

Security Survey of Bitcoin

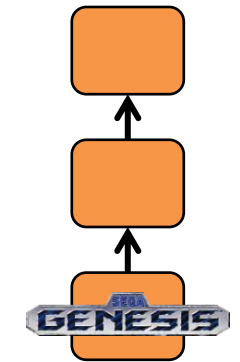
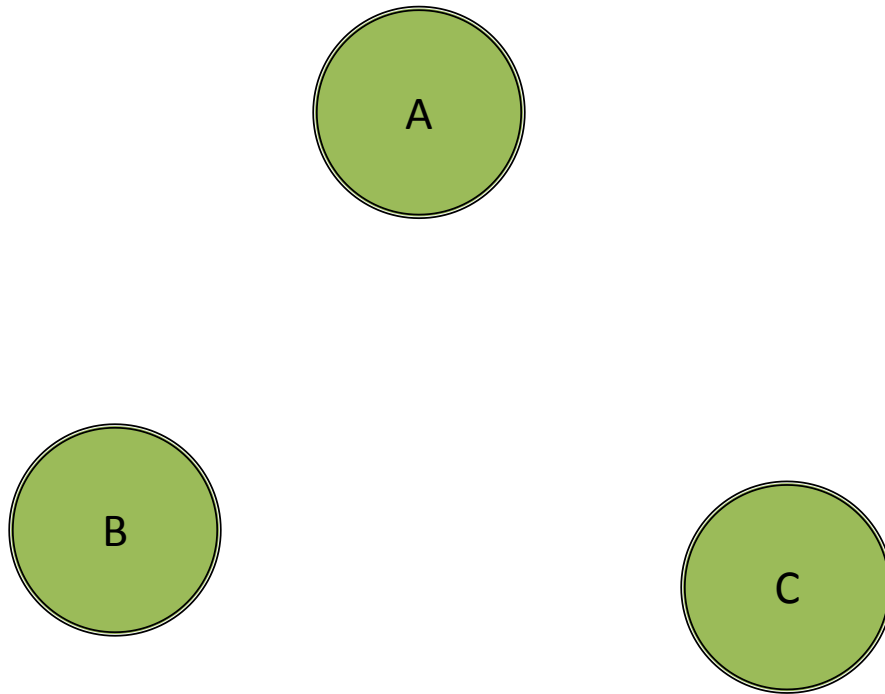
Ruven Chu and Andrew He

March 11, 2011

Bitcoin background

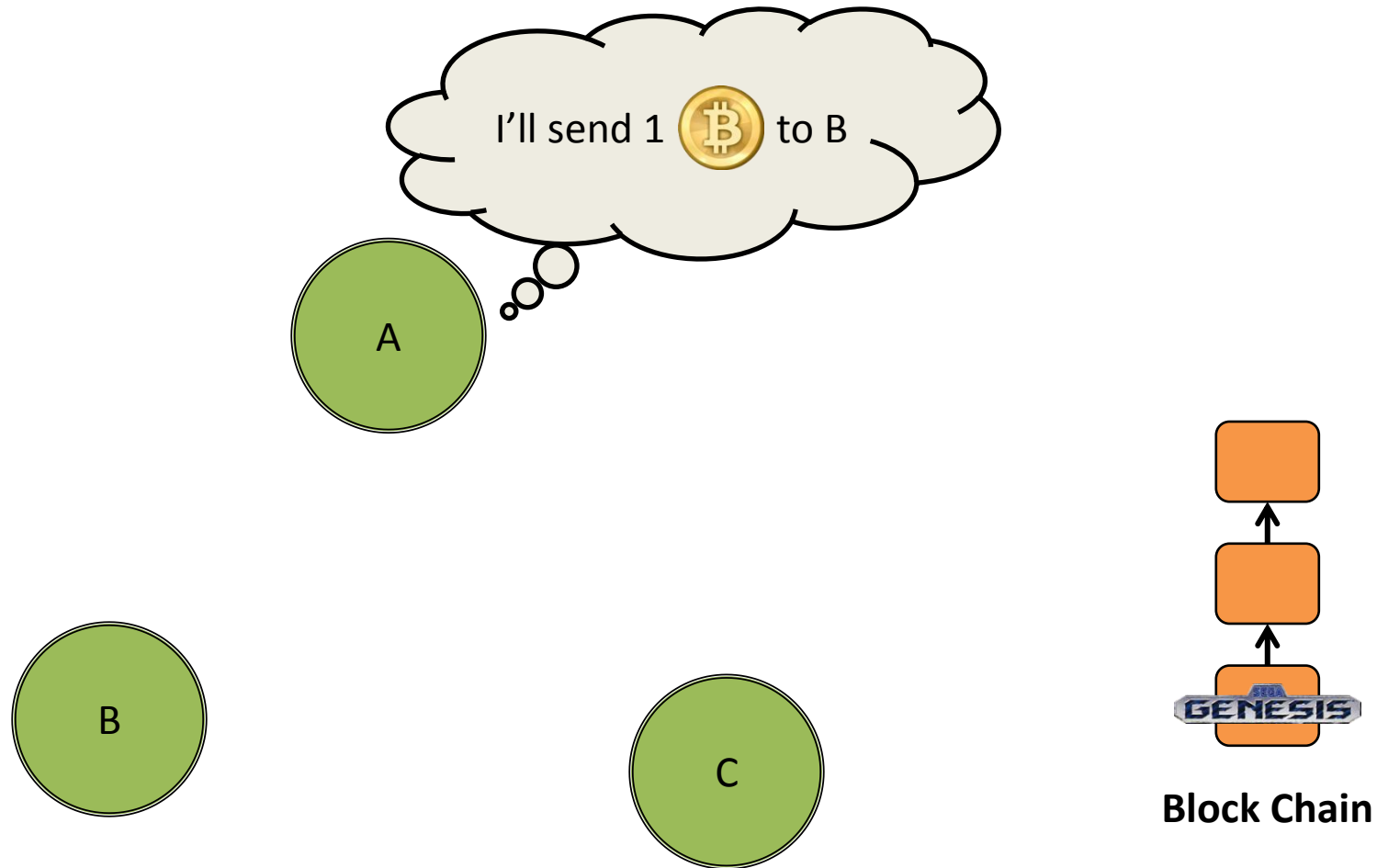
- Distributed digital currency, no centralized trust
- Coins are exchanged via broadcast messages (transactions)
- Transactions are gathered into blocks
- Nodes “approve” blocks by solving CPU-intensive problems
- Approved blocks are added to the block chain, which represents a complete timeline of transactions

