

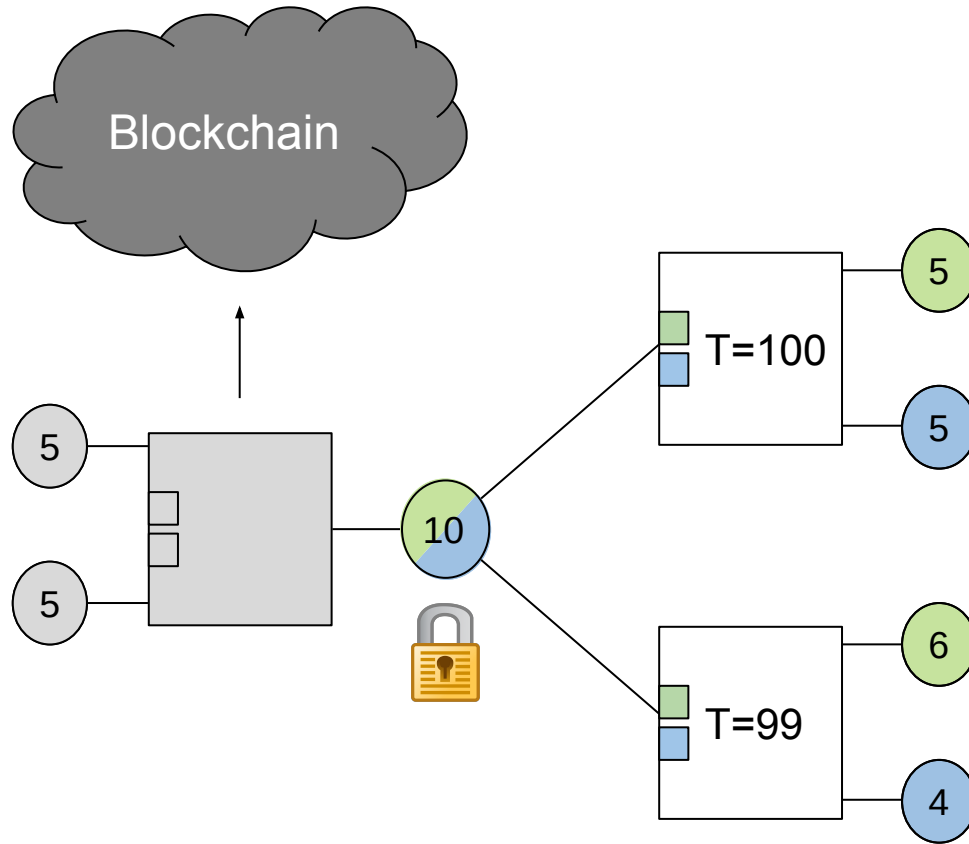
# Incentivizing Payment Channel Watchtowers



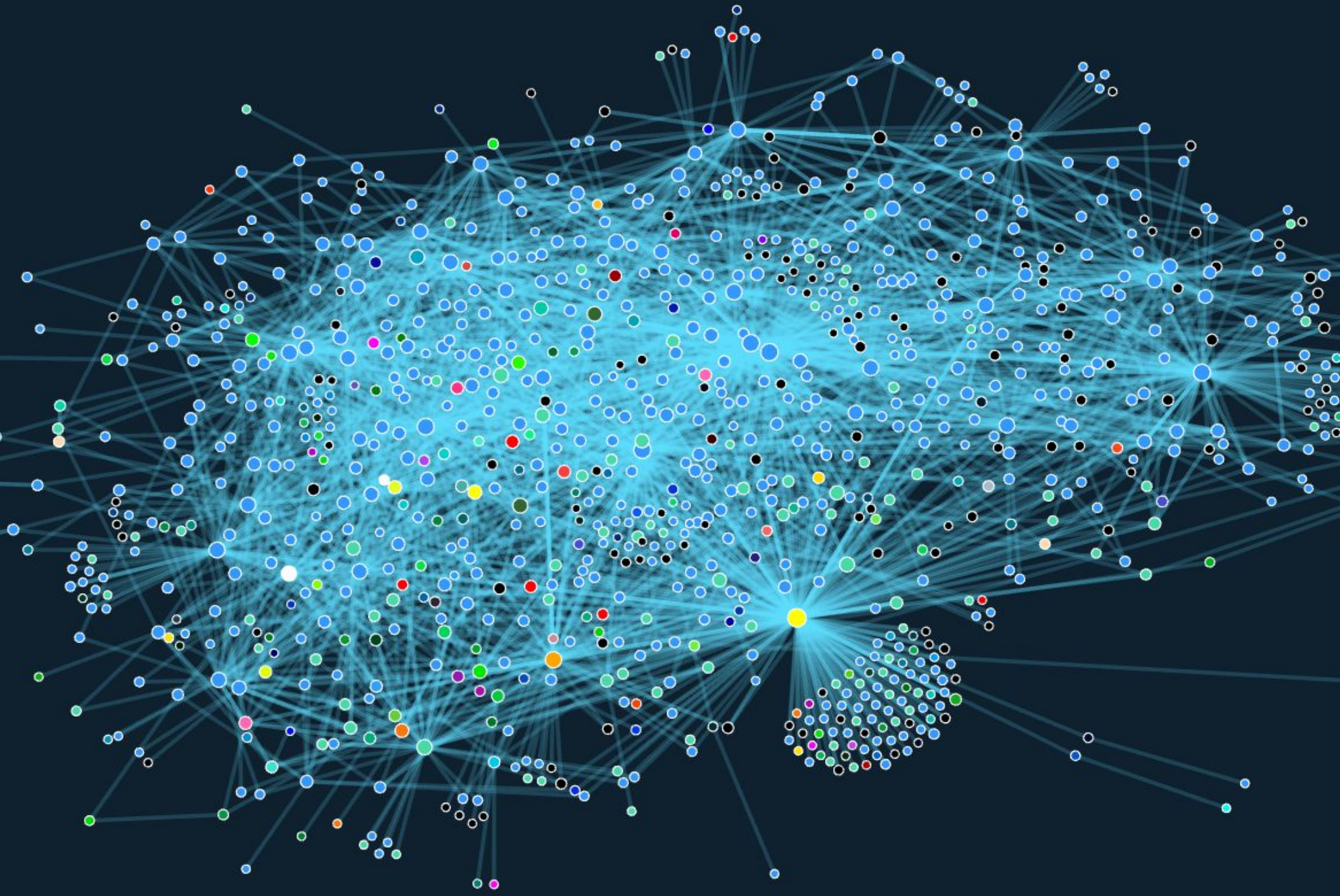
**Zeta Avarikioti &**

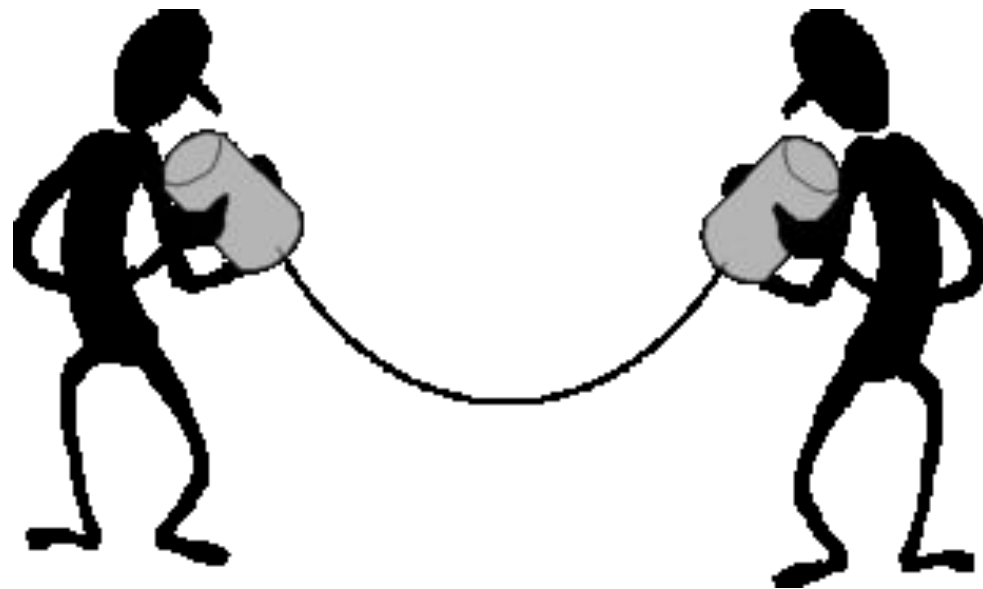
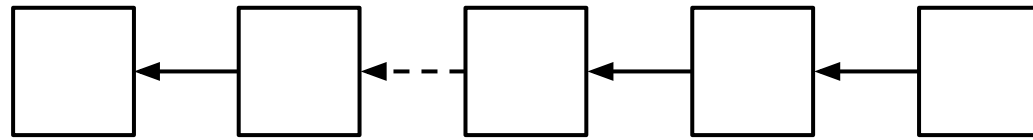
*Felix Laufenberg, Jakub Sliwinski, Yuyi Wang, Roger Wattenhofer*

