IAIK

TU Graz

SCIENCE
PASSION
TECHNOLOGY

A Correctable Public Blockchain

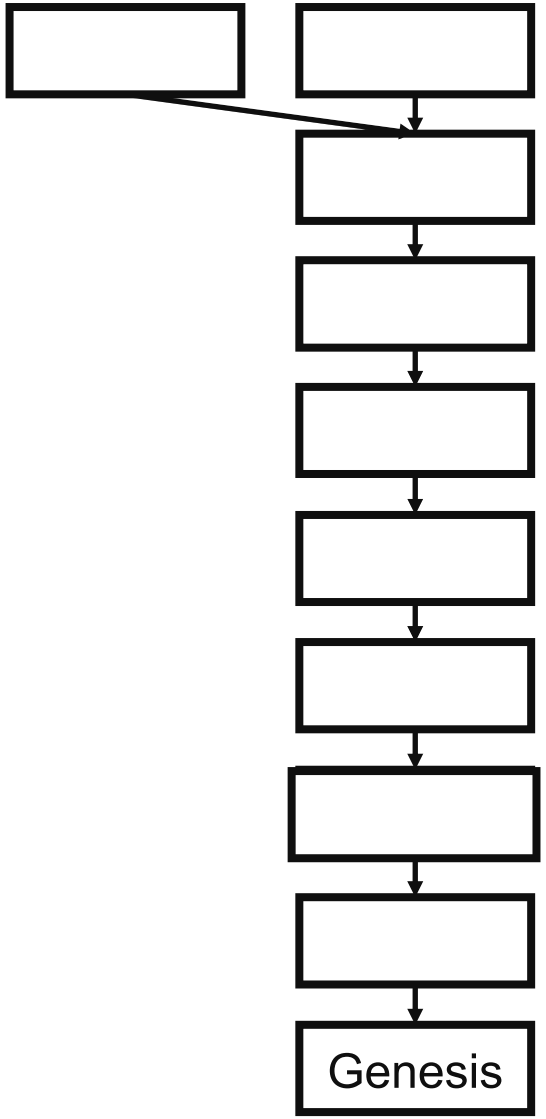
Alexander Marsalek | amarsalek@iaik.tugraz.at
Thomas Zefferer | tzefferer@a-sit.at

Institute of Applied Information Processing and Communications
Graz University of Technology, Austria

06.08.2019

Background

- What are:
  - Miners
  - Transactions
  - Blocks
  - Proof-of-Work
  - Block rewards
  - Consensus algorithms