A simplified example

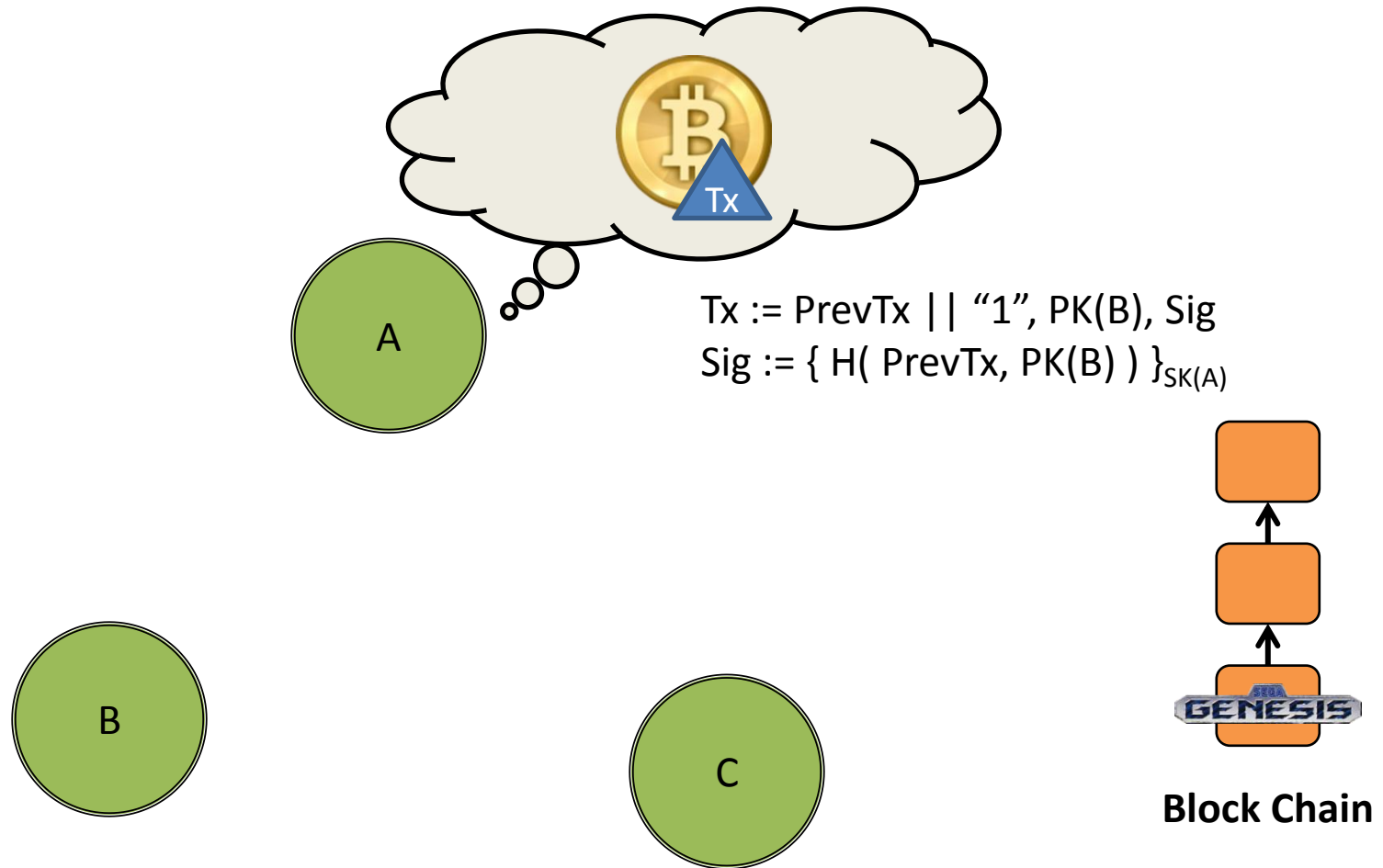


Block Chain

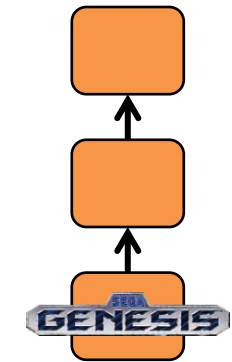
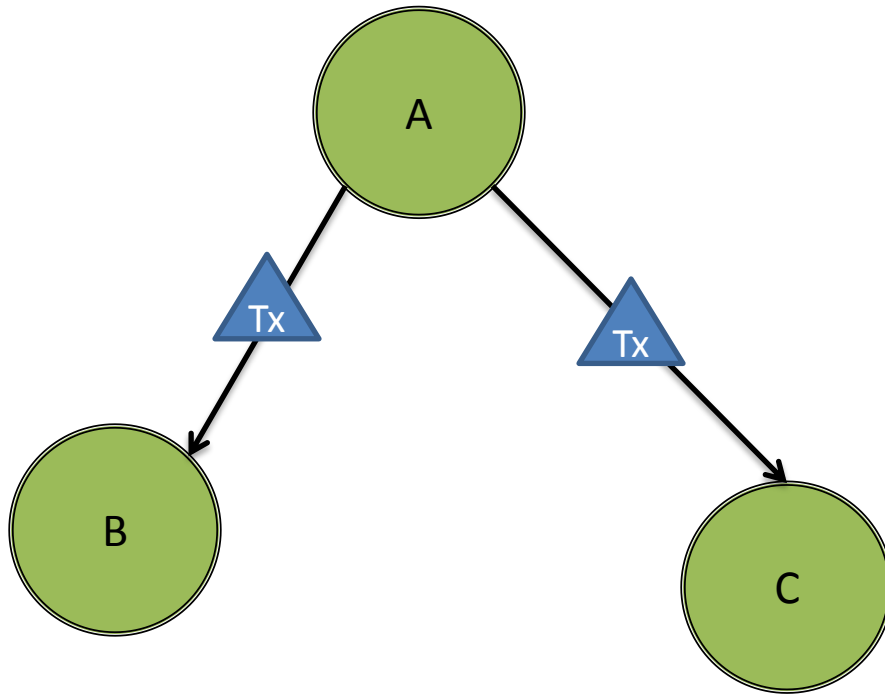
A simplified example



A simplified example

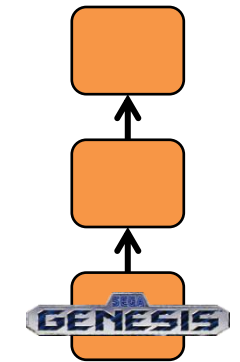
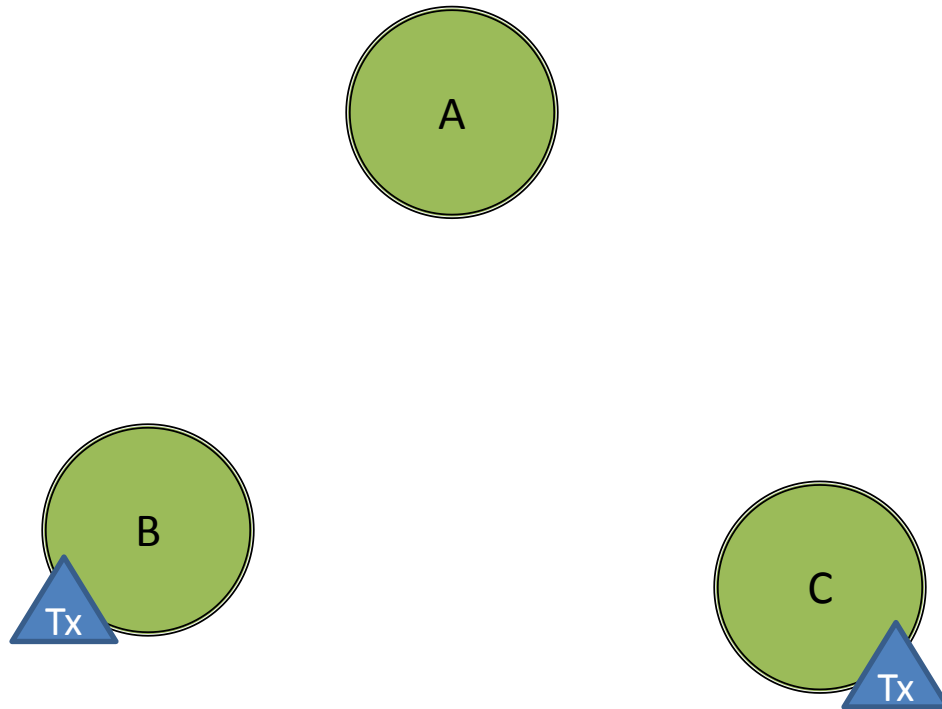