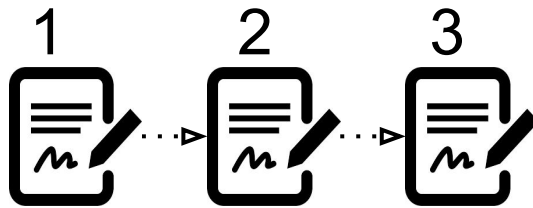
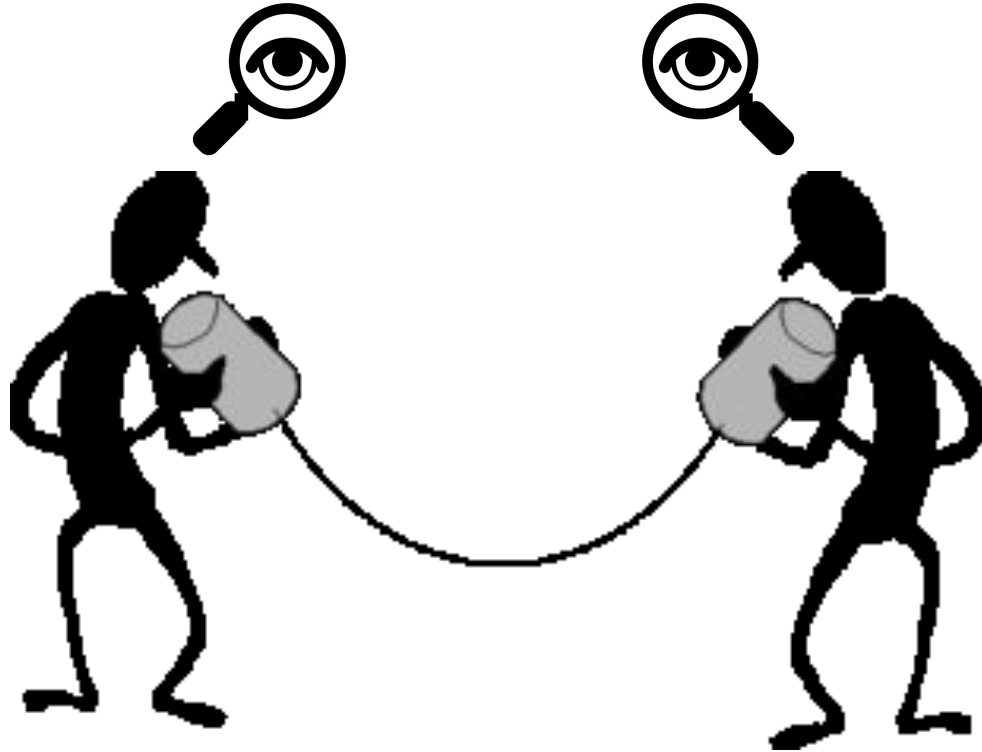
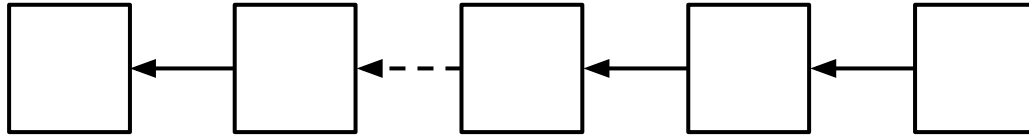
# Micropayment Channel

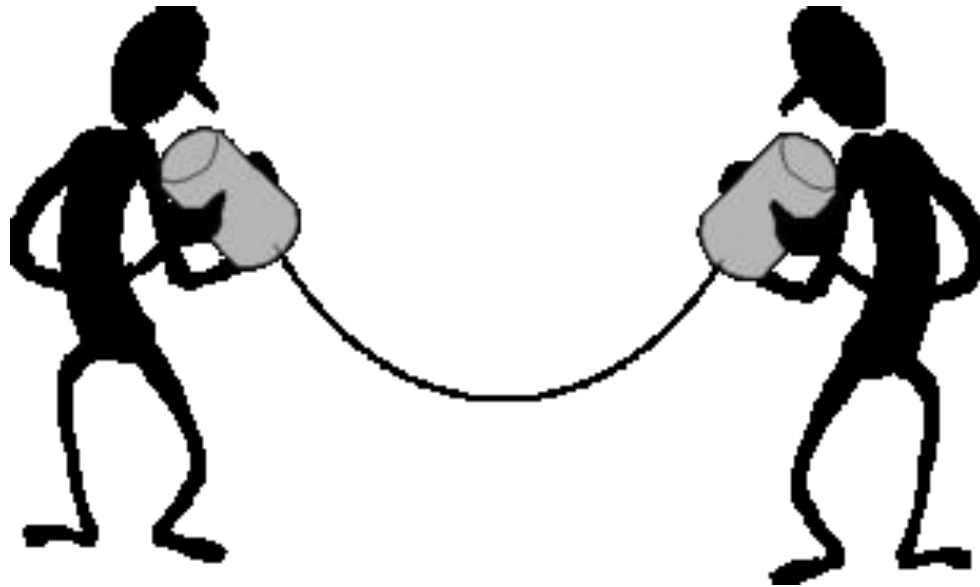
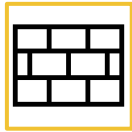
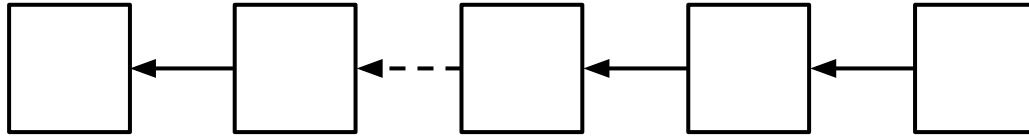


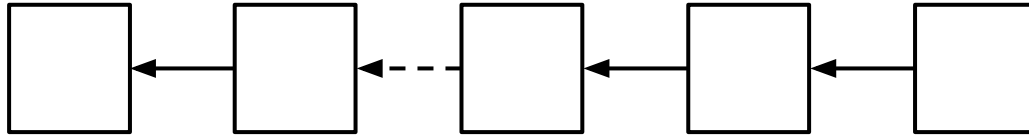




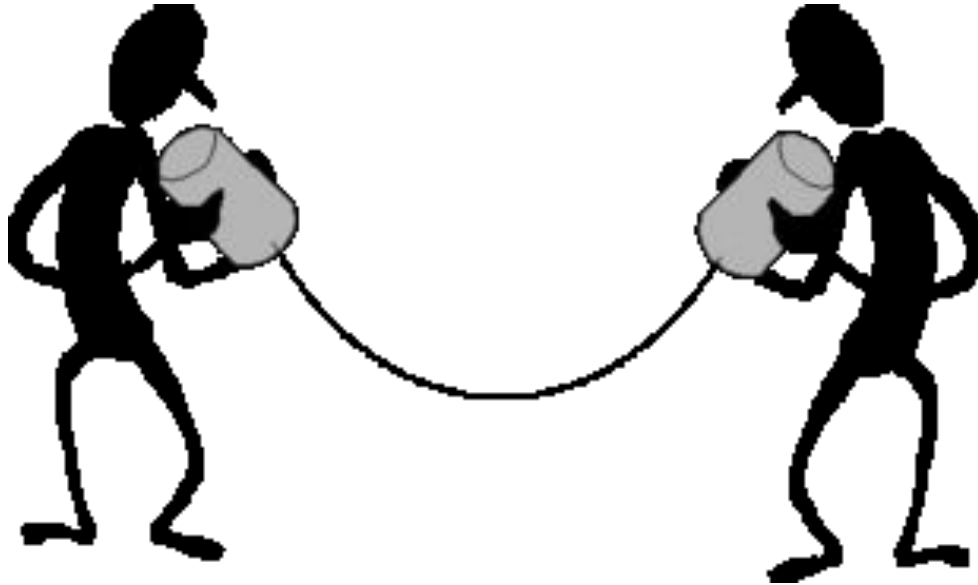
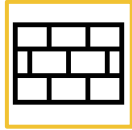


