上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

The construction of distributed multicast tree in bitcoin network

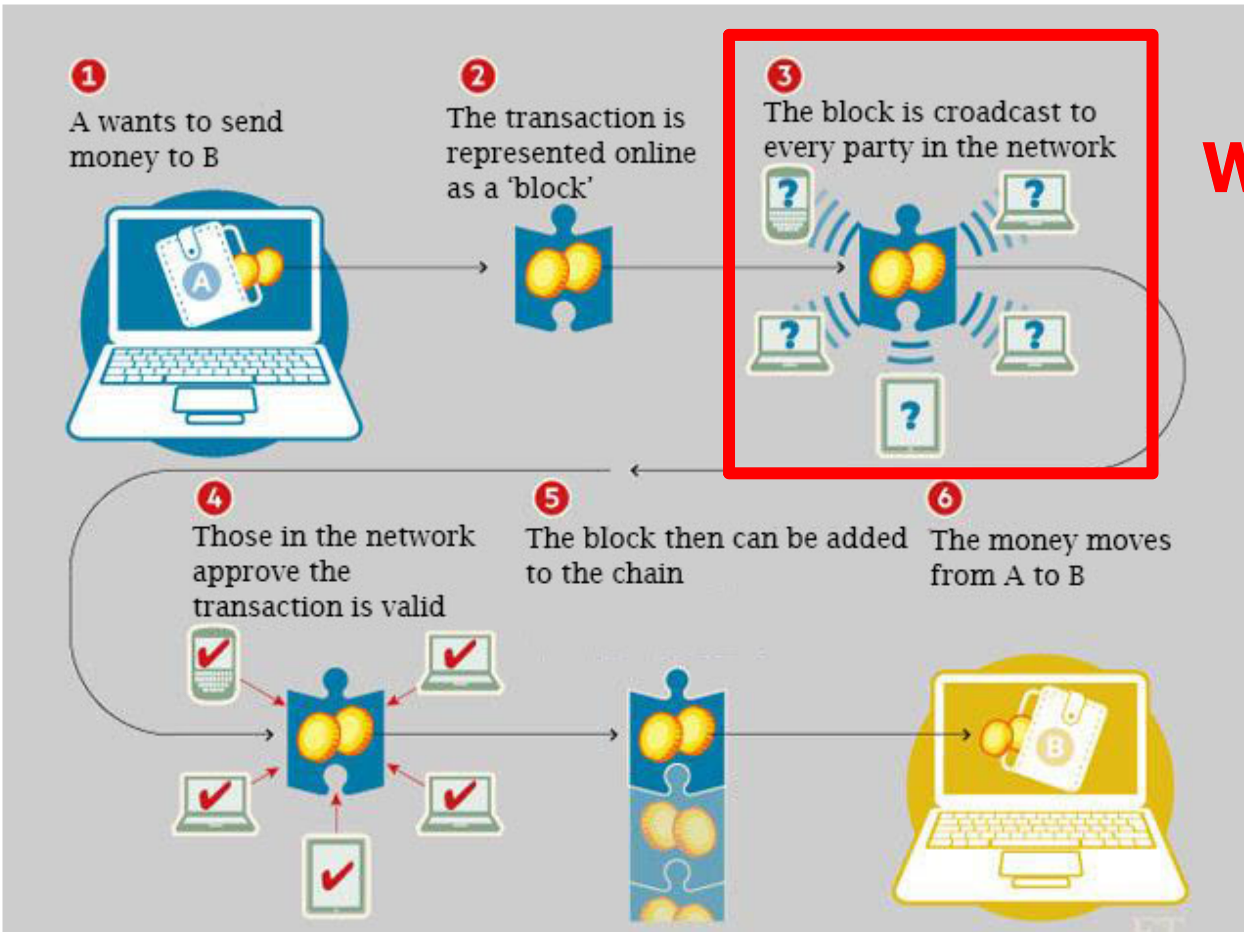
Yichi Zhang

515021910011

Contents

Introduction

How a blockchain works?



Weakness ?

Introduction

Any weakness?

→ **1 second**

→ **15 seconds**

→ **1 hour**

The broadcast and verification process is time & energy consuming which makes the transaction time consuming and costly.

Introduction

In this project, we

- propose a time-saving and low cost algorithm to construct a distributed multicast tree;
- analyze the performances of the algorithm, including tree length, time complexity and energy efficiency;
- compare our proposed algorithm with centralized algorithm.