A simplified example



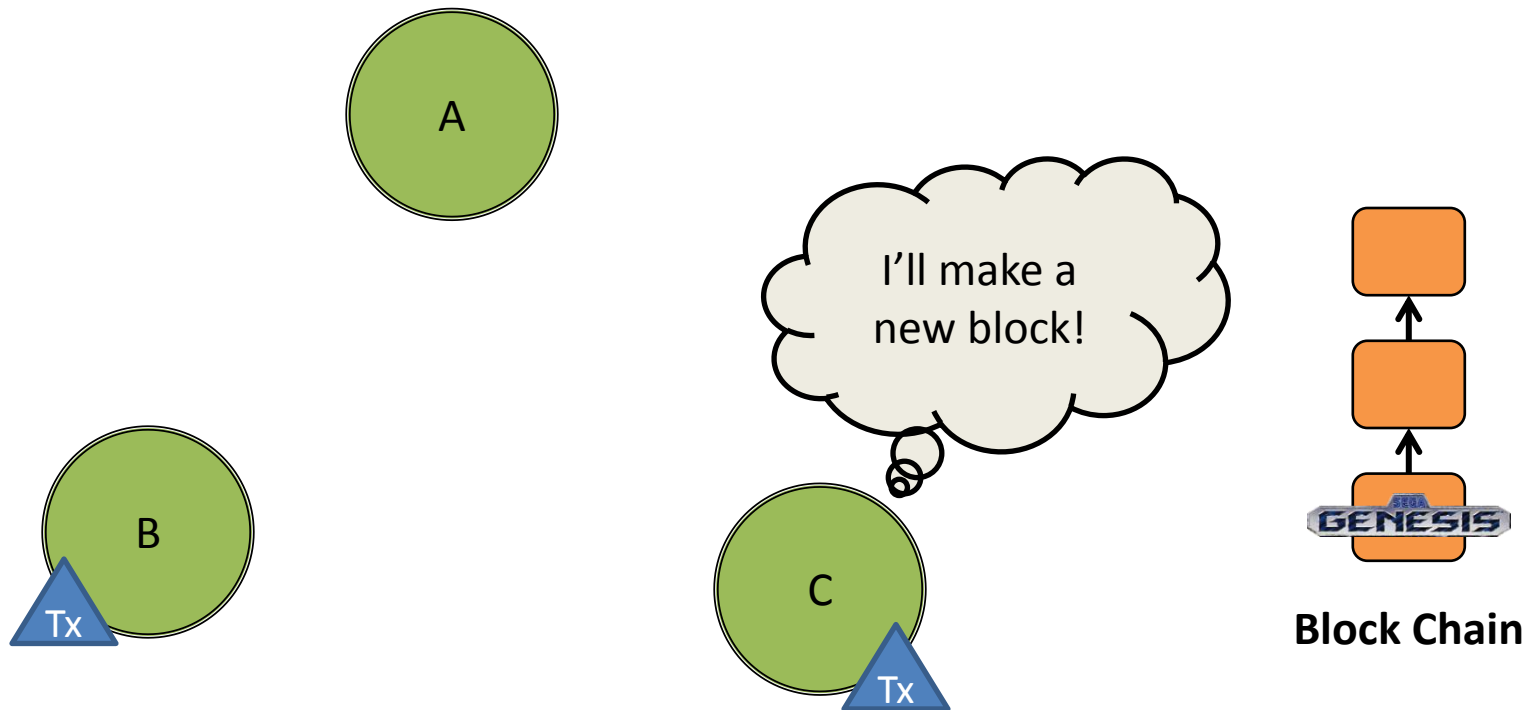
Block Chain

A simplified example

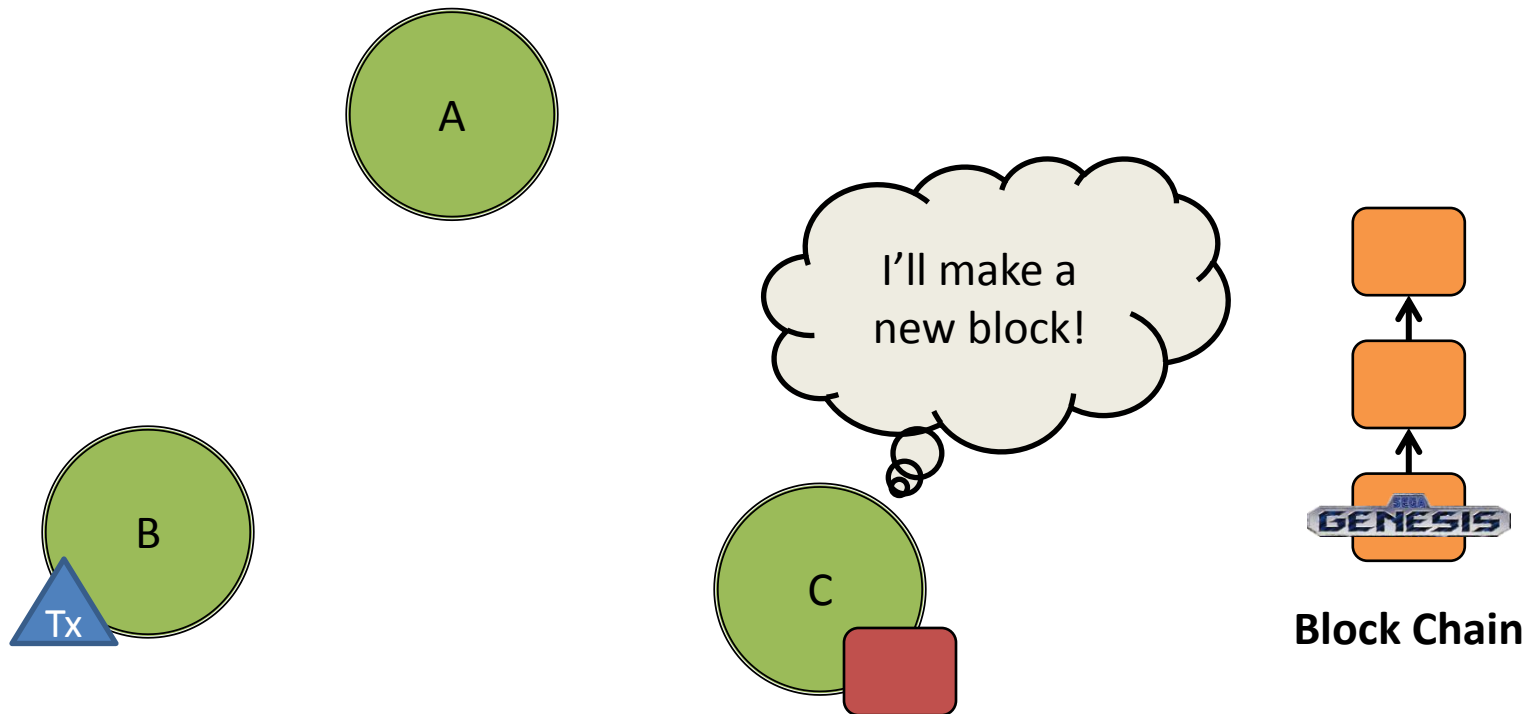


Block Chain

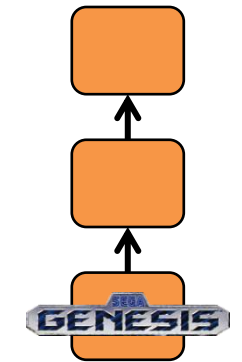
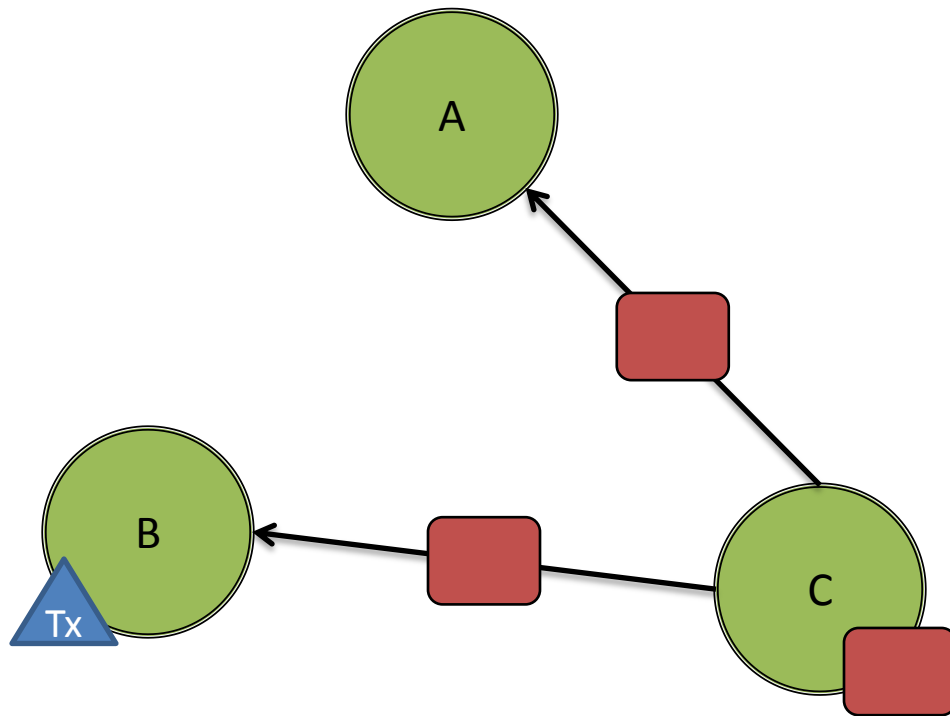
A simplified example



