UNIVERSITY OF BIRMINGHAM

BlockVotes

An e-voting system based on blockchain and ring signature

Yifan Wu
MSc Computer Science
Supervisor: **David Galindo**

Contents

BLOCK VOTES

BACKGROUND

PROBLEM & TERMINOLOGY & OBJECTIVES

PROTOCOL

AN E-VOTING SCHEME

BLOCKVOTES

IMPLEMENTATION & TECHNOLOGY STACK & TOOLS

DEMO

A WHOLE FLOW OF E-VOTING DEMO VEDIO

BLOCK VOTES

01 BACKGROUND

PROBLEM & TERMINOLOGY & OBJECTIVES

About the e-voting

1 Definition

E-voting is the use of electronic devices, such as voting machines or a web browser, to cast votes.

2 Major Terminologies

In addition, ideal e-voting systems have **ballot-privacy, individual-verifiability** which is better than existing voting system.

Terminologies

PRIVACY

Ballot-privacy (BP)

No outside observer can determine for whom a voter voted.

Coercion-resistance (CR)

A voter cannot interact with a coercer during the election to prove how she is voting.

VERIFIABLITY

Individual verifiability (IV)

A voter can verify that the ballot containing his voteis in the published set of “all” (as claimed by the system) votes.

Universal verifiability (UV)

Anyone can verify that the result corresponds with the published set of “all” votes.

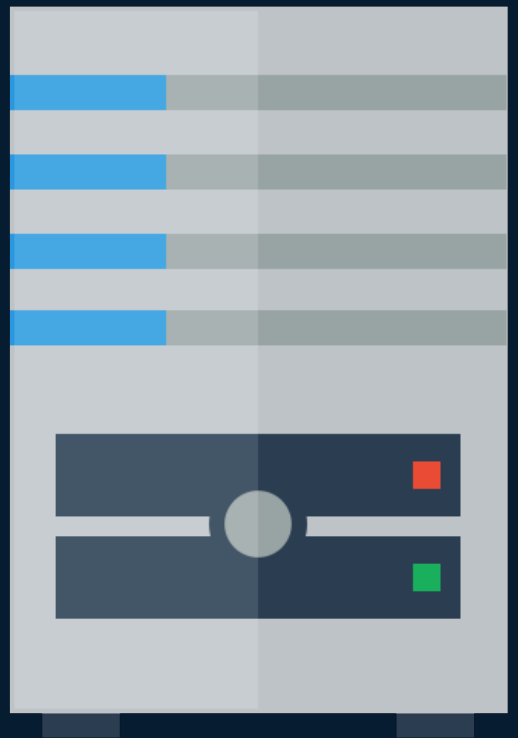
“

HOW TO CREATE A SYSTEM

WITH SOME OF THESE FEATURES?

”

