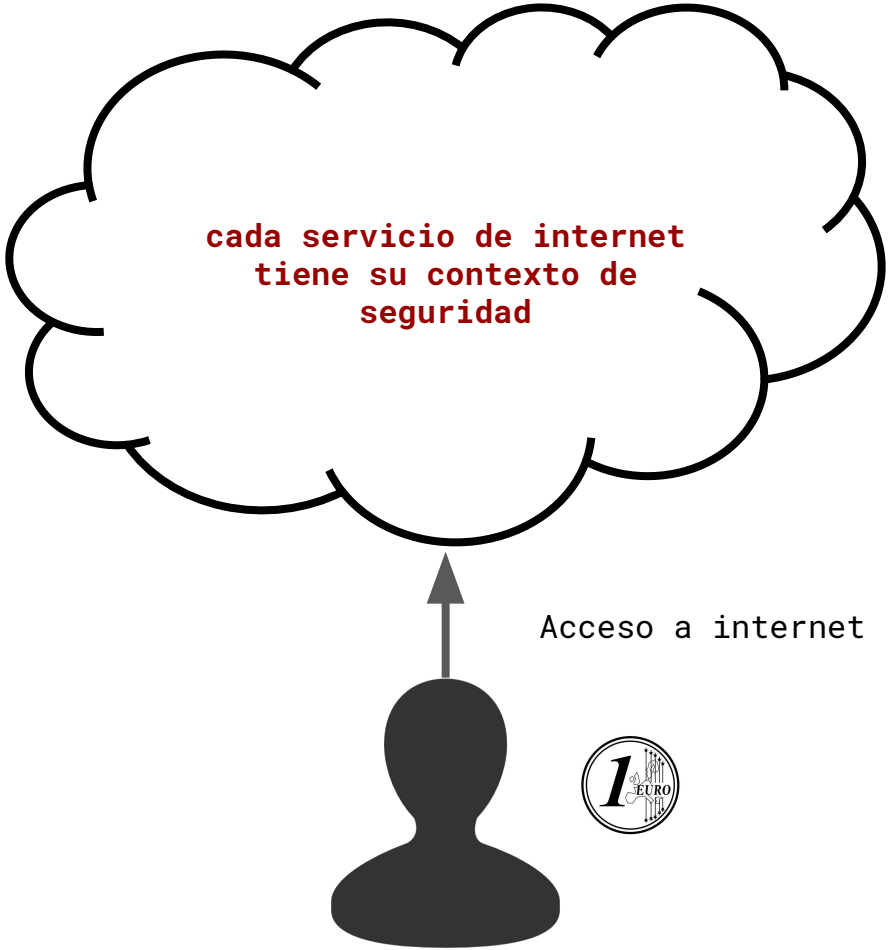
ethereum como un
único computador global seguro