A simplified example

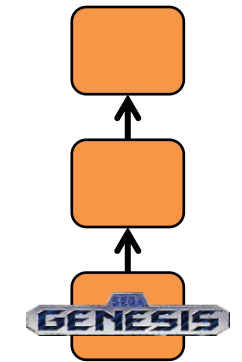
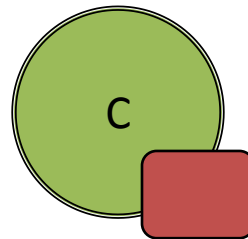
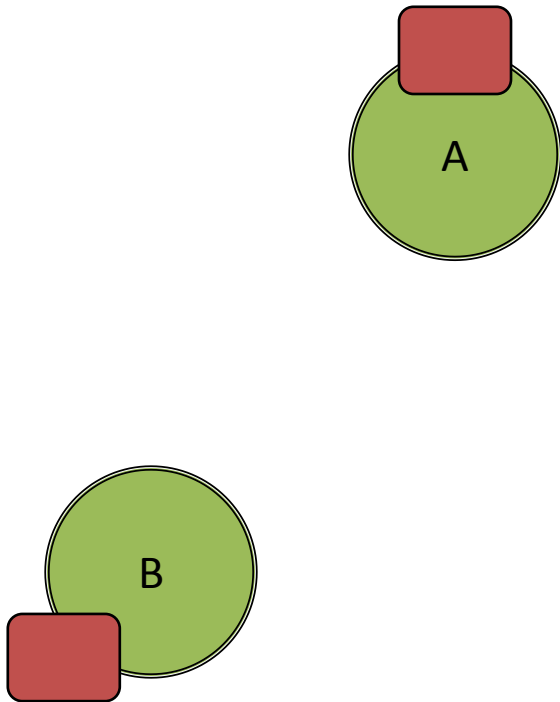