Network Model

Assumptions:

1. The network in our model is a mobile one.
2. The number of nodes in the network is large enough
3. $\boldsymbol{W_i}$: The weight of node i. $(0 \leq W_i \leq 1)$
4. $\boldsymbol{W_{min}}$: The sum of every node's weight has to be larger than $\mathrm{W_{min}}$.

Termination condition:

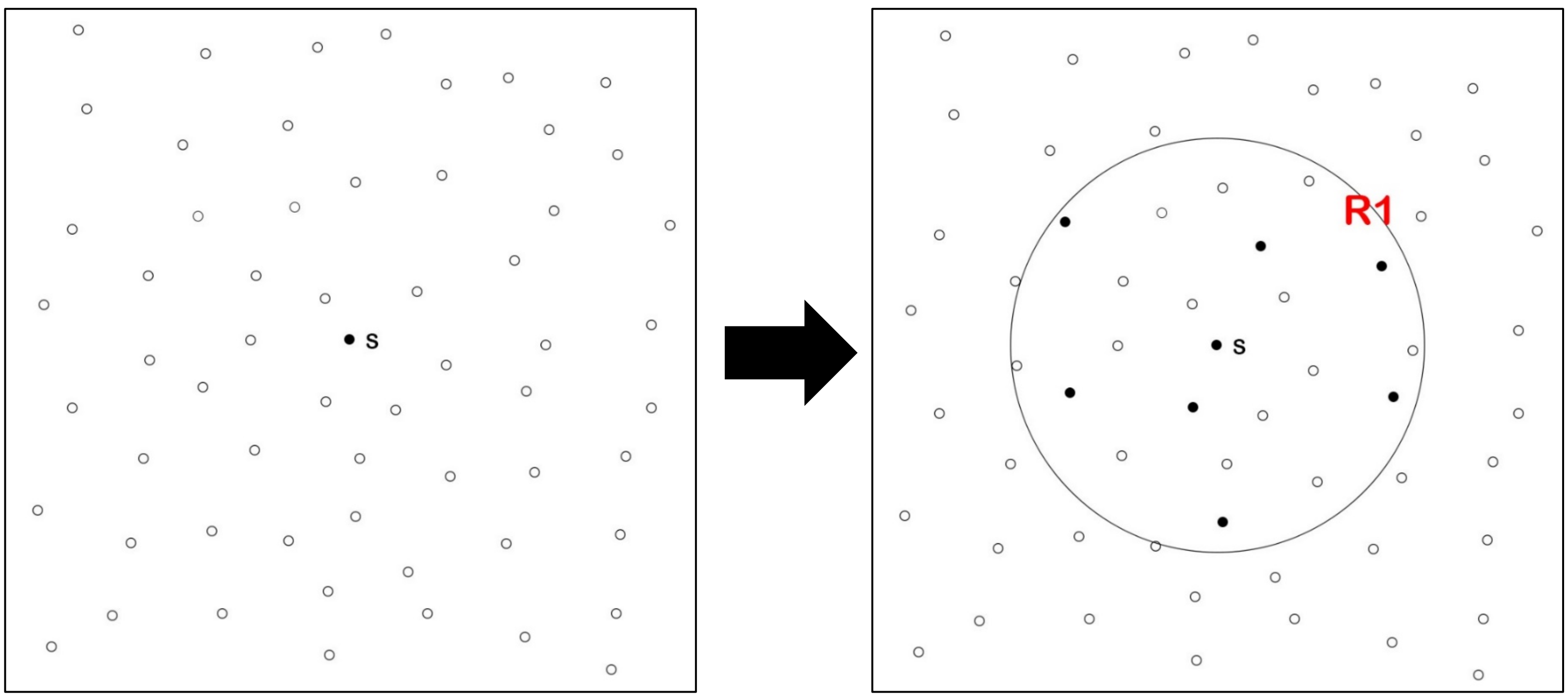
$$\sum_{i}^{n} W_i \geq W_{min}$$

Network Model

Algorithm

Phase1: Searching and identifying receivers

The source node(miner) broadcast its location to a area with radius R1, then every node with a $W_i \geq 0.9$ is chosen as a receiver. Before this phase, nodes don't know whether it's a receiver or not.