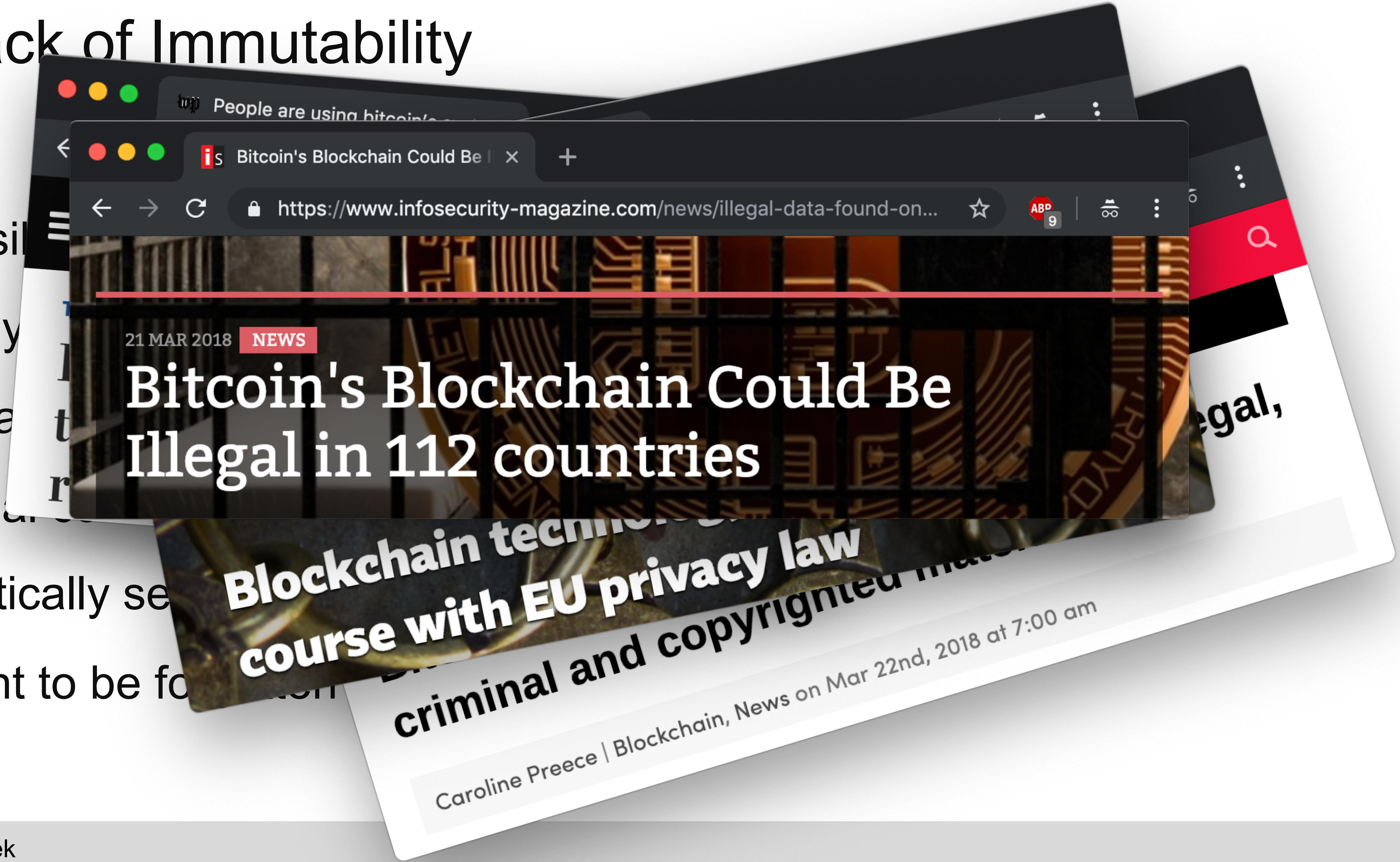


Public Blockchain – Key Features

- Transparency
- Integrity
- Censorship resistance
- Robustness
- Prevent fraud
- Eliminate TTP
- Immutability

Drawback of Immutability

- Impossi
  - Copy
  - Viola
  - Illega
  - Politically se
  - Right to be fo



People are using bitcoin's

Bitcoin's Blockchain Could Be I

https://www.infosecurity-magazine.com/news/illegal-data-found-on...

21 MAR 2018 NEWS

Bitcoin's Blockchain Could Be Illegal in 112 countries

Blockchain techno

course with EU privacy law

egal,

criminal and copyrighted mater

Caroline Preece | Blockchain, News on Mar 22nd, 2018 at 7:00 am

Main Goal

- Create correctable blockchain that allows to correct erroneous data and to delete malicious data without changing the trust assumption!

Subgoals

1. No change in trust assumption
   - No special or trusted nodes
   - No secret keys
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
4. Accountability
5. Scalability
6. Robustness – dynamic changes in miner set
7. Prevent centralization
8. Editing of money transactions

Goals

1. No change in trust assumption
2. Selective removal of data
   - Remove data from ledger
   - Making it inaccessible
3. Redaction based on distributed consensus
4. Accountability
5. Scalability
6. Robustness – dynamic changes in miner set
7. Prevent centralization
8. Editing of money transactions

Goals

1. No change in trust assumption
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
   - Majority decision
4. Accountability
5. Scalability
6. Robustness – dynamic changes in miner set
7. Prevent centralization
8. Editing of money transactions

Goals

1. No change in trust assumption
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
4. Accountability
   - Changes must be replicable
5. Scalability
6. Robustness – dynamic changes in miner set
7. Prevent centralization
8. Editing of money transactions

Goals

1. No change in trust assumption
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
4. Accountability
5. Scalability
   - Must work independent from the number of miners
6. Robustness – dynamic changes in miner set
7. Prevent centralization
8. Editing of money transactions