IF IT IS IN THE TRADITIONAL WAY…

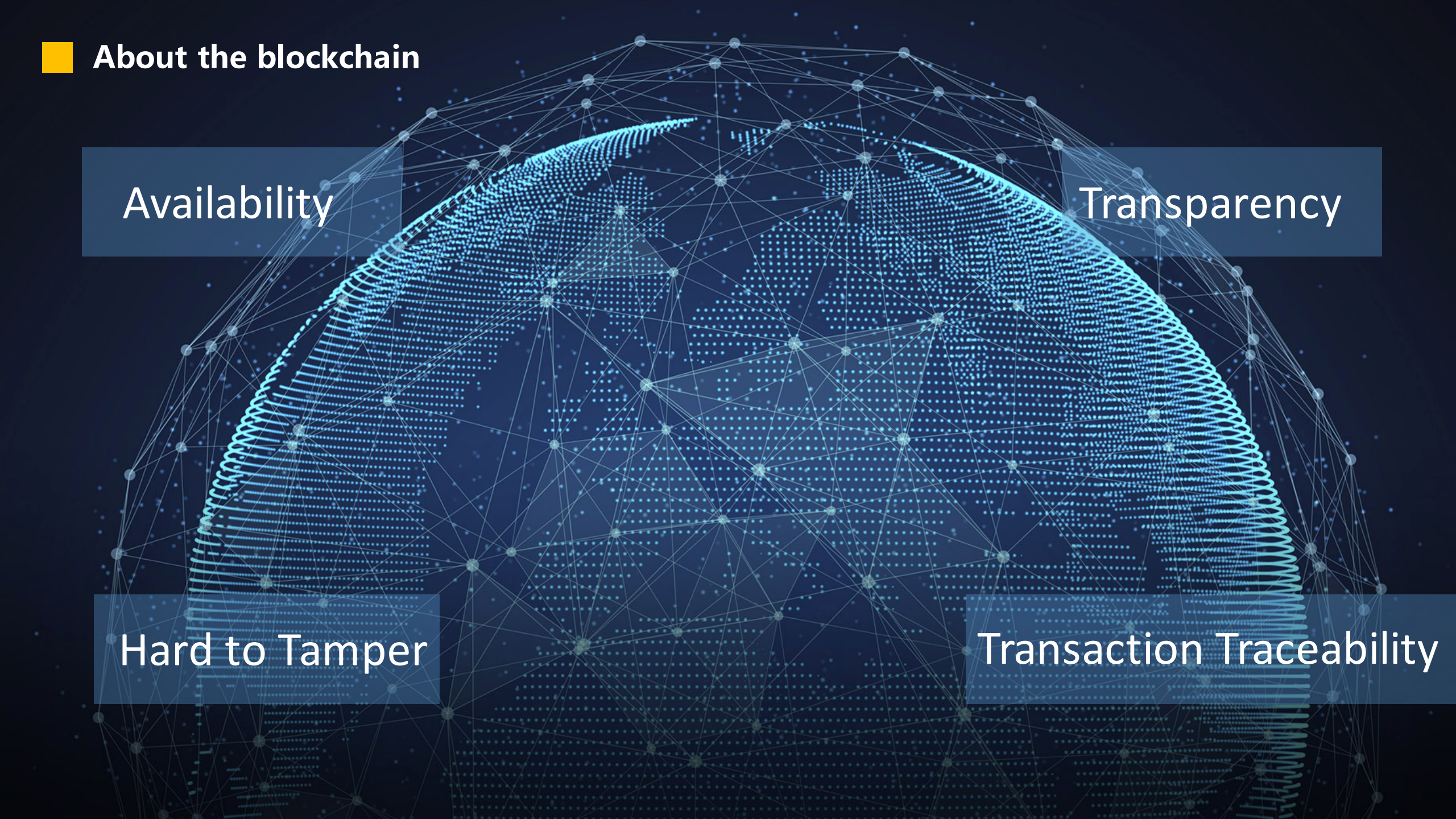


- ✗ Lack of Transparency
- ✗ Lack of Privacy
- ✗ Single Point of Failure

About the blockchain

Decentralized Public Ledger

About the blockchain



Transaction / Bitcoin

Bob

mxLqfJvTTEojWVZVTanEcXs1kXaBkdoqfX

0.305 BTC

reference: haha

Alice

n4Kc1AwFos3aZRvD3Tc9imzeMeA8E9DEUr

Encode the Reference:

OP_RETURN = Encode(reference)

Transaction / Bitcoin

BITCOIN TESTNET TRANSACTION

025e4fd916832c4028b1bcc446c8a41c10798fbea49793ce245ccf700e621d4f

Using *hex2bin()*
To decode the
OP_RETURN

TX Value	**0.28500000 TBTC**	**Total Inputs**	0.30500000 tBTC
Confirmations	22,145 CONFIRMATIONS	**Total Outputs**	0.28500000 tBTC
Block	1156835 Main Chain	**Fee**	0.02000000 tBTC
Relay time	Wednesday, August 9th 2017, 0:18:28 +01:00	**Fee / KB**	0.09661836 tBTC
Time until confirmed	after 23 seconds	**Size**	207 bytes
		Encoded Message	This transaction contains encoded data view

1 INPUTS — Total Inputs: 0.30500000 tBTC

mxLqfJvTTEojWVZVTanEcXs1kXaBkdoqfX (0.30500000)

2 OUTPUTS

OP_RETURN view decoded message

n4Kc1AwFos3aZRvD3Tc9imzeMeA8E9DEUr (0.28500000)

INPUT SCRIPTS

3045022100ae906a357c927d170f19710aca1de3c5ebcbe2c60fe9626b24ed876d7f23fa
d40220354d0b0c254679817deac98f4fcfa33be48eaf74c77a2e0b4db2046747cb2b3d01
02ce592b293c6688ca587dea59780acca8da8215d4d3261db338e9ea39fc46ae19

OUTPUT SCRIPTS

OP_RETURN 68616861

+ 1 more

DECODED OP_RETURN

The messages below are 'he
A lot of these 'messages' cor

6a0468616861
haha

Transaction / Bitcoin

What if...

