Polimi Fintech Journey

An End-to-end Voting-system Based on Bitcoin

Stefano Bistarelli

bista@dmi.unipg.it

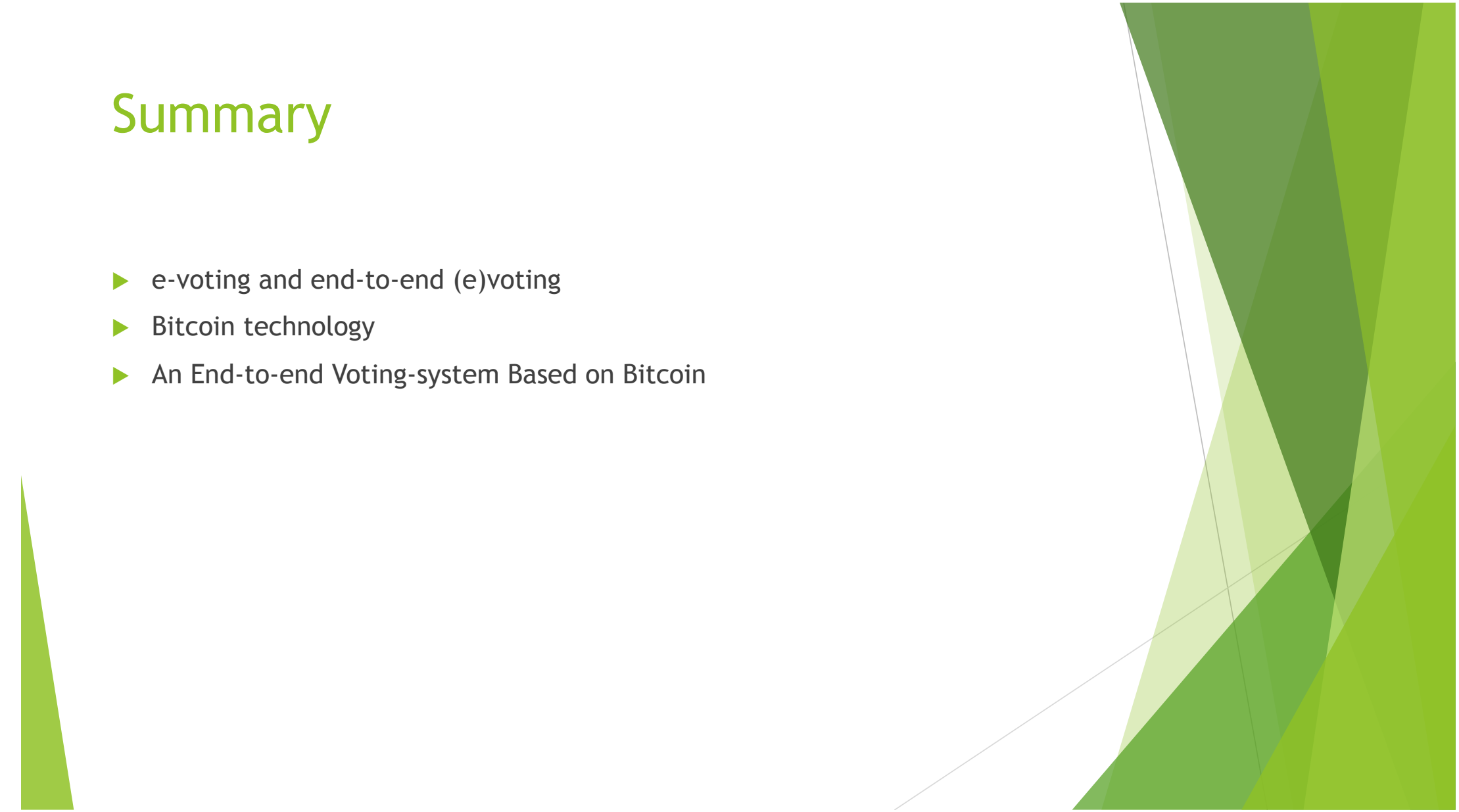
cini Cybersecurity National Lab

http://www.dmi.unipg.it/cybersecuritylab

from:
Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, Francesco Santini: An end-to-end voting-system based on bitcoin. SAC 2017: 1836-1841

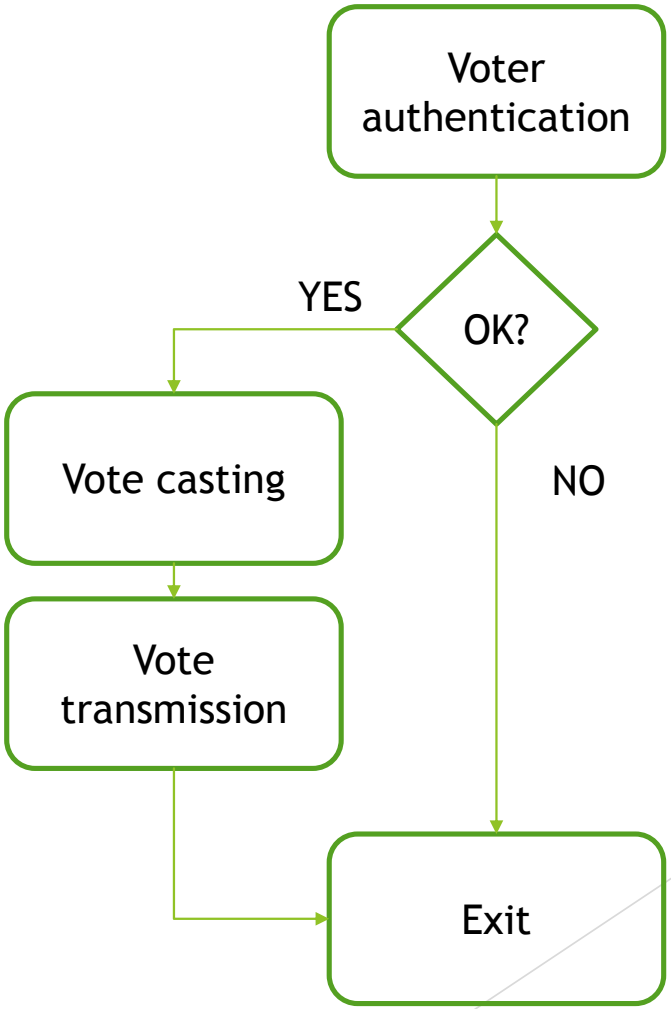
Summary

- e-voting and end-to-end (e)voting
- Bitcoin technology
- An End-to-end Voting-system Based on Bitcoin