A simplified example



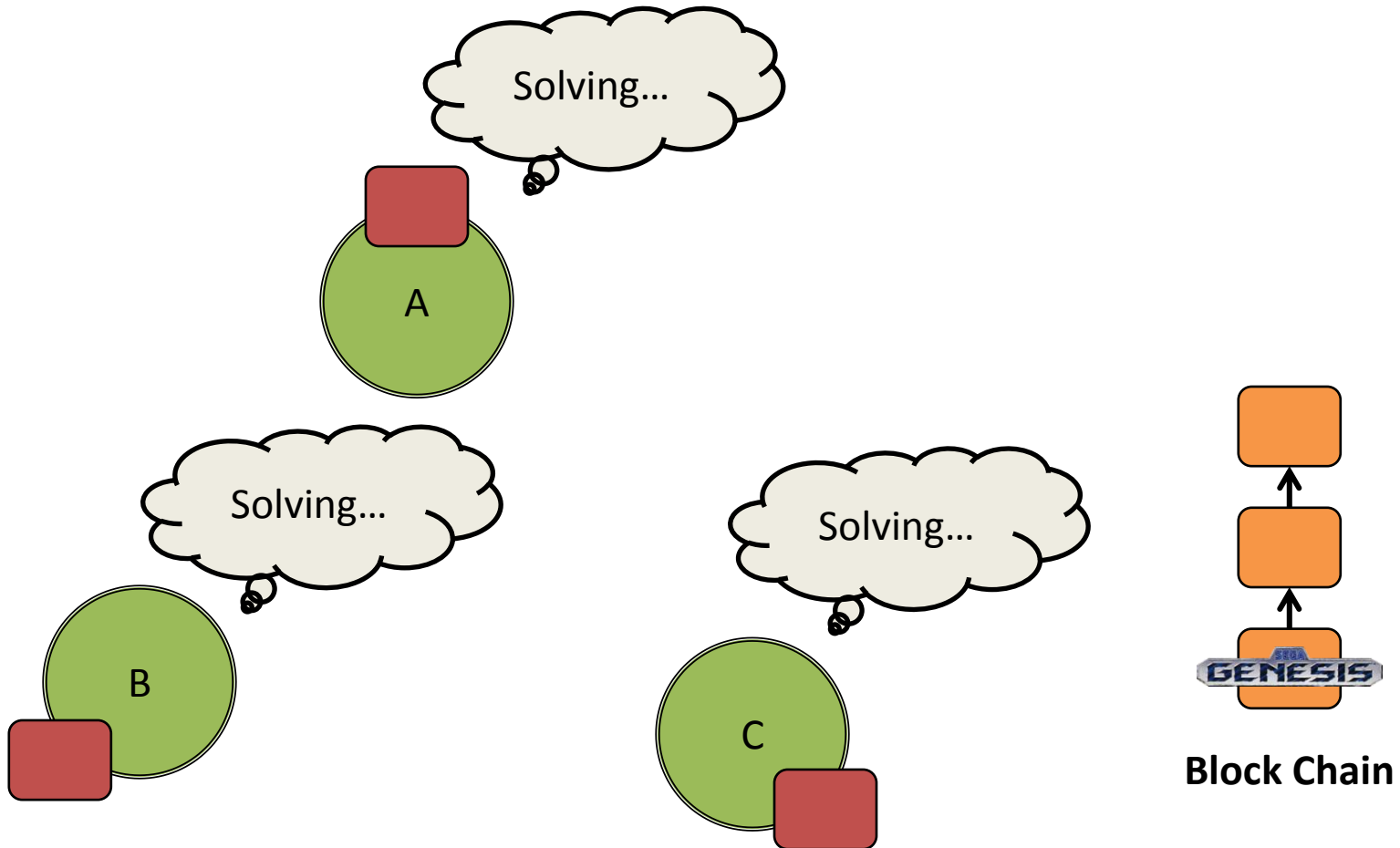
Block Chain

A simplified example

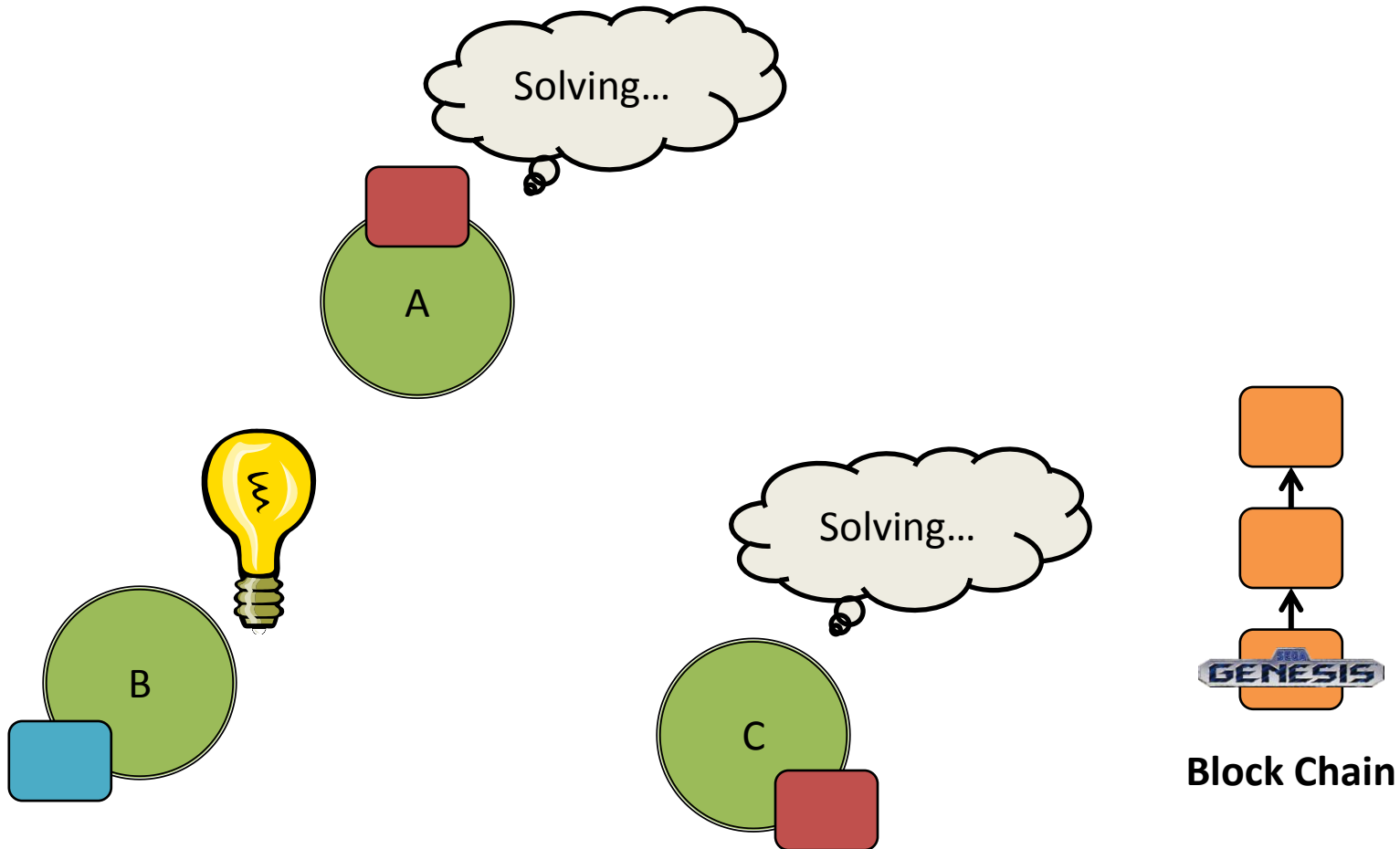


Block Chain

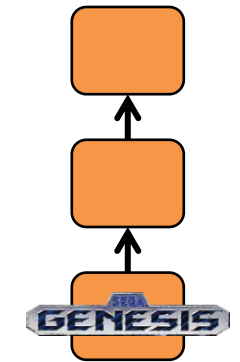
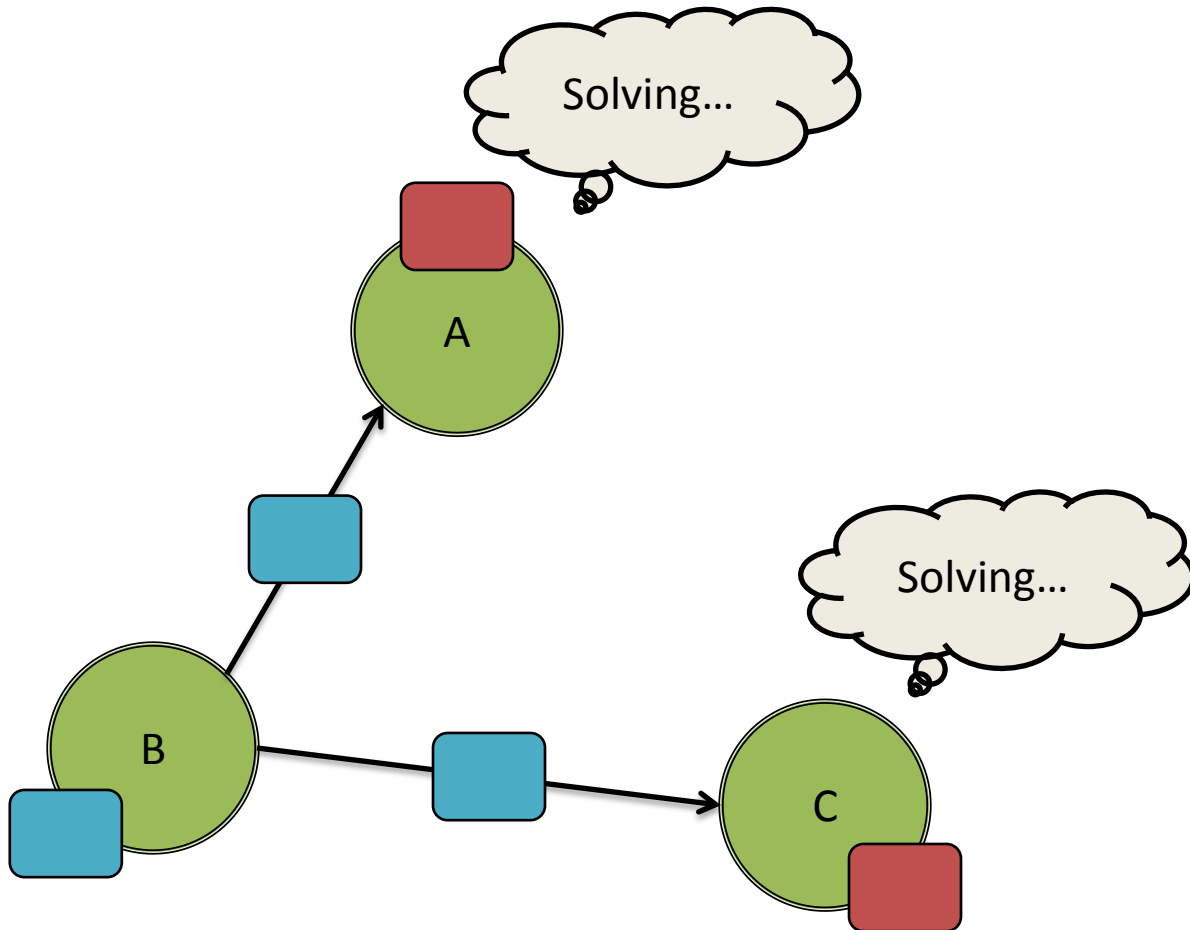
A simplified example



