Randomized View Reconciliation in Permissionless Distributed Systems

Ruomu Hou Irvan Jahja Loi Luu

Prateek Saxena Haifeng Yu

Presenter

NUS National University of Singapore

IEEE International Conference on Computer Communications

15-19 April 2018 // Honolulu, HI // USA

Our Contributions in a Nutshell

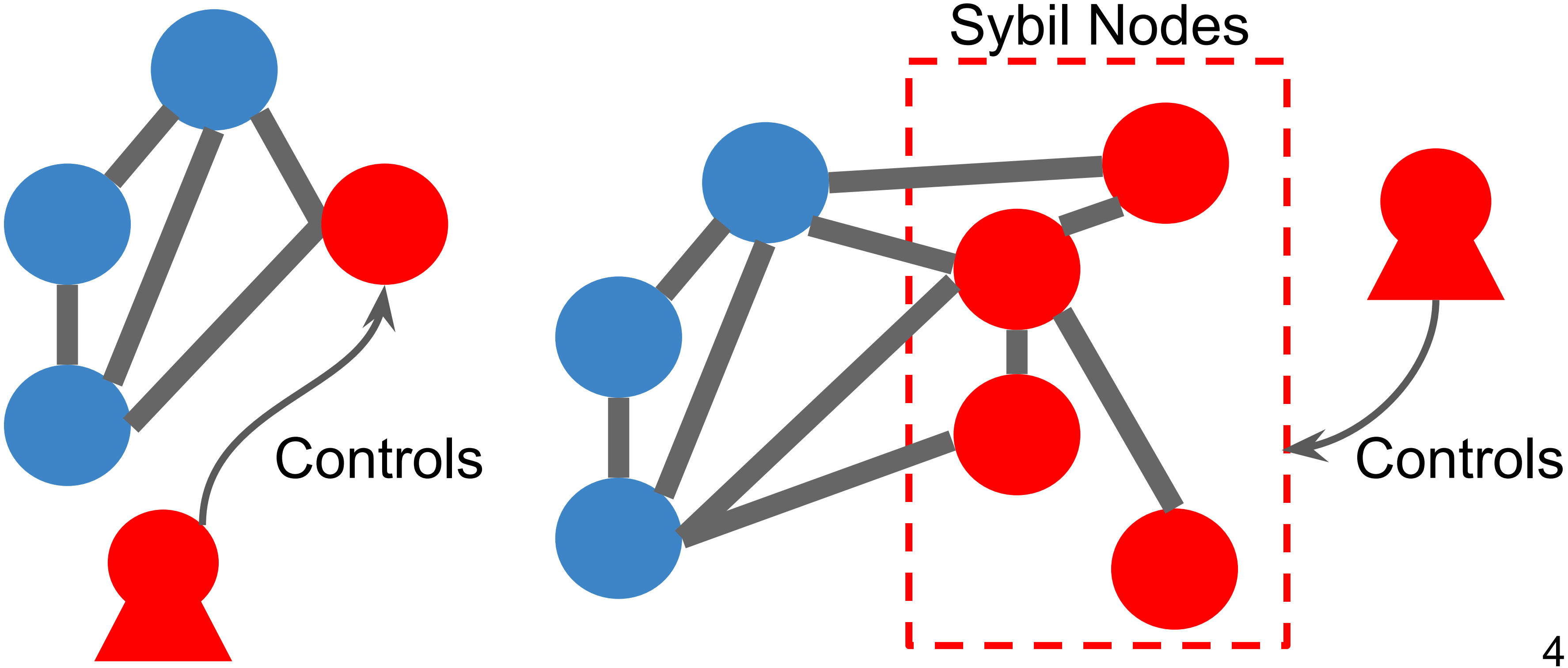
Protocol for view divergence

	Running time
Andrychowicz et al, CRYPTO 2015	θ(N)
Our contribution	**θ(ln N / ln ln N)**

Permissionless Distributed System

- N honest nodes
- Nodes join the system without permission
  - No central authority
  - Set of nodes and N are not known