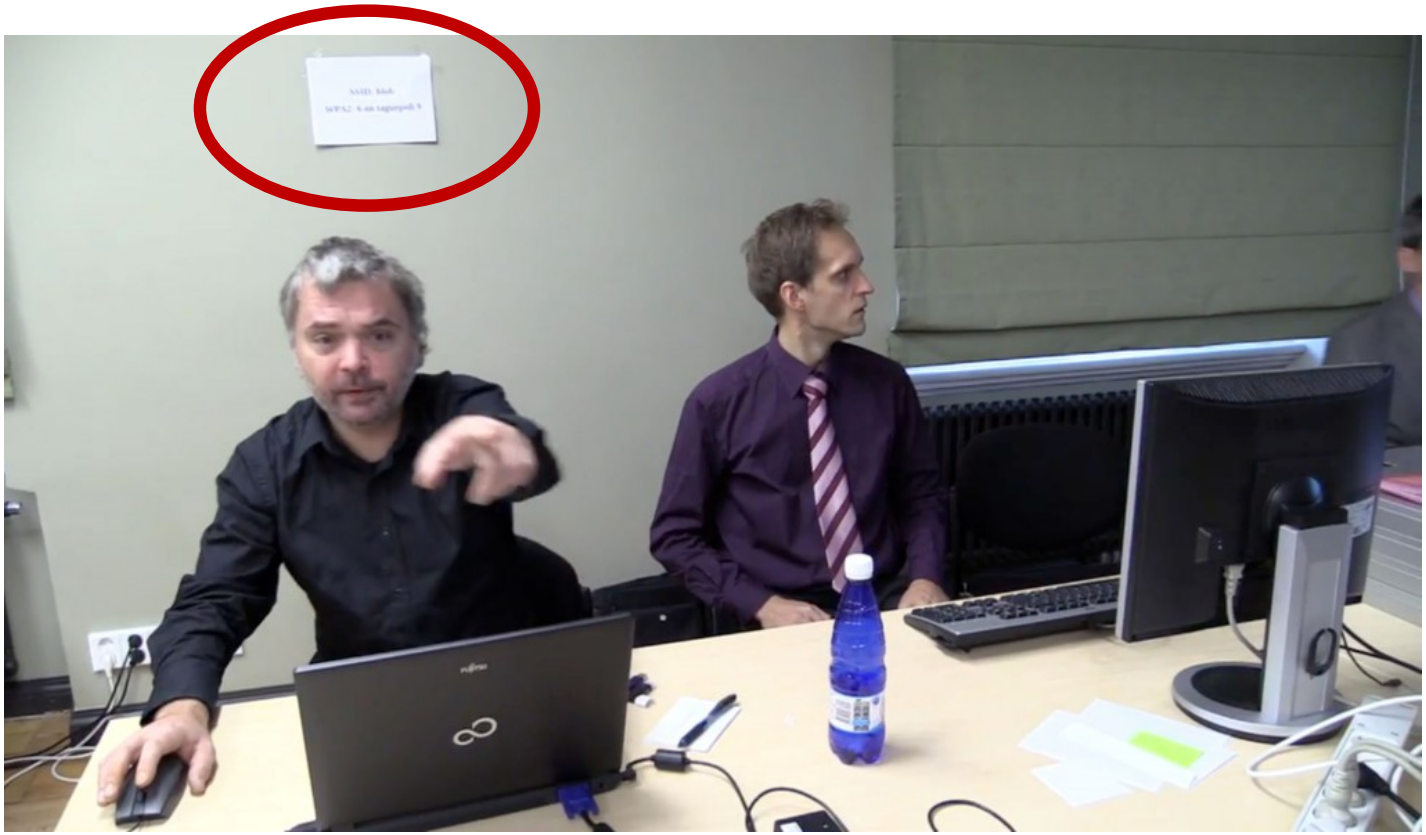


Voting systems

- electronic voting (also known as e-voting) is voting using electronic systems to aid casting and counting votes



E-voting in Estonia .. BEST PRACTICE????



Some criticism to some e-voting platforms

- Extreme Centralization
  - Single point of Failure
- Components of the architecture acting as a black box
- Not transparent polls

- This work only if we **completely trust** processes, servers, DBs, SWs, and on the officers working to maintain the architecture

E2E Voting systems

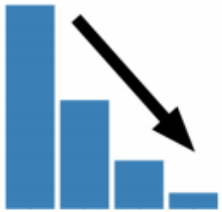
- End-to-end auditable or end-to-end voter verifiable (E2E) voting systems
  - attempt to cover the entire path from voter attempt to election totals, giving:
    - Voter auditing, and
    - Universal verifiability.
- Ex: helios
  Trust the vote.

bitcoin

Peer-to-peer transactions

No need for third parties

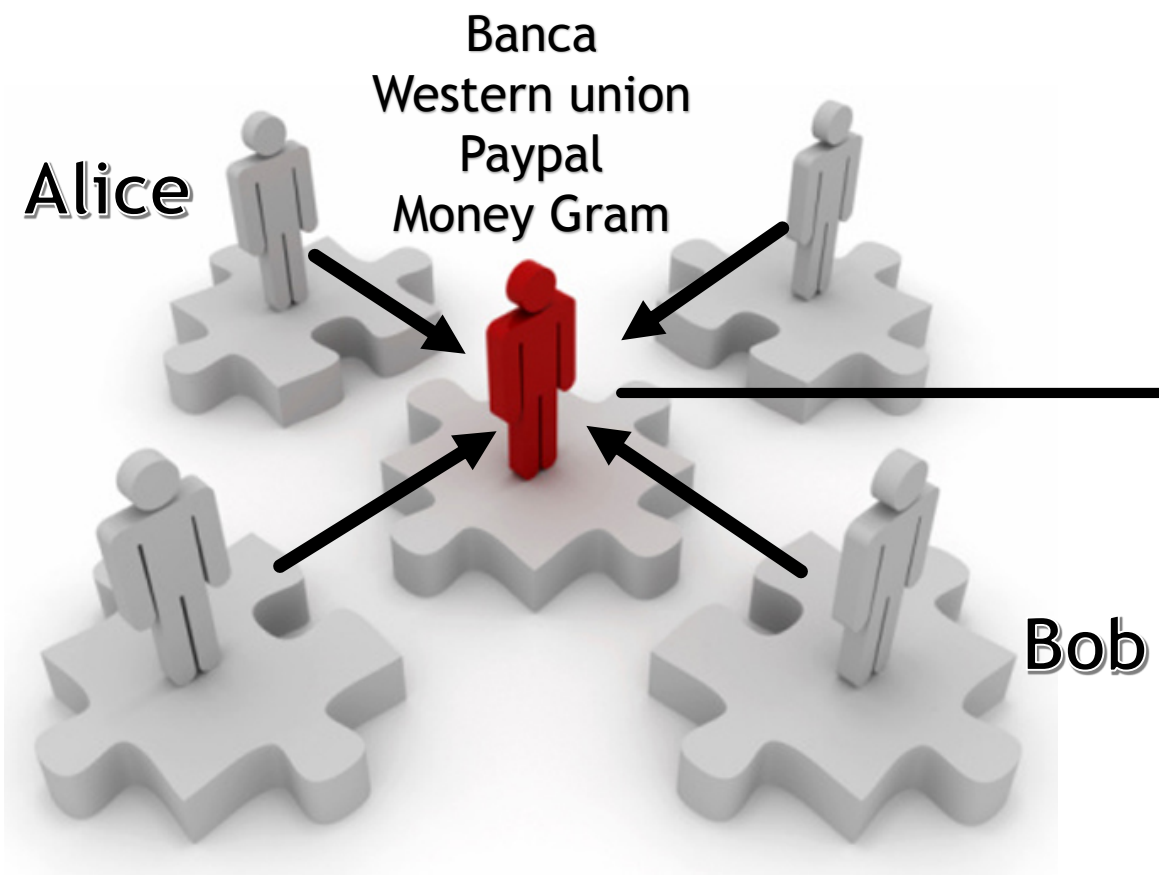
Worldwide payments



Low processing fees

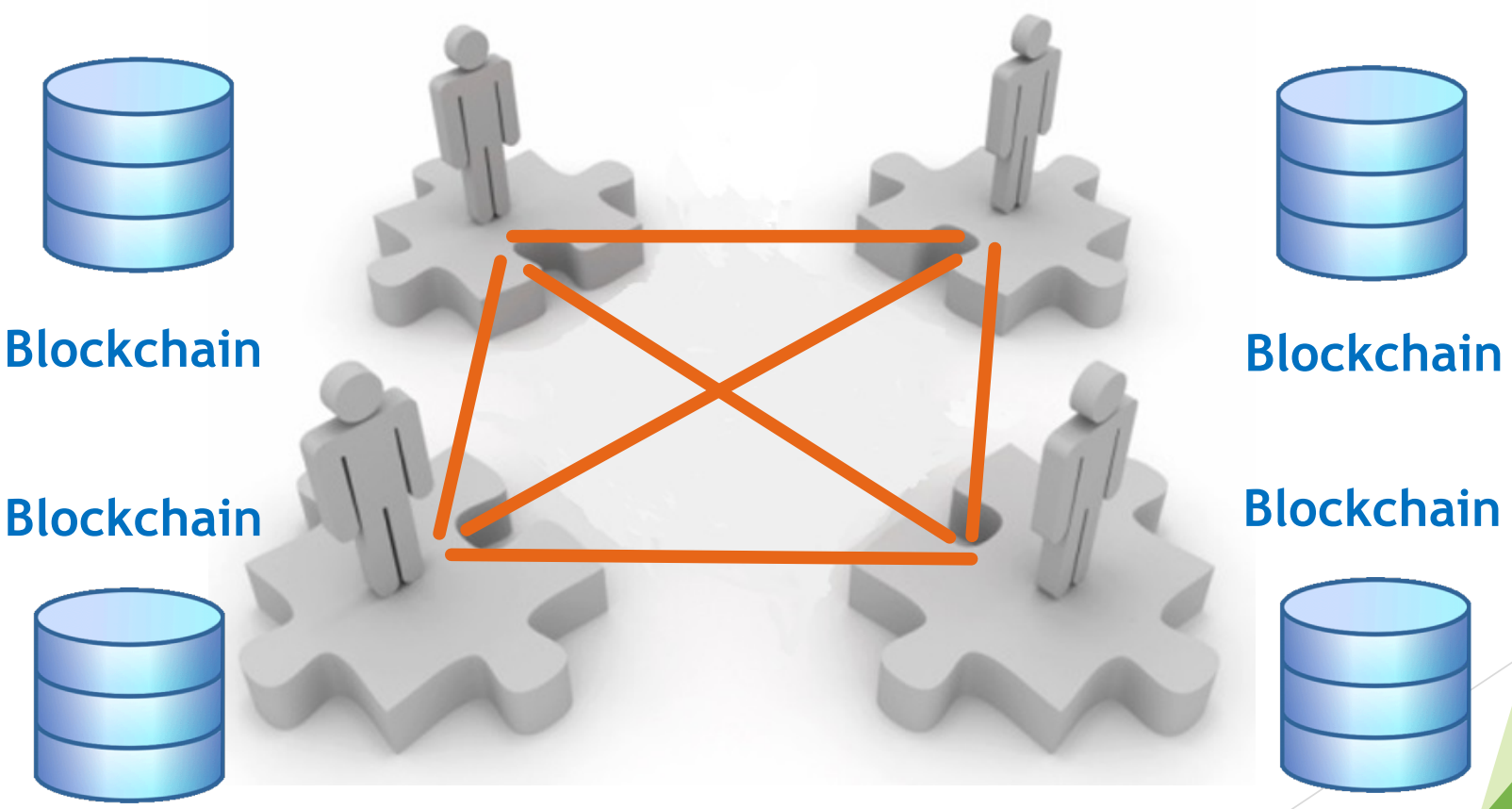
- 2008 S. Nakamoto. **Bitcoin: A peer-to-peer electronic cash system**. Whitepaper sent on cryptography mailing list.
- 2009 first version of bitcoin node implementation **Bitcoin-Qt**: start of the network and generation of the first bitcoins.