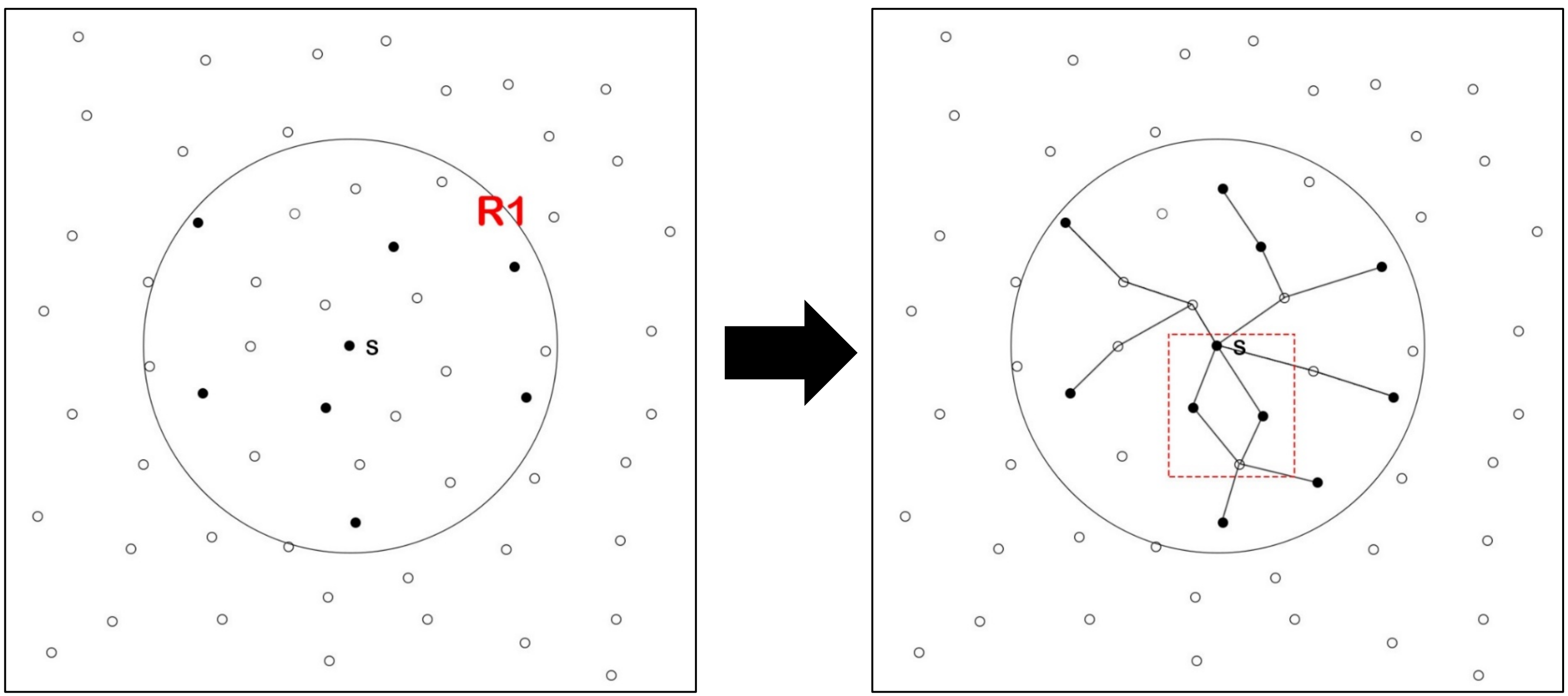


Network Model

Phase2: Connecting to neighbor nodes

Firstly, each receiver choose a node that has a shorter Euclidean distances to the source to connect to.

