Electronic Voting System Implementation Through Bitcoin Blockchain Technology

Cassie Schultz

Electronic Voting

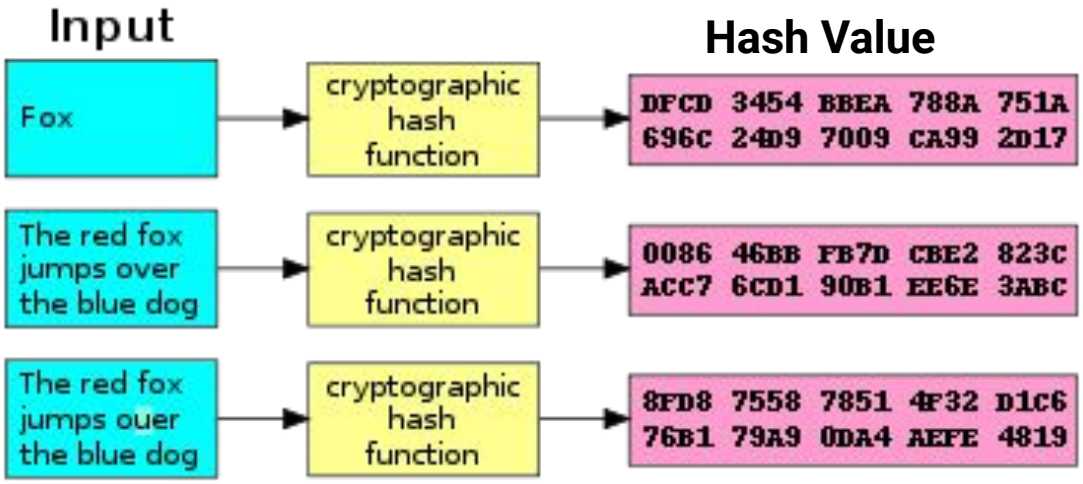
- Electronic voting (e-voting) is voting that uses electronics to aid in the voting process.
- Most voters use hand-marked paper ballots

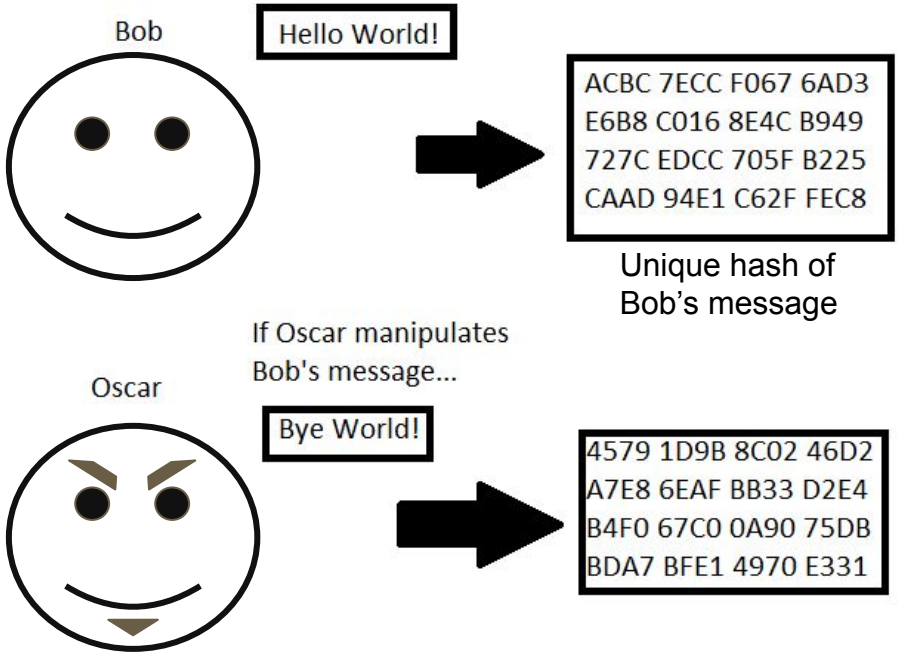
Outline

- Background Information
  - Cryptographically Secure Hash
  - Asymmetric Cryptography
  - Digital Signatures
  - Blind Signatures
  - Intro to Blockchain
- Using Blockchain for E-Voting
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

Background - Cryptographically Secure Hash

- Mathematical algorithms that map data to a bit array
- Used to verify integrity message are unaltered.
- Easy to compute
- Impossible to reverse