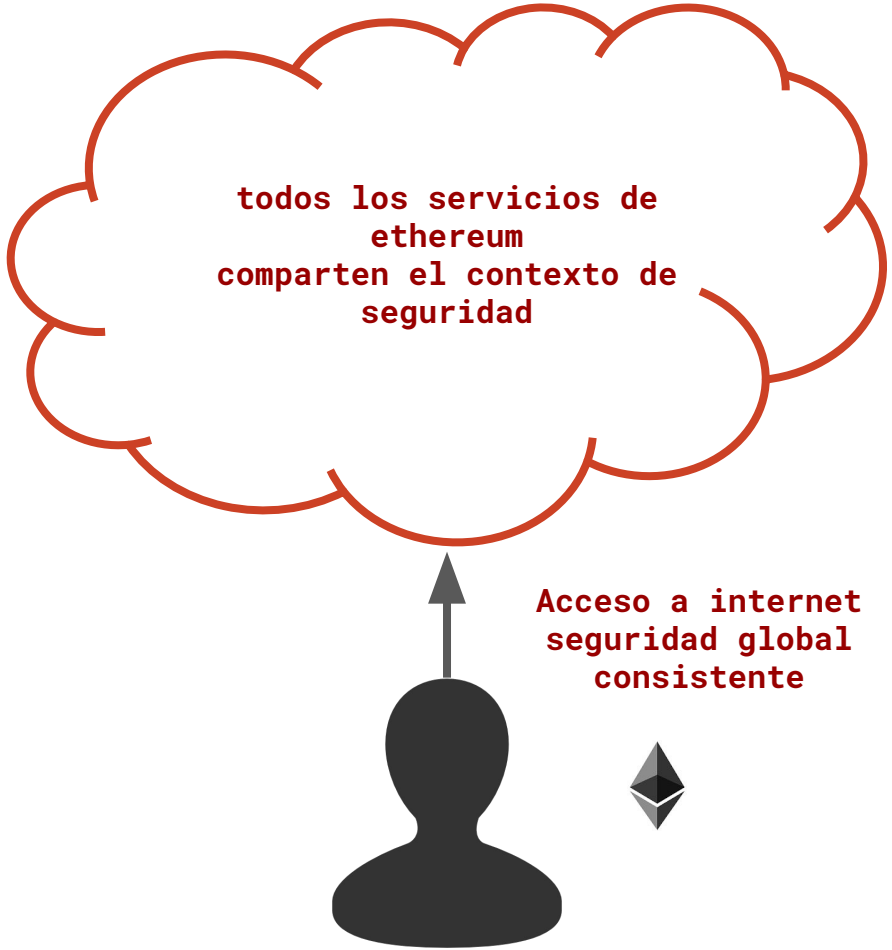


adria@codecontext.io

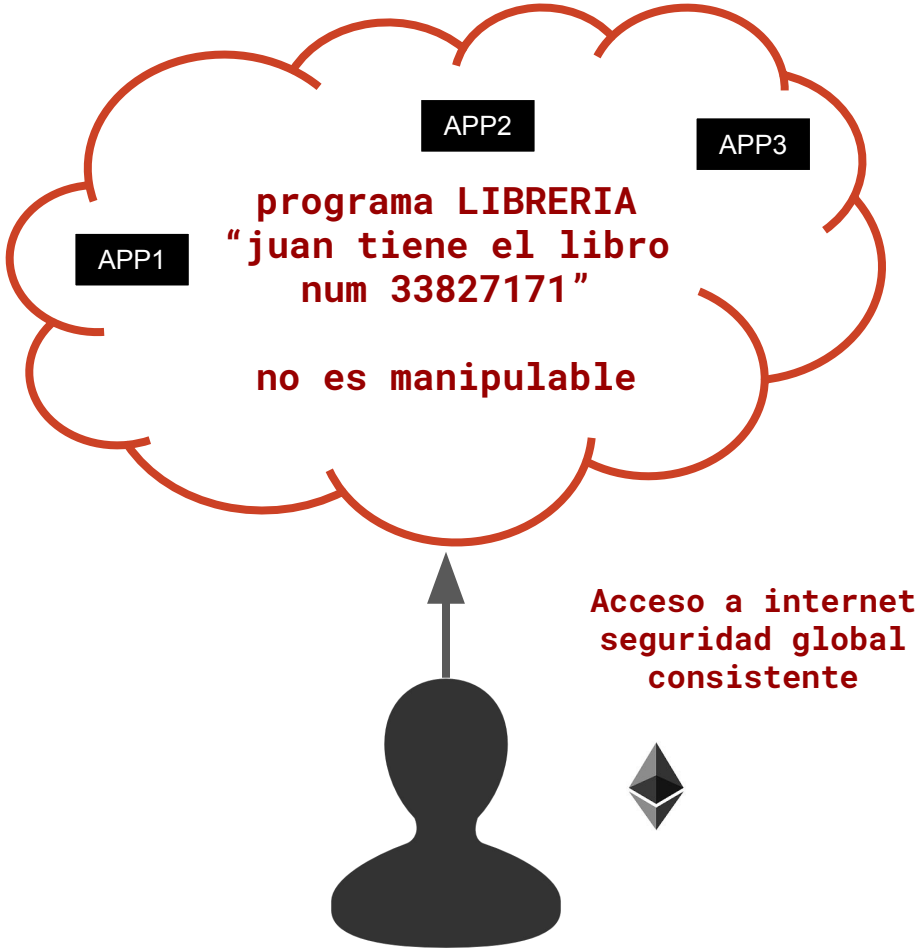

APP2
APP1
APP3
DNS

adria@codecontext.io





adria@codecontext.io



adria@codecontext.io

“juan tiene el libro num 33827171”
los que consensuamos que ethereum no es manipulable
y es una fuente de autoridad descentralizada

