Stochastic Modelling of Blockchain Systems

Collaboration with Shaowen Liu (Deutsche Bundesbank), Paolo Tasca (UCL)

Claudio J. Tessone

URPP Social Networks

Universität Zürich[UZH]

Outlook

1. Introduction
   - Bitcoin network
   - Research Questions
   - Stylised facts
2. Modelling approach
3. Results
4. Conclusions

Introduction

The first slide should be generic about bitcoin. pervasiveness, impact, development.

Please insert some figure. See example.tex to see how to do it.

Networks in Bitcoin

In Bitcoin there are two networks at play: Economic transactions, P2P Network

The first slide should be generic about bitcoin. pervasiveness, impact, development.
Please insert some figure. See example.tex to see how to do it.

Networks in Bitcoin

In Bitcoin there are two networks at play: Economic transactions, P2P Network

This is a note page

- Please, write here some notes of the general idea of what this slide contains

Introduction

The first slide should be generic about bitcoin. pervasiveness, impact, development.
Please insert some figure. See example.tex to see how to do it.

Networks in Bitcoin

In Bitcoin there are two networks at play: Economic transactions, P2P Network

The first slide should be generic about bitcoin. pervasiveness, impact, development.
Please insert some figure. See example.tex to see how to do it.

Networks in Bitcoin

In Bitcoin there are two networks at play: Economic transactions, P2P Network

This is a note page

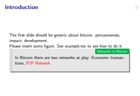
- Please, write here some notes of the general idea of what this slide contains

Introduction

The first slide should be generic about bitcoin. pervasiveness, impact, development.
Please insert some figure. See example.tex to see how to do it.

Networks in Bitcoin

In Bitcoin there are two networks at play: Economic transactions, P2P Network



This is a note page

- Please, write here some notes of the general idea of what this slide contains

Specific on bitcoin network

- Here we are interested in the bitcoin P2P network. DESCRIBE IT
- Consensus Protocol DESCRIBE IT
-

Please insert some figure. See example.tex to see how to do it. If necessary, split this slide into many

For this slide, the notes are very important.

Specific on bitcoin network

- Here we are interested in the bitcoin P2P network. DESCRIBE IT
- Consensus Protocol DESCRIBE IT
-

Please insert some figure. See example.tex to see how to do it. If necessary, split this slide into many

Stochastic modelling in Complex Systems

- Give some examples about systems that can be described in terms of a Gillespie algorithm (without mentioning it explicitely)
- Now the match should be clear

- Give some examples about systems that can be described in terms of a Gillespie algorithm (without mentioning it explicitely)
- Now the match should be clear

Notes on what you meant

Research Questions

- Generic research question: Why modelling?
- And this is the second on Why modelling
- specifically we address in this talk
- What happens if we alter the nature of the Bitcoin topology in terms with efficiency

- Generic research question: Why modelling?
- And this is the second on Why modelling
- specifically we address in this talk
- What happens if we alter the nature of the Bitcoin topology in terms with efficiency

Notes on what you meant

Stylised facts

- The P2P bitcoin network : size, average degree, cite references, mention some things that are known
- The distribution of hashing powers
- Some other thing you may fancy adding

Stylised facts

- The P2P bitcoin network : size, average degree, cite references, mention some things that are known
- The distribution of hashing powers
- Some other thing you may fancy adding

Notes on what you meant

Model description (i)

Model ingredient

- Network Topology.
  Network topology provides the connection relationship among nodes in consensus mechanism. Currently we apply Erdős-Rényi Model and Barabási-Albert model
- Agent/Node
  Each agent is a miner, which has its owe attributes (e.g.,state,hash power) and behavior (e.g.,gossip,mining).
- Block Tree
  For simplicity and efficiency, blockchain is not stored individually, instead, all nodes share one global block tree.

Model description (i)

Model ingredient

- Network Topology.
  Network topology provides the connection relationship among nodes in consensus mechanism. Currently we apply Erdős-Rényi Model and Barabási-Albert model
- Agent/Node
  Each agent is a miner, which has its owe attributes (e.g.,state,hash power) and behavior (e.g.,gossip,mining).
- Block Tree
  For simplicity and efficiency, blockchain is not stored individually, instead, all nodes share one global block tree.