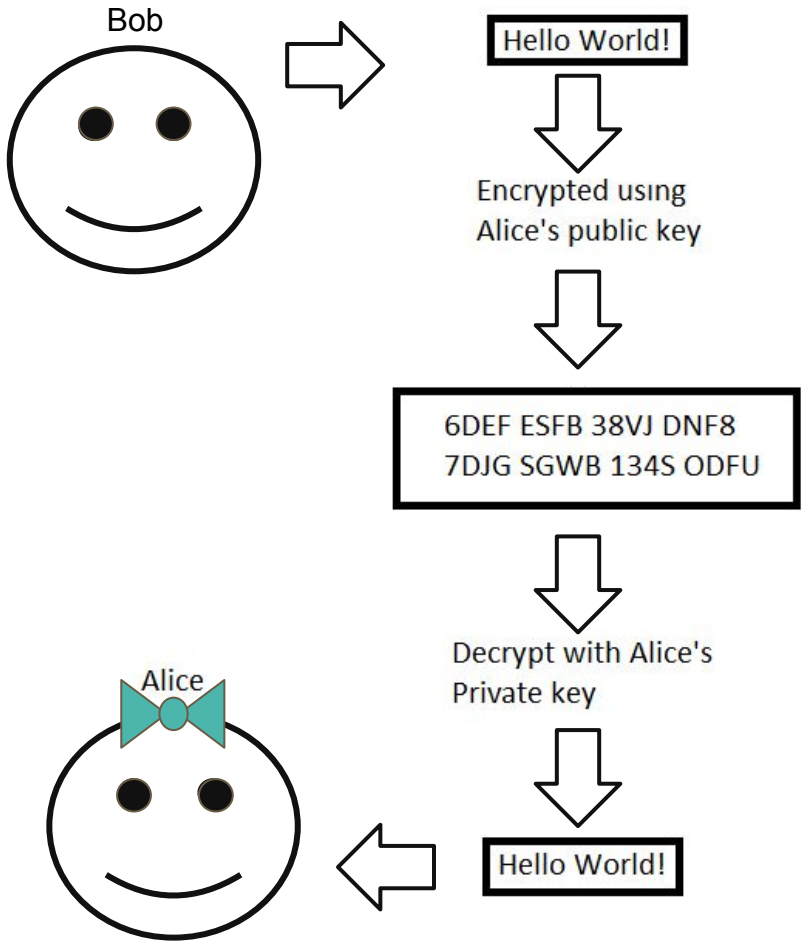

Bob
Hello World!
ACBC 7ECC F067 6AD3
E6B8 C016 8E4C B949
727C EDCC 705F B225
CAAD 94E1 C62F FEC8
Unique hash of
Bob's message
If Oscar manipulates
Bob's message...
Oscar
Bye World!
4579 1D9B 8C02 46D2
A7E8 6EAF BB33 D2E4
B4F0 67C0 0A90 75DB
BDA7 BFE1 4970 E331

Outline

- Background Information
  - Cryptographically Secure Hash
  - **Asymmetric Cryptography**
  - Digital Signatures
  - Blind Signatures
  - Intro to Blockchain
- Using Blockchain for E-Voting
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

Background- Asymmetric Cryptography

- Each participant gets a key pair
  - Private key, Public key
- Security relies on the private key staying private
- Public key only encrypts
- Private key decrypts



Outline

- Background Information
  - Cryptographically Secure Hash
  - Asymmetric Cryptography
  - **Digital Signatures**
  - Blind Signatures
  - Intro to Blockchain
- Using Blockchain for E-Voting
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

Background - Digital Signatures

- Used to confirm the source, and the integrity of a message
- The goal of these signatures is not to hide the message

RSA Signatures - Key Generation

1. Two prime numbers p and q are chosen
2. Compute n = pq
    a. n will be used as a modulus later on

1. **p** = 61, **q** = 53
2. **n** = 61*53 = 3233

RSA Signature Key Generation -Euler's Phi Function

- For prime numbers, φ(p) = p-1
- multiplicative function:
  - φ(pq) = φ(p)(φ(q)
  - φ(pq) =(p-1)*(q-1)
- φ(n) will be used in subsequent steps

1. p=61, q=53, n= p*q = 3233
2. φ(n)=60*52=3120

RSA Signatures - Key Generation

Remember...

1. **p** = 61, **q** = 53
2. **n** = 3233
3. **φ(n)** = 3120

4. Choose integer e (Public Exponent)

5. Compute d (Private Exponent)
   - d*e ≡ 1 (mod φ(n))

Public key = (n, e)

Private key = (p, q, d)

4. 1 < e < φ(n), let **e** = 17
   - GCD(17, φ(n)) = 1
5. **d** = 413
   - 1 = (17*413) mod 3120

Public key = (n = 3233,e = 17)

Private key = (p = 61, q = 53, d = 413)

Signing A Message

- *h = hash(m);*
- *Alice attaches h^d as signature to message*

Hello World

Alice's creates a hash of her message

a591 a6d4 0bf4 2040
4a01 1733 cfb7 b190
d62c 65bf 0bcd a32b
57b2 77d9 ad9f 146e

Alice attaches the hash to her message as a 'signature'