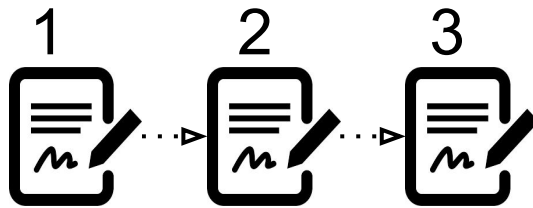
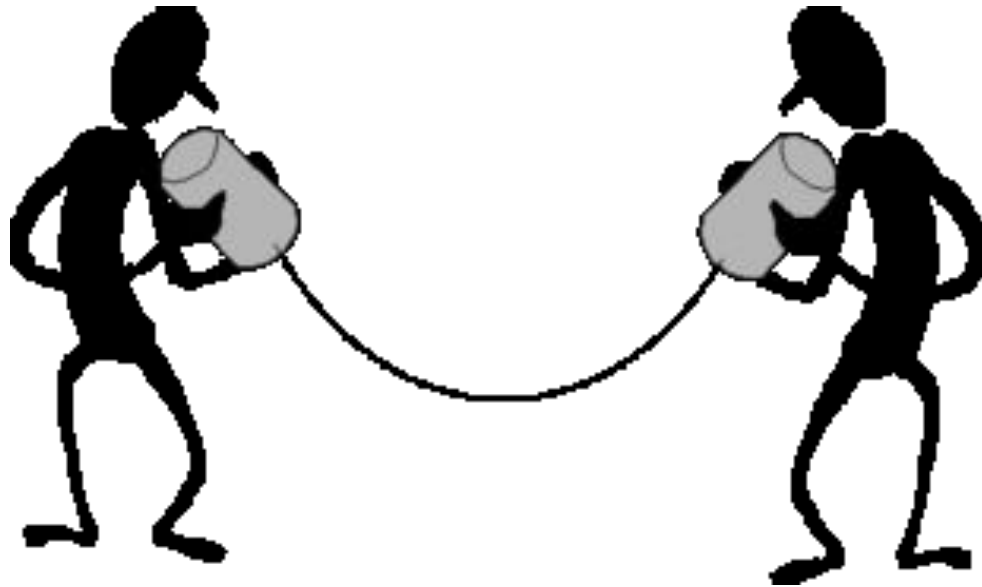
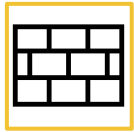
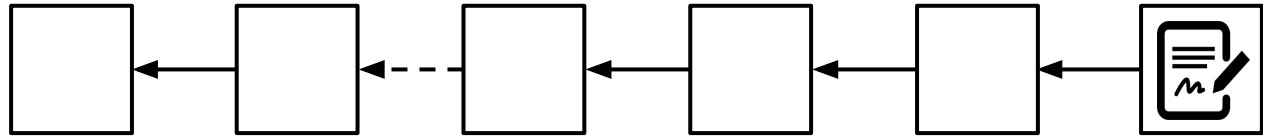






2

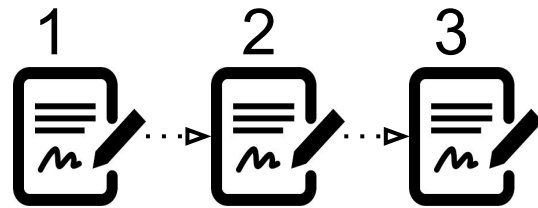
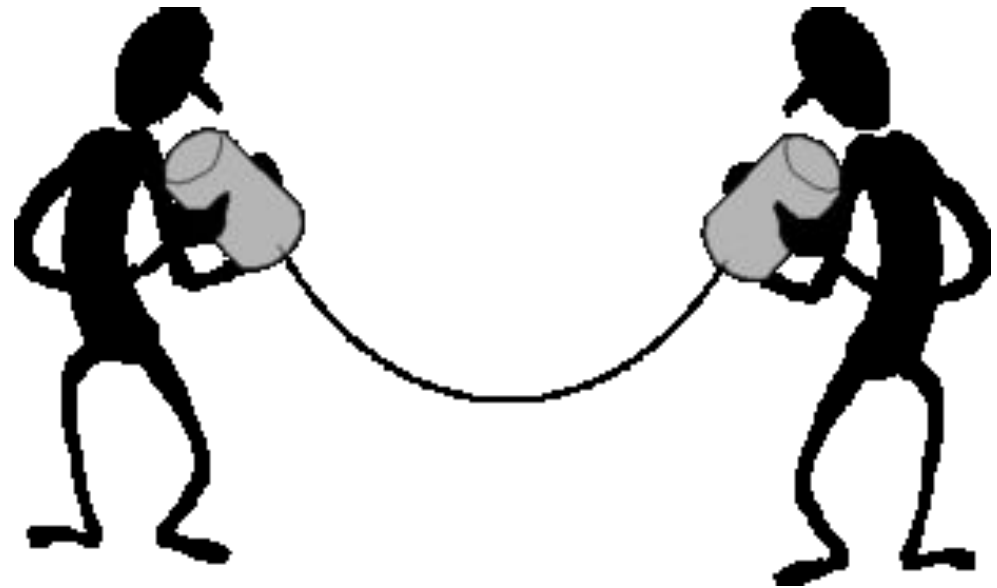
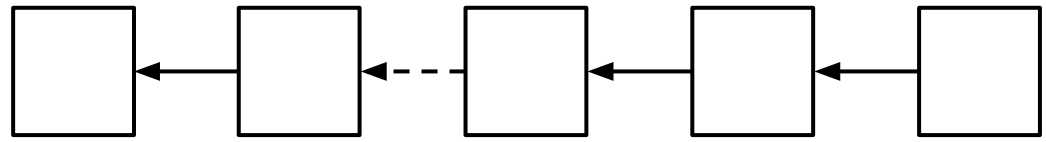




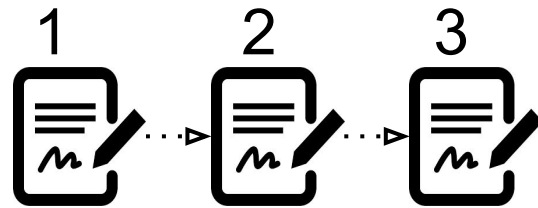
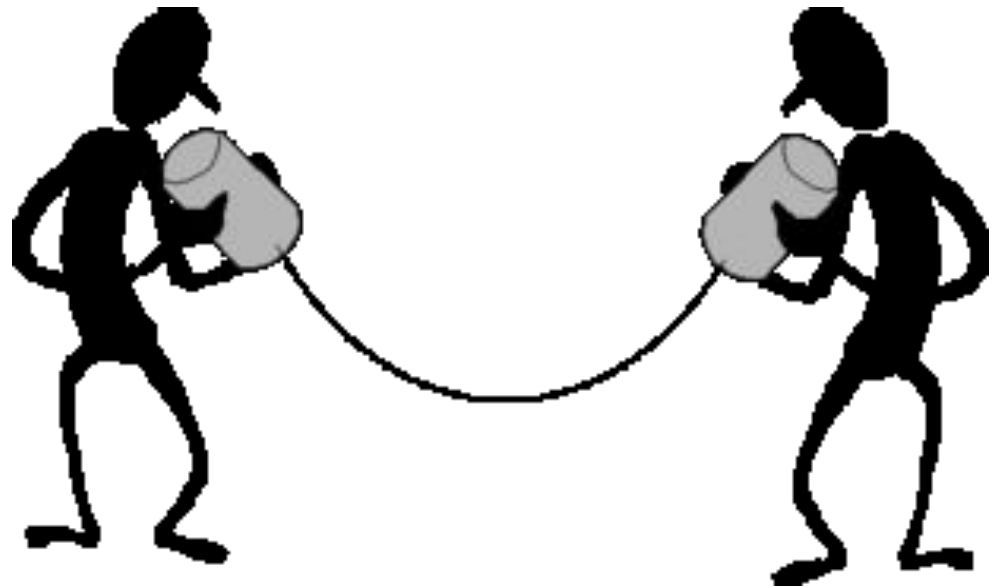
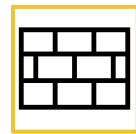
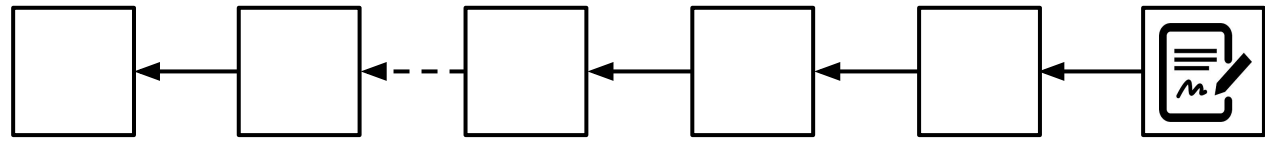