consensuamos que juan tiene el libro 33827171

adria@codecontext.io

“juan tiene XXXXXXXXXX”
los que consensuamos que ethereum no es manipulable
y es una fuente de autoridad descentralizada

consensuamos que juan tiene **XXXXXXXXXX**

-> Virtualización “no copiable” de entidades
(tokenización)

adria@codecontext.io

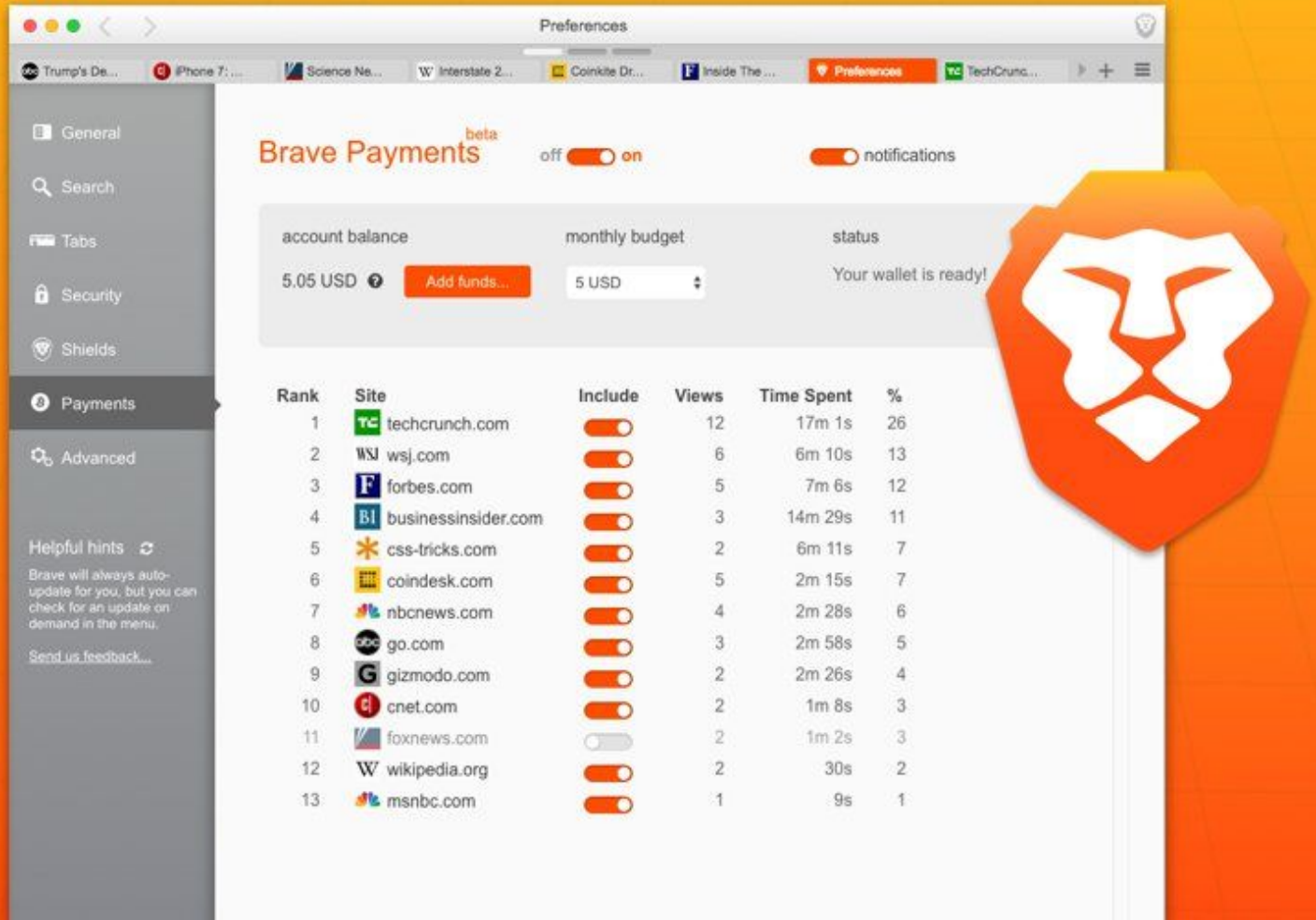
“juan tiene 2000 ETH”
los que consensuamos que ethereum no es manipulable
y es una fuente de autoridad descentralizada