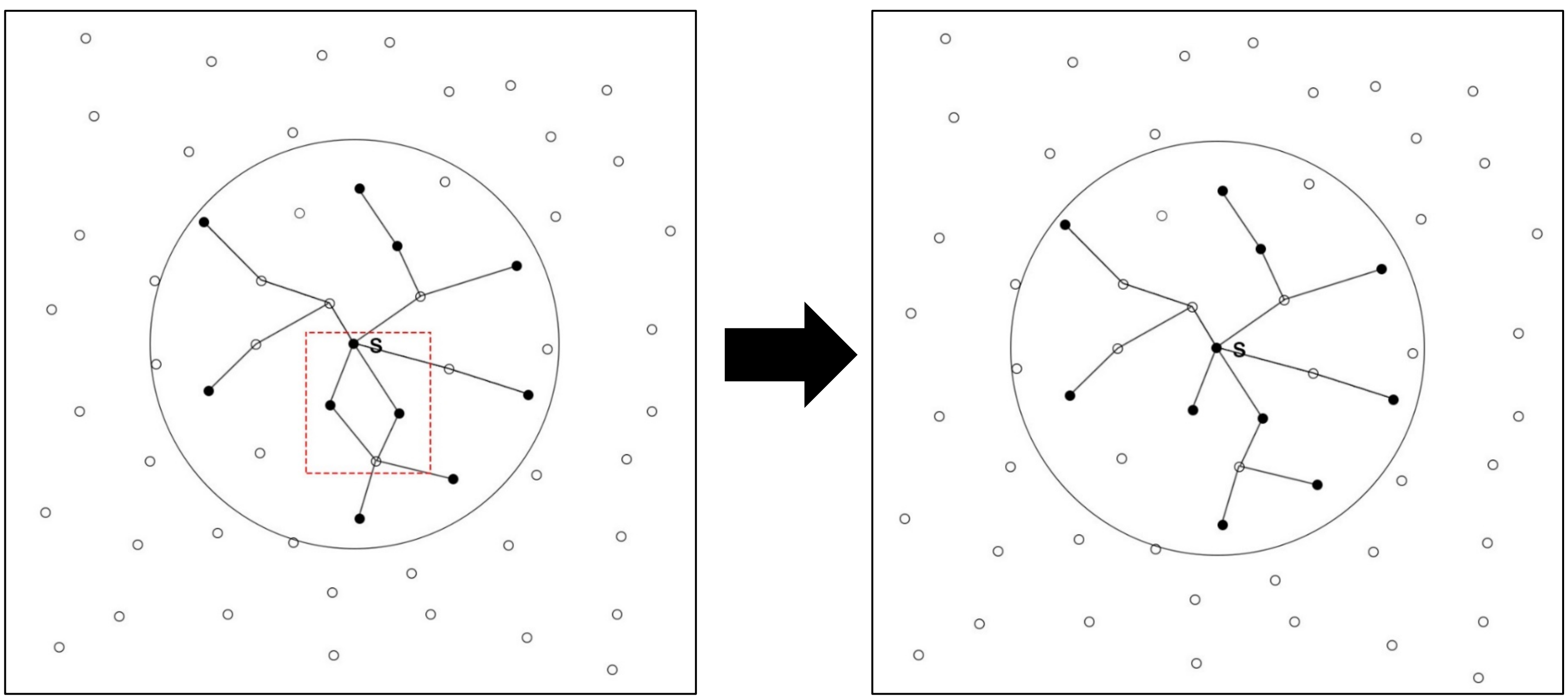
Then every chosen node begin to do the same thing the receivers have done, until there is no closer node then the node itself which means this node connects to the source directly.



Network Model

Phase3: Eliminating circles

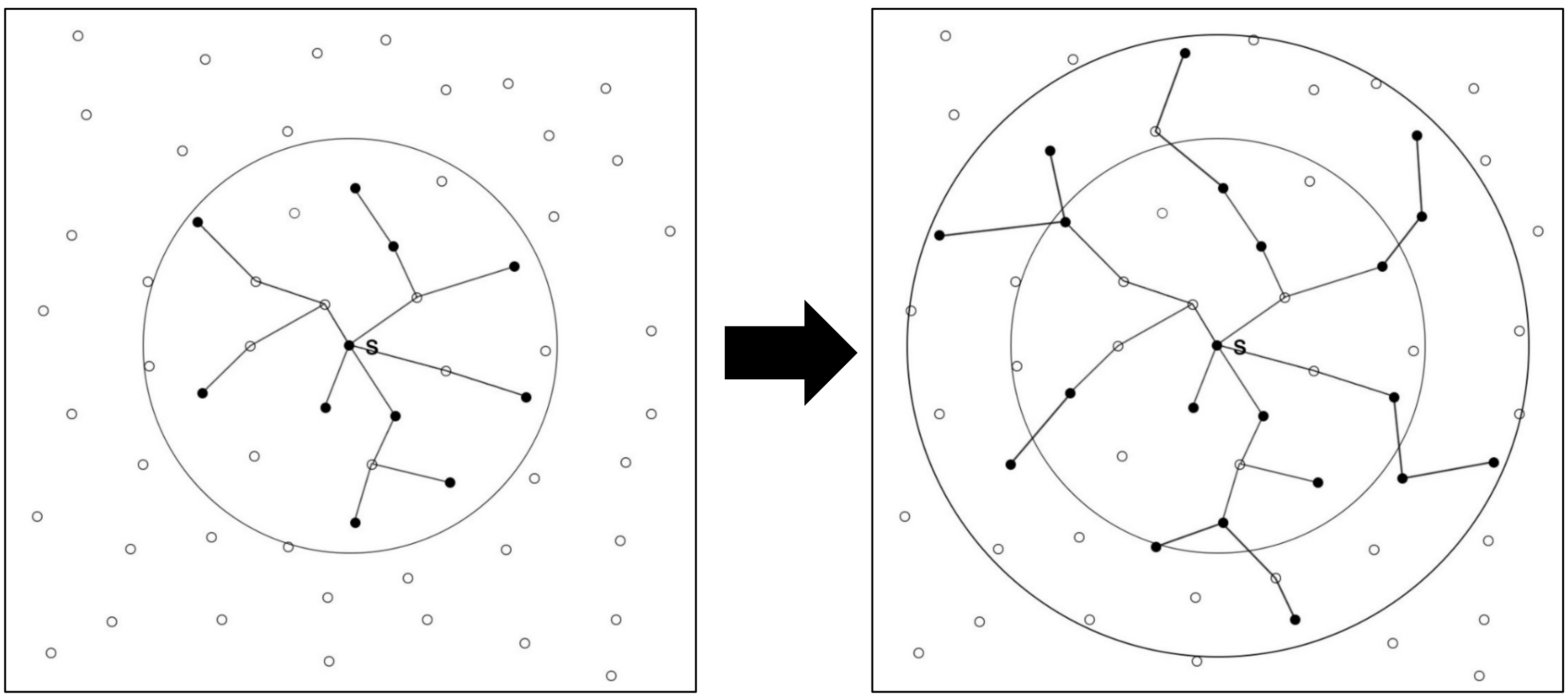
Each node chosen in the phase2 begins to check if it’s in a circle and if the redundant edges are located, delete message will be sent to the two nodes of each redundant edge and eliminate this edge.