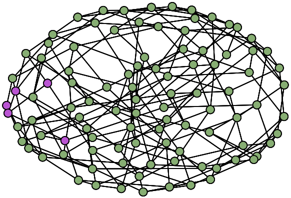
Notes

- In bitcoin network, there are nodes and miners. But currently in our model, we assume all nodes could mine. All nodes have hash power. But, we could easily apply pure node(no mining) by adjusting its hash power to zero.
- In general, the model is in block level. Has nothing to do with transactions. But, as gillespie algorithm is open for stacking new function, in theory, I think it is able be expended to transaction level.

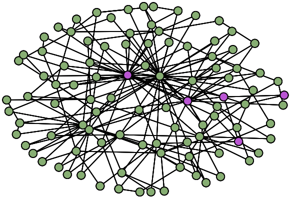
Model description (ii)

Network Topology

- To construct a common network, we apply 2 type of network topology: Erdős-Rényi Model and Barabási-Albert model.



Erdős-Rényi Model, Degree = 4



Barabási-Albert model, Degree = 2

Network Topology

- To construct a common network, we apply 2 type of network topology: Erdős-Rényi Model and Barabási-Albert model.


Erdős-Rényi Model, Degree = 4


Barabási-Albert model, Degree = 2

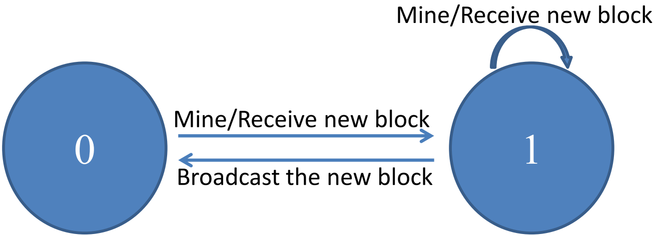
Notes

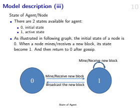
- The great advantage of this model is its flexibility. It could be easily tuned to any netwrok topology.
- As for bitcoin network, a new node is usually bootstrapped by connecting to nodes in the seedlist, which makes the topology similar to Barabási-Albert model.

Model description (iii)

State of Agent/Node

- There are 2 states available for agent:
  - 0, initial state
  - 1, active state
- As illustrated in following graph, the initial state of a node is 0. When a node mines/receives a new block, its state become 1. And then return to 0 after gossip.





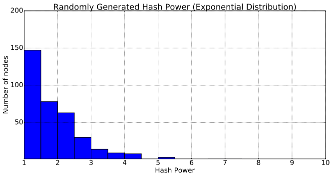
Notes

- The chart also shows a special case: if a node with active state mines/receives a new block, it will keeps its state.

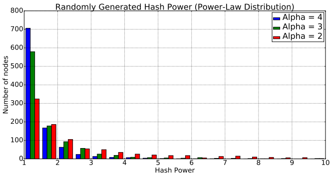
Model description (iii)

Hash Power of Agent

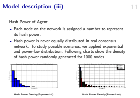
- Each node on the network is assigned a number to represent its hash power.
- Hash power is never equally distributed in real consensus network. To study possible scenarios, we applied exponential and power-law distribution. Following charts show the density of hash power randomly generated for 1000 nodes.



Hash Power Density(Exponential)



Hash Power Density(Power-Law)



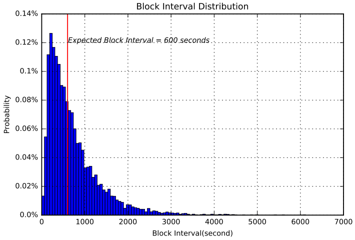
Notes

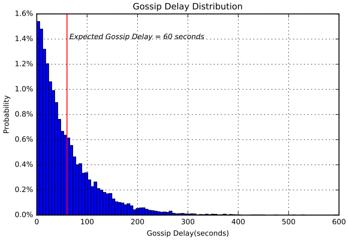
- Currently, the difficulty adjustment is not applied yet. So the 'hash power' of each miner is constant in each reptition.

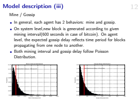
Model description (iii)

Mine / Gossip

- In general, each agent has 2 behaviors: mine and gossip.
- On system level,new block is generated according to given mining interval(600 seconds in case of bitcoin). On agent level, the expected gossip delay reflects time period for blocks propagating from one node to another.
- Both mining interval and gossip delay follow Poisson Distribution.