Voter A

mxLqfJvTTEojWVZVTanEcXs1kXaBkdoqfX

(Voter address is anonymity for all)

0.305 BTC

Refers(OP_RETURN):
Candidate Name

Election Authority

n4Kc1AwFos3aZRvD3Tc9imzeMeA8E9DEUr

(Make this address public to all voters)

“

IS IT PERFECT NOW?

”

About the blockchain

“ NOT YET

The attacker who wants to
modify the voting result
can use his own bitcoin address to
vote **twice or more.** ”

Ring Signature

m Message to sign

SK_i Private key of member i

Pk_i Public key of member i

Sign a message:

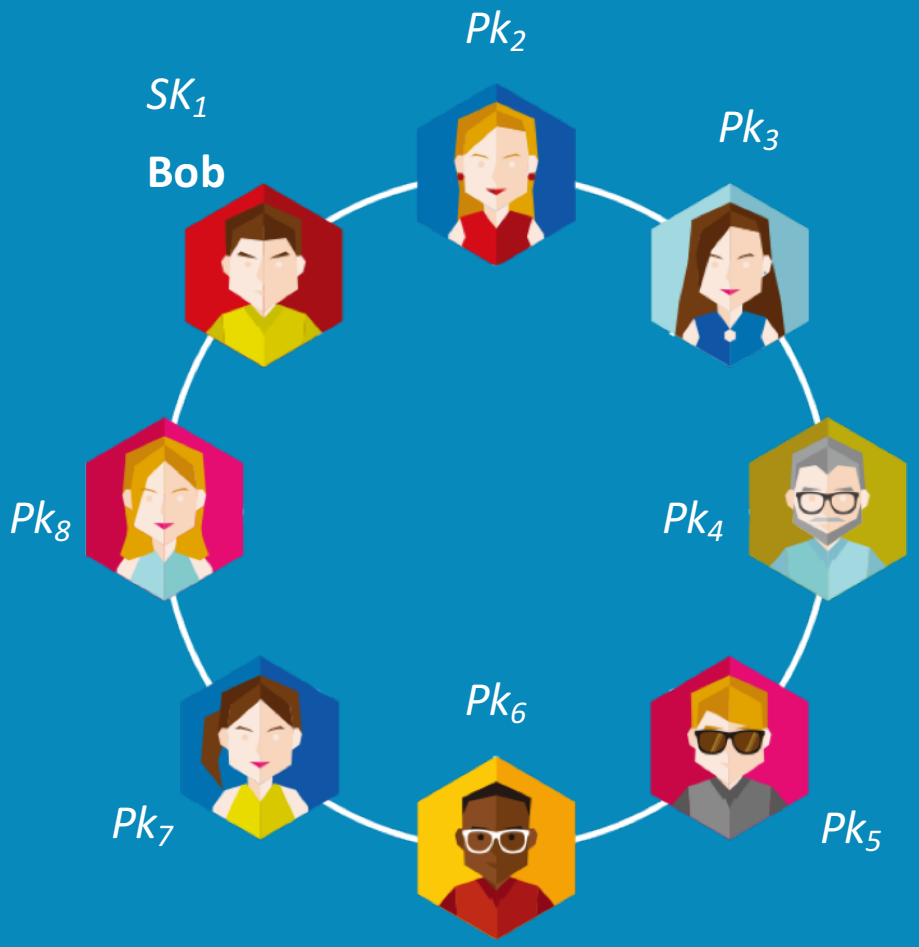
$\sigma(m, Sk_i, P_1, P_2 \ldots P_n)$

Verify a signature:

verify(m, σ, $P_1, P_2 \ldots P_n$)

What if make the OP_RETURN like this?