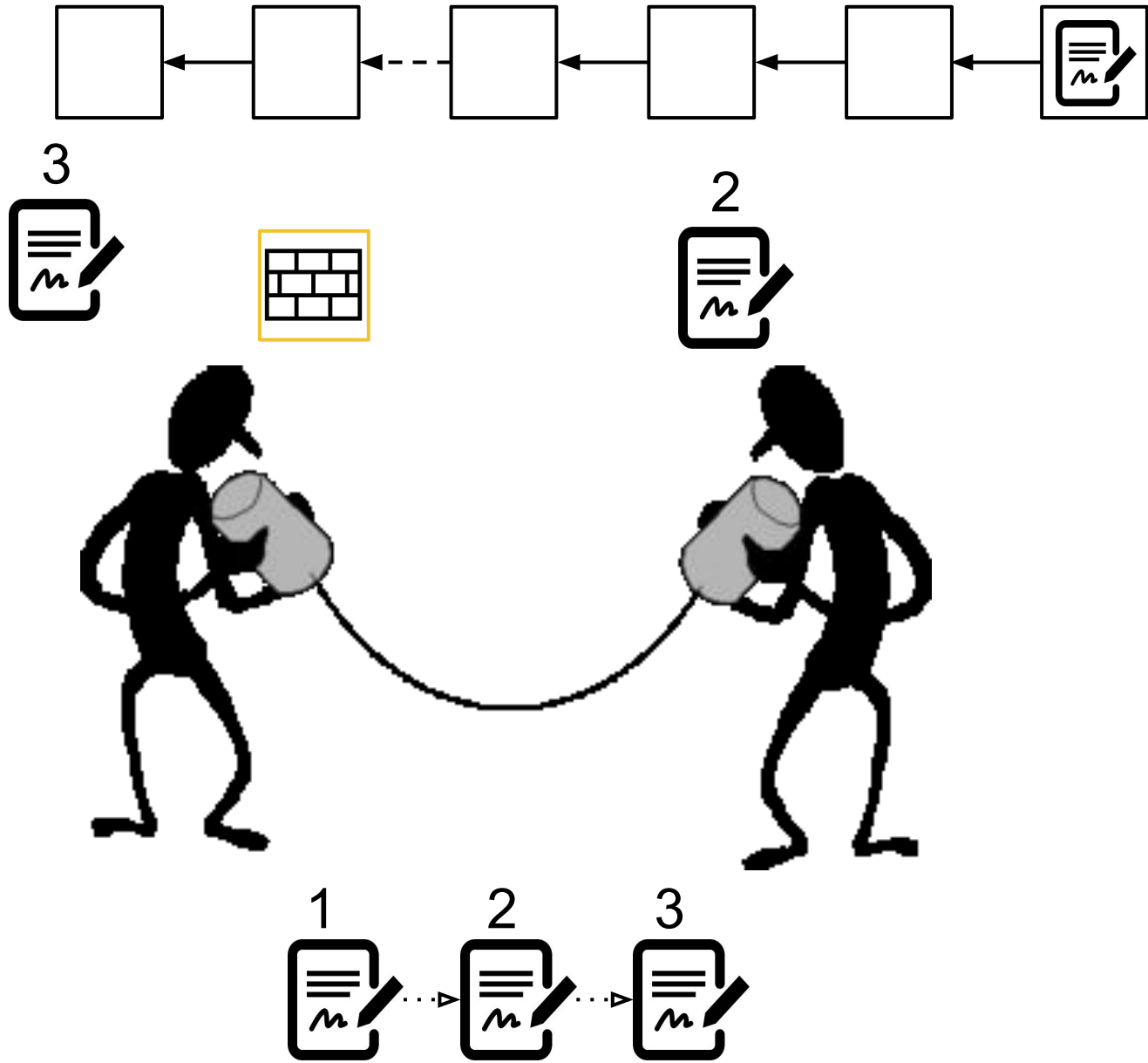












# Original Watchtowers

## Privacy

99a73f590ba0809ff36b4bd1d994b5c3ba9d051376159d35c44cd82703cdf9d8

2018-09-27 14:38:30

17jFkgpNLBvDEYGqjbm8JWUYVASzLbr8dp



1JGR17sPd8TPkdJxbHPC117oPFV1AYiXVG  
3MWSbWigsP9378DeorPQnTkyGjVrYWPI6f

4.45825827 BTC  
0.00390679 BTC

4.46216506 BTC

**TXID:** 51b78168d94ec307e2855697209275d4  
**identifier**

77e05d8647caf29cb9e38fb6a4661145  
**key**

# Original Watchtowers

## Privacy

99a73f590ba0809ff36b4bd1d994b5c3ba9d051376159d35c44cd82703cdf9d8		2018-09-27 14:38:30
17jFkgpNLBvDEYGqjbm8JWUYVASzLbr8dp	→	1JGR17sPd8TPkdJxbHPC117oPFV1AYiXVG 3MWSbWigsP9378DeorPQnTkyGjVrYWPI6f
		4.45825827 BTC 0.00390679 BTC
		4.46216506 BTC