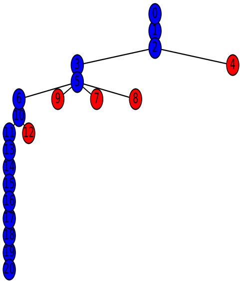
Notes

- the distribution chart for block interval is only for on-chain blocks.
- The peak of block interval distribution is larger than zero, because this is absolute interval time which includes also the gossip delay.
- I'm not sure whether net delay is clear for everyone, so I use gossip delay.
- The detail gossip process is, the node will exchange block information with its neighbor one by one, comparing the height of its new block H_{self} with its neighbors'(H_{nb}).
  - if $H_{self} > H_{nb}$, update neighbor's view of blockchain.
  - if $H_{self} < H_{nb}$, update its own view of blockchain.
  - if $H_{self} = H_{nb}$, continue gossiping with other neighbors.

Model description (iii)

Block Tree

- The node does not store block chain seperately, instead, all nodes in network build one global block tree.
- When the node mines a new block, the block will be stacked on a global bock tree. By storing block id on block tree, each node could have its local view of blockchain.



Block Tree. Red for Orphaned blocks.

Model description (iii)

Block Tree

- The node does not store block chain seperately, instead, all nodes in network build one global block tree.
- When the node mines a new block, the block will be stacked on a global bock tree. By storing block id on block tree, each node could have its local view of blockchain.

Block Tree. Red for Orphaned blocks.

Notes

Measures

Summarize for Tuning Parameters

- Network Topology
- Average Netowrk Degree
- Number of Nodes
- Hash Power Distribution
- Expected Value for Gossip Delay
- Expected Value for Block Interval

Average Netowrk Degree, just for Erdős-Rényi Network.

Measures

Performance Measurement

- Number of blocks
  number of total blocks, number of orphaned blocks,number of valid blocks
- Branches
  number of branches, the longest branches(with the most blocks)
- Propagation time
  Propagation time measure the time one block needs to reach all nodes. Specifically, we measure average propagation time and max propagation time.

Measures

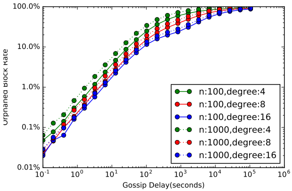
Performance Measurement

- Number of blocks
  number of total blocks, number of orphaned blocks,number of valid blocks
- Branches
  number of branches, the longest branches(with the most blocks)
- Propagation time
  Propagation time measure the time one block needs to reach all nodes. Specifically, we measure average propagation time and max propagation time.

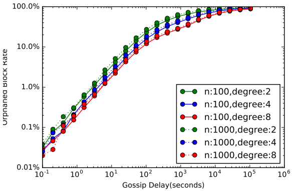
Notes on what you meant

Results (i): Number of Orphaned Blocks

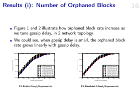
- Figure 1 and 2 illustrate how orphaned block rate increase as we tune gossip delay, in 2 network topology.
- We could see, when gossip delay is small, the orphaned block rate grows linearly with gossip delay.



F1.Erdős-Rényi/Exponential.



F2.Barabási-Albert/Exponential.

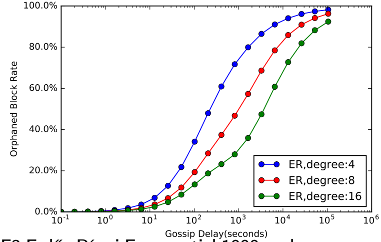


Notes

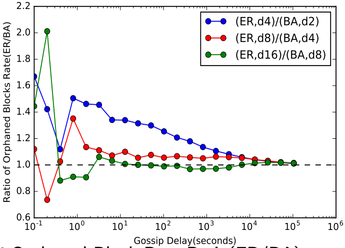
- All test is based on 100-day simulation, or around 14400 blocks. In both chart, the number of orphaned blocks move slowly to the ceiling value in the end.
- some simple observations, e.g., number of orphanded block increase as network size larger/degree smaller
- As the simulation day is fixed, the total block number is constant. Number of orphaned blocks and orphaned block rate behave the same.
- If the explanation for 'plateau effect' make sense, it could apply to the overall chart. Thus, the line in the chart should more or less mirror the cumulative distribution of block interval.

Results (i): Number of Orphaned Blocks

- In this chart, we put the results from 2 topology together. To give a clearer view, the chart shows only for network with 1000 nodes.We could clearly observe that, with the small degree, BA model generates less orphaned blocks than ER model. But BA's advantage disappears as degree increases.



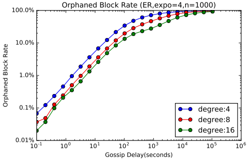
F3.Erdős-Rényi,Exponential,1000 nodes.