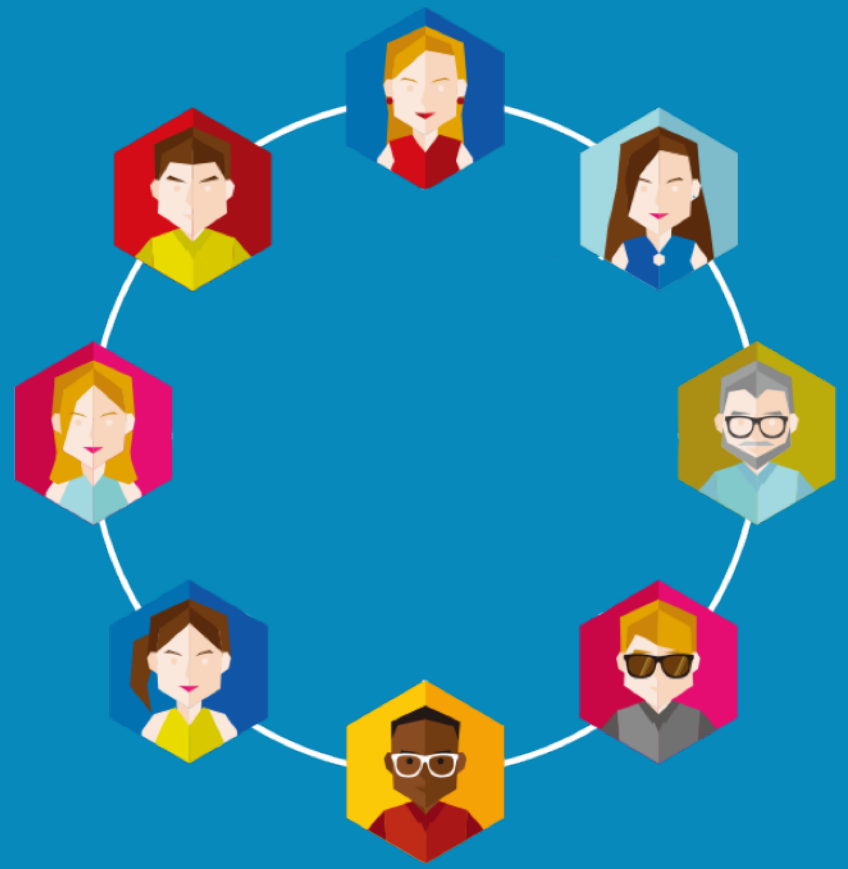
commitment(σ,*Candidate Name*)



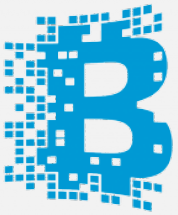
“WHY RING SIGANTURE”

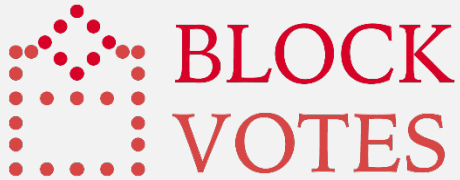
Compared to group signature

- ✓ No administrator
- ✓ Free Structure, every member is equal
- ✓ Everyone is anonymous



Summary





E-voting

A real e-voting system for Registration Authority, Election Authority, Voters, Candidates

Blockchain

The public ledger to store the information of signatures and candidate id. It protect the privacy of voters

Ring Signature

A signature algorithm to sign the candidate id to ensure the verifiability of individual and universal

BlockVotes

An e-voting system based on blockchain and ring signatures.

The network of blockchain can choose the bitcoin and the testnet

BLOCK VOTES

02 PROTOCOL

AN E-VOTING SCHEME

Definition and Assumption

Voter (V_i)

The voters should be a set of list.
For each voter to vote can be defined as V_i .
The voter should transfer his public key(PK_i) to EA .

Candidate(C_i)

The candidates should be a set of list.
For each candidate to vote can be defined as C_i

Registration Authority

The voter(V_i) should register in RA to get ready to vote.
The candidate(C_i) should register in RA with his information and the RA will give him the id of candidate.

Election Authority

The EA is responsible for creating a vote, limiting the voter numbers of the voting, paying the voting fees for the bitcoin address(A_i) generated automatically in the backend.
The EA has its own bitcoin address(A_E).

Assumption: Registration Authority and Election Authority will not correspond.