Goals

1. No change in trust assumption
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
4. Accountability
5. Scalability
6. Robustness
   - Must be robust against changes in the miner set
7. Prevent centralization
8. Editing of money transactions

Goals

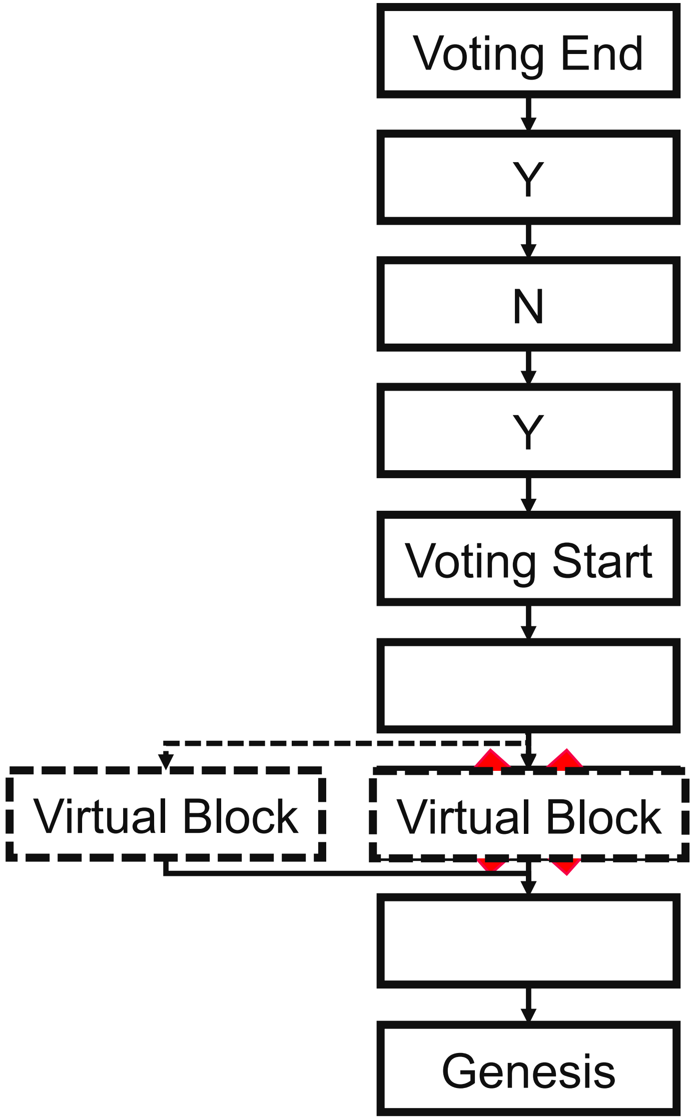
1. No change in trust assumption
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
4. Accountability
5. Scalability
6. Robustness – dynamic changes in miner set
7. Prevent centralization
   - No shared-key approach
   - Every miner should have power proportional to her computation power
8. Editing of money transactions

Goals

1. No change in trust assumption
2. Selective removal of data – Make it inaccessible
3. Redaction based on distributed consensus
4. Accountability
5. Scalability
6. Robustness – dynamic changes in miner set
7. Prevent centralization
8. Editing of money transactions
   - It should be possible to remove malicious data, also from payment transaction

Idea

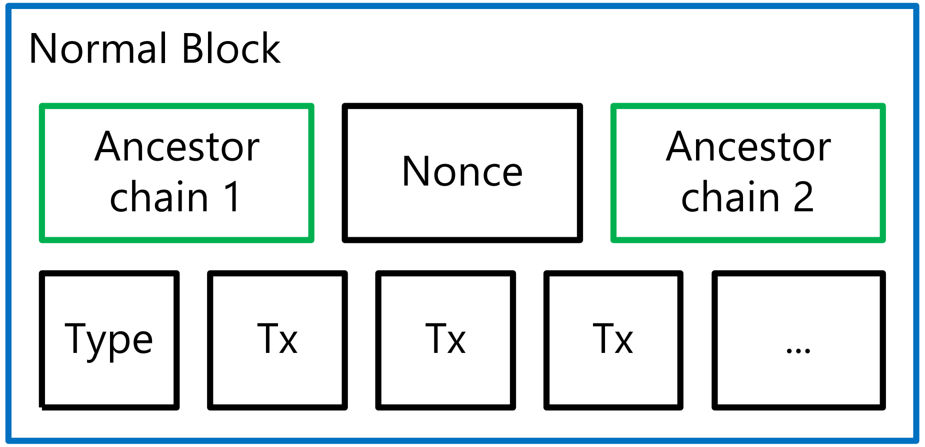
- Create election TX
- Miner validate TX against policy
- Voting starts
- Majority decides
- If won:
    - Replace block with virtual block
- Security?
    - Use second chain