Before Bitcoin technology

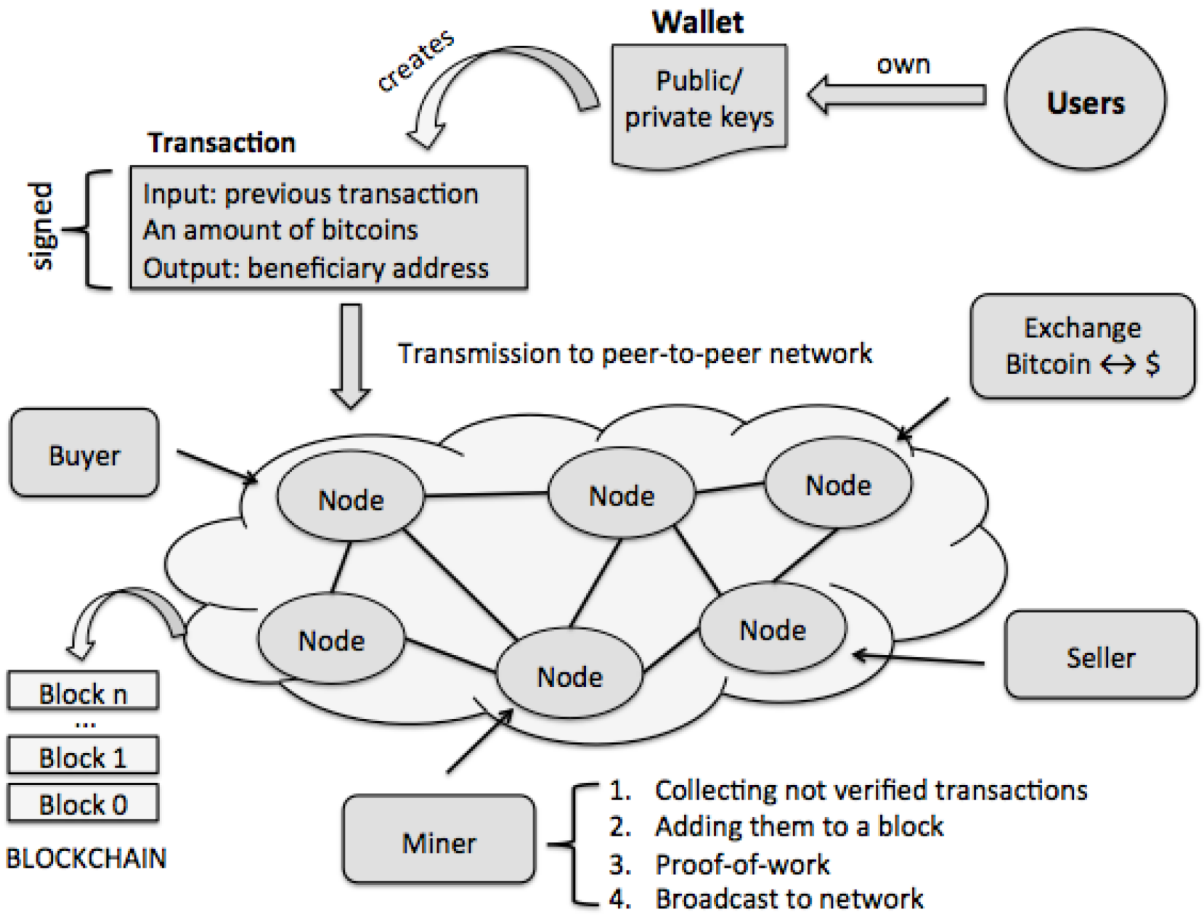


Financial DB with all the transactions

After Bitcoin



Bitcoin ecosystem



BITCOIN Transaction

Public key ALICE

Private key ALICE

Public Key BOB

Private key BOB

Transactionn-1	Transactionn	transaction n+1
• amount ofBTC • Link transactionn-2 • Lock transaction to K_Pub_Alice • Unlock transazione n-2 (Key signature)	• amount of BTC • Link transactionn-1 • Lock transaction to K_Pub_Bob • Unlock transactionn-1 (K_Priv_Alice)	• amount of BTC • Link transaction n • Lock transaction to KPubCharlie • Unlock transaction n (K_Priv_Bob)