Network Model

Phase4: Repeat phase1 to 3 in area with radius R_i

Because the number of receivers is unknow at the beginning, so if the total weight of all the nodes in radius $\boldsymbol{R_1}$ is no more than W_{max}, we have to find more nodes in a radius $\boldsymbol{R_2}$ until in $\boldsymbol{R_k}$ the total weight is larger than W_{max}. The receivers in $\boldsymbol{R_i}$ $(1 < i \leq k)$ only have to connect with the leaf node in $\boldsymbol{R_{i-1}}$.



Length Analyze

Assume that nodes are uniformly distributed in πR_1^2. Then the length of the temporary tree among m receivers is denoted as L_V. The expected tree length is

$$E(L_V) \leq c\sqrt{m},\ c = 2.311$$

Proof points:

- Uniformly distribution
- Circle area → polar coordinate system
- Expected total length

Length Analyze

- $f(R)$: length for a receiver $(R,0)$ to connect with S

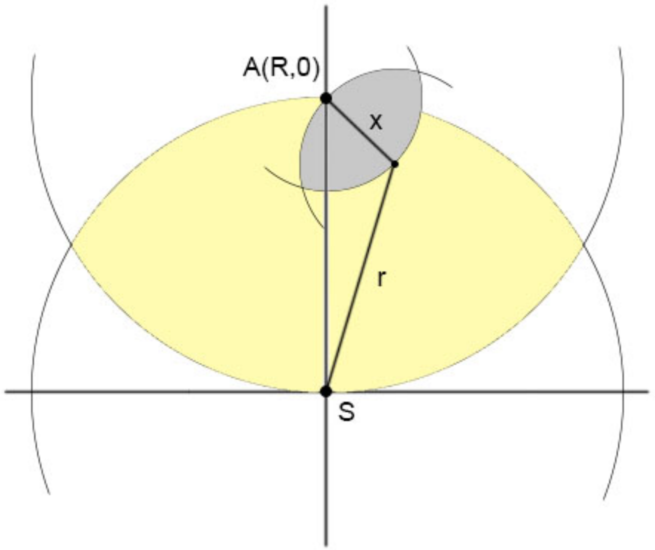
$$f(R)=\int_0^{\frac{\pi}{6}}d\theta\int_0^{2Rsin\theta}f(r,\theta)dr+\int_{\frac{\pi}{6}}^{\frac{5\pi}{6}}d\theta\int_0^{R}f(r,\theta)dr+\int_{\frac{5\pi}{6}}^{\pi}d\theta\int_0^{2Rsin\theta}f(r,\theta)dr$$

$$f(r,\theta)=x[1-\left(\frac{1}{3}-\frac{\sqrt{3}}{4\pi}\right)x^2]^{m-1}$$

$$x=\sqrt{R^2+r^2-2Rrsin\theta}$$

- $E(L_v)$: the expected length of the temporary tree

$$E(L_v)\le 2\pi\int_0^{R1}f(R)dR\le 2.311\sqrt{m}$$



Thank You