Hello World

a591 a6d4 0bf4 2040
4a01 1733 cfb7 b190
d62c 65bf 0bcd a32b
57b2 77d9 ad9f 146e

Say h= 65,

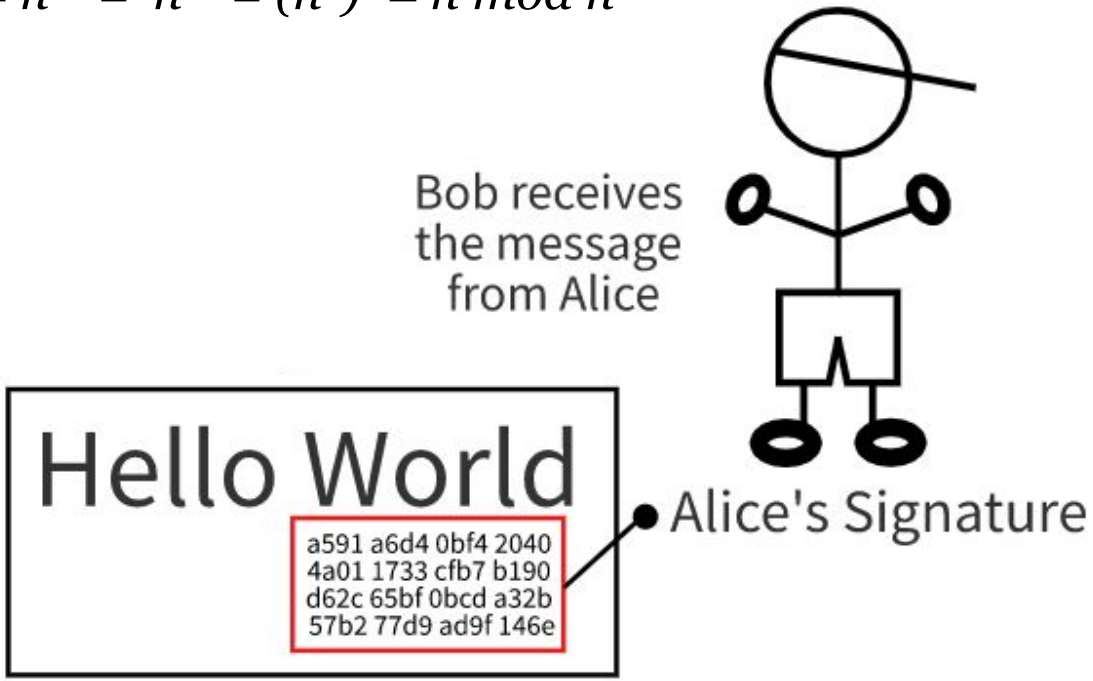
h^d (mod n) = Alice's Signature:

65^{413} (mod n) = Alice's Signature

Receiving A Signed Message

$$(h^e)^d = h^{ed} = h^{de} = (h^d)^e \equiv h \bmod n$$

- Bob raises Alice's signature value to the power of e
- Bob can then compare the hash value with Alice's hash value.



Outline

- Background Information
  - Cryptographically Secure Hash
  - Asymmetric Cryptography
  - Digital Signatures
  - **Blind Signatures**
  - Intro to Blockchain
- Using Blockchain for E-Voting
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

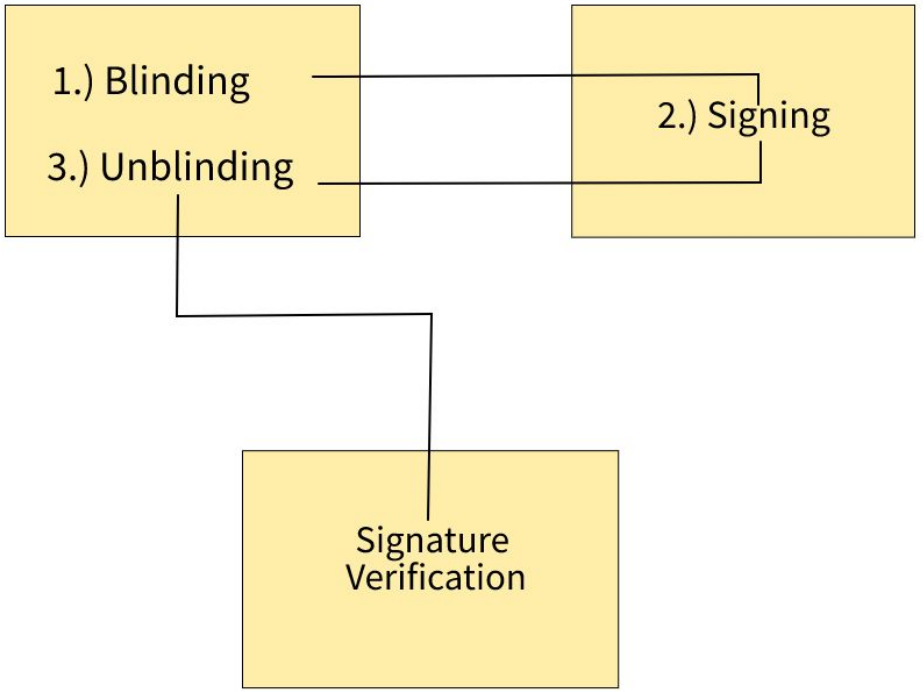
Blind RSA Signatures

m′ = blinded message
s′ = blind signature
s = signature (unblinded)
r^e = blinding factor

1. Send product of message and blinding factor
   a. $m' = mr^e \pmod n$

2. Signer signs document
   a. $s' = (m')^d \pmod n$

3. *s′* is sent back and blinding factor is removed
   a. $s = s' * r^{-1}$
      $= m^d * r^{ed} * r^{-1}$
      $= m^d * r * r^{-1}$
      $= m^d$