Send of the transaction

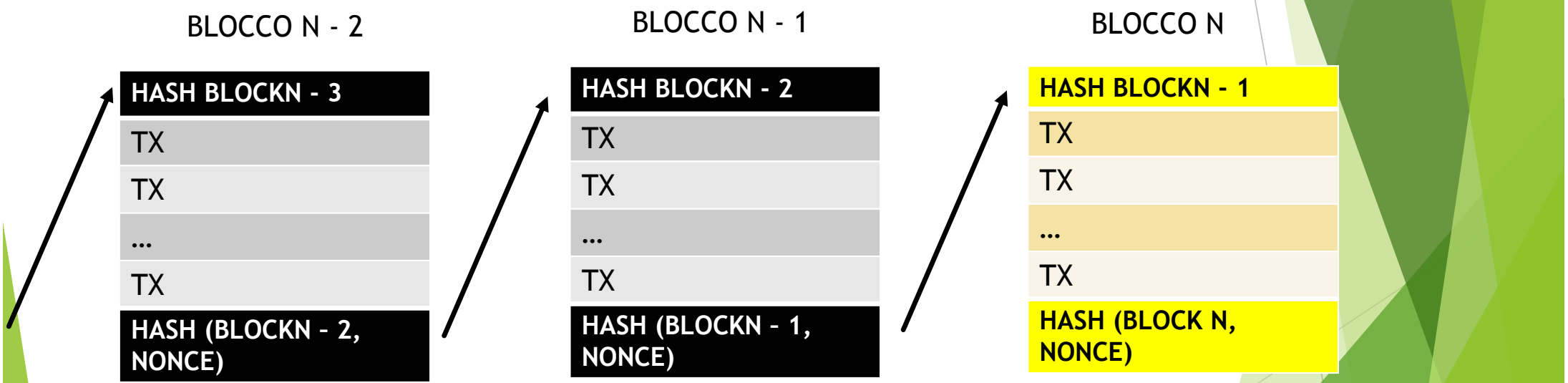
1 – ALICE broadcast the transaction

Transaction n

BROADCAST

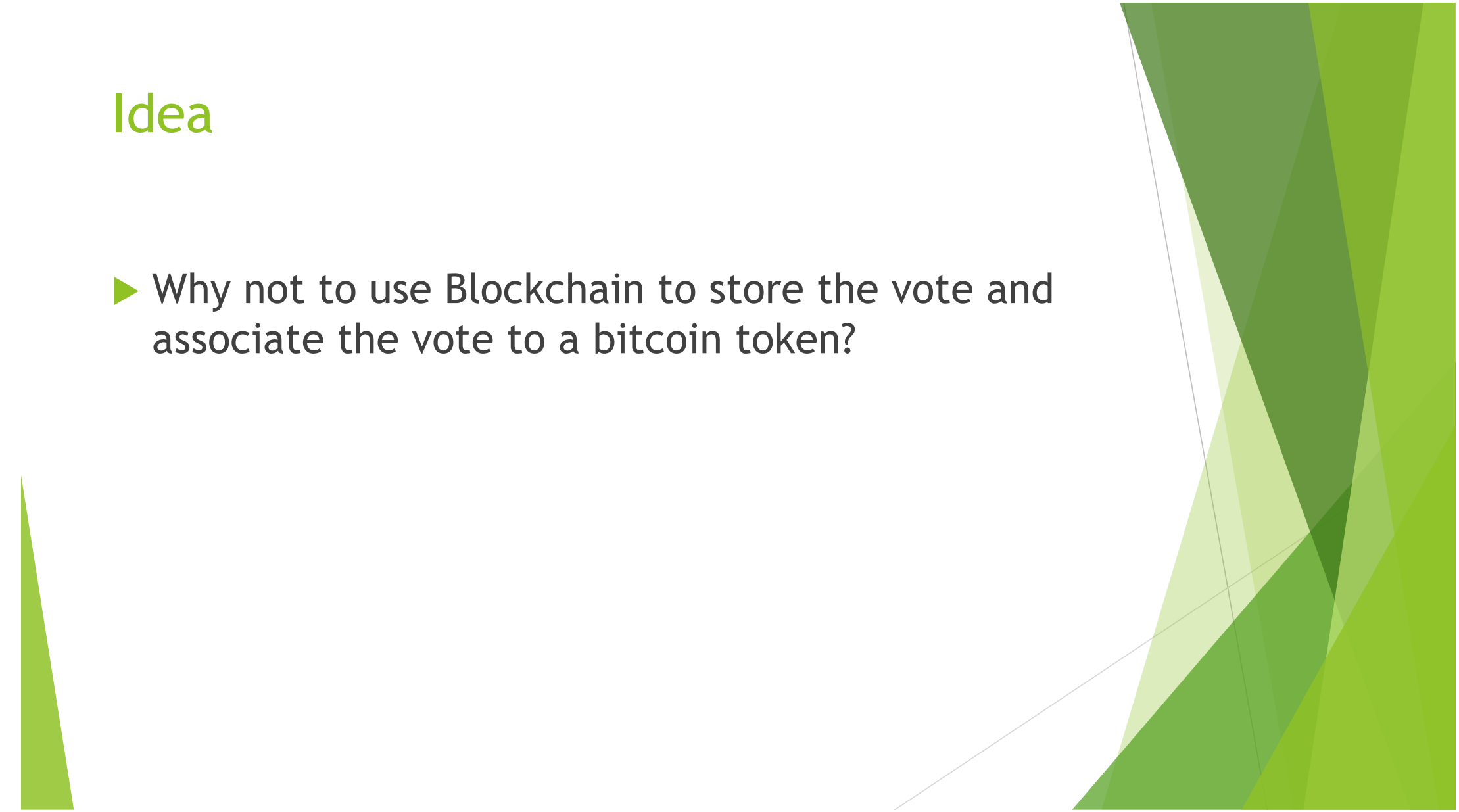
BLOCKCHAIN

4 – All the node (verify and) accept the block and add the block at the end of the blockchain



Idea

- Why not to use Blockchain to store the vote and associate the vote to a bitcoin token?



Voting phases

1. Pre-voting Phase:
    a) Candidate nomination and registration process,
    b) Voter registration process.
2. Voting Phase:
    a) Voter authentication,
    b) Vote casting,
    c) Vote transmission and confirmation.
3. Post-voting Phase:
    a) Counting
    b) Result,
    c) Audit administration.

1. Pre-voting Phase

a) Candidate nomination and registration process


K_PUB_CANDIDATO1_BITCOIN


K_PUB_CANDIDATO2_BITCOIN

b) Voter registration process.

- The public key of a registered voter will be charged with an amount of bitcoins, which represents the election token to be spent
- Each voter generates her public/private keys, associated to her wallet.