**TXID:** 51b78168d94ec307e2855697209275d4  
**identifier**

77e05d8647caf29cb9e38fb6a4661145  
**key**

**Watchtowers**



# Original Watchtowers

## Privacy

99a73f590ba0809ff36b4bd1d994b5c3ba9d051376159d35c44cd82703cdf9d8

2018-09-27 14:38:30

17jFkgpNLBvDEYGqjbm8JWUYVASzLbr8dp



1JGR17sPd8TPkdJxbHPC117oPFV1AYiXVG  
3MWSbWigsP9378DeorPQnTkyGjVrYWPI6f

4.45825827 BTC  
0.00390679 BTC

4.46216506 BTC

**TXID:** 51b78168d94ec307e2855697209275d4  
**identifier**

77e05d8647caf29cb9e38fb6a4661145  
**key**

## Watchtowers

# Original Watchtowers

**Overhead**

**Altruism**

**storage**

**why participate?**

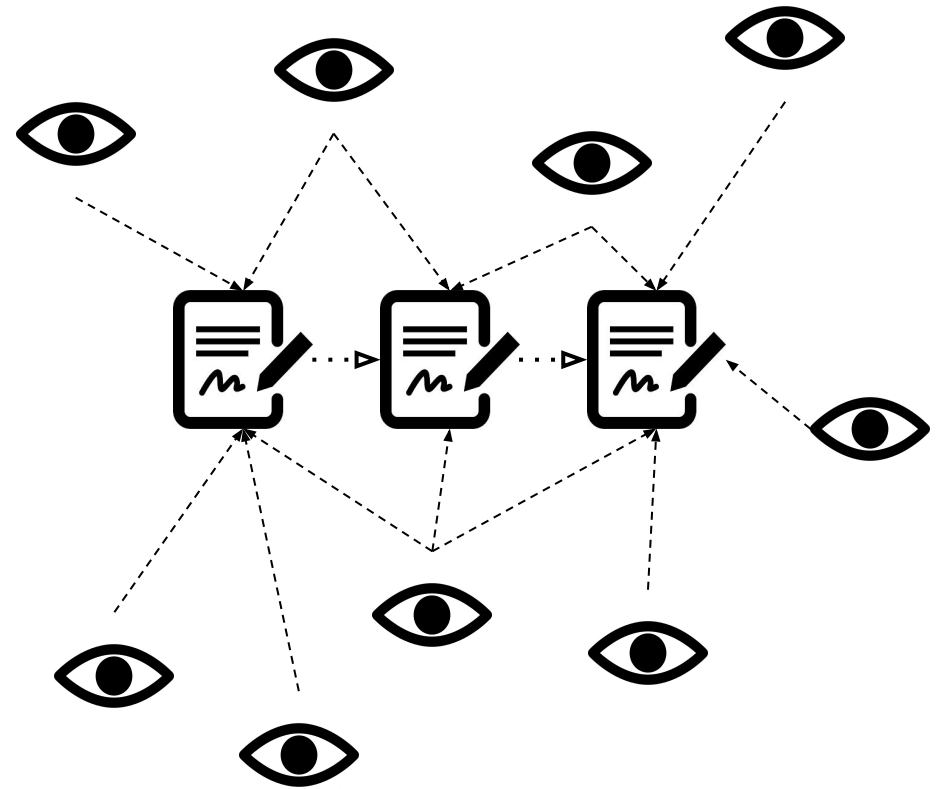