Sybil Attack

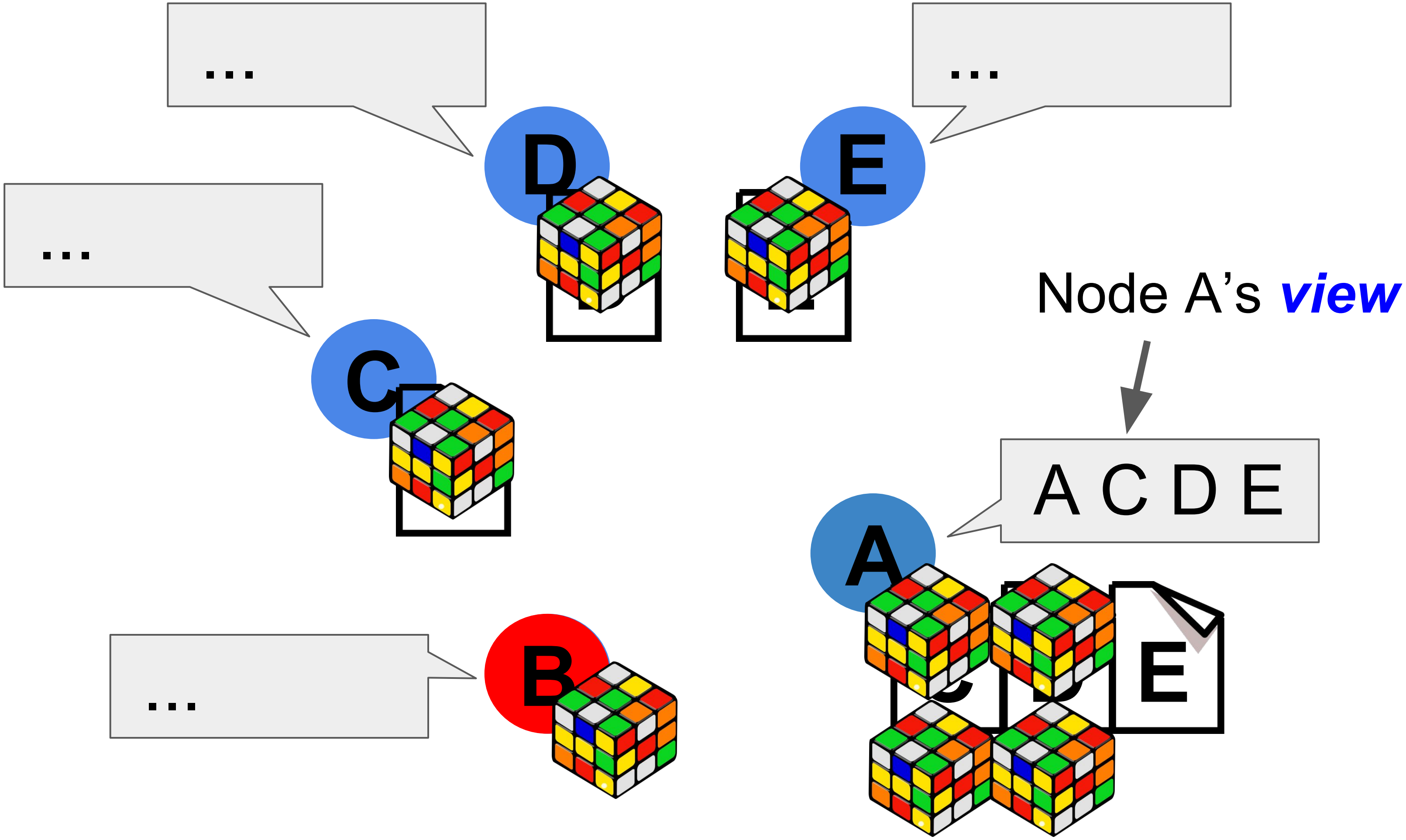


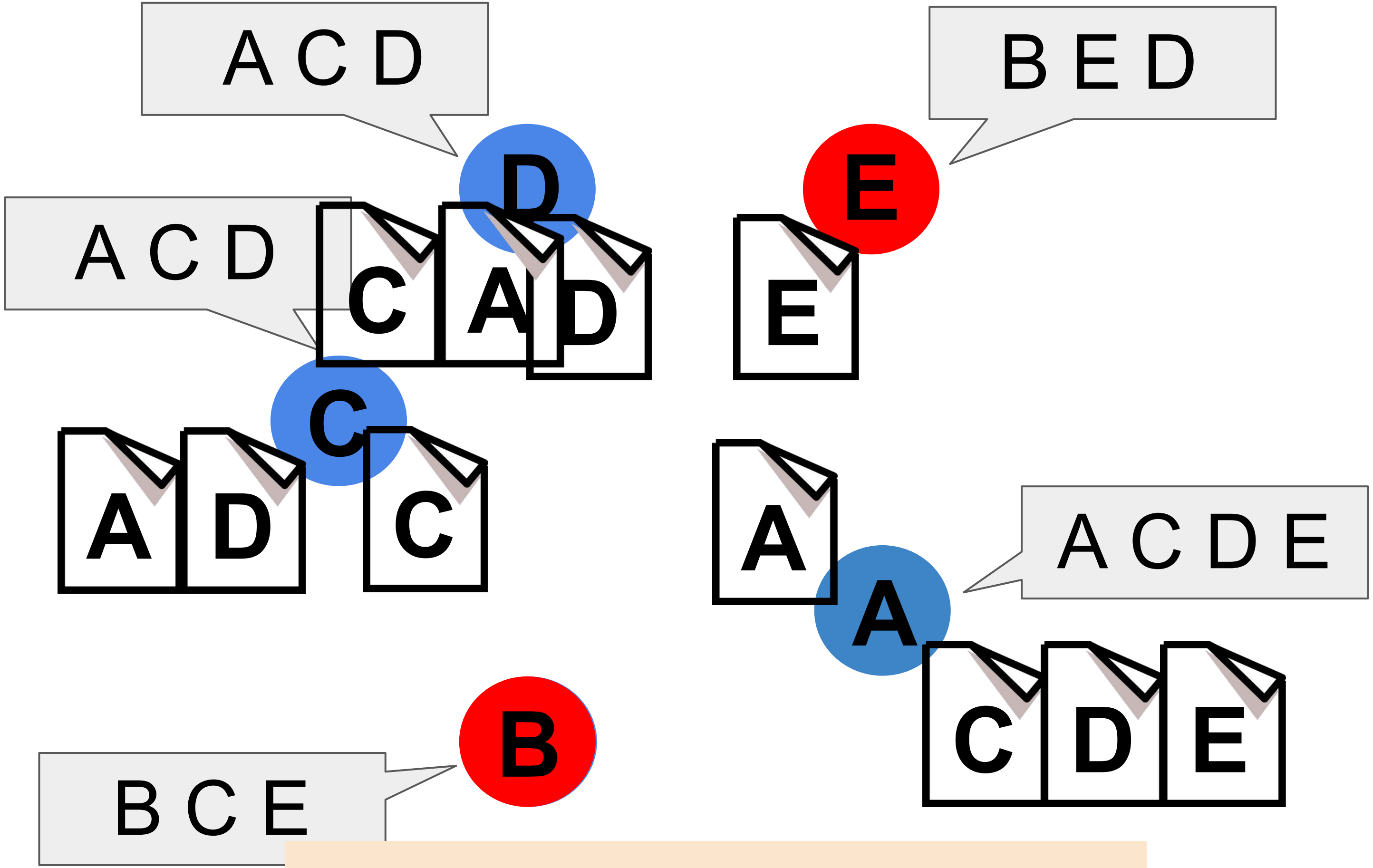
Computational Puzzle

- Non-trivial computation
  - E.g., reversing a hash function
    - Given y, find any x such that: hash(x) = y
- Challenge — Solution