Normal Block

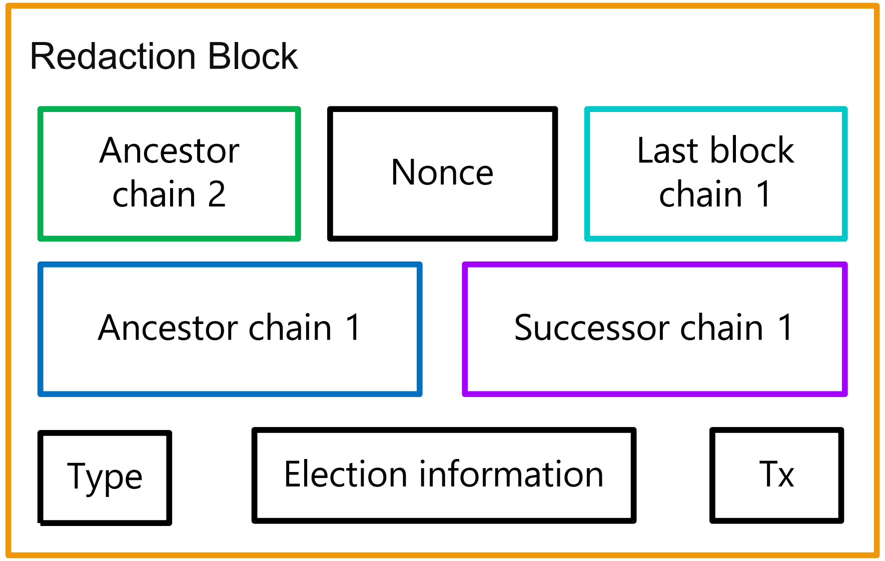
2 new fields

- Type
    - Normal block
    - Virtual block
- Ancestor chain 2
    - Points to last Redaction block



Redaction Block

- Ancestor chain 2
- Last block chain 1
- Ancestor chain1
- Successor chain 1
- Election information