Protocol - Preparation Stage

Election Authority

1. The EA save his own private key(A_E) of the bitcoin into the system.
2. The EA create a new voting item with the voting id(L_i), title, limitation of the voting numbers(n) and the description of this voting item.
3. The system will generate the numbers of the n bitcoin addresses(A) as the addresses pool automatically.

Protocol - Registration Stage

1. Register

2. Candidate id

Candidate (C_i)

Registration Authority

1. The candidate takes his passport and goes to the *RA* in real life.
2. The RA verifies his identity and ask his name, his description and save it into system.
3. The RA will give him his candidate id(*Ci*).

Protocol - Registration Stage

1. Register

2. Email with Code

Voter (V_i)

Registration Authority

1. The voter(V_i) takes his passport and goes to the *RA* in real life.
2. The RA verifies his identity and ask the email address of the voter, sending him an email with registration code link as LK_i to avoid multiple registration.
3. The LK_i is generated random and has no relationship with the voters name and email address.

Protocol - Registration Stage

3. Open the link from the email

4. Generate keys and saves pub key

Voter (V_i)

Registration Authority

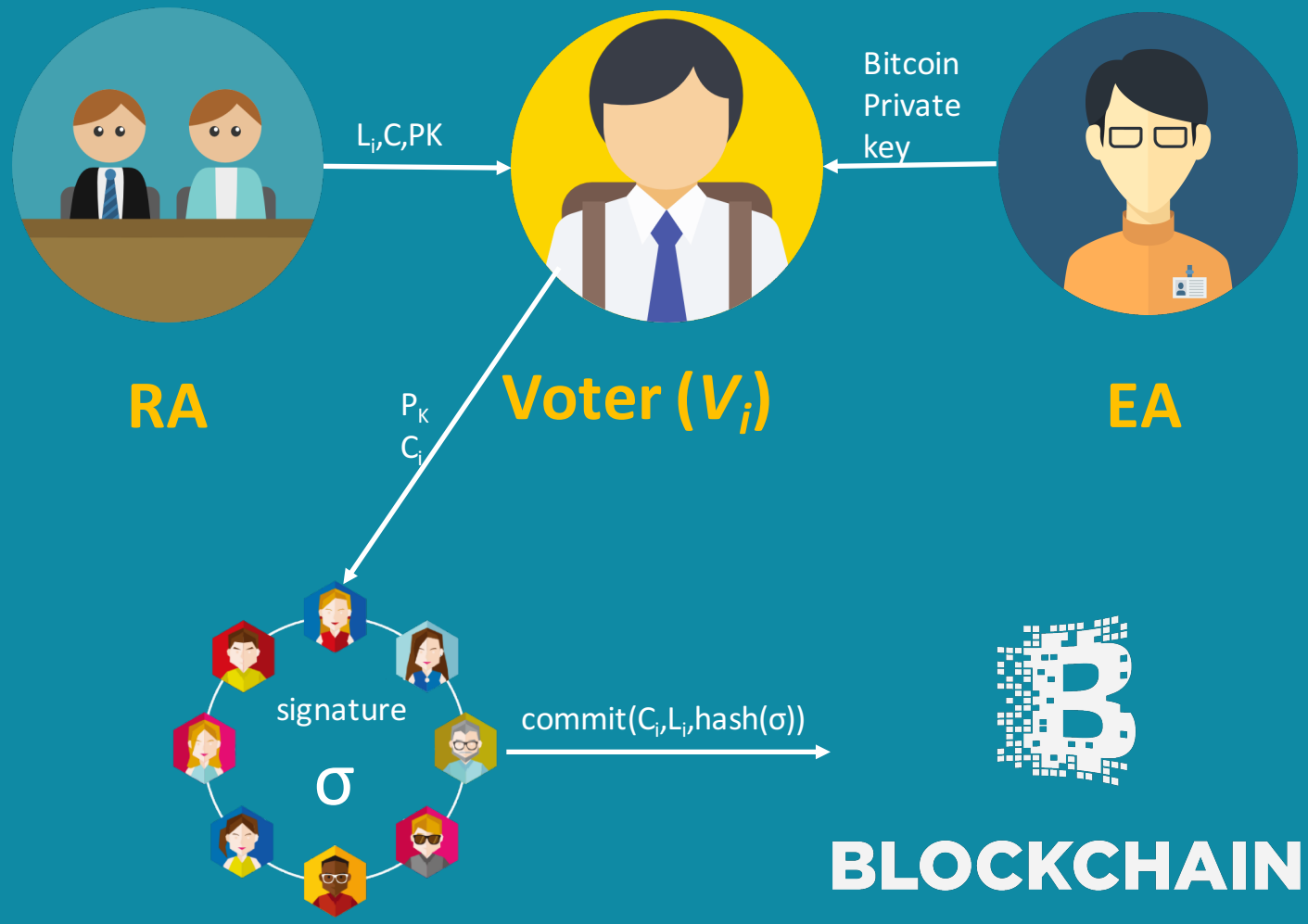
1. The voter opens the registration links LK_i.
2. The voter V_i generate his key pair (SK_i, PK_i).
3. The voter V_i save his public key PK_i into the system.
4. At the end of the registration, the set of voters should be fixed as a number of n.
5. The hash value of each public key (*hash(PK),PK)* should storage as a set *Set* into the system.