**lookup time**



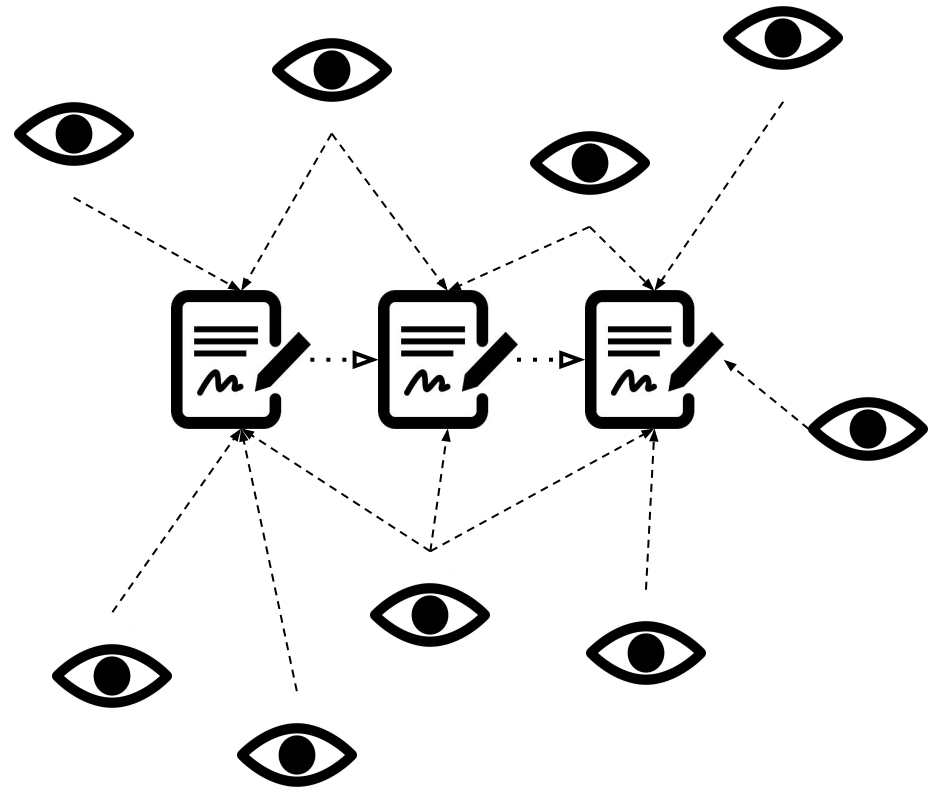




# Free Market



- **Security**
- **Incentives**
- **Overhead**
- **Privacy**

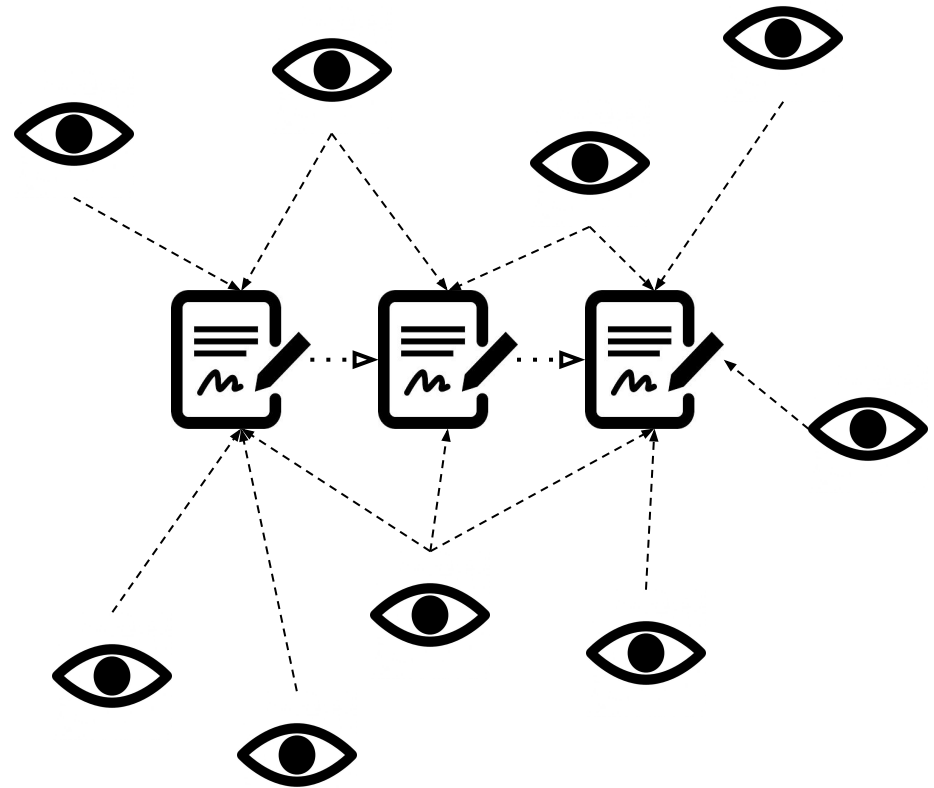


- **Security**

- **Incentives**

- **Overhead**

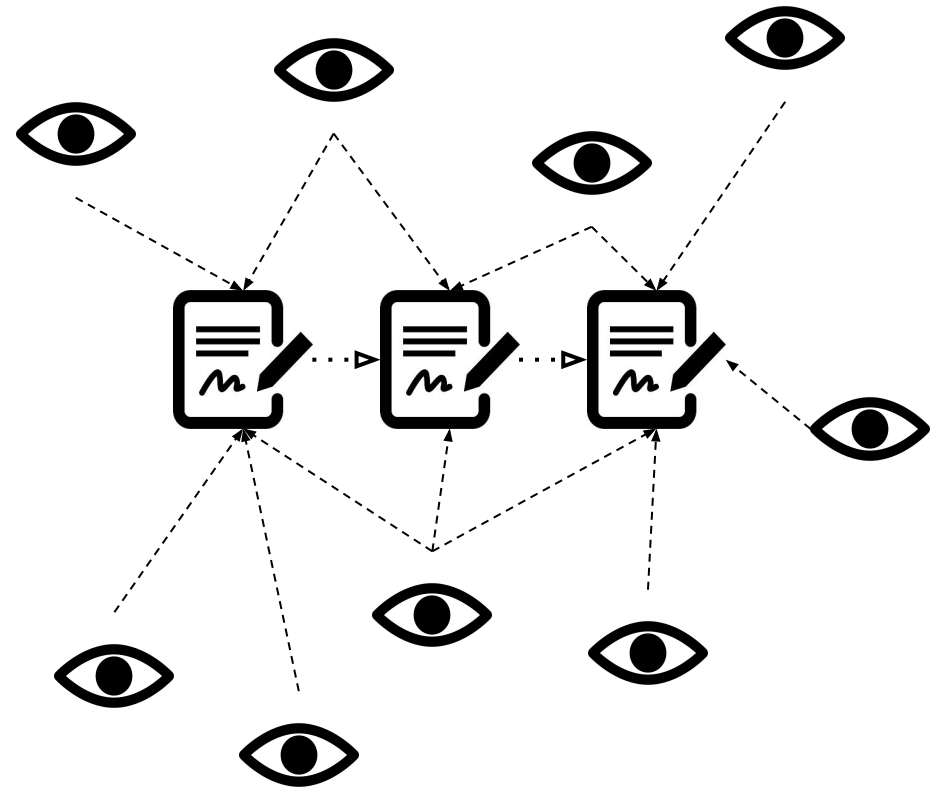
- **Privacy**





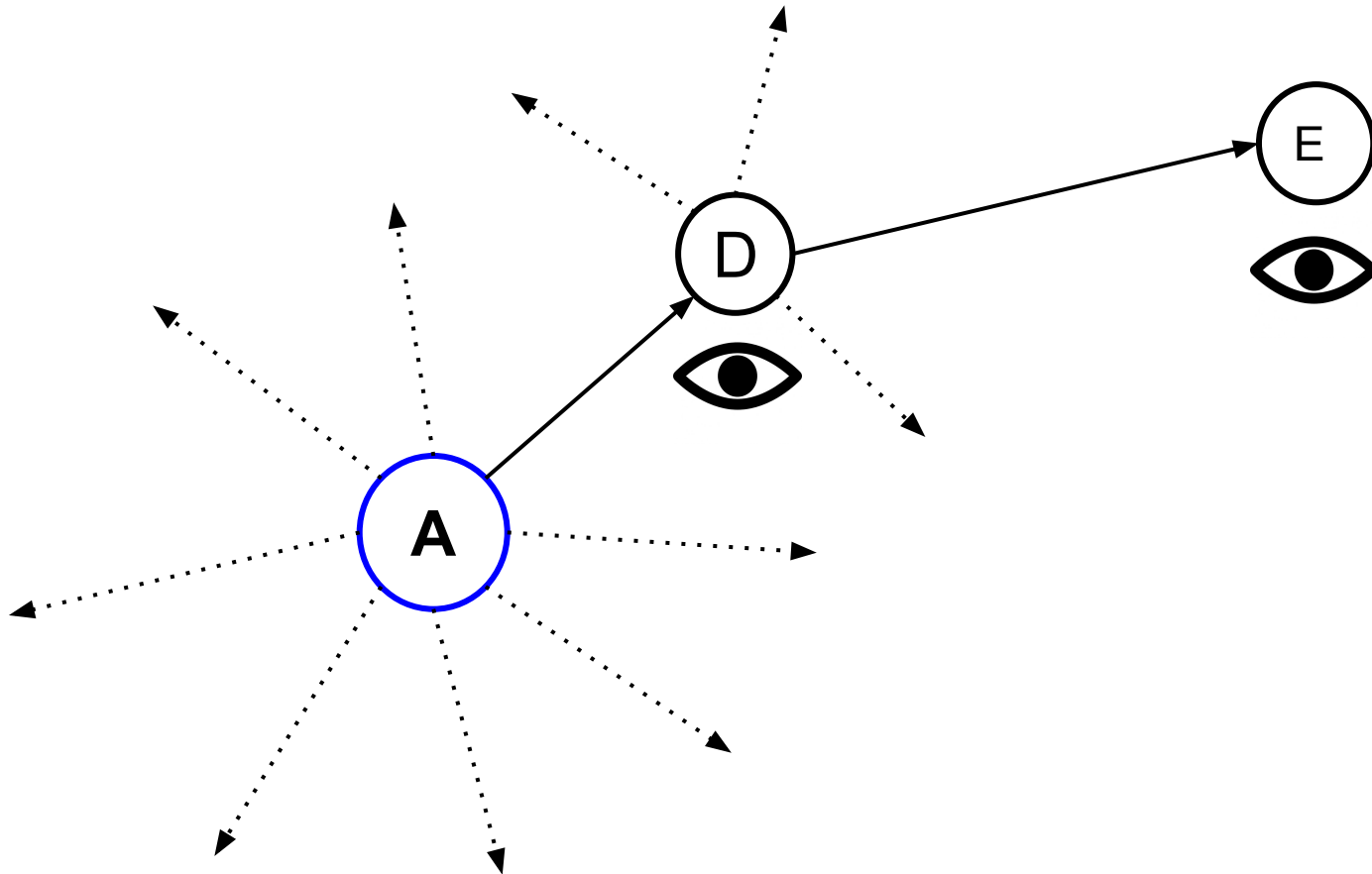
# Centralization

- Security
- Incentives
- Overhead
- Privacy

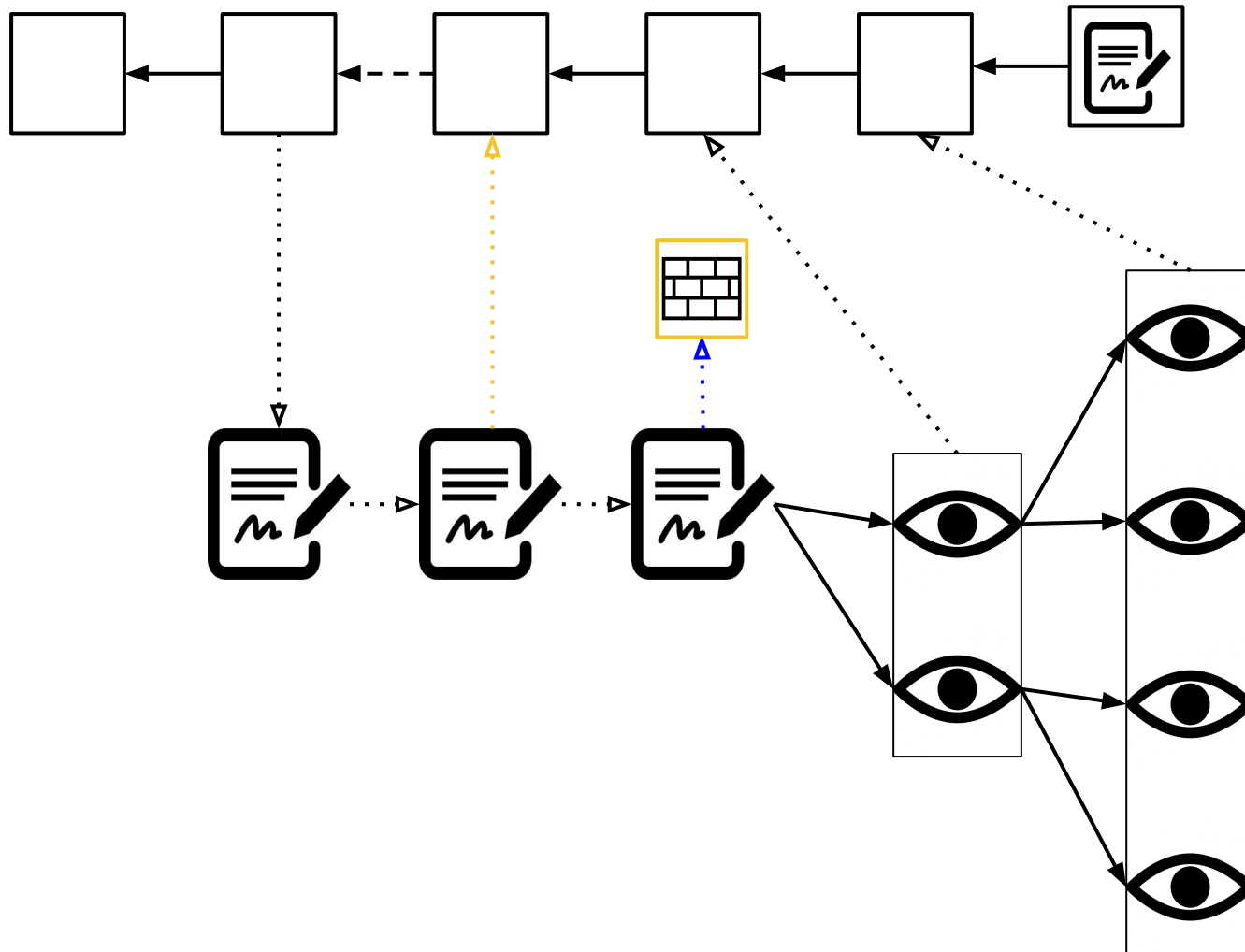


**enforce who gets the reward  
by protocol design!**

# Phase 1: Disclose & Cascade



## Phase 2: Watch & Commit



# The DCWC Protocol

- **Security**
- Incentives
- Overhead
- Privacy

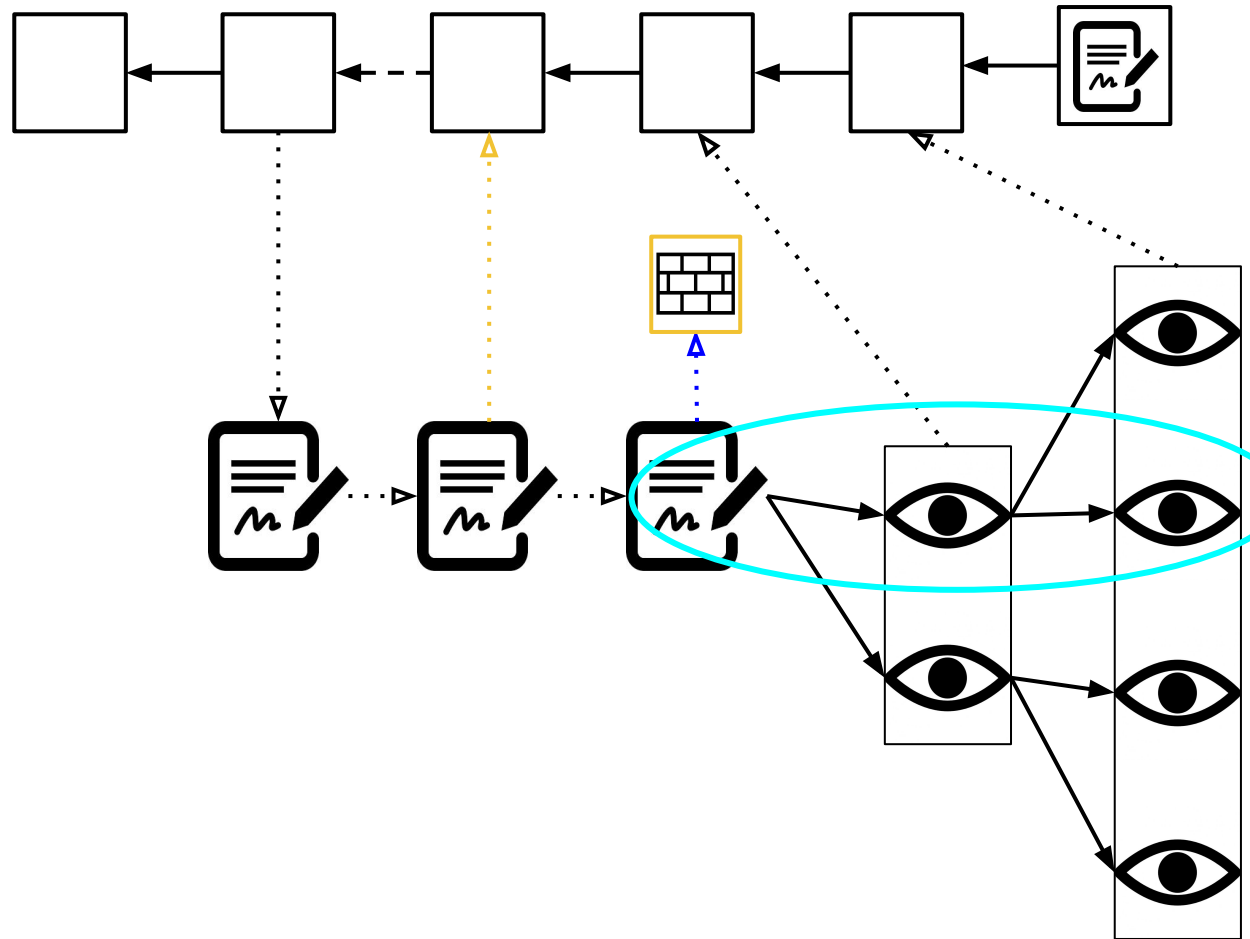