A simplified example

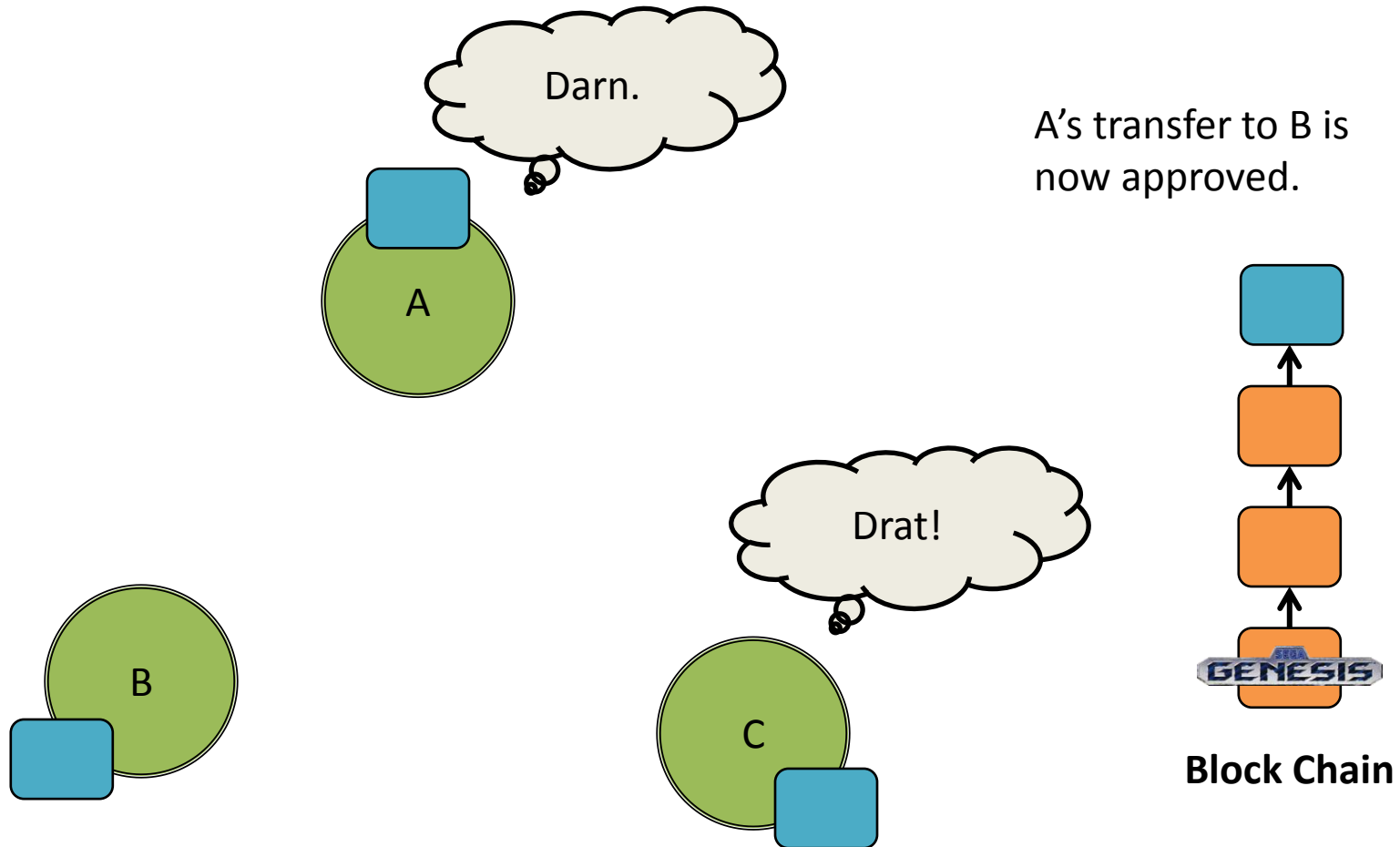


A simplified example



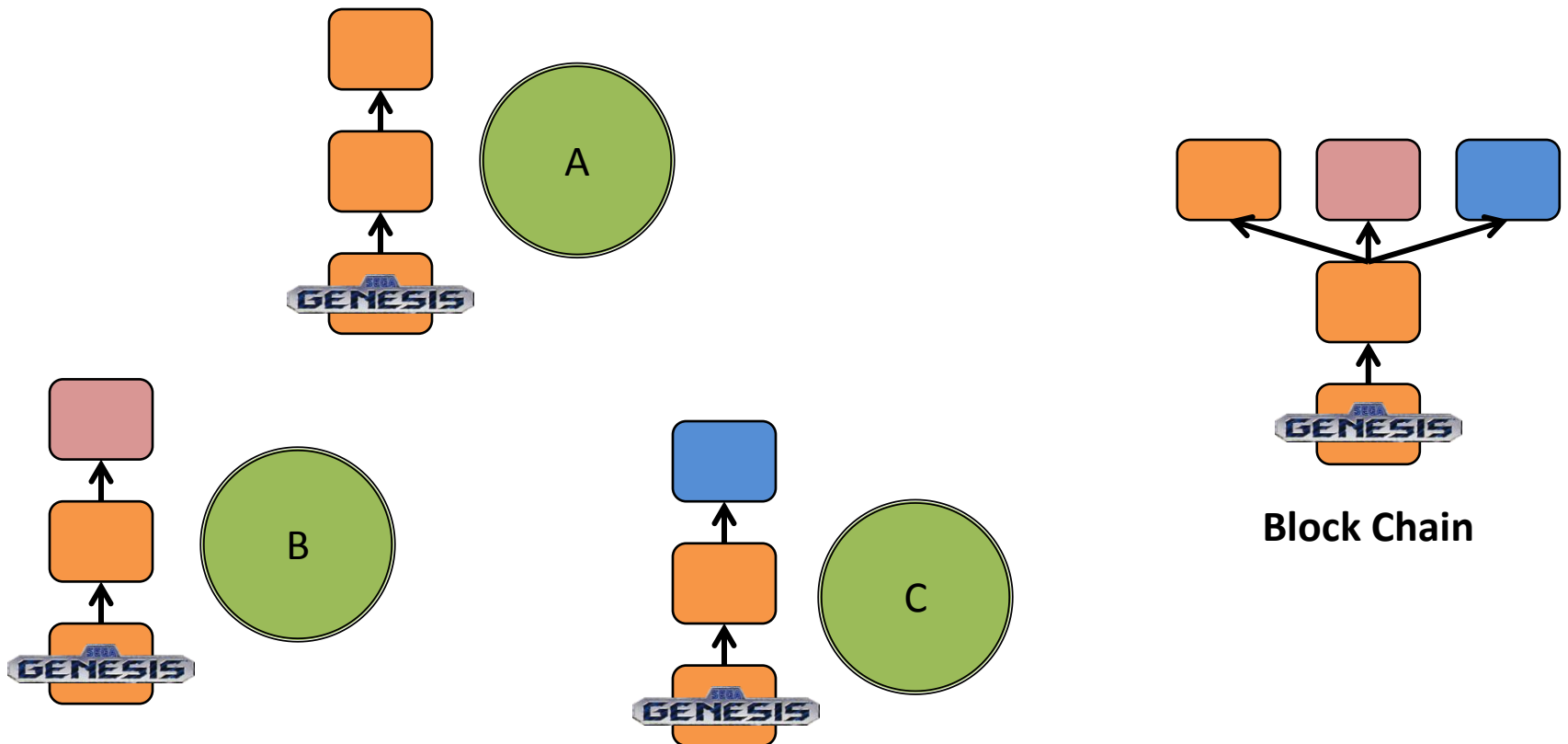
Block Chain

A simplified example



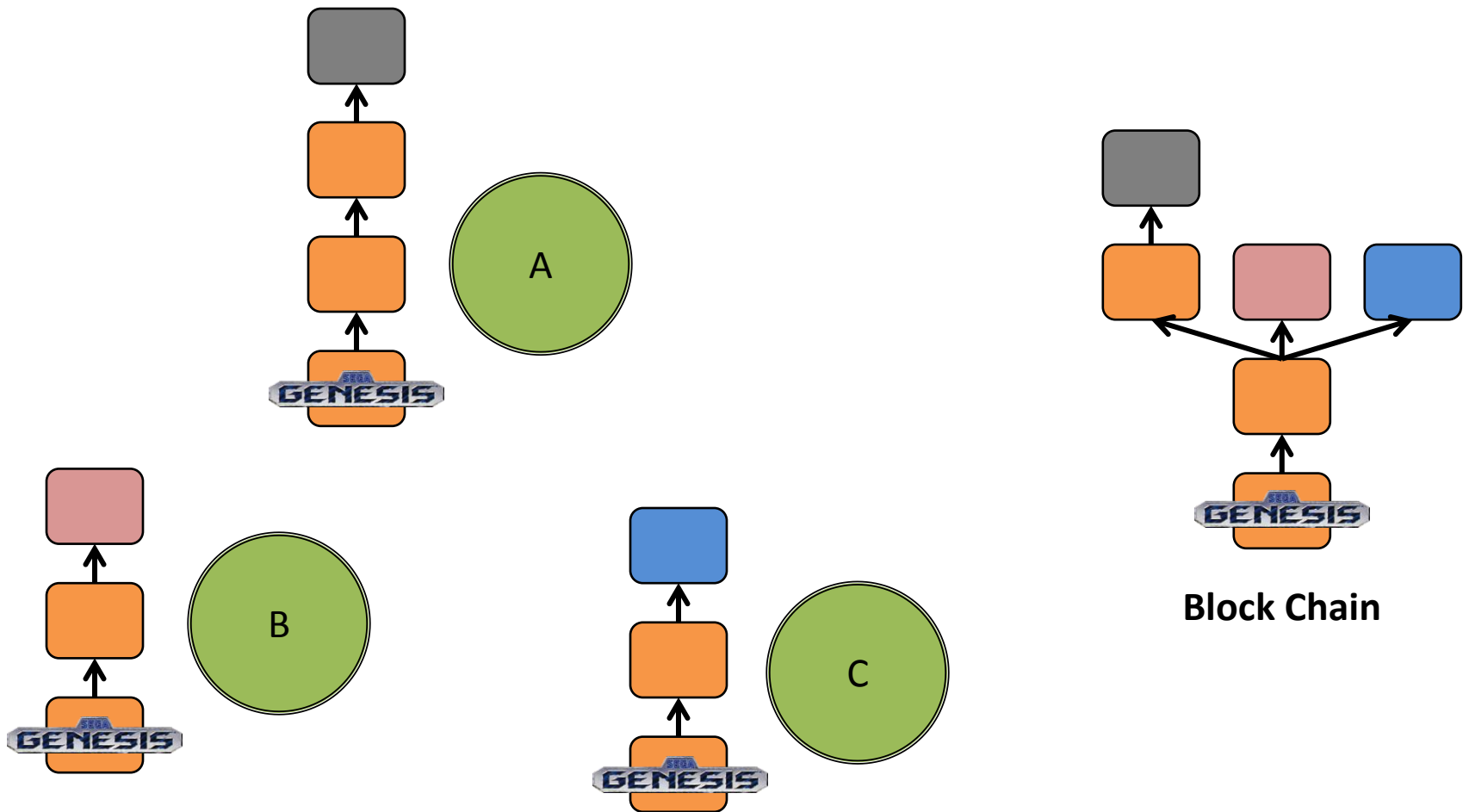
Branching

- Nodes can actually have different chains from one another
- The block chain can branch to reflect these differences