Protocol - Publish Stage

Election Authority

1. The EA start the voting .
2. EA creates *k* BTC in his own bitcoin.
3. EA pays a fixed amount of bitcoin *k* to each A_i for the voting costs with an OP_RETURN including the $hash(PK_i)$.

Protocol - Vote Stage



1. The voter chooses the candidate C_i he vote for and the current voting id L_i.
2. The RA returns the public keys set PK to the voter.
3. The voter use his private key SK_i and all public keys PK to sign the signature of the candidate C_i as $\sigma(C_i,Sk_i,PK)$. The system saves the set of $(\sigma,hash(\sigma))$ at the same time.
4. The voter select a bitcoin address A_i to publish from the bitcoin address pool and EA returns the private key of the address to voter.
5. The voter V_i pays all A_i's balance the to EA's address with an OP_RETURN of the commitment(hash($\sigma(C_i,Sk_i,PK)$),Ci,Li).

Protocol – Tally Stage

Anyone

BLOCKCHAIN

1. The system will return all sets of $(\sigma, hash(\sigma))$ and all public keys PK automatically.
2. The system will fetch all transactions in EA's bitcoin address automatically.
3. The system will fetch the OP_RETURN code form each transaction and verify the signature validity.
4. The system will count each valid transaction and add 1 to the candidate C_j.
5. If the voter Ai is absent, count it as the abstain from voting.
6. If bitcoin transaction history has more than twice transactions from the same A_j, count the first and ignore others.

Protocol – Verify Stage

Voter (V_i)

BLOCKCHAIN

1. The system will return all public keys *PK* automatically.
2. For each voter V_i, he can use a set of all public keys *PK*, the ring signature σ, the candidate *Ci* to verify the his vote.
3. The voter V_i can use the transaction id to fetch the commitment from the blockchain to verify if the signature is published in the right way.