consensuamos que juan tiene 2000 ETH

adria@codecontext.io

ethereum como el **sistema operativo del internet descentralizado**


DECENTRALIZE
ALL THE THINGS
memegenerator.net


Preferences
Trump's De...
iPhone 7: ...
Science Ne...
Interstate 2...
Coinkite Dr...
Inside The ...
Preferences
TechCrunc...
General
Search
Tabs
Security
Shields
Payments
Advanced
Helpful hints
Brave will always auto-update for you, but you can check for an update on demand in the menu.
Send us feedback...
Brave Payments beta
off on
notifications
account balance
5.05 USD
Add funds...
monthly budget
5 USD
status
Your wallet is ready!
Rank Site Include Views Time Spent %
1 techcrunch.com 12 17m 1s 26
2 wsj.com 6 6m 10s 13
3 forbes.com 5 7m 6s 12
4 businessinsider.com 3 14m 29s 11
5 css-tricks.com 2 6m 11s 7
6 coindesk.com 5 2m 15s 7
7 nbcnews.com 4 2m 28s 6
8 go.com 3 2m 58s 5
9 gizmodo.com 2 2m 26s 4
10 cnet.com 2 1m 8s 3
11 foxnews.com 2 1m 2s 3
12 wikipedia.org 2 30s 2
13 msnbc.com 1 9s 1

BALANCE

Deposit	Withdraw	Transfer
Token	Wallet	EtherDelta
SNT	0.000	0.000
Amount		Deposit
ETH	0.004	0.000
Amount		Deposit

Make sure SNT is the token you actually want to trade.
Multiple tokens can share the same name.

VOLUME

Pair	Daily	Bid	Offer
GRX	273677	0.012500000	0.012490000
PPT	70863	0.024510000	0.024695000
RDN	109845	0.011500000	0.011580260
ERC20	107023720	0.000000300	0.000000325
PPP	455015	0.001694000	0.001719999
VERI	2931	0.194200051	0.197500000
COB	1918910	0.000253461	0.000250000
ZRX	843052	0.000480000	0.000492919
OMG	20964	0.018000500	0.018000000
BLUE	2757077	0.000199000	0.000205000
GRID	172377	0.002748000	0.002749140
GMT	3248645	0.000107700	0.000107700
AION	130514	0.002400001	0.002430000
EOS	60619	0.005119462	0.005564999

ORDER BOOK

0.000127710	2000.000	0.255
0.000110000	5999.000	0.660
0.000110000	1000.000	0.110
0.000094000	3734.364	0.351
0.000093477	19460.240	1.819
0.000087778	10000.000	0.878
SNT/ETH	**SNT**	**ETH**
0.000074500	13422.819	1.000
0.000074093	24116.000	1.787
0.000073980	33792.917	2.500
0.000071262	20000.000	1.425
0.000071261	4000.000	0.285
0.000071200	235.911	0.017