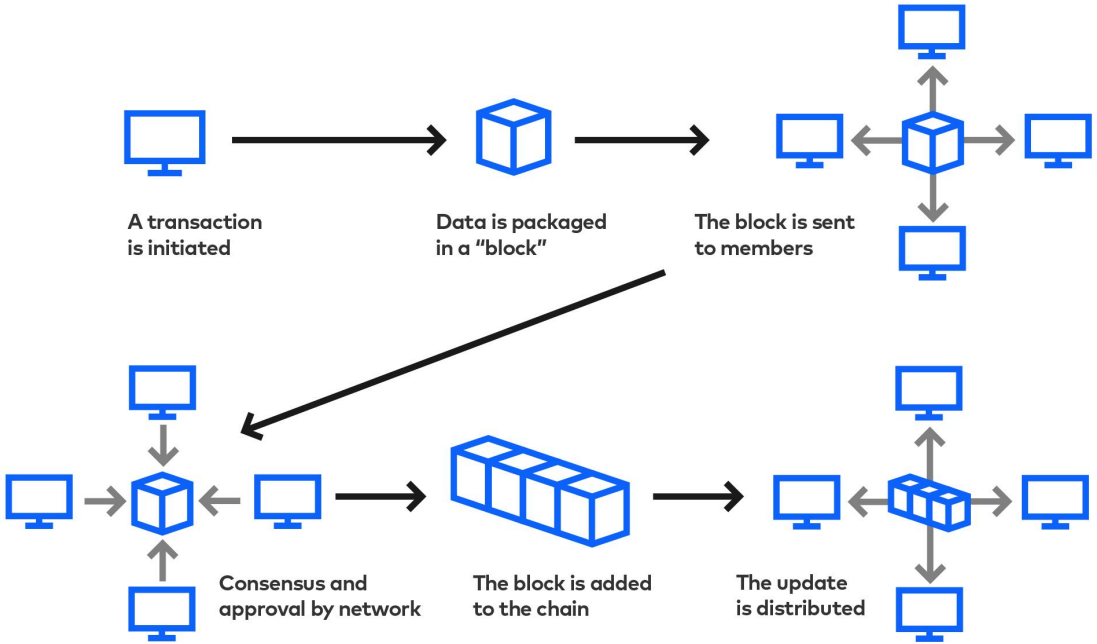


Outline

- Background Information
  - Cryptographically Secure Hash
  - Asymmetric Cryptography
  - Digital Signatures
  - Blind Signatures
  - **Intro to Blockchain**
- Using Blockchain for E-Voting
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

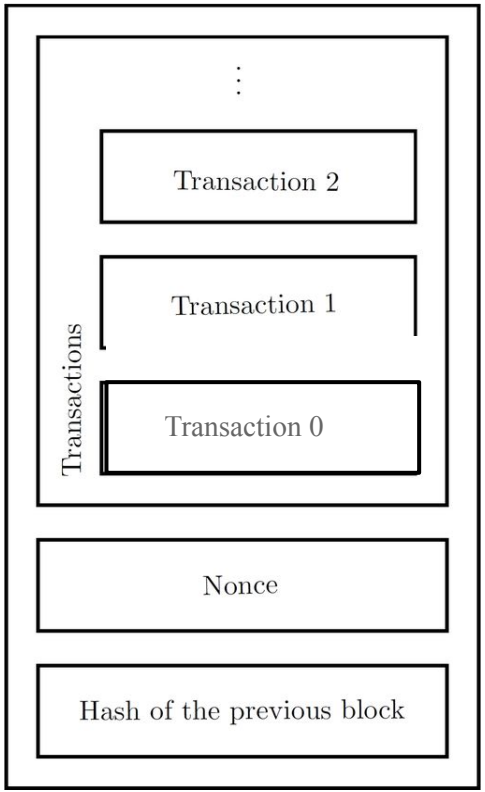
Introduction to Blockchain

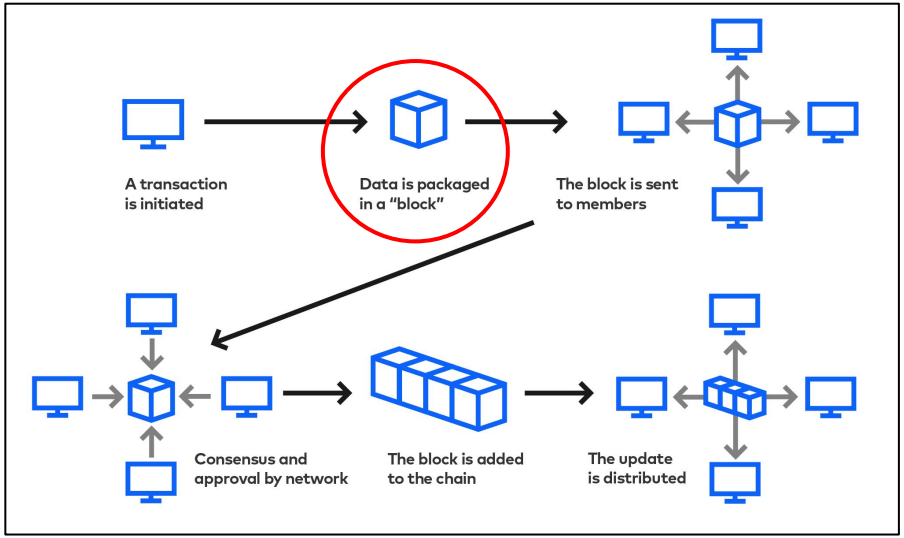
- Blockchain is a specific type of database (Distributed ledger)
- Blockchains store data in blocks that are then chained together
- Most common use so far has been as a ledger for transactions.