BLOCK VOTES

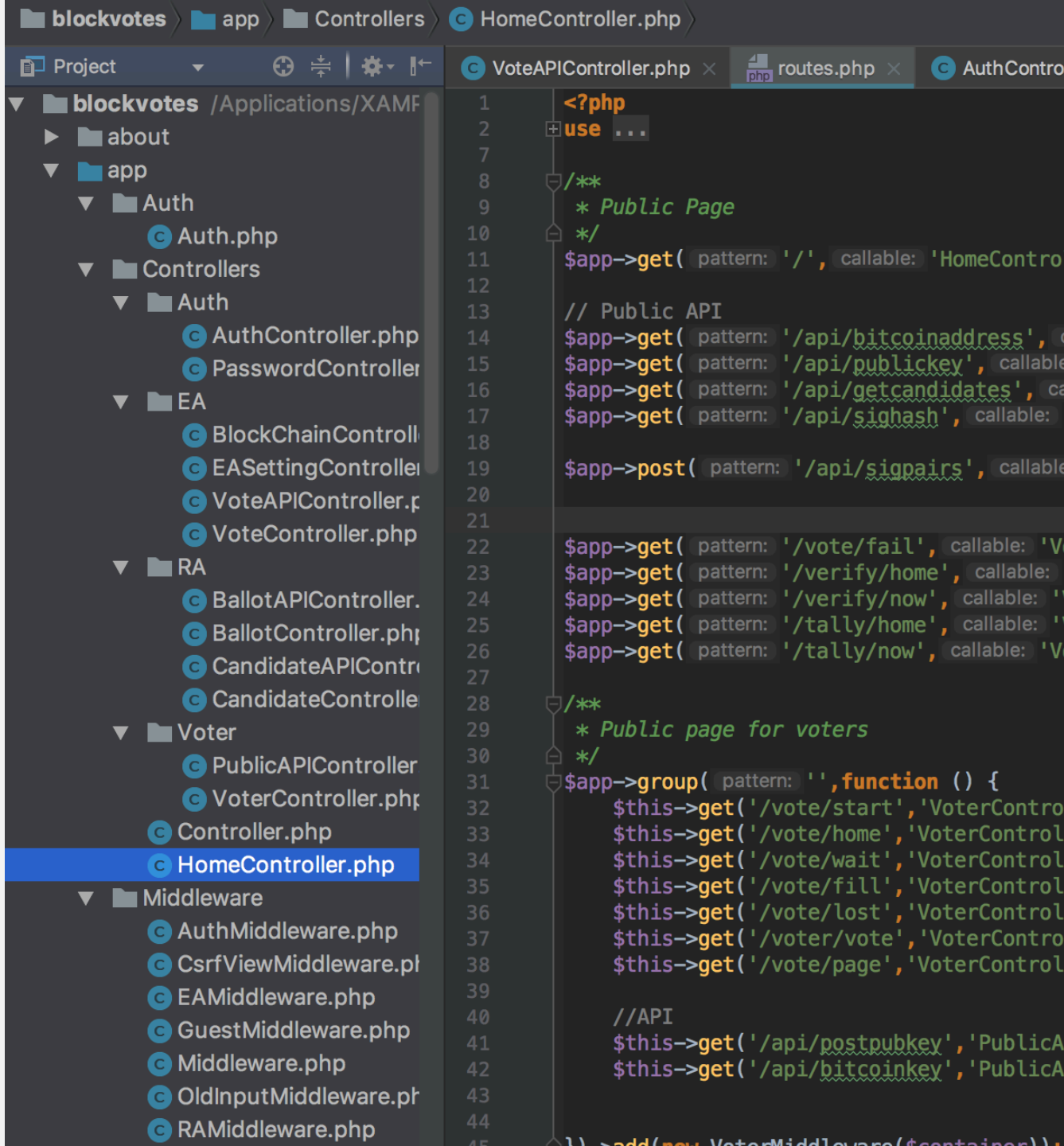
03 BlockVotes

IMPLEMENTATION & TECHNOLOGY STACK & TOOLS

Technology Stack

BIG PROJECT

- ✓ Login and logout
- ✓ User role control
- ✓ Public APIs to list bitcoin address, public keys and etc..
- ✓ Generate the bitcoin address into WIF format
- ✓ Sending the emails
- ✓ Switch the network of blockchain
- ✓ Create a bitcoin transaction into hex format
- ✓ Publish the voting result to blockchain
- ✓ Use ring signature algorithm to sign voting result
- ✓ Tally the votes in real time
- ✓ Verify the votes in real time
- ✓ ....