challenge solution

- Adversary has limited computational power


...
...
...
...
Node A's *view*
A C D E
A
B
C
D
E



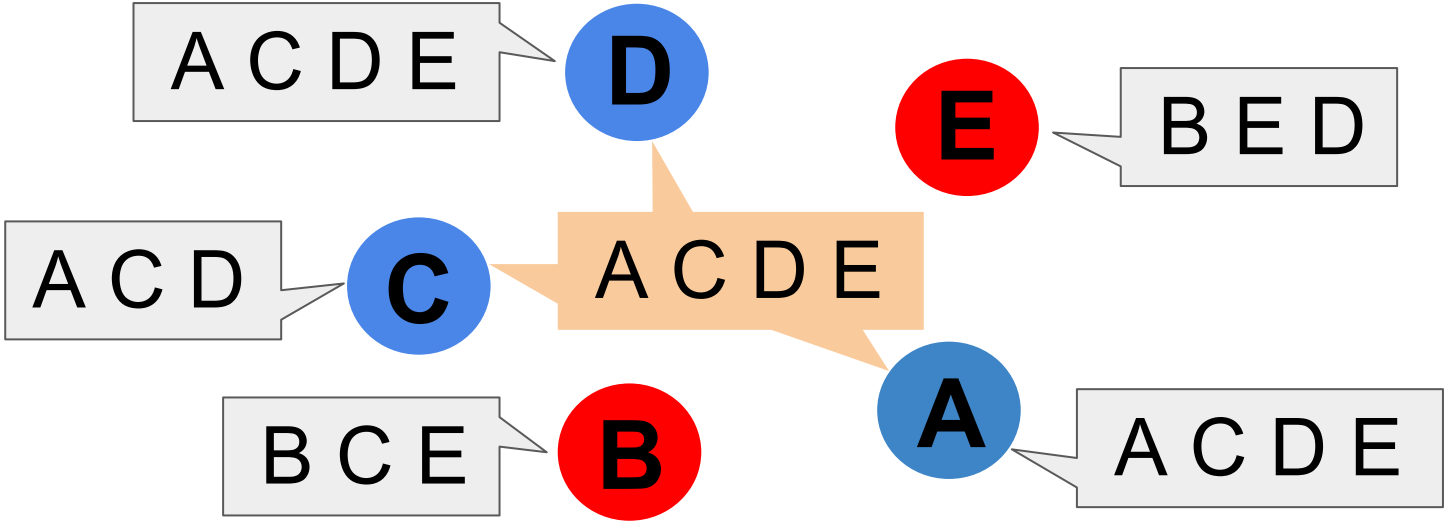
View divergence

View Divergence

- View divergence <u>breaks</u> the basis of many protocols
- Protocols in distributed algorithms traditionally are permissioned and requires same views
    - "Authenticated algorithms for byzantine agreement" (Dolev et. al, 1983)
    - "The byzantine general problem" (Lamport et. al, 1982)
    - "Protocols for secure computations" (Yao, 1982)
- Overlay protocols requires same view for bootstrapping
    - "Towards a scalable and robust DHT" (Awerbuch et al, 2009)
    - "Highly dynamic distributed computing with byzantine failures" (Guerraoui et. al, 2009)

View Reconciliation Protocol

- Andrychowicz and Dziembowski (CRYPTO 2015)



<u>Agree on a final, common view</u>

Our Contributions

- Recall N = number of honest nodes

	Running time	Total communication
Andrychowicz et al, CRYPTO 2015	$\theta(N)$	$\theta(N^2)$
Katz et al, 2014	$\theta(N)$	$\theta(N^2)$
Our contribution	$\boldsymbol{\theta(\ln N / \ln \ln N)}$	$\boldsymbol{\theta(N \ln^2 N / \ln \ln N)}$

Our Contributions

State-of-the-art	θ(N)	$\theta(N^2)$
Our contribution	**θ(ln N / ln ln N)**	**$\theta(N \ln^2 N / \ln \ln N)$**

- Alleviates bottleneck issue
  - Many security protocols have polylog complexity
    - “Towards a scalable and robust DHT” (Awerbuch et al, 2009)
    - “Highly dynamic distributed computing with byzantine failures” (Guerraoui et. al, 2009)
  - The overhead of previous θ(N) view reconciliation protocols would have been the bottleneck!