https://www.slalom.com/insights/how-blockchain-will-disrupt-your-industry

Introduction To Blockchain





- Nonce = number used once
- Each block holds the hash of the previous block

Proof of Work

"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

= 2^252.253458683

"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

= 2^255.868431117

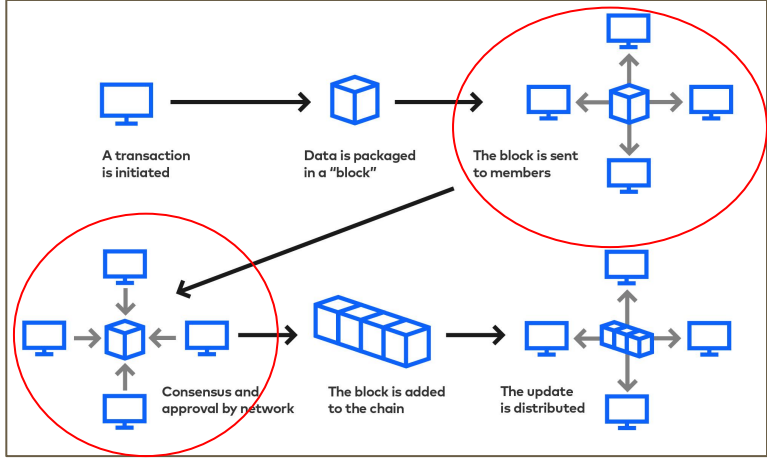
...

"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
= 2^254.782233115

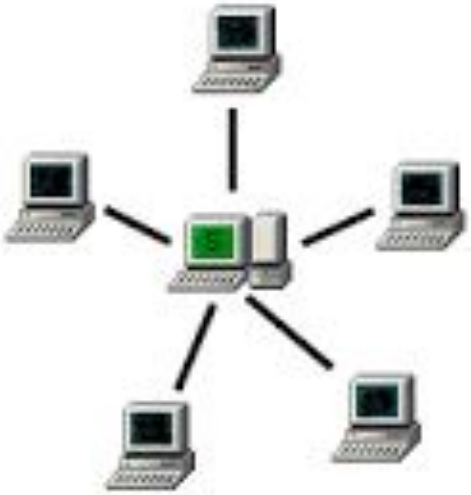
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