K_PUB1_BITCOIN

K_PRIV1_BITCOIN

X BITCOIN = 1 VOTO


K_PUB2_BITCOIN

K_PRIV2_BITCOIN

X BITCOIN = 1 VOTO


K_PUB3_BITCOIN

K_PRIV3_BITCOIN

X BITCOIN = 1 VOTO

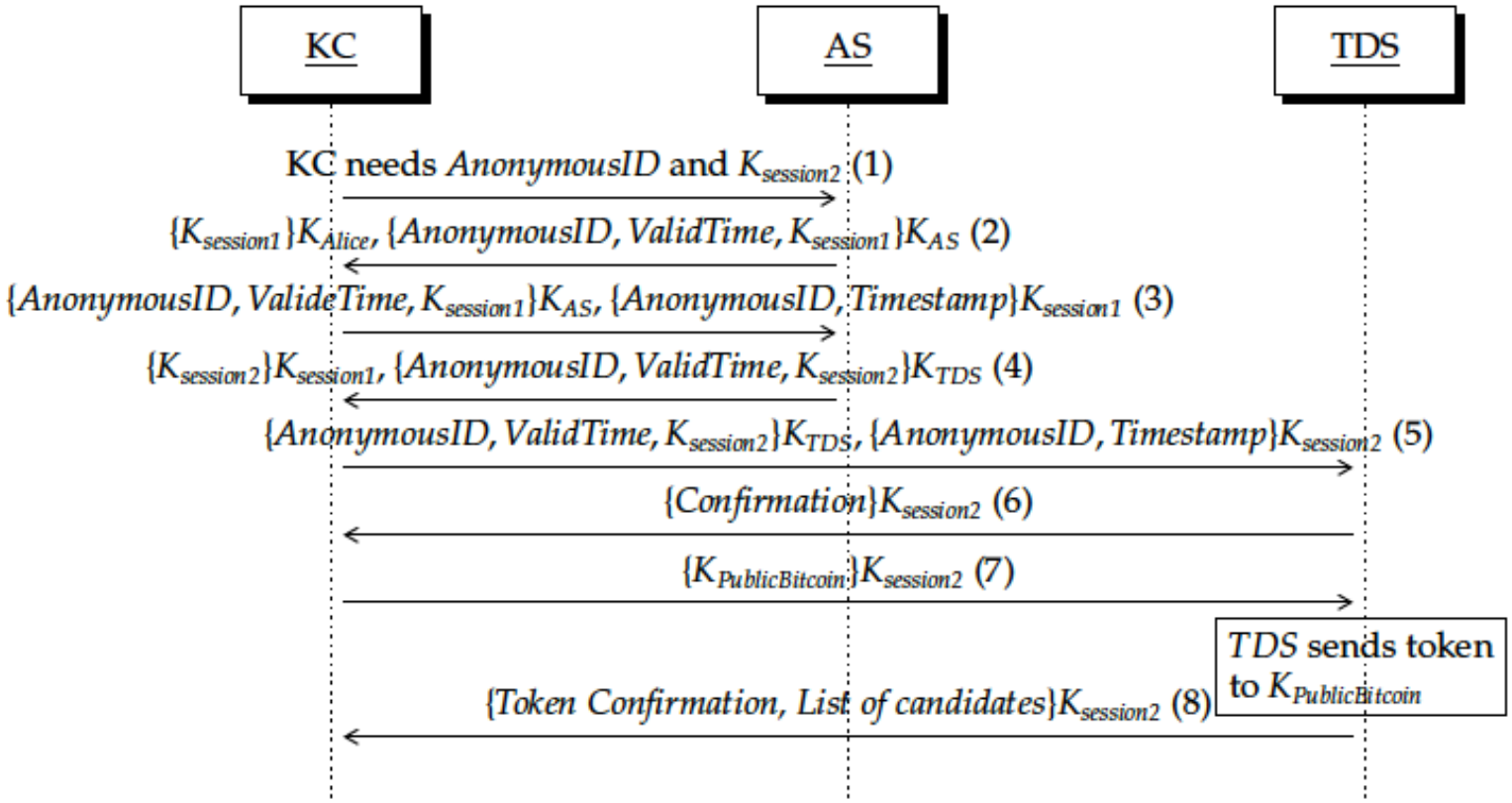

K_PUB4_BITCOIN

K_PRIV4_BITCOIN

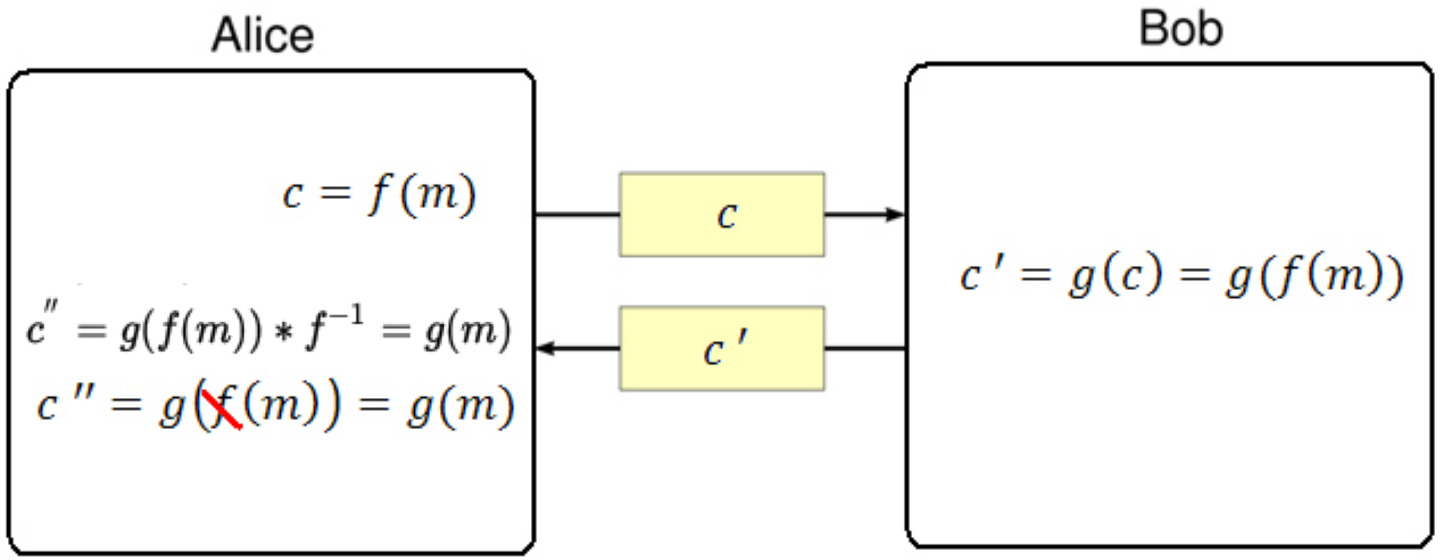
X BITCOIN = 1 VOTO

- However, a public key cannot be directly associated with voter's identity, otherwise anonymity of electors would be not guaranteed
  - Anonymous Kerberos authentication-protocol (RFC 6112: Anonymity Support for Kerberos, APRIL 2011)
  - Blinded Signature

Anonymous Kerberos (RFC8062 (ex 6112)



Blinded Signature (Chaum 1983 Advances in Cryptology Proceedings of Crypto)

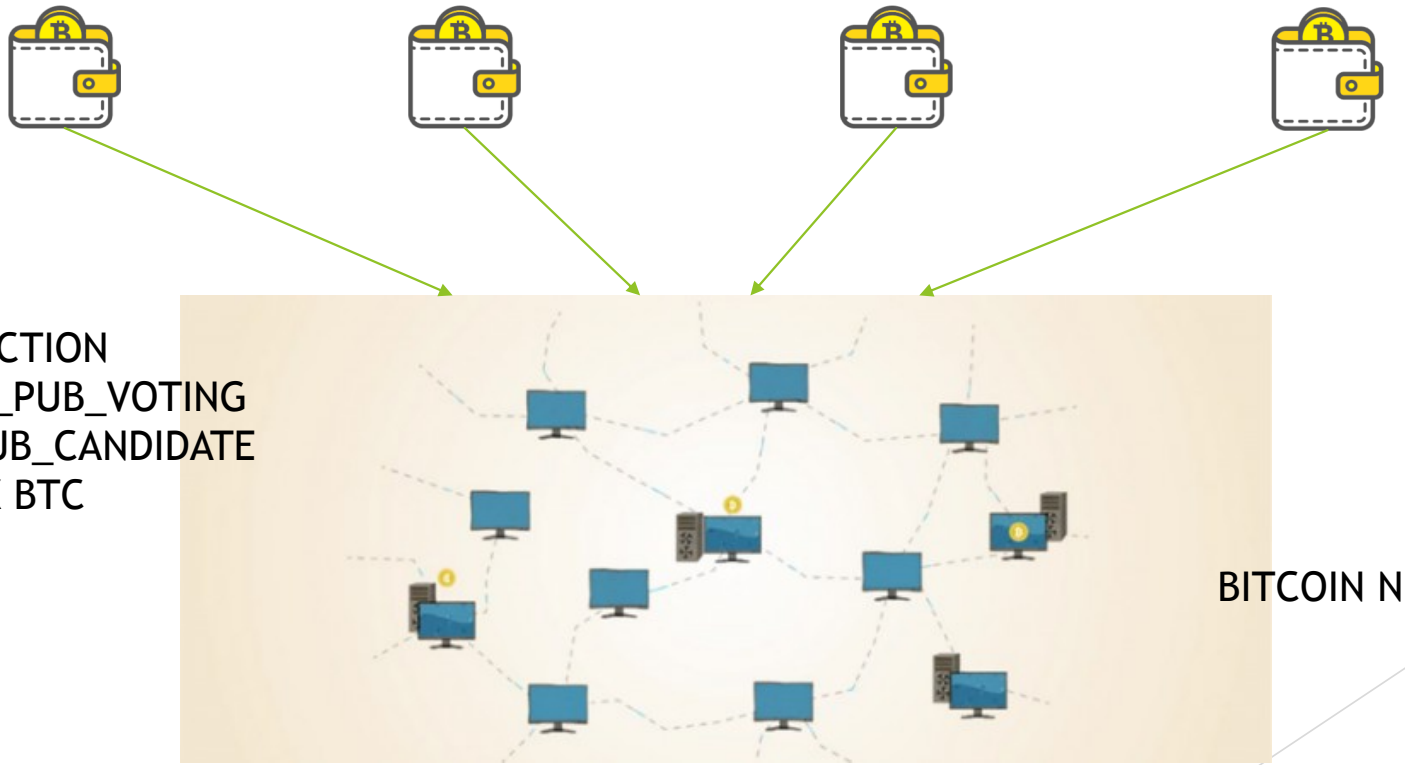


Voting Phase

- Voter authentication
  - Any voter owing a token received in the previous step is authorised to vote
- Vote casting
  - Coincide with a payment to the candidate (sending the token to the candidate)
- Vote transmission and confirmation
  - Coincides with the insertion of the transaction in the mempool and the mining of a block containing the transaction by the miner