Technology Stack

BIG PROJECT

14 Controllers

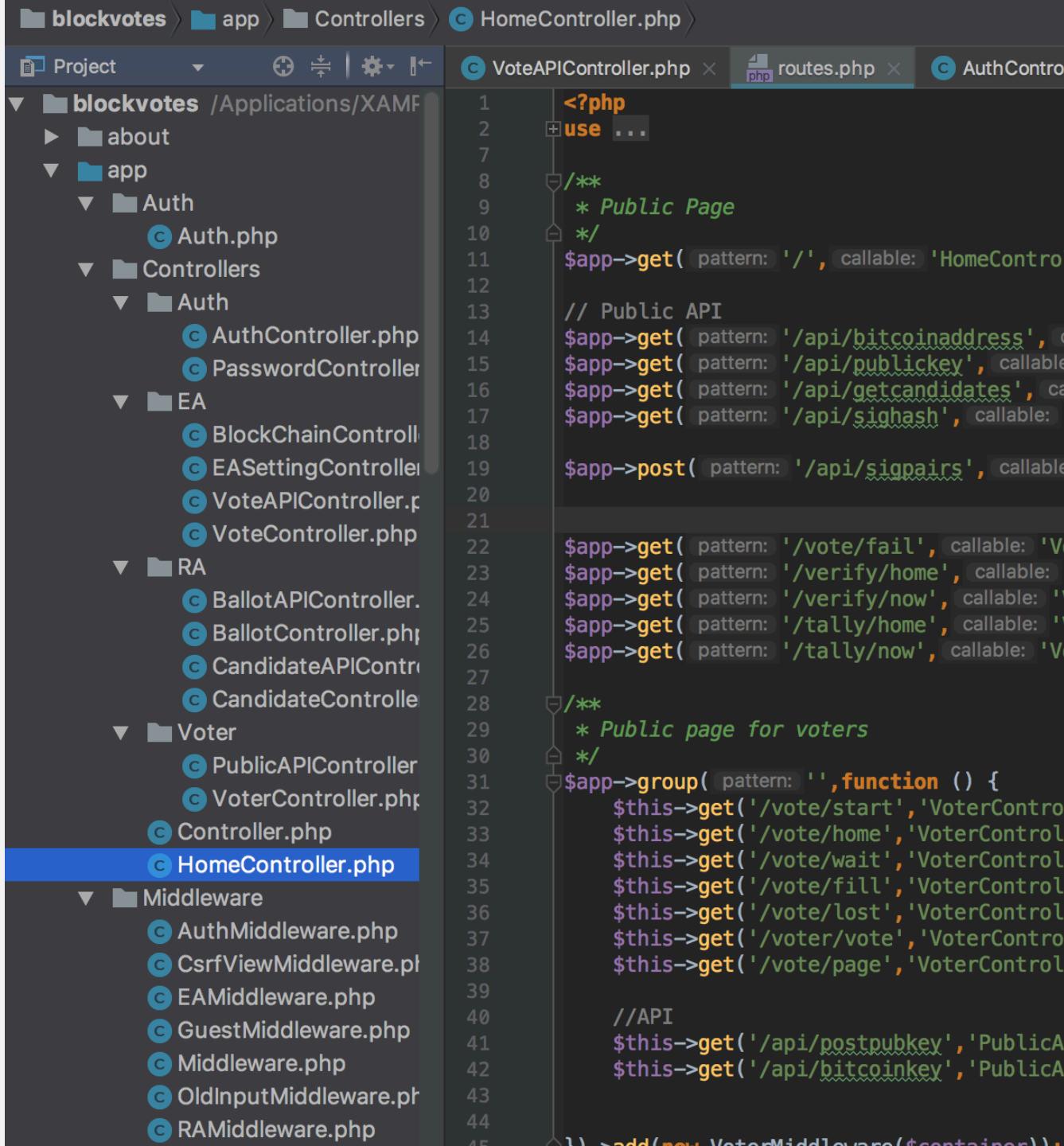
7 Models

10 Middleware

15 Own APIs

17 JavaScript

25 HTMLs



Technology Stack

Third Party

BitcoinJS

+

jes / ring-signatures

Code | Issues 0 | Pull requests 0 | Projects 0

Javascript ring signatures tool

4 commits | 1 branch

Branch: master | New pull request

jes Clarify key verification output

jsbn.js	Initial commit
jsbn2.js	Initial commit
jsencrypt.js	Initial commit
prng4.js	Initial commit
ring.js	Verify keys

Third Party Contribution

BitcoinPHP / BitcoinECDSA.php

Watch 13 | Star 36 | Fork 23

Code | Issues 0 | Pull requests 0 | Projects 0 | Insights

Fixed testnet WIF format bug #36

New issue

Merged rgex merged 1 commit into `BitcoinPHP:master` from `yfgeek:master` 8 days ago

Conversation 1 | Commits 1 | Files changed 1 +13 −1

yfgeek commented 9 days ago — Contributor

Thank you for providing this **awesome bitcoin library** for PHP.
Unfortunately, I've occurred the WIF format bug when using **testnet network.**
This is due to the getWif($compressed) method doesn't judge the network.
I fixed this bug directly and it works now.

Here are what I've done.
Cheers!

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

BLOCK VOTES

04 DEMO VEDIO

A WHOLE FLOW OF E-VOTING DEMO VEDIO

UNIVERSITY OF BIRMINGHAM

BlockVotes

Thank you

Name: **Yifan Wu**
Supervisor: **David Galindo**