Redaction Block

Ancestor chain 2

Nonce

Last block chain 1

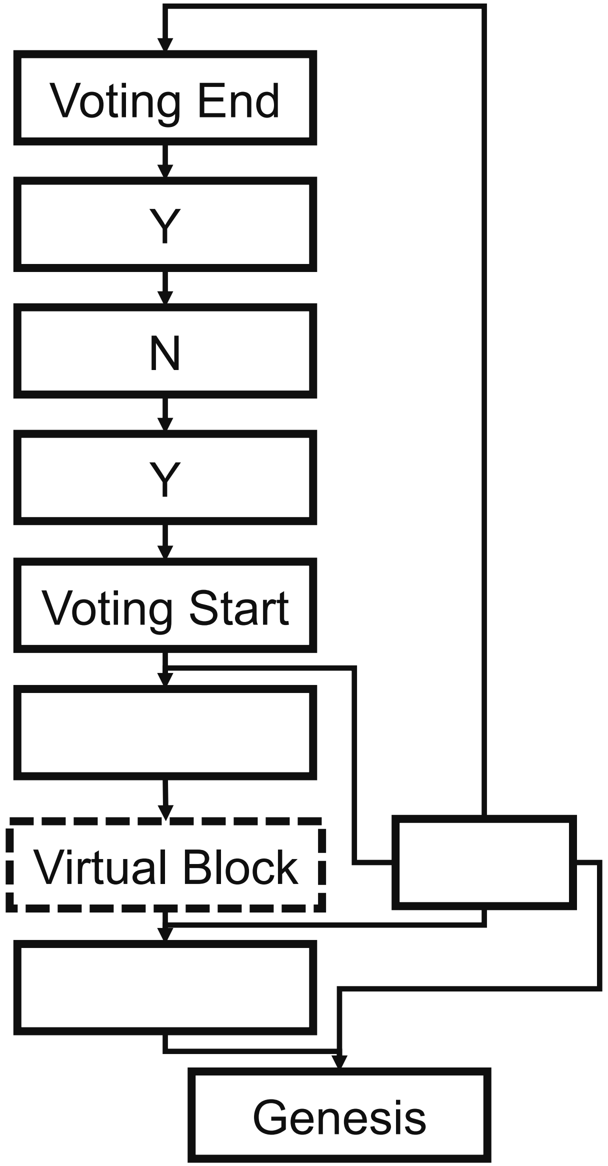
Ancestor chain 1

Successor chain 1

Type

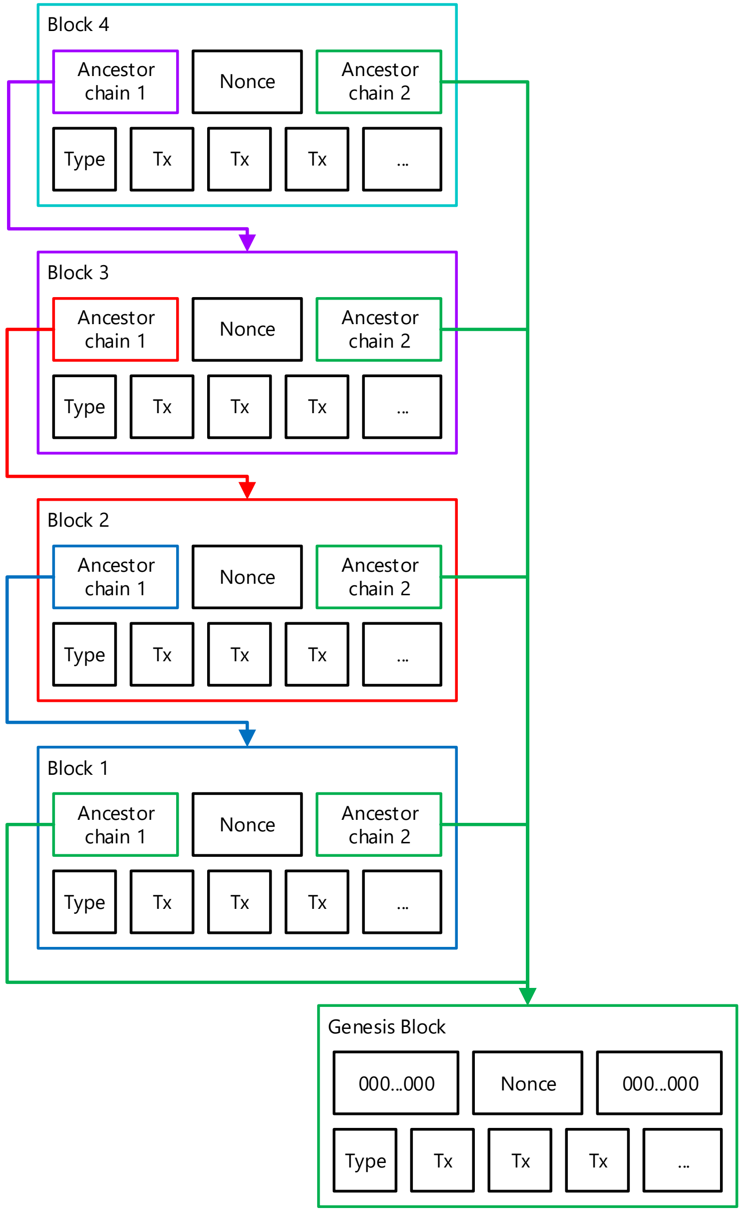
Election information

Tx

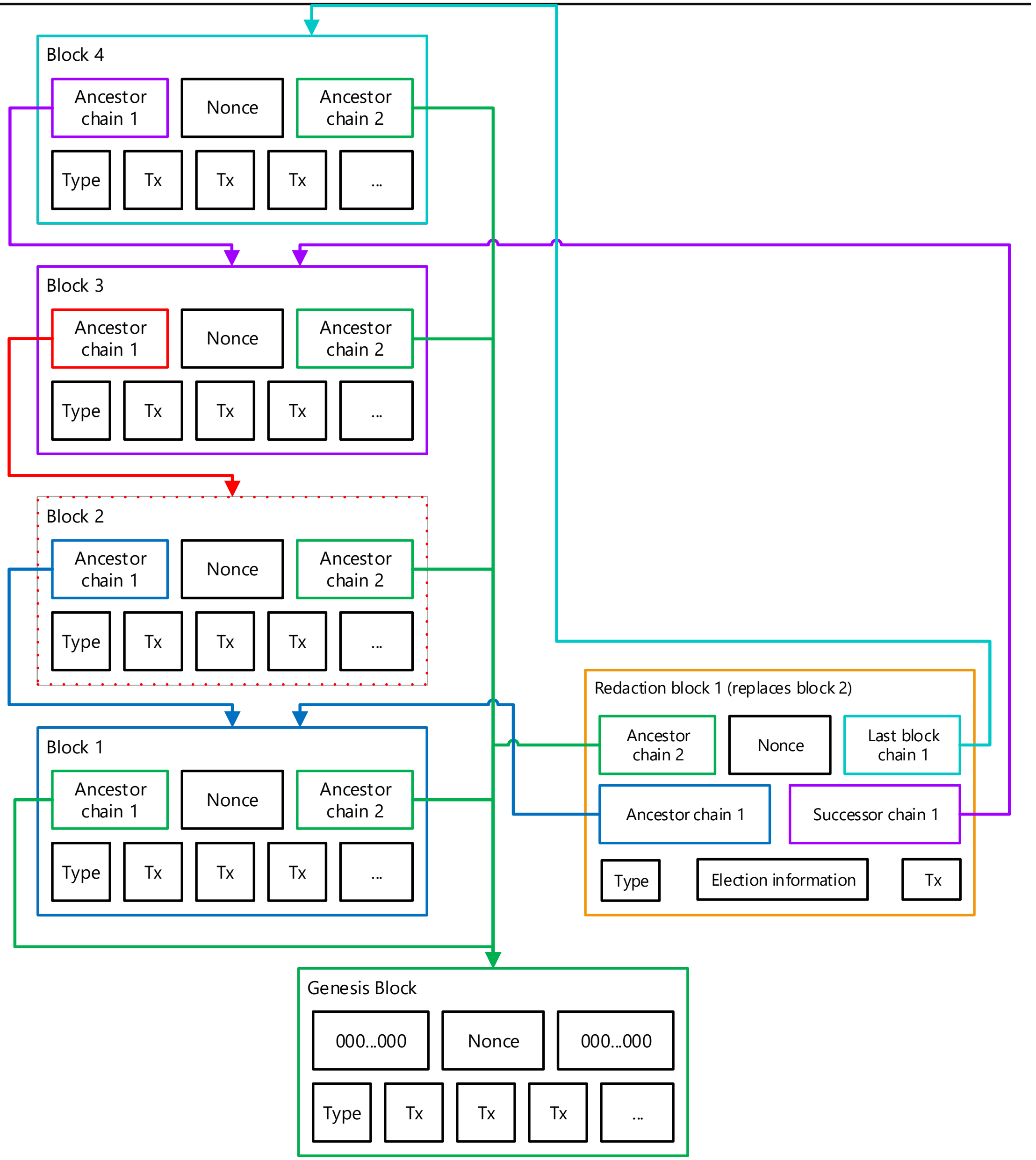


- All block in chain 2 are of this type