NEW ORDER

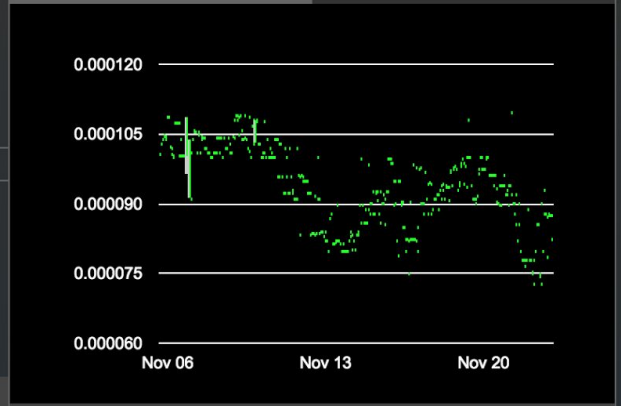
Buy | Sell

SNT	Amount to buy
SNT/ETH	Price
ETH	Total
Expires	10000

Buy

PRICE CHART

Price | Depth



MY TRANSACTIONS

Important | Trades | Orders | Funds

Notices

The only official URL for EtherDelta is https://etherdelta.com. Bookmark it once and use the bookmark.

Do not send your tokens directly to the smart contract, or they will be lost and unrecoverable. Use the Deposit form (upper left) to send the proper deposit transaction.

The only official representatives in the chat room are ETHERDELTAZACK_TWITTER, ETHERDELTAREP1_TWITTER, ETHERDELTAREP2_TWITTER, ETHERDELTAREP3_TWITTER, ETHERDELTAREP4_TWITTER, and ETHERDELTAUX_TWITTER.

Disclaimer

EtherDelta is a decentralized trading platform that lets you trade

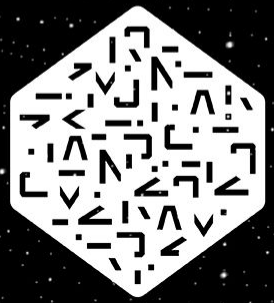
TRADES

SNT/ETH	SNT	ETH
0.000076940	5981.457	0.460
0.000082500	363.000	0.030
0.000087553	14.250	0.001
0.000087553	2835.750	0.248
0.000087650	347.403	0.030
0.000087770	6200.000	0.544
0.000087387	6000.000	0.524
0.000078500	3549.742	0.279
0.000087770	1000.000	0.088
0.000087770	300.000	0.026
0.000071200	0.154	0.000
0.000071200	1540.935	0.110
0.000000000	0.000	0.000
0.000000000	0.000	0.000
0.000000000	0.000	0.000
0.000000000	0.000	0.000
0.000000000	0.000	0.000