Branching

- Once one branch becomes longer, all nodes switch over



The double-spending problem

- Node A might try to send the same coin to B and C
- Node A thus creates two conflicting transactions

The double-spending problem

- Node A might try to send the same coin to B and C
 - Node A thus creates two conflicting transactions
- Safeguard: a node that receives conflicting transactions will only accept the one transaction it sees first

Security properties / threat model

- No branch of the block chain should include double-spends
- No node's "idea" of the block chain should include double-spends
- Model a network attacker:
 - This is realistic, since communications are unencrypted
 - Attacker is an "imperfect" broadcaster
- Include idea of CPU power in the model

Murphi model

type

```
  TransId:          0..TransCount;
  ValidTransId:     1..TransCount-1;
  ...
  CurrentTrans:     1..TransCount;
  WorkAmount:       0..MaxWork;
  AgentId:          union {ParticipatorId, IntruderId}
  Blockchain:       array[ValidTransId] of Message;
  TransChain:       multiset[TransCount] of ValidTransId;
```

Agent : record

```
  chain: Blockchain;
  validchain: TransChain;
```

...

```
  workleft: WorkAmount;
```

end;

var

```
  age: array[AgentId] of Agent;
  cur: CurrentTrans;
  tra: Blockchain;
```

Invariant

```
invariant "nobody legally double pays"
  forall i: ParticipatorId do
    forall j: ParticipatorId do
      i != j
      ->
        checknodoublepay(age[i],age[j])
    end
  end;
end;
```

```
function checknodoublepay(one: Agent; two: Agent) : boolean;
var combined: TransChain;
var total: BlockChain;
var counts: CoinCounts;
begin
  undefine combined;
  undefine total;
  for i: ValidTransId do
    if MultisetCount(j:one.validchain,one.validchain[j] = i) > 0
    | MultisetCount(j:two.validchain,two.validchain[j] = i) > 0 then
      MultisetAdd(i, combined);
      if !isundefined(one.chain[i].id) then
        total[i] := one.chain[i];
      end;
      if !isundefined(two.chain[i].id) then
        total[i] := two.chain[i];
      end;
    end;
  end;
  counts := getcounts(total, combined);
  for i:AgentId do
    if counts[i] < 0 then
      return false;
    end;
  end;
  return true;
end;
```

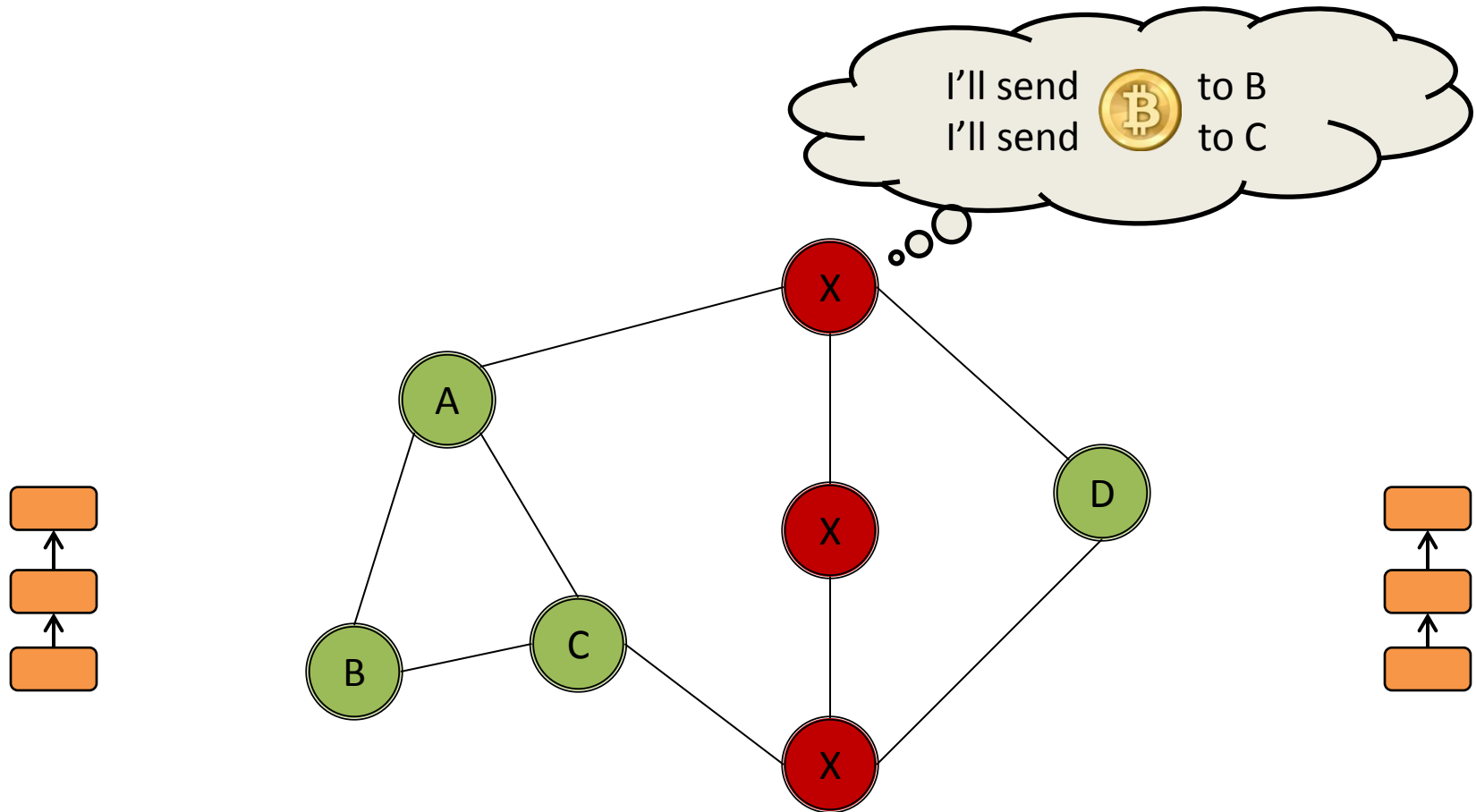
Double-spending attacks

- 1) Network segmentation
 - 2) Majority control of the network (w.r.t. CPU power)
- These are known attacks; our model didn't reveal any previously-unknown attacks.