< **2^239.61238653**

Introduction to Blockchain- Peer-To-Peer Network

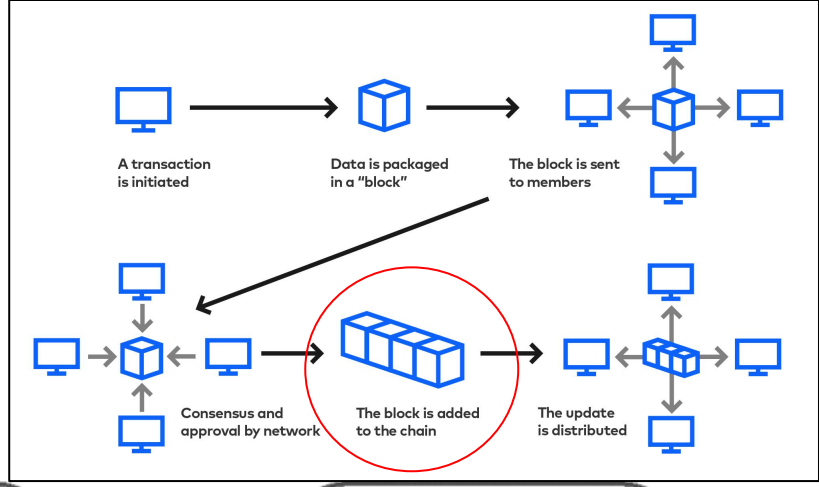


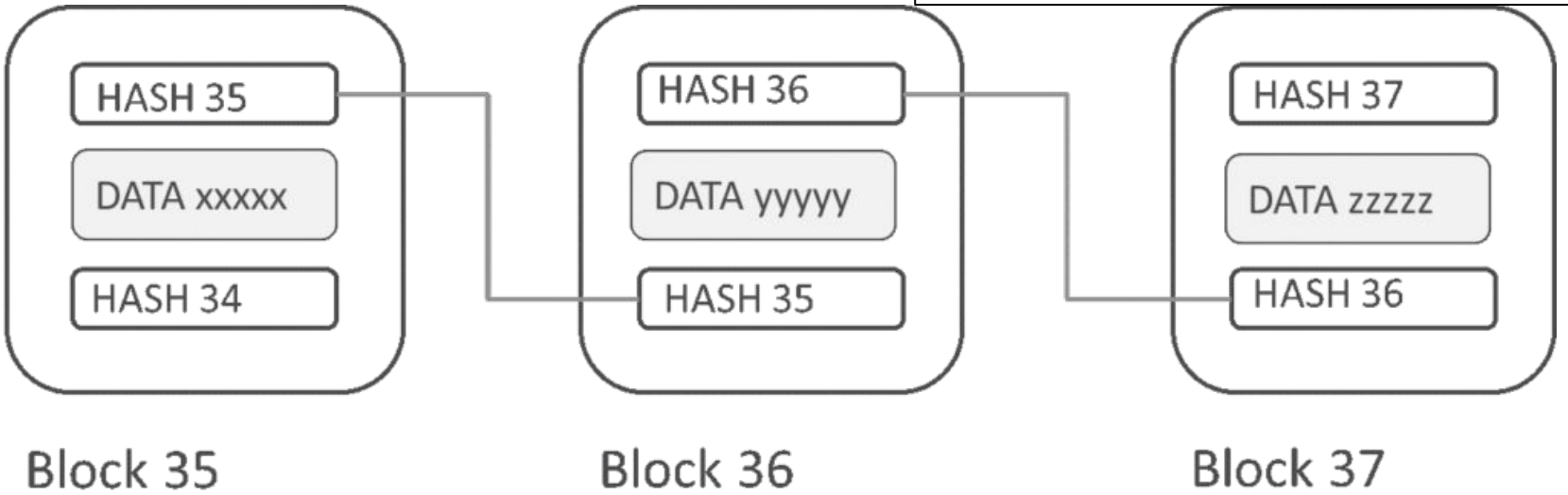
Server Based Network vs. Peer-To-Peer Network



- Decentralized communication model
- Each device = a node
- All nodes hold equal power

Intro to Blockchain





https://www.google.com/url?sa=i&url=https%3A%2F%2Fblog.trendmicro.com%2Fgdpr-vs-blockchain-technology-vs-the-law

Outline

- Background Information
  - Cryptographically Secure Hash
  - Asymmetric Cryptography
  - Digital Signatures
  - Blind Signatures
  - Intro to Blockchain
- **Using Blockchain for E-Voting**
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

Using Blockchain for E-Voting

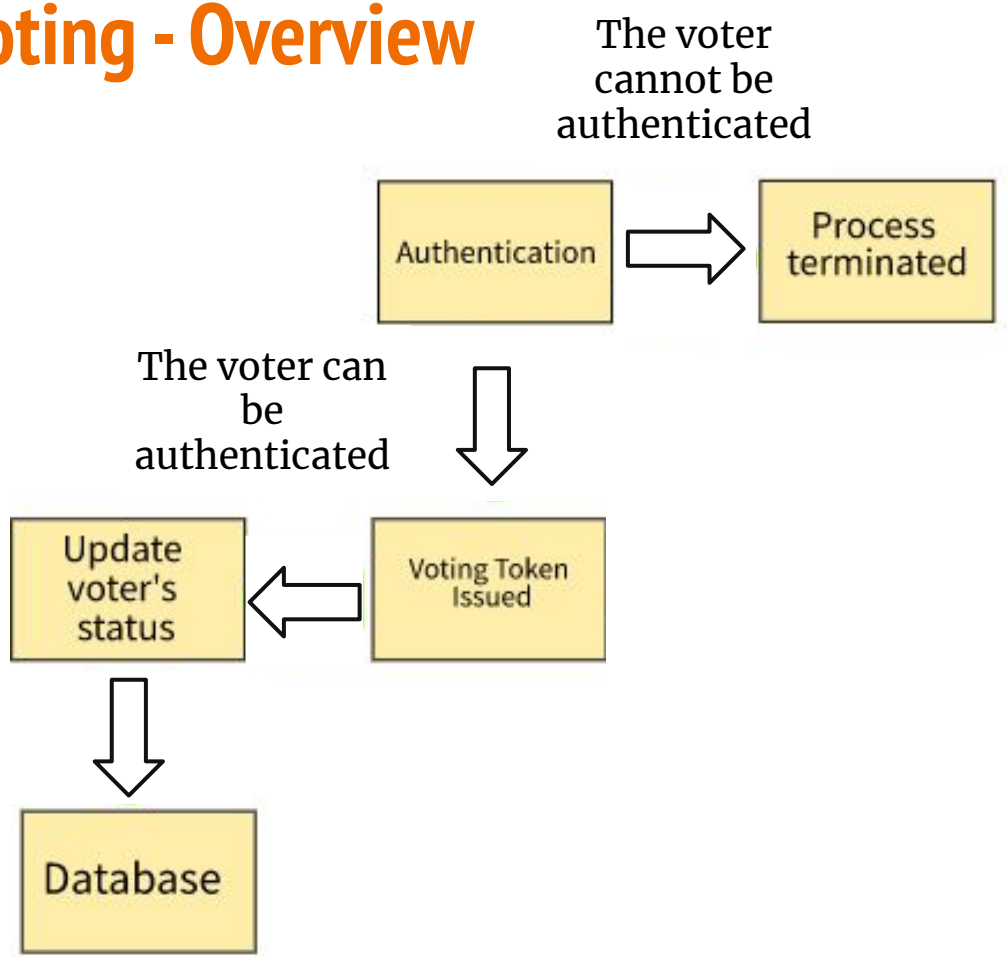
End-to-end Voting with Non-permissioned and Permissioned Ledgers:

Stefano Bistarelli ·Ivan Mercanti ·Paolo Santancini ·Francesco Santin

- Published March 2020

Using Blockchain for E-Voting - Overview

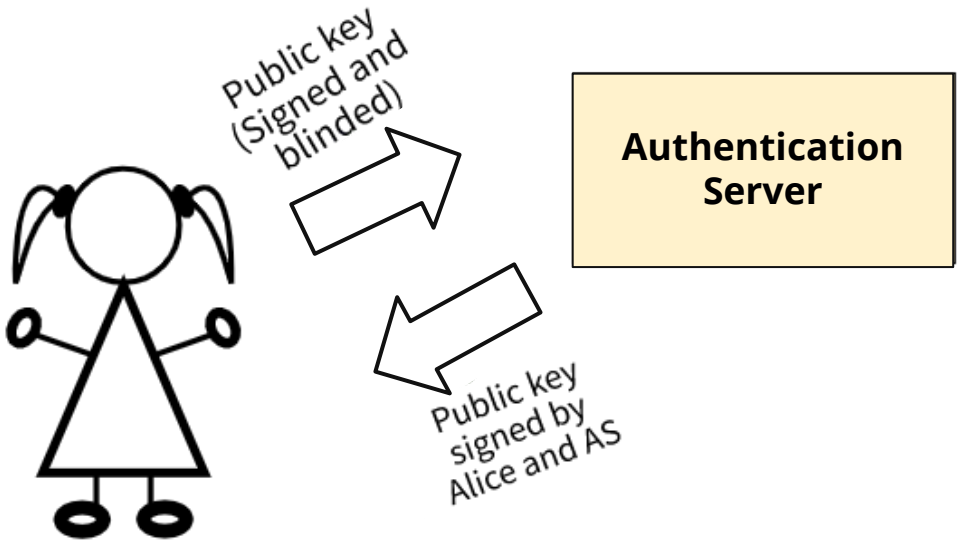
- Pre-Voting phase
  - Candidate nomination



Pre-voting Phase -Voter Authentication

Authentication Service (AS)