# The DCWC Protocol

- Security
- **Incentives**
- Overhead
- Privacy



# The DCWC Protocol

- Security
- Incentives
- Overhead
- Privacy



# The DCWC Protocol

- Security
- Incentives
- **Overhead**
- Privacy

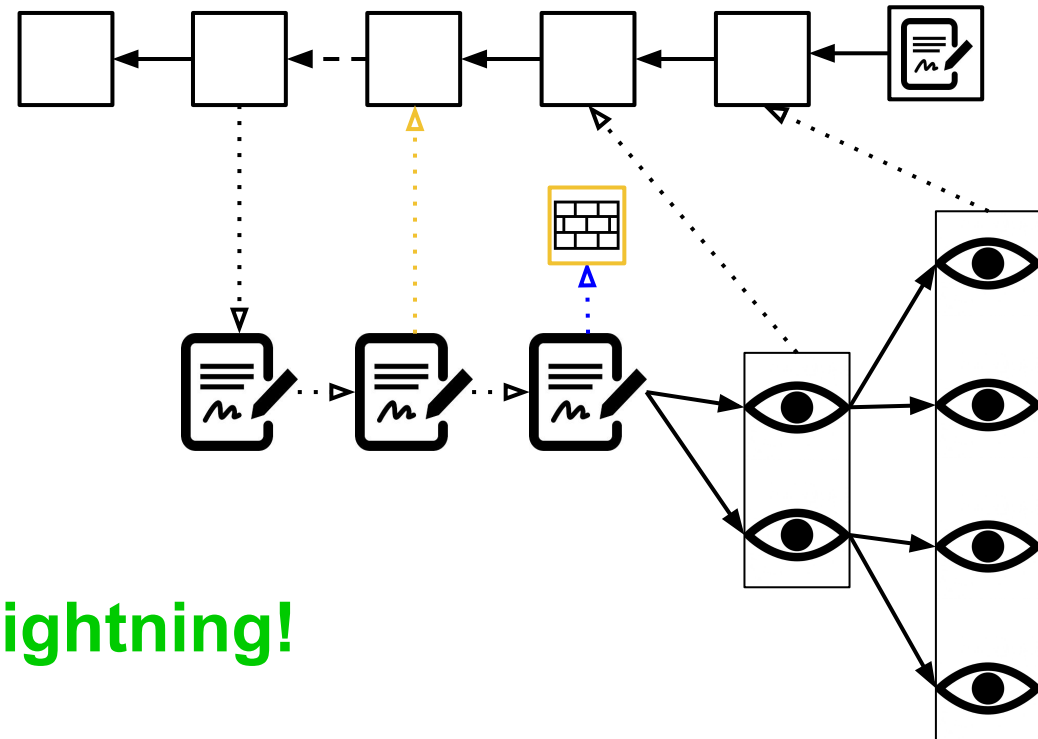
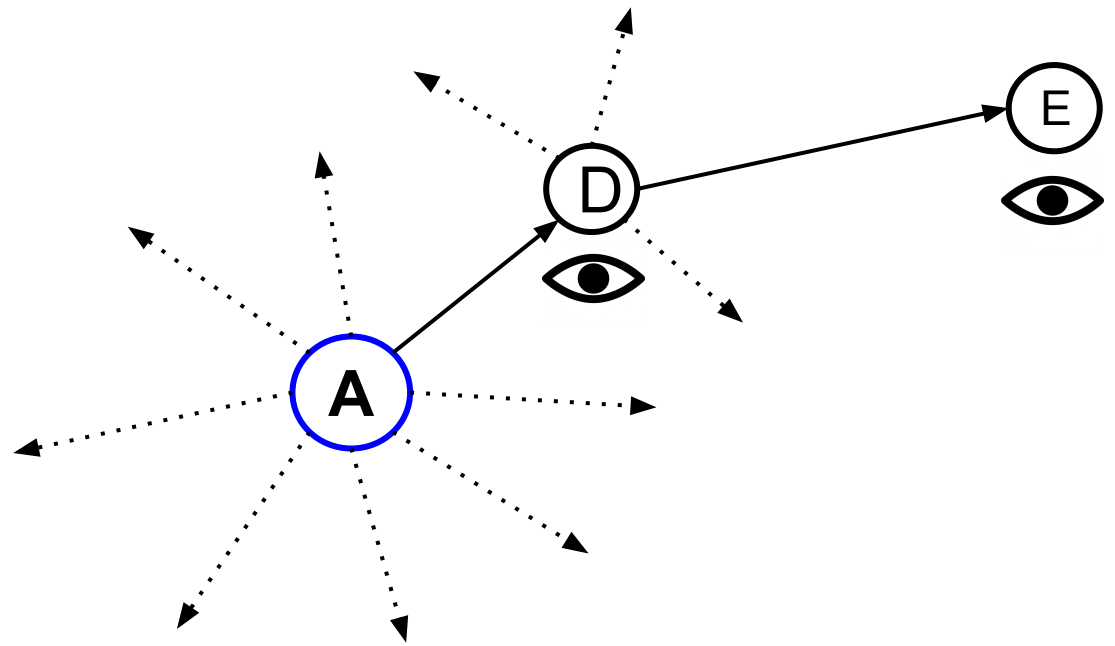
# The DCWC Protocol

- Security
- Incentives
- Overhead
- **Privacy**



# The DCWC Protocol

- Security
- Incentives
- Overhead
- Privacy



**No forks or changes in Lightning!**

## More...

- **Incentive for participation**
- More privacy
- Lower overhead



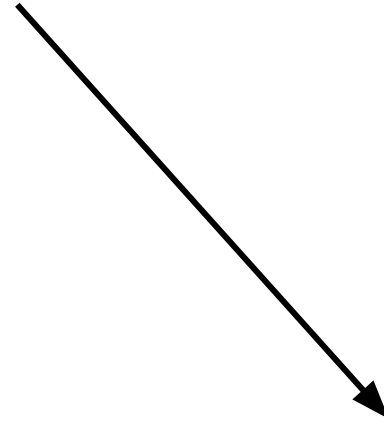
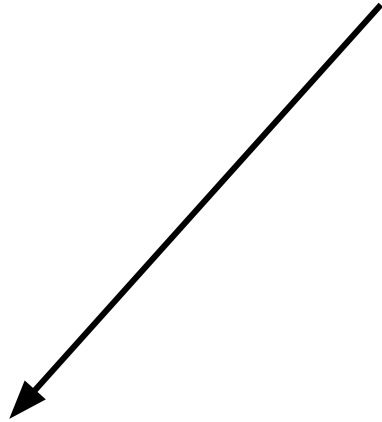
**What if there are no frauds?**