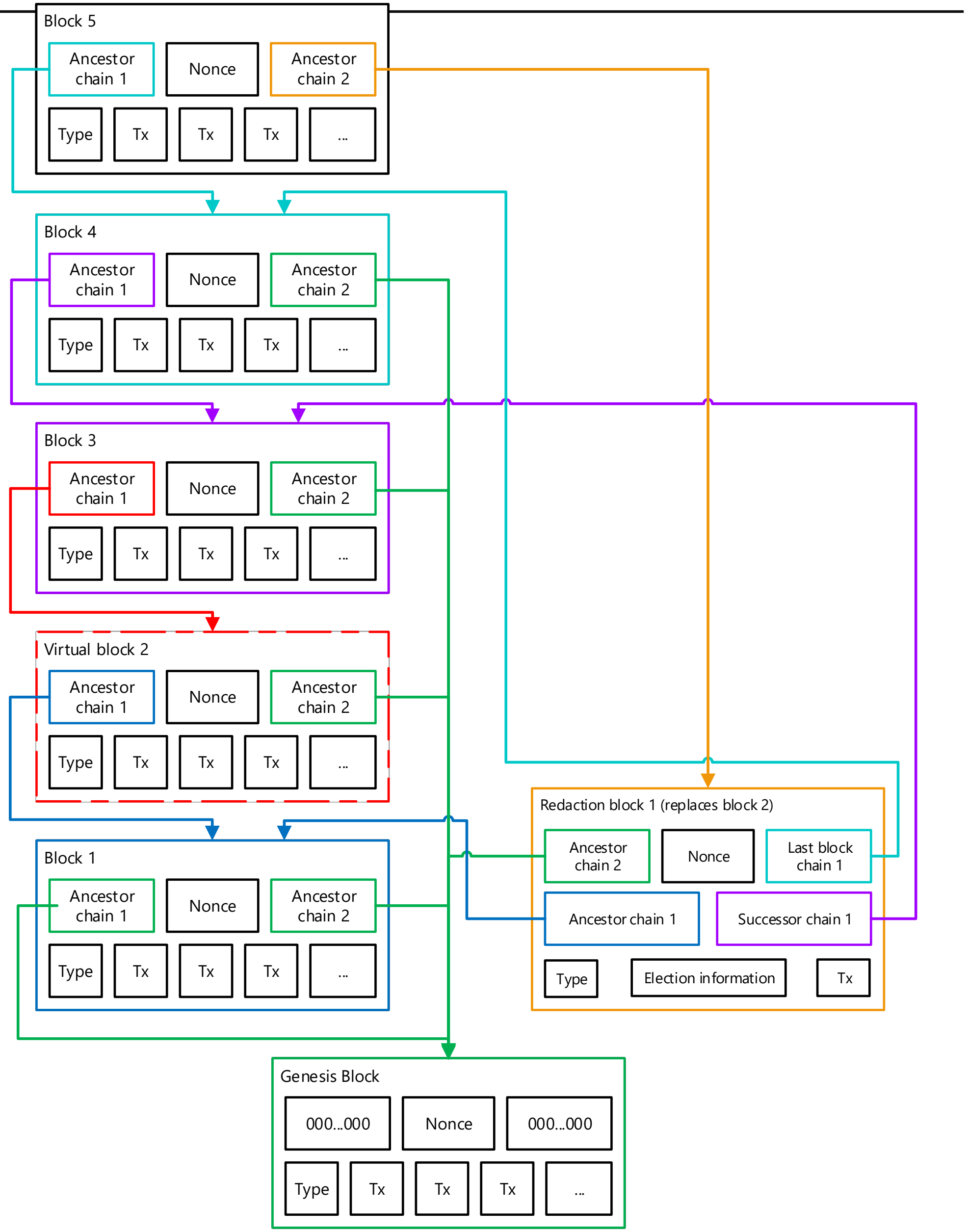
- Voting to decide which data to delete
- Virtual block replaces original block
- Second (linked) chain approves virtual block



- Voting to decide which data to delete
- Virtual block replaces original block
- Second (linked) chain approves virtual block



- Voting to decide which data to delete
- Virtual block replaces original block
- Second (linked) chain approves virtual block



Added Rules

When voting is over

- Won: Next block must be a redaction block
- Lost: Next block must be a normal block