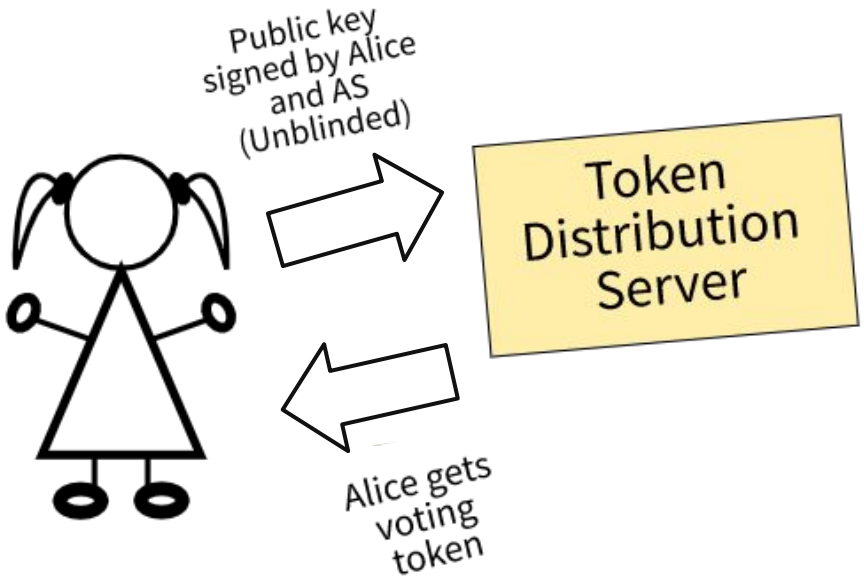
- Non-anonymous Authentication



Pre-Voting -Token Distribution

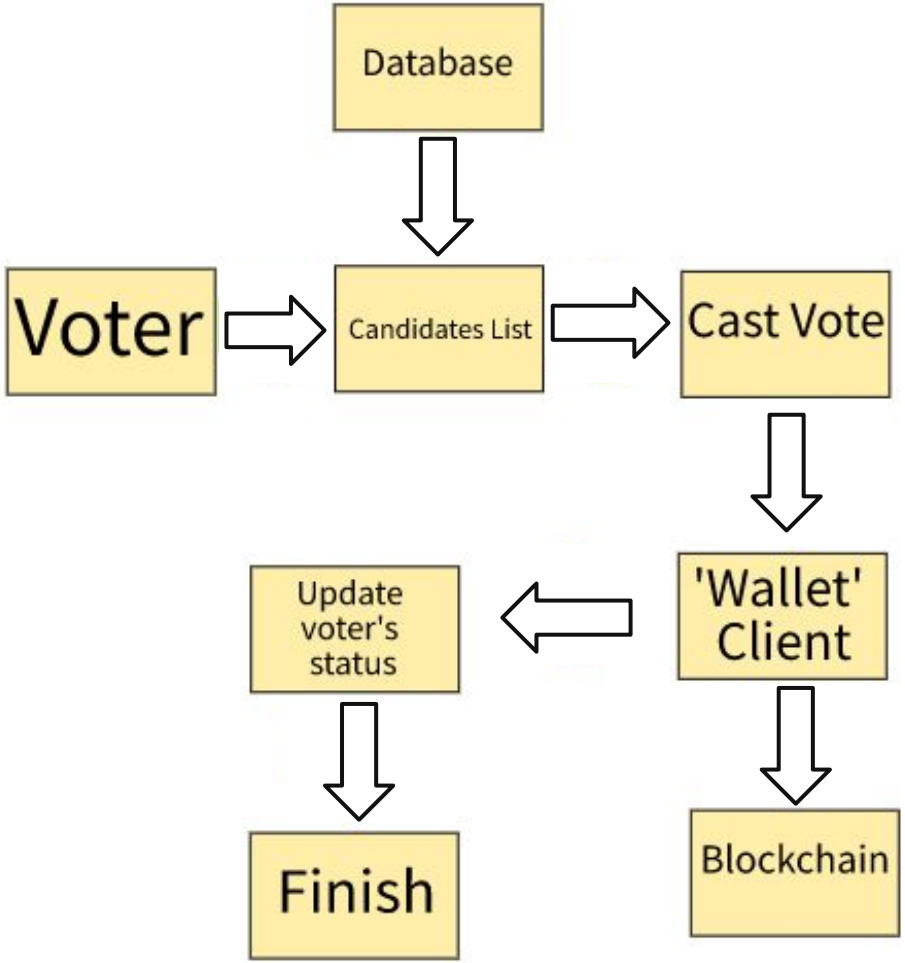
Token Distribution Service(TD)

- Anonymous distribution of tokens to Authenticated voters



Voting Phase

- Wallet within voting application hides the complicated aspects of the transactions from the user



Post Voting Phase

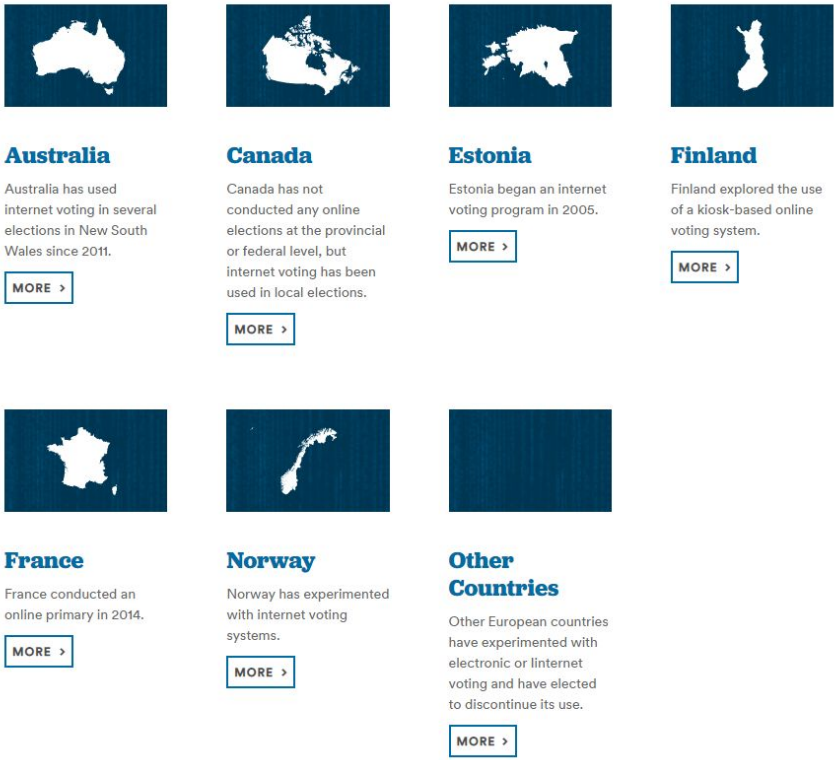
- Votes are counted by taking the sum of tokens received by each candidate
- Votes can be verified using permanently stored source information

Outline

- Background Information
  - Cryptographically Secure Hash
  - Asymmetric Cryptography
  - Digital Signatures
  - Blind Signatures
  - Intro to Blockchain
- Using Blockchain for E-Voting
  - Pre-voting phase
  - Voting phase
  - Post-voting
- Practical considerations

Practical Considerations

- Other countries have experimented with internet voting
- Experts are advising against it, considering it very insecure at this moment



https://verifiedvoting.org/international-internet-voting

References

- M. Bistarelli and S. Santancini. End-to-end voting with non-permissioned and permissioned ledgers. Journal of grid computing, March 2019.
- S. Nagaraj, G. Raju, and V. Srinath. Data encryption and authentication using public key approach. Procedia Computer Science (2015).
- International Conference on Computer, Communication and Convergence (ICCC 2015).
- B. P. Sloane Brakeville. Blockchain basics: Introduction to distributed ledgers. (June 2018)

Questions?