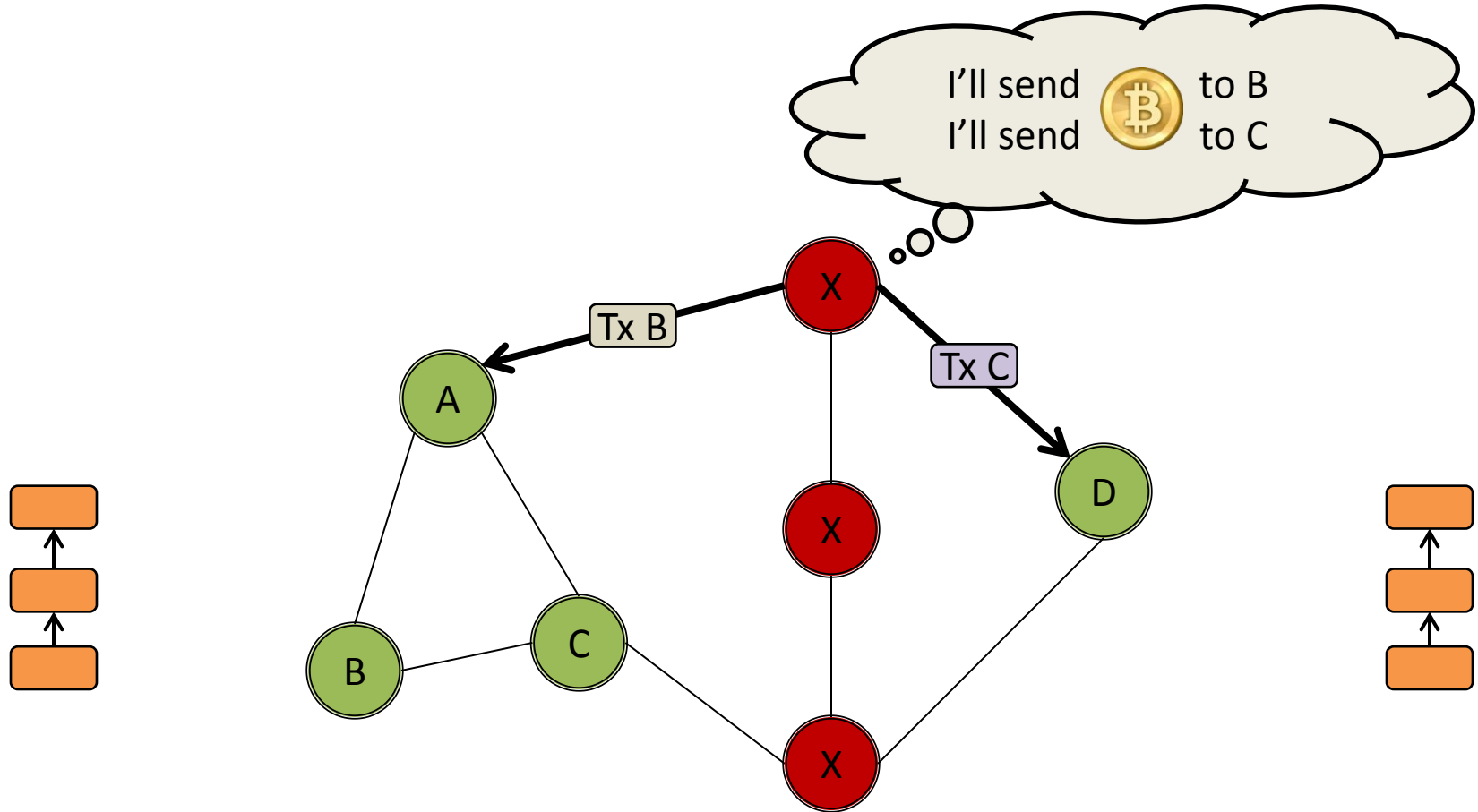
Segmentation

- Attacker divides the network into two subgraphs that can't communicate with each other
- Spend a coin twice: once in each subgraph

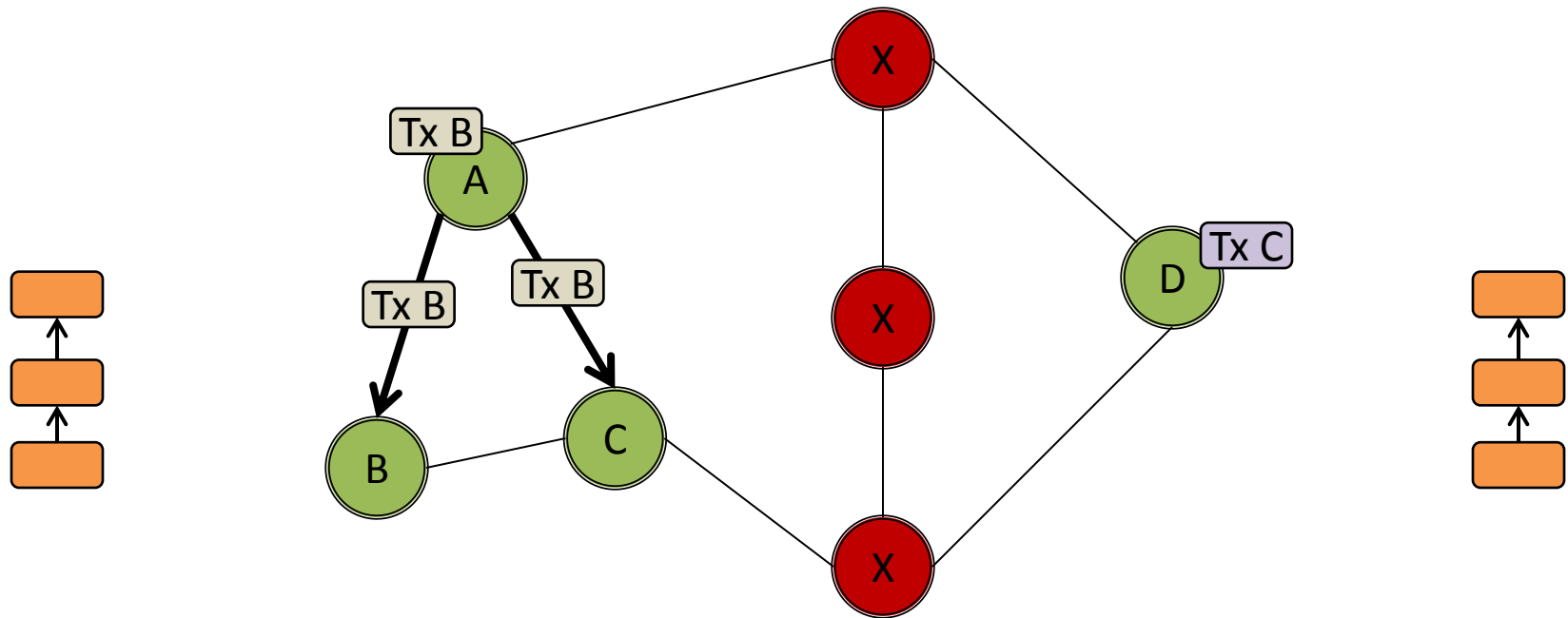
Segmentation example



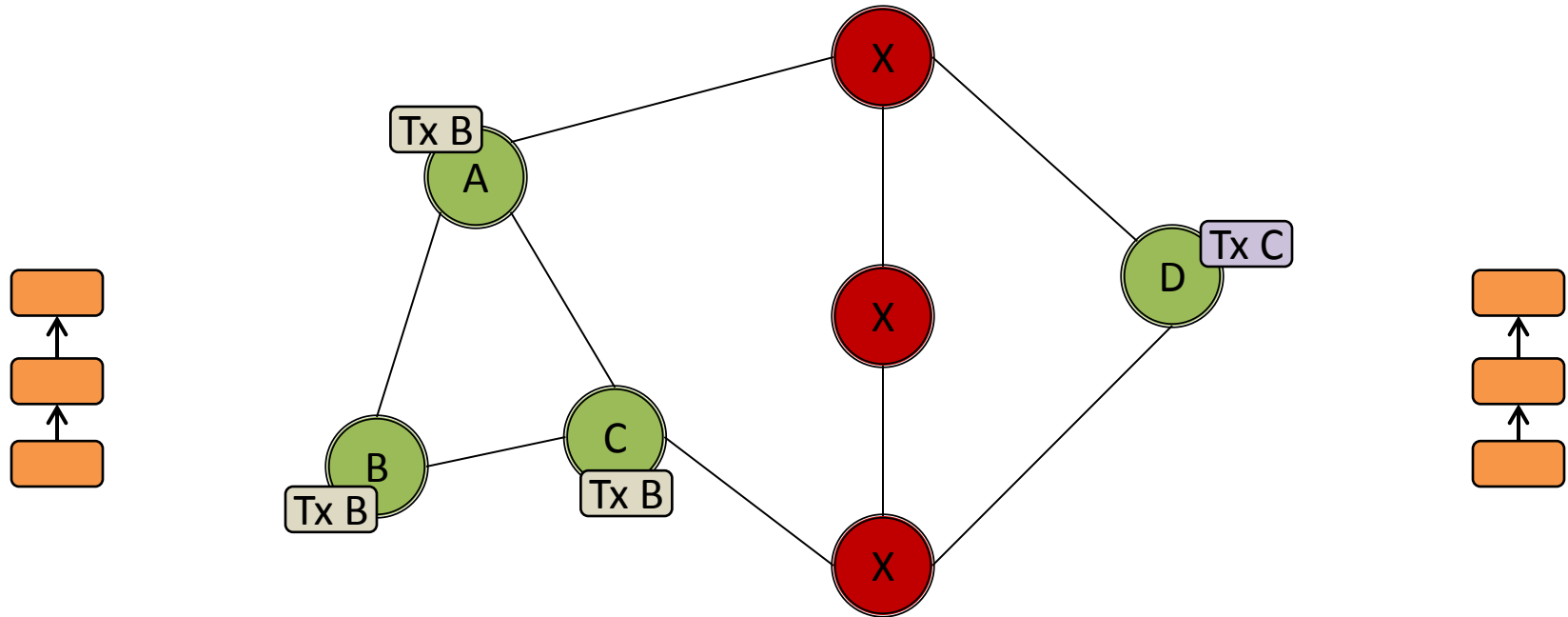
Segmentation example