Vote casting

K_PUB1_BITCOIN K_PUB1_BITCOIN K_PUB1_BITCOIN K_PUB1_BITCOIN

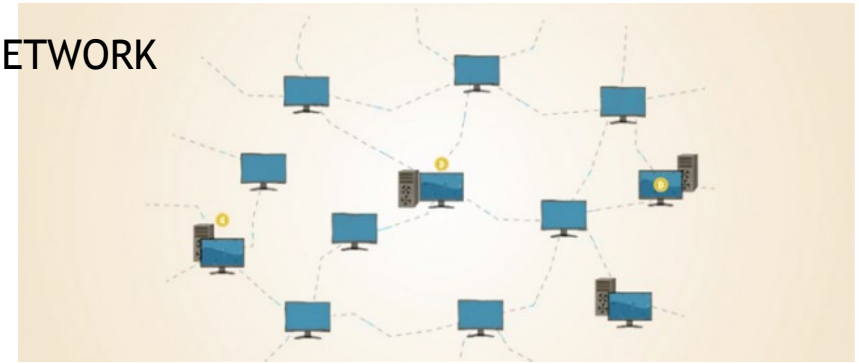


TRANSACTION
FROM K_PUB_VOTING
TO K_PUB_CANDIDATE
VALUE X BTC

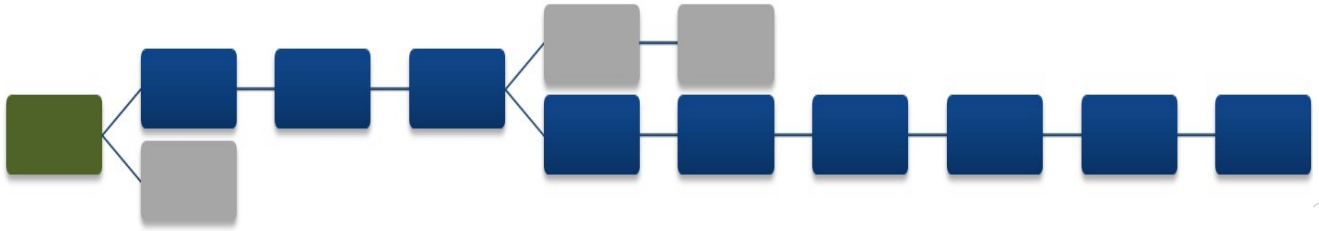
BITCOIN NETWORK

Vote transmission:
INSERT OF THE VOTE IN BLOCKCHAIN

BITCOIN NETWORK

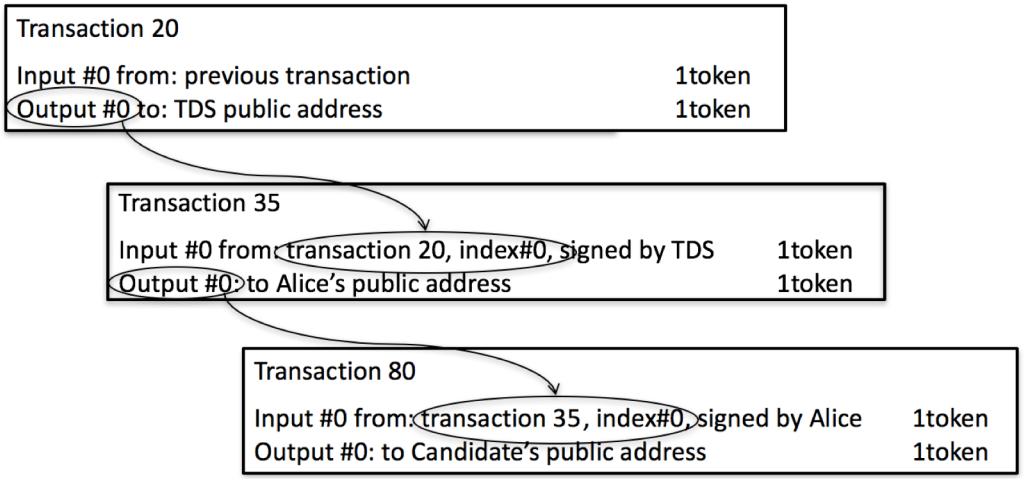


BLOCKCHAIN

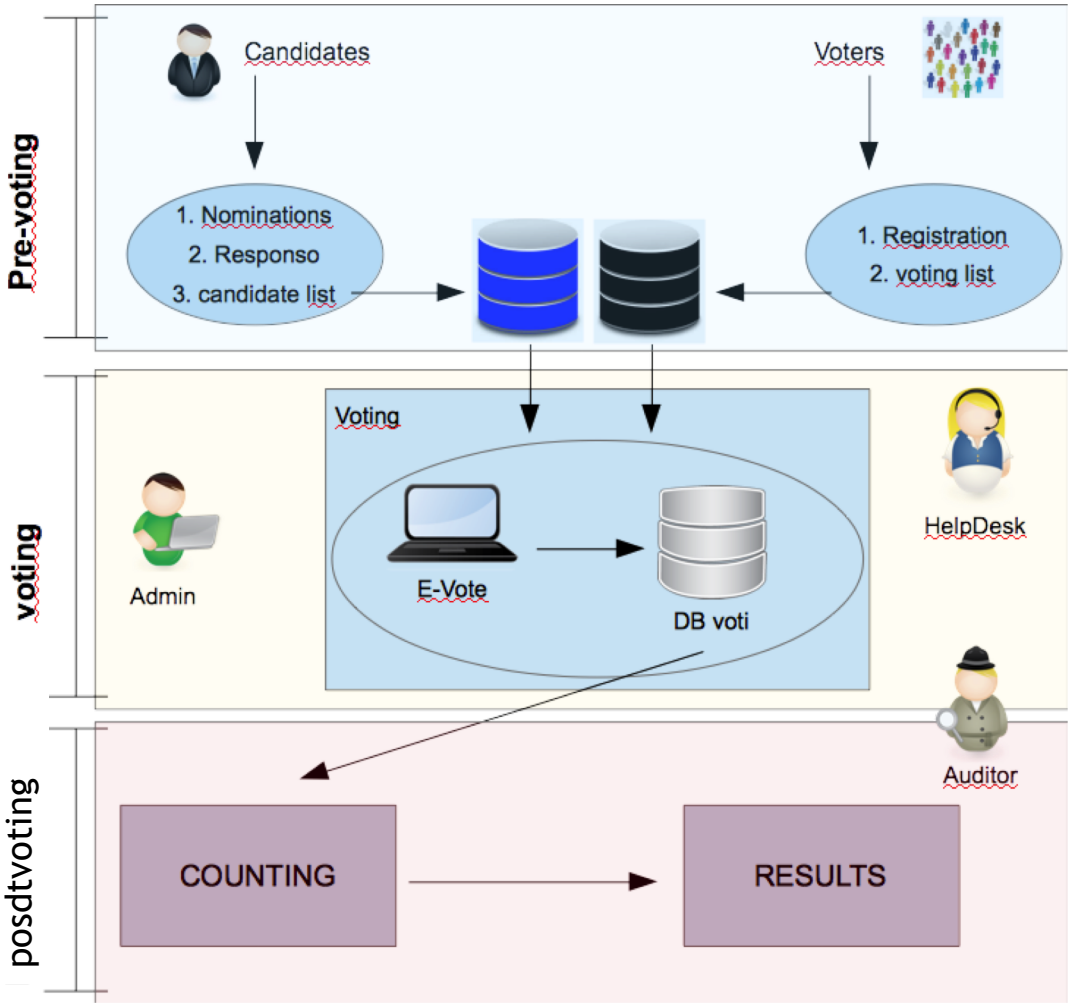


Post-voting Phase

- Counting
- Result
- Audit administration

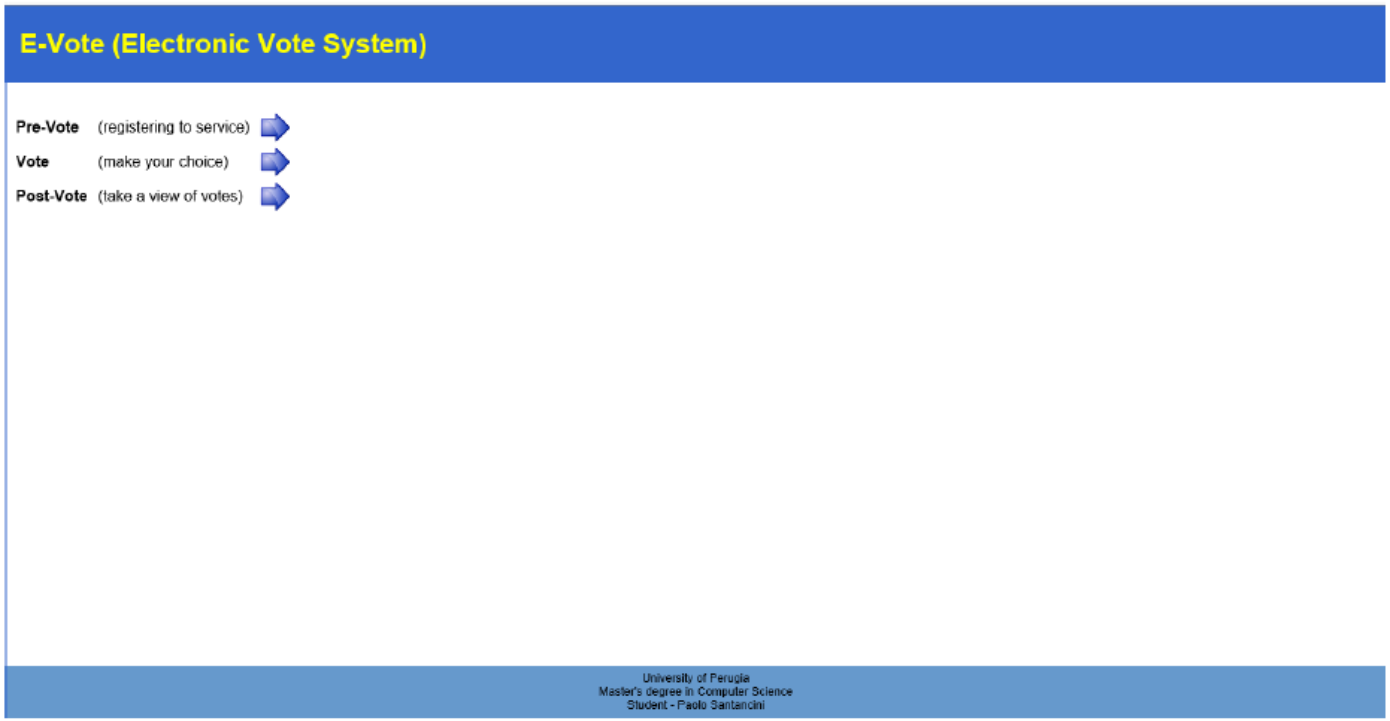


The architecture



… E-Voting System *(some examples)*

Homepage



Bitcoin token vs colored coin assets

- Colored Coins describes a class of methods for representing and managing real world assets on top of the Bitcoin Blockchain.
- Open Assets is a Colored Coin implementation based on the OP_RETURN operator. Metadata is linked from the Blockchain and stored on the web.