UPDATES

Tweets by etherdelta


MAKER

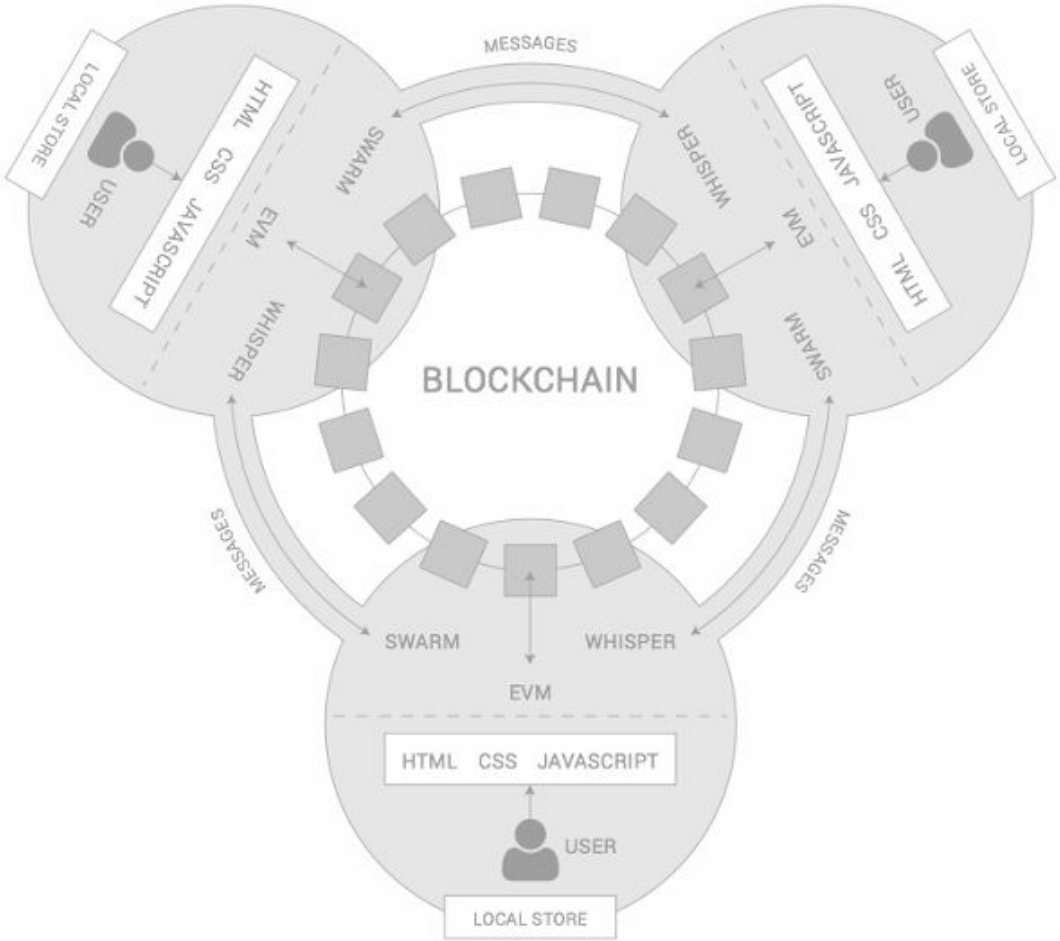


NUMERAI

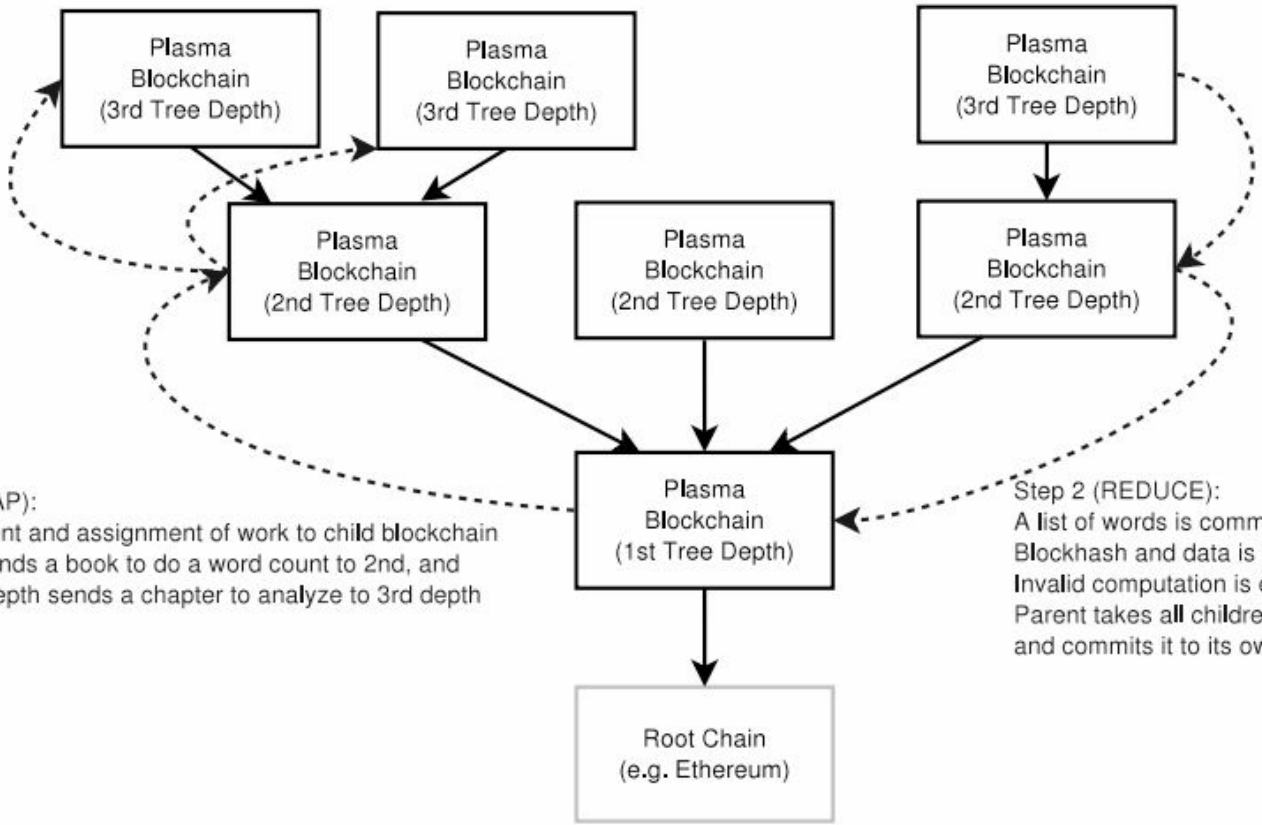
adria@codecontext.io

no únicamente ethereum

adria@codecontext.io



adria@codecontext.io



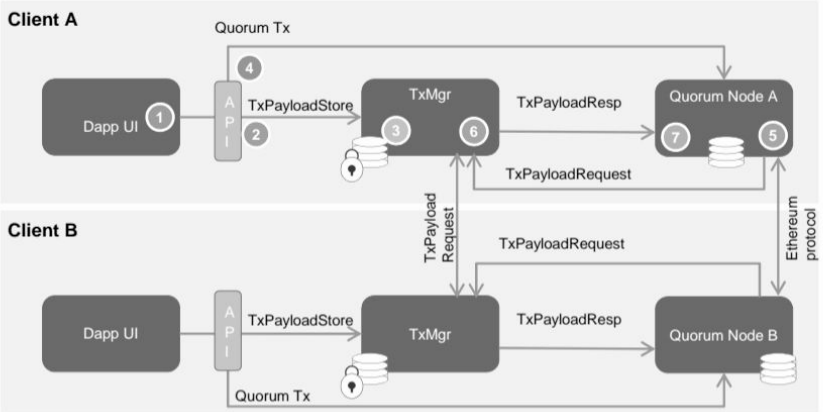
Step 1 (MAP):
Commitment and assignment of work to child blockchain
E.g. 1st sends a book to do a word count to 2nd, and
2nd tree depth sends a chapter to analyze to 3rd depth

Step 2 (REDUCE):
A list of words is committed to and the proof is merklelized
Blockhash and data is committed to the parent.
Invalid computation is enforcible and if proven is penalized.
Parent takes all children and further combines the wordlist
and commits it to its own parent.

adria@codecontext.io

A pragmatic approach to privacy

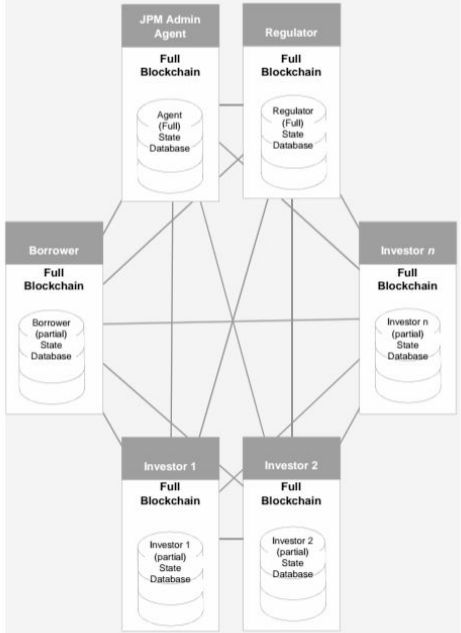
Simple Privacy Design



1. Dapp sends transaction to Quorum Node, specifying recipient and transaction payload
2. **Prepare Tx Payload Record** by generating a symmetric key, encrypt the payload with symmetric key, hash of the encrypted payload, encrypt the symmetric key with the public keys of the parties to the Tx, then send to the TxMgr for storage.
3. **TxMgr** validates the sending signature and stores the TxPayload message
4. **Tx sent** to the Quorum node containing only the hash of the encrypted payload generated in step 2.
5. **Quorum Node** receives a new block for validation containing the private Tx. It requests the payload data from the TxMgr (passing its Pubkey, TxHash, Sig).
6. **TxMgr** validates the signature, looks up the TxHash and if the requester is party to the Tx, return the encrypted payload and encrypted Symmetric key.
7. **Quorum Node** decrypts the symmetric key, decrypts the Tx Payload and sends to the EVM for contract code execution.