On View Divergence in BitCoin

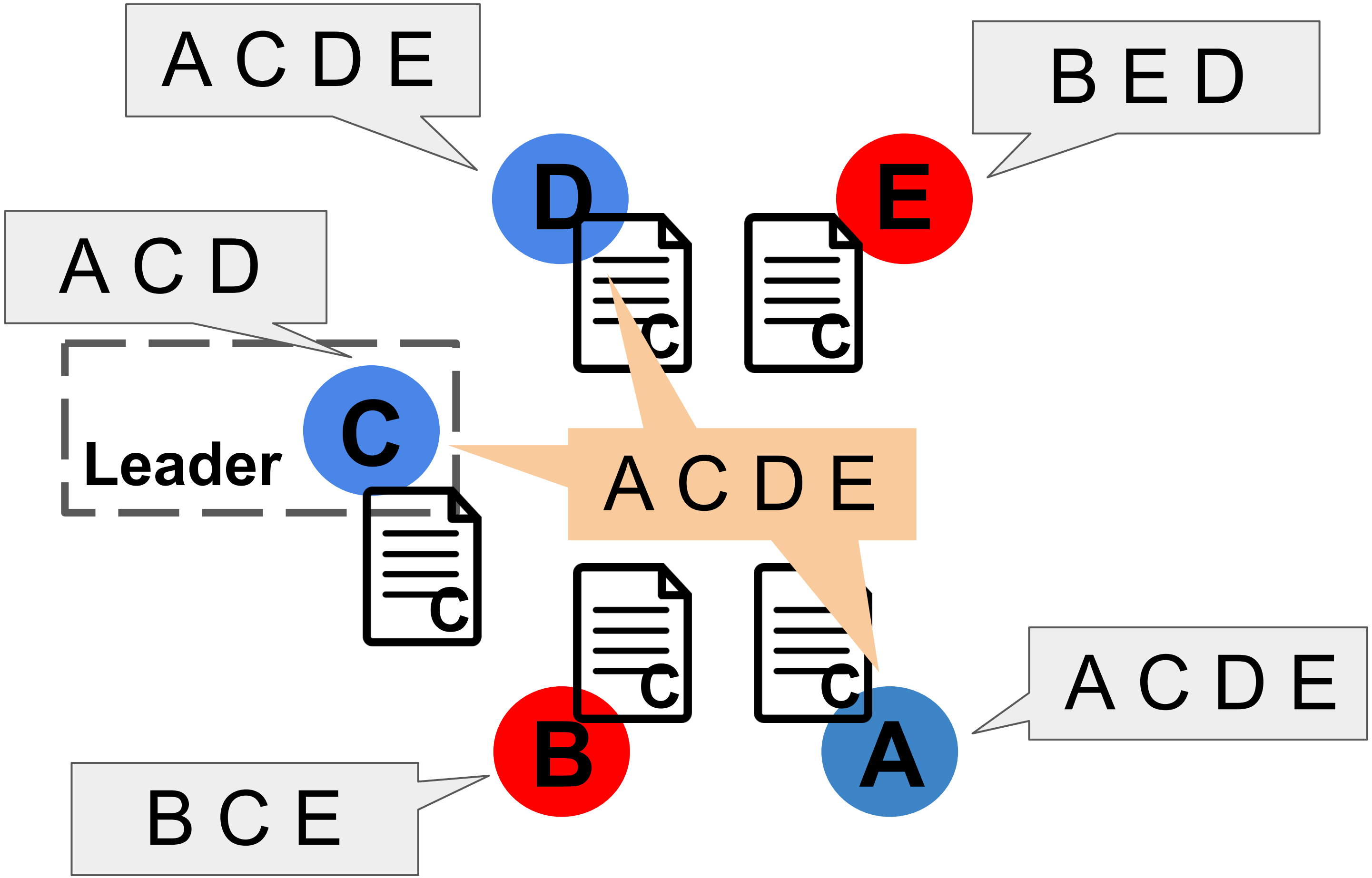
- BitCoin <u>does not</u> solve view divergence
- E.g., Eclipse attack
  - "Eclipse attacks on bitcoins peer-to-peer network" (Heilman et. al, 2015)
- Our protocol together with existing overlay protocols would prevent such an attack on BitCoin!

Our Approach

- Existing protocols are deterministic
- Randomization
  - Has δ error, similar to many security protocols
    - 256-bit AES: attacker has at least 2^{256} probability of guessing the key correctly
  - Our complexity scales with log (1\δ)

Our Approach

- RandomizedViewReconcile (RVR)
- RVR uses randomization to obtain better performance
  - Utilize computational puzzles to elect a leader probabilistically
    - Traditionally puzzles used only to challenge computational power limitation of adversary
  - Randomized sampling and gossipping


A C D E
B E D
A C D
D
E
Leader
C
A C D E
A C D E
B
A
B C E

Some Challenges

- How to handle malicious leader, missing leader, multiple leaders?
- How to spread leader's proposal efficiently?
- No common estimate on N: How to determine when the protocol should finish?
- All results were proven, details in the paper

Conclusions

RVR solves view divergence with probability 1 - δ.
RVR has a time complexity of $\Theta(\frac{\ln N}{\ln \ln N} \ln \frac{1}{\delta})$
and communication complexity of $\Theta(N \ln \frac{N}{\delta})$

- We presented the first view reconciliation protocol with polylog(N) time complexity
  - Previously known protocol has θ(N) tc
- Bridges many existing permissioned security protocols to work under the permissionless settings

Thank you!