Technical Requirements:

- Web Server Apache;
- DBMS Mysql;
- Perl CGI;
- Bitcoin BlockChain (https://bitcoin.org/);
- Open Asset Protocol (Colored Coins https://github.com/OpenAssets/open-assets-protocol/blob/master/README.md);
- Asset Wallet (es. Coinprism API, Coin Spark, Spark Bit…).


BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE W
Transazione Ottieni informazioni su una transazione bitcoin
7a95eaabf0345ef78968cc90e04dcef5c88365bc85401c51f6cf3b8be0cf86df
12uReoPiKuehmsrwQJRGFGG3iqyeUenJsV (0.005968 BTC - Produzione)
1DdiNJANwreKArsNWsdjetkNKiadpgFGDf - (non spesi) 0.000006 BTC
Impossibile decodificare l'indirizzo di output - (non spesi) 0 BTC
12uReoPiKuehmsrwQJRGFGG3iqyeUenJsV - (Speso) 0.005952 BTC
0.005958 BTC

coinprism Wallet Explorer

coinvote

- Information
- Coin holders

Asset ID	AYhL6SECPJdkaByyWr8pT2hnE1w52dKoCU
Ticker	coinvote
Type	Other
Issuer	Adminvote The authenticity of the issuer could not be verified
Divisibility	Indivisible
Asset definition URL	https://cpr.sm/rbEOLx28GW

Contract Details

> E-Voting system coins

09380db6f2d15d600760093d469b6b87650a26ec86d5a3efb4f6ad36931b567f

Tuesday, January 19, 2016 10:31:37 AM — Confirmed

Bitcoin

← coinvote	-0.000106	akY5FE3AkQjEbxUXicvqh38dhBq1HYXD5k2 Fees	0.000006 0.0001

coinvote — AYhL6SECPJdkaByyWr8pT2hnE1w52dKoCU

← coinvote	-1	akY5FE3AkQjEbxUXicvqh38dhBq1HYXD5k2	1

Classical bitcoin vs OAP

- Voting Token can be:
  - X = **one Satoshi** (10^{-8} Bitcoin) + the mining fee (10^{-4} bitcoin) (2 times the number of the voters(1 for sending the token in the prevote phase, and 1 for the vote phase)),
    - $N^* 10^{-8} + 2N 10^{-4}$
    - If 1000 voters and current price 1B= 7637 euro,
    - cost (for voting only) would have been 1527 euro

Classical bitcoin vs OAP

- Voting Token can be:
  - **An asset** (any solution OAP compliant (CoinPrism, CoinSpark, SparkBit) the cost to issue a new asset with CoinPrism is $6* 10^{-6} + 10^{-4}$; this need to be paid 1 time at the beginning to create asset, and 2N times to transfer assets in the prevote and vote phase
    - $(2N+1)(6* 10^{-6} + 10^{-4})$
    - If 1000 voters and current price 1B= 7637 euro,
    - cost (for voting only) would have been 1619 euro

Satisfied properties

- Eligibility and Authentication:
  - Only authorised voters are able to vote; this is accomplished by the pre-voting phase
- Verifiability and Auditability:
  - It is possible to verify that all the votes have been correctly accounted for in the final tally, and there are reliable and demonstrably authentic election records. The block-chain implements such a public election record, which is public: to modify a block is computationally hard.
- Uniqueness:
  - No voter is able to vote more than once. Doublevoting is prevented by the fact double-spending of tokens is impossible in Bitcoin (see also the post-voting phase in Sec. 3).
- Accuracy:
  - Election systems should record the votes correctly, with an extremely small error-tolerance. The protocol reliability resistance is due to the presence of reliable miners, stimulated by gaining bitcoins as reward.
- Integrity:
  - Votes should not be able to be modified, forged, or deleted without detection. When a transaction is confirmed in the block-chain, votes cannot be deleted or modified. If a vote is modified on the client-side, the voter can detect it once the corresponding transaction is in the block-chain.
- Vote anonymity:
  - Neither election authorities nor anyone should be able to determine how any individual voted. Public-keys of voters cannot be associated with their identity (see the pre-voting phase in Sec. 3).
- Counting and Recounting:
  - Voting system must provide easy functions for counting and recounting, in case of any question about the final voting result. Each valid transaction is permanently stored in the block-chain.

Unsatisfied properties

- Receipt-freeness (Uncoercibility).
  - To prevent this, it is possible to adopt permissioned block-chains, where the right to read the block-chain can be granted only to some users. For instance, each voter can read only the block where her transaction is registered in order to still maintain the verifiability property; some official entities can be instead allowed to read the whole block-chain with the purpose to count votes. In this way, unless the coercer is on-site during the voting process, the elector can vote for other candidates.
- Data confidentiality and Neutrality.
  - Votes must be protected from external reading during the voting process. Once a vote has been broadcast to the peer-to-peer network, it is not confidential anymore, and can influence successive voters, who can freely read the block-chain and know candidates' addresses. Permissioned block-chains can be used also in this case, in order to prevent other users to scan the whole block-chain and mine all the votes for each candidate.