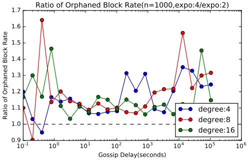


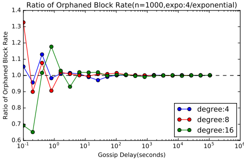
F4.Orphaned Block Rate Ratio(ER/BA).

Results (i): Orphaned Block Rate (Power law)

- First chart shows orphaned block rate for scenario hashrate follow powerlaw distribution. expo=4,1000 nodes
- Second chart take ratio of orphaned block rate,expo=4/expo=2. It shows orphaned block rate tends to be higher with higher expo.
- Last chart take ratio of orphaned block rate, expo=4/exponential.It shows Powerlaw(expo=4) and exponential perform the same.

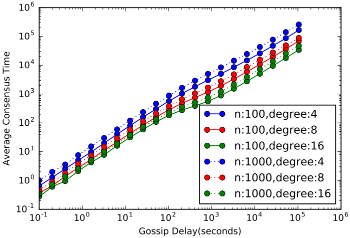




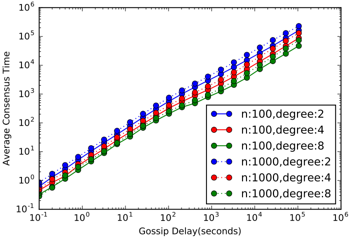


Results (ii): Consensus times

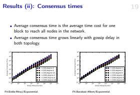
- Average consensus time is the average time cost for one block to reach all nodes in the network.
- Average consensus time grows linearly with gossip delay in both topology.



F4.Erdős-Rényi/Exponential.



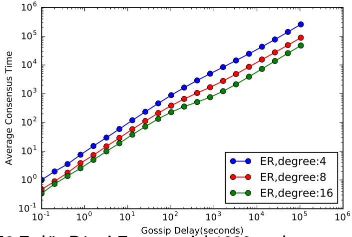
F5.Barabási-Albert/Exponential.



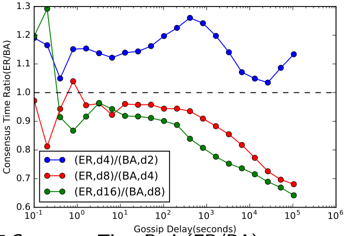
- the smaller the degree/the larger the network, the longer the avg consensus time.
- some details about propagation time
  - propagation time is only recorded for on-chain blocks.
  - In many cases(especilly when net-delay is large), the block is more likely to free ride its descendant to reach all nodes. For example,
    node one holds blockchain: b1-b2-b3-b5-b6-b7
    node two holds blockchain: b1-b2-b4
    When node one gossips with node two, in the surface, it's block b7 who is propagating. But in fact, b3,b5 and b6 all benefit from b7's propagation. This explains why in video 3, we never see a color occuping the whole map, but consensus is achieved under map.

Results (ii): Consensus Time

- F6 shows the consensus time for 1000 nodes ER network
- F7 calculates the ratio of consensus time(ER/BA) in three different degree level. There is no clear stylized pattern.



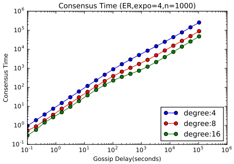
F6.Erdős-Rényi,Exponential,1000 nodes.

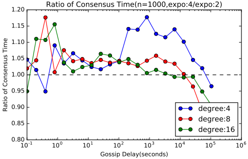


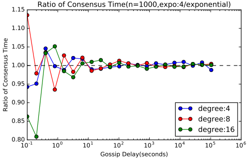
F7.Consensus Time Ratio(ER/BA).

Results (ii): Consensus Time(power law)

- First chart records the consensus time for scenario hashrate follow powerlaw distribution. expo=4,1000 nodes
- chart 2 takes ratio of orphaned block rate,expo=4/expo=2. For most of the time, expo=4 takes longer consensus time
- Last chart take ratio of orphaned block rate, expo=4/exponential.It shows generally Powerlaw(expo=4) and exponential perform the same.