Normal blocks always reference last redaction block

Redaction blocks must build a valid chain

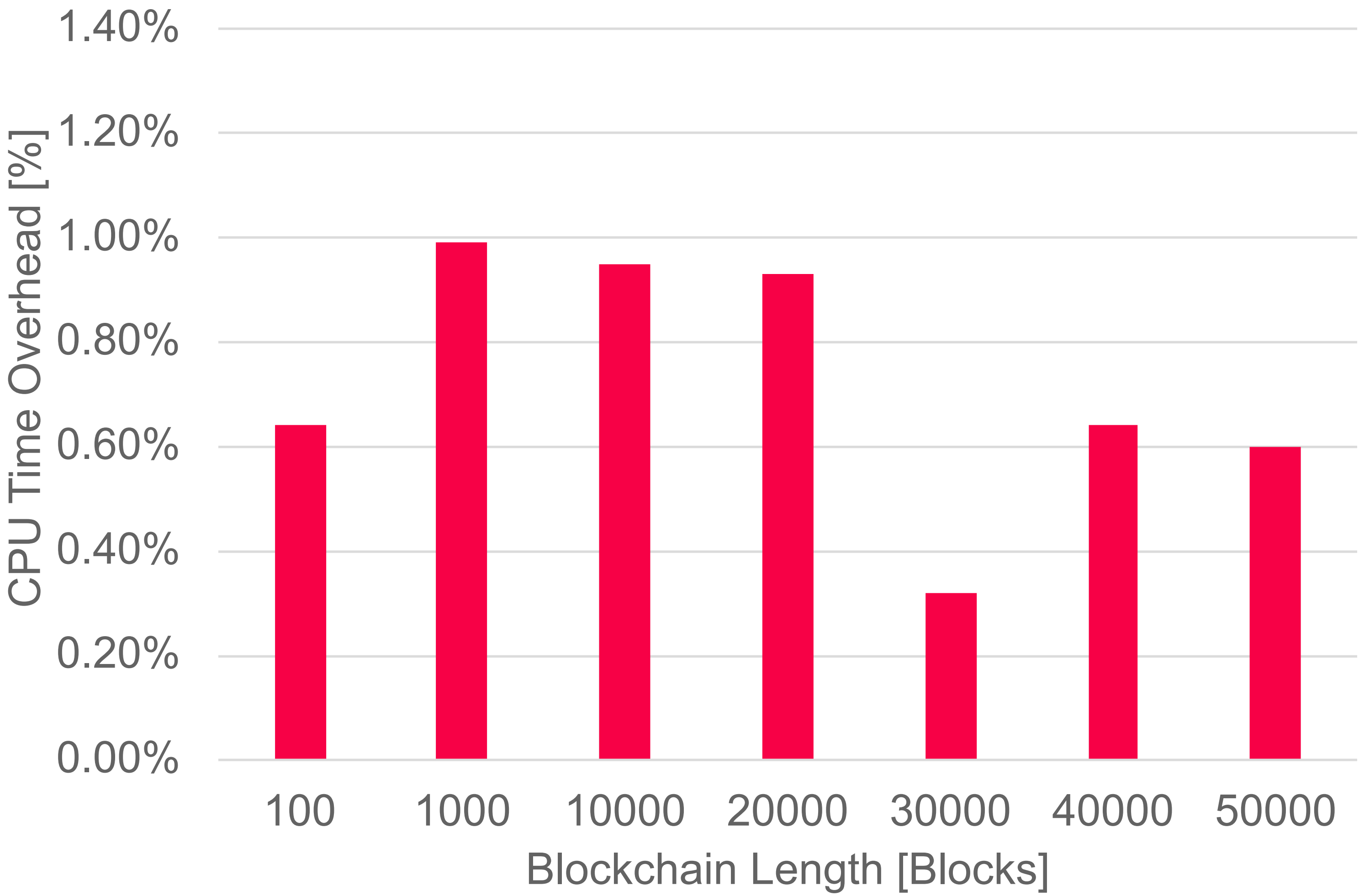
- All virtual blocks must be part of the main chain
- Virtual blocks are seen as having the hash of the block they replace

Evaluation

Evaluation Setup

- Different blockchain lengths
  - 100, 1000, 10k, 20k, 30k, 40k, 50k blocks
- 1% of blocks are being corrected

Performance Overhead



Conclusions

- Approach allows to edit or remove data from public blockchain
- Deletion based on majority decision
    - Trust assumptions unchanged
- Only small performance overhead