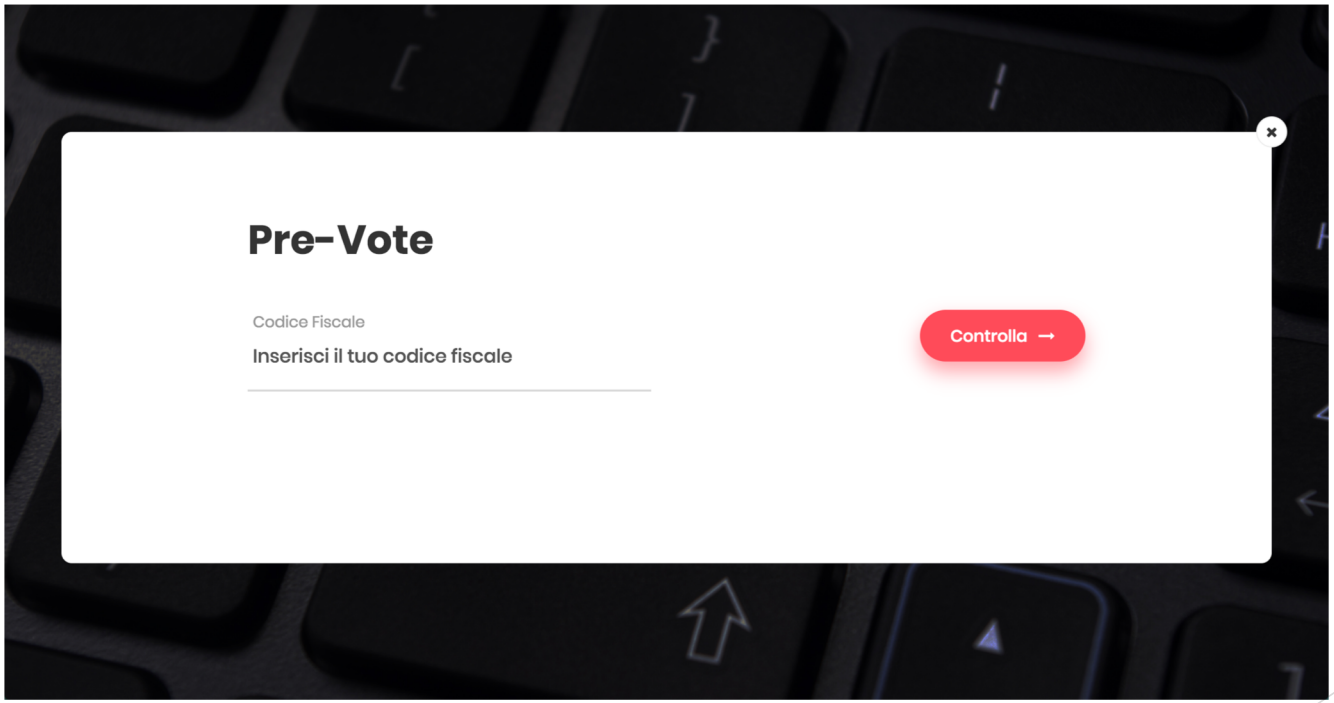
Current and future work: Multichain

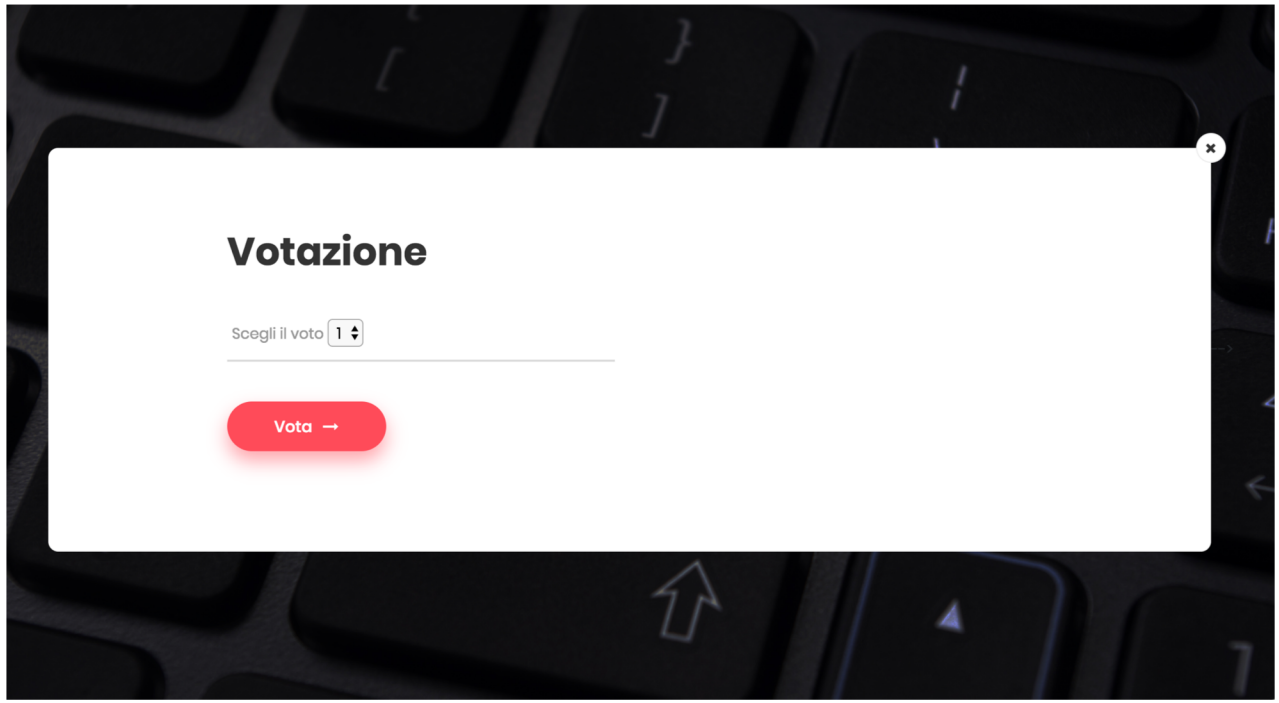
MultiChain

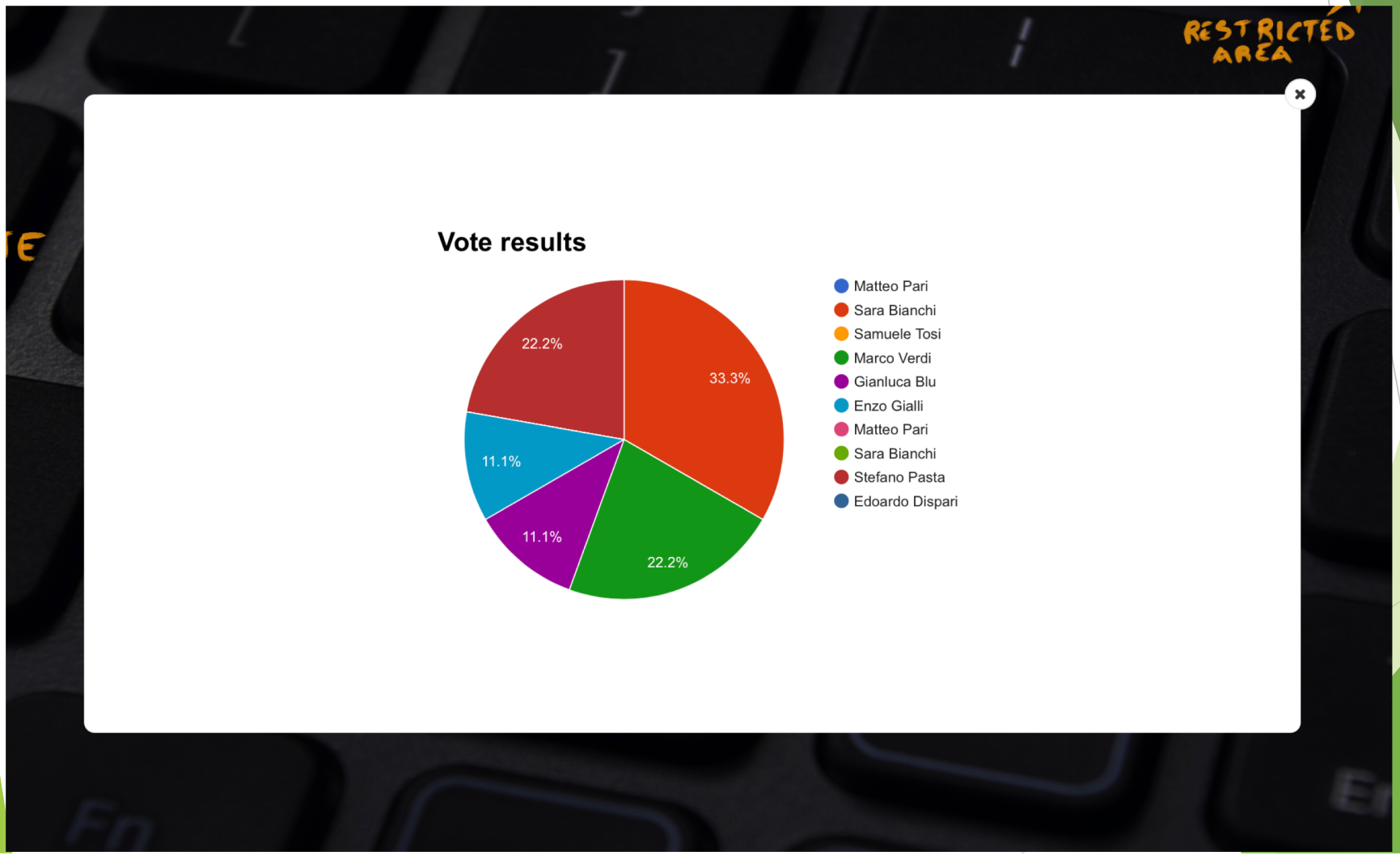
Private Blockchain Platform

Coin Sciences Ltd
www.multichain.com

Current and future work: Multichain


Pre-Vote
Codice Fiscale
Inserisci il tuo codice fiscale
Controlla →


Votazione
Scegli il voto 1
Vota →


RESTRICTED AREA
Vote results
33.3%
22.2%
22.2%
11.1%
11.1%
Matteo Pari
Sara Bianchi
Samuele Tosi
Marco Verdi
Gianluca Blu
Enzo Gialli
Matteo Pari
Sara Bianchi
Stefano Pasta
Edoardo Dispari


Admin
RESTRICTED AREA
2ND
VOTE
Vote
VOTE
1ST
SIGN IN
3RD
SEE RESULTS

Polimi Fintech Journey

An End-to-end Voting-system Based on Bitcoin

Stefano Bistarelli

bista@dmi.unipg.it

cini Cybersecurity National Lab

http://www.dmi.unipg.it/cybersecuritylab

from:
Stefano Bistarelli, Marco Mantilacci, Paolo Santancini, Francesco Santini: An end-to-end voting-system based on bitcoin. SAC 2017: 1836-1841