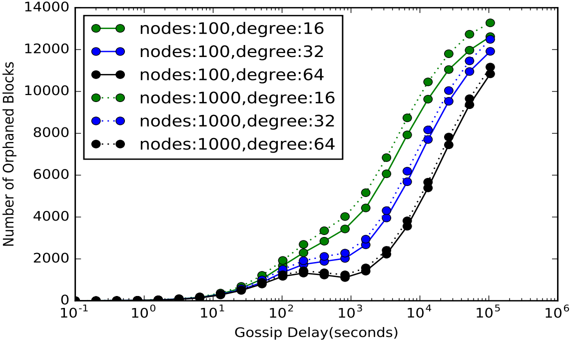






Results (iii): Plateau Effect

- Plateau effect is insteresting evidence, which shows that as gossip delay increase, the number of orphaned block cease to increase for a while.



F7.Erdős-Rényi/Exponential.

Results (iii): Plateau Effect

A possible explanation

- There is no robust math yet to prove this. But we think this could be related to block generating rate.
- Detail explain, see notes.

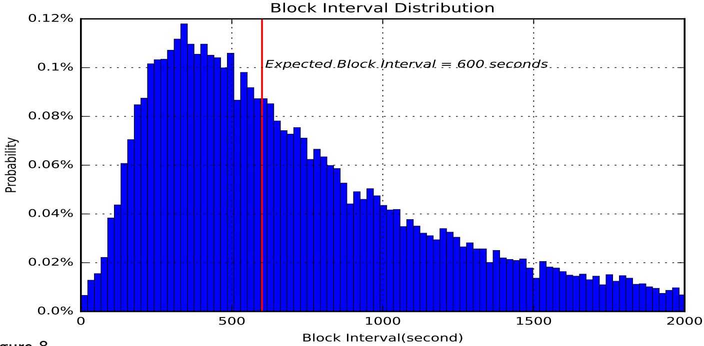


Figure 8

Results (iii): Plateau Effect

A possible explanation

- There is no robust math yet to prove this. But we think this could be related to block generating rate.
- Detail explain, see notes.

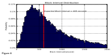


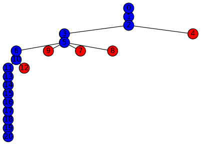
Figure 8

F8 is an amplified version of block interval distribution. We could understand how orphaned block generated by associating block generating time with consensus time. Not absolutely but it happens that, if consensus time is smaller than the generating time of next block, an orphaned block is avoided; if consensus time is larger than the generating time of next block, an orphaned block is possible to be generated. So, imagin if a given consensus time T cut the distribution in F8 into 2 parts, then its left side is the place where orphaned blocks born. Let's say the peak of F8 is 300 seconds. As consensus time changes from 0 to 300 seconds, the opportunity to generating orphaned block increase sharply. But as consensus time goes on increasing, the number of possible orphaned bloce still increases, but it slows down sharply. So, 300 seconds is the reverse point in this case. And the more effecient*(larger degree) a network is, the stronger it reacts to the reverse point.

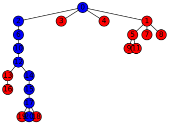
Results (iv): Network Evolution Demo

To understand the network evolution intuitively, here we illustrate the block tree and network evolution video in three different gossip delay scenarios.

gossip delay=1s(video)



gossip delay=100s(video)



gossip delay=1000s(video)

Conclusions

- By tuning different parameters in consensus mechanism, we get to know exactly how consensus performance is influence by those parameters.
- We first compare the consensus performance based on 2 popular network topology. It turns out that, in general, BA tends to produce less orphaned blocks than ER.
- Also, we examined the relationship between gossip delay and average consensus time.
- By study 'plateau effect', we could understand better how block intervel distribution and average consensus time could jointly influence the number of orphaned blocks.

Conclusions

- By tuning different parameters in consensus mechanism, we get to know exactly how consensus performance is influence by those parameters.
- We first compare the consensus performance based on 2 popular network topology. It turns out that, in general, BA tends to produce less orphaned blocks than ER.
- Also, we examined the relationship between gossip delay and average consensus time.
- By study 'plateau effect', we could understand better how block intervel distribution and average consensus time could jointly influence the number of orphaned blocks.

notes

Vision

- What can we do with this?
  Provide test data and basic knowledge for current blockchain improvement and future blockchain design.
  The model is expected to simulate more consensus mechanism(e.g., proof of stake.), such we are able to provide performance measurement across platform.
- Why is this important
- Highly efficient, strong base for arbitrary questions

URPP Social Networks

AND4.42, Andreasstrasse 15, 8050 Zurich, Switzerland

✉ claudio.tessone@business.uzh.ch

http://www.socialnetworks.uzh.ch

Universität Zürich[UZH]