TxPayload includes:
- Hash of encrypted Tx payload (TxHash)
- Party 1 Public Key encrypted Symmetric Key
- Party 2 Public Key encrypted Symmetric Key
- Party *n* Public Key encrypted Symmetric Key

Full Blockchain, Partial State dB



adria@codecontext.io

Polkadot

What

Scalable heterogeneous multi-chain, allowing a large number of validatable, globally-coherent dynamic data structures to be hosted side-by-side

Why

In traditional blockchains, the way parties execute transactions is tied to how parties reach consensus

⇩

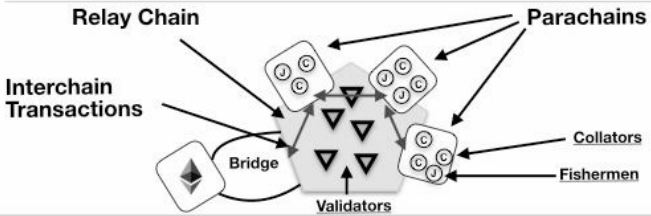
Multiple actors with different requirements are bundled by the same rules of the protocol, resulting in obstacles to scalability

Ecosystem

Collator
Assist in producing blocks:
- Maintain parachain by collecting transactions and creating unsealed blocks

Fisherman
Monitor network
- Detect and proof bad behavior of validators for a one-off bounty reward

Nominator
Select good validators:
- Secure the relay chain by staking tokens to signal trust for particular validator



Tokens: DOT issued via crowdsale

- Validators stake tokens to participate in consensus
- Nominators stake tokens to select good validators
- Fishermen get reward for detecting bad behaviors
- Other holders use tokens to govern network by voting on the relay chain

Use Cases

No specific application functionality (i.e. applicable for all blockchain use cases):
- Encrypted consortium chains
- High-frequency chains with very low block times

Main Innovations

Polkadot provides parallelized chains with pooled security and trust-free interchain transactability It means all aspects of each chain (parachain) may be conducted in parallel by a different segment of the network, allowing the network to scale. No action on the part of Ethereum is necessary to enable trustless transaction forwarding between Ethereum and Polkadot.

Main Features

- Minimal: by itself has as little functionality as possible
- Simple: no complexity in the base protocol
- General: no unnecessary requirements, constraints, limitations for parachains
- Robust: stable, economically sound and secure

Makes Possible

- Provides solution for scalability issues of current blockchain protocols via parallelized chains and interchain transactions
- Addresses the divergent needs of multiple parties and applications to a near optimal degree under the same framework

adria@codecontext.io

i ?

adria@codecontext.io

Un modelo de negocio que conozcais

Diseñad una gobernanza para una organización 100% horizontal

Qué valor aportan los intermediarios?

Cread nuevos actores que aporten ese valor en el modelo horizontal

Diseñad modelo criptoeconómico, coste por transacción más bajo

Desplegad en ethereum

Vosotros sois los nuevos intermediarios

Vitalik Buterin Follow
Feb 3 · 10 min read

Zk-SNARKs: Under the Hood

This is the third part of a series of articles explaining how the technology behind zk-SNARKs works; the previous articles on quadratic arithmetic programs and elliptic curve pairings are required reading, and this article will assume knowledge of both concepts. Basic knowledge of what zk-SNARKs are and what they do is also assumed. See also Christian Reitwiessner's article here for another technical introduction.

adria@codecontext.io

https://blockchaincatalunya.org/

https://www.meetup.com/ethereumbcn/

adria@codecontext.io / @codecontext

MOLTES GRÀCIES