**What if there are no frauds?**



**Premiums!**

# Cheating Watchtowers?

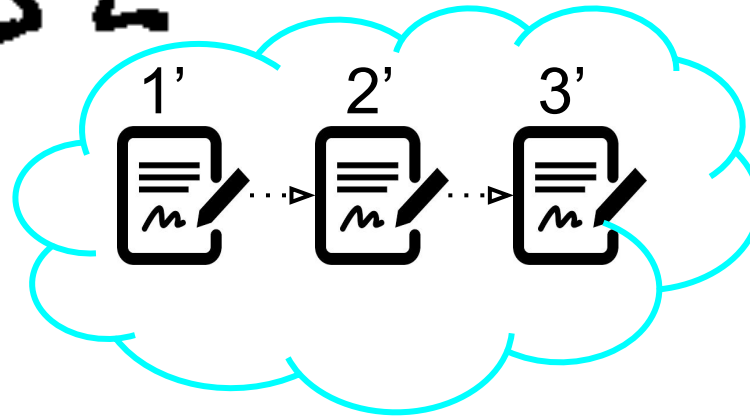
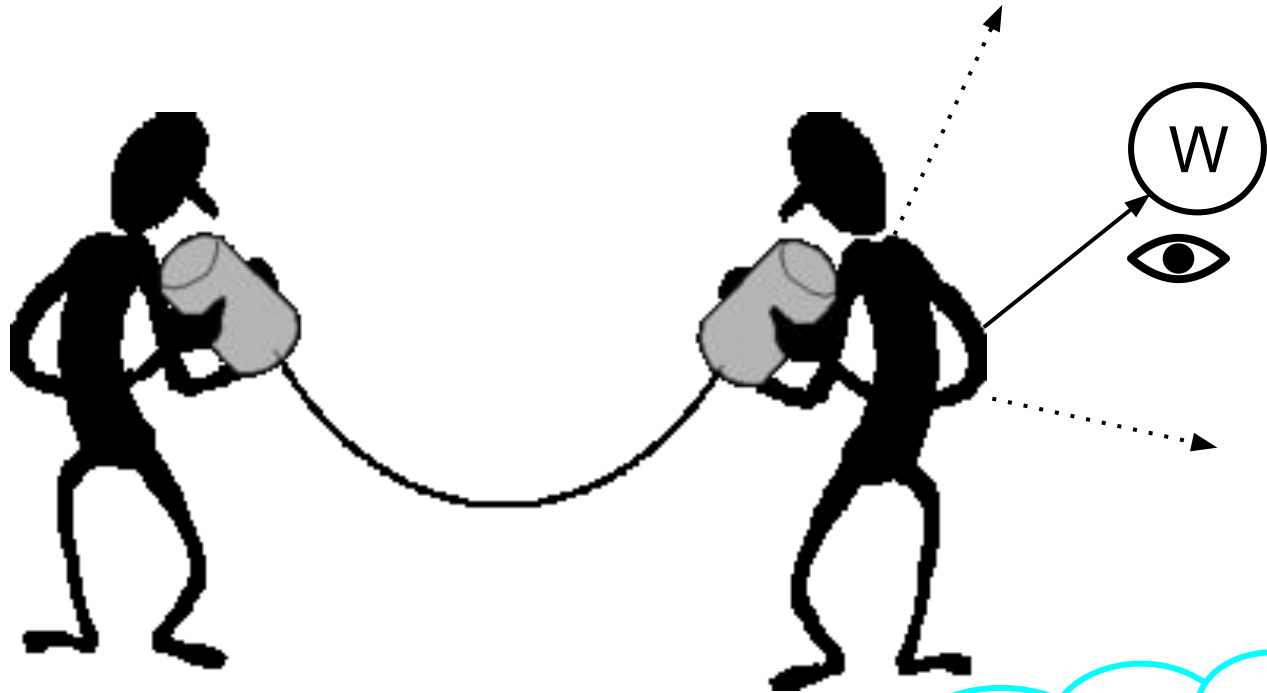
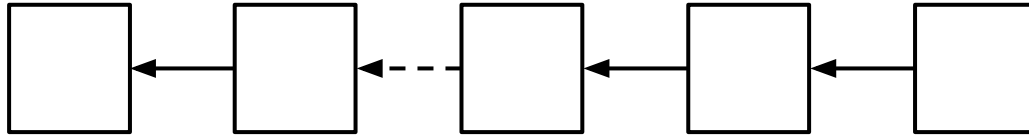




# What if there are no frauds?

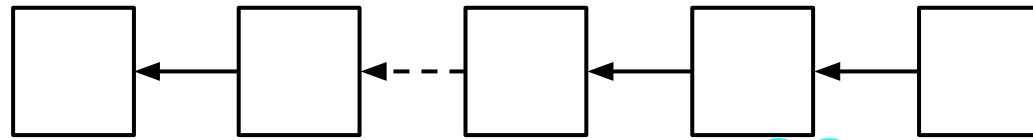


work in progress...

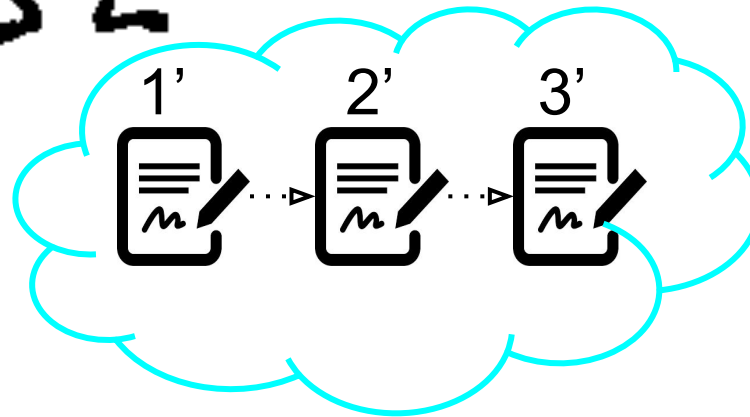
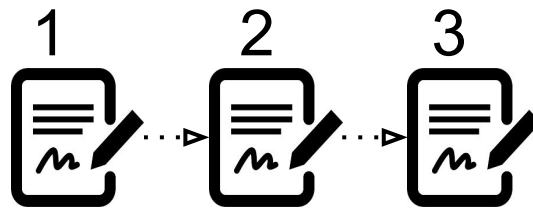
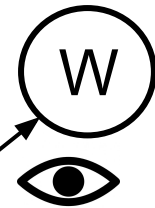
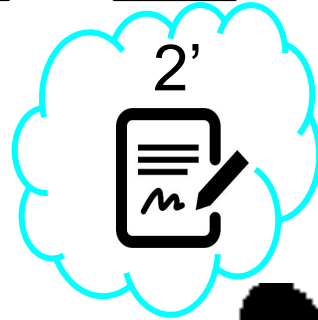


work in progress...





=



work in progress...

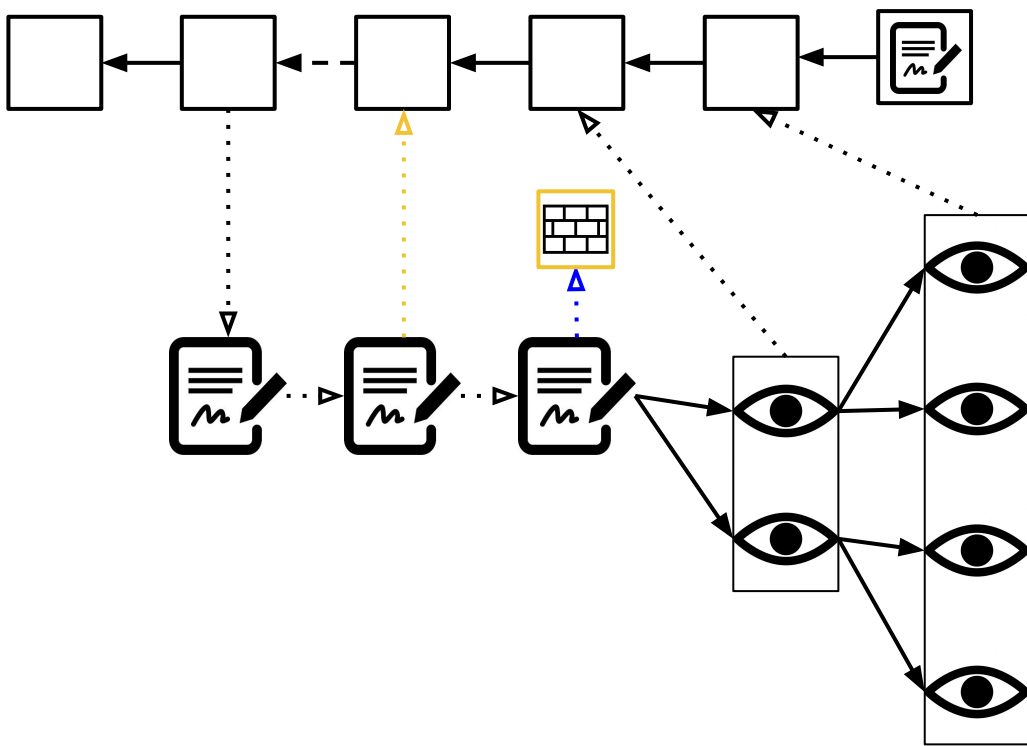
## More...

- Incentive for participation
- **More privacy**
- Lower overhead



## More...

- Incentive for participation
- More privacy
- **Lower overhead**



## Incentivizing Watchtowers

Work in progress...



*Thank you!*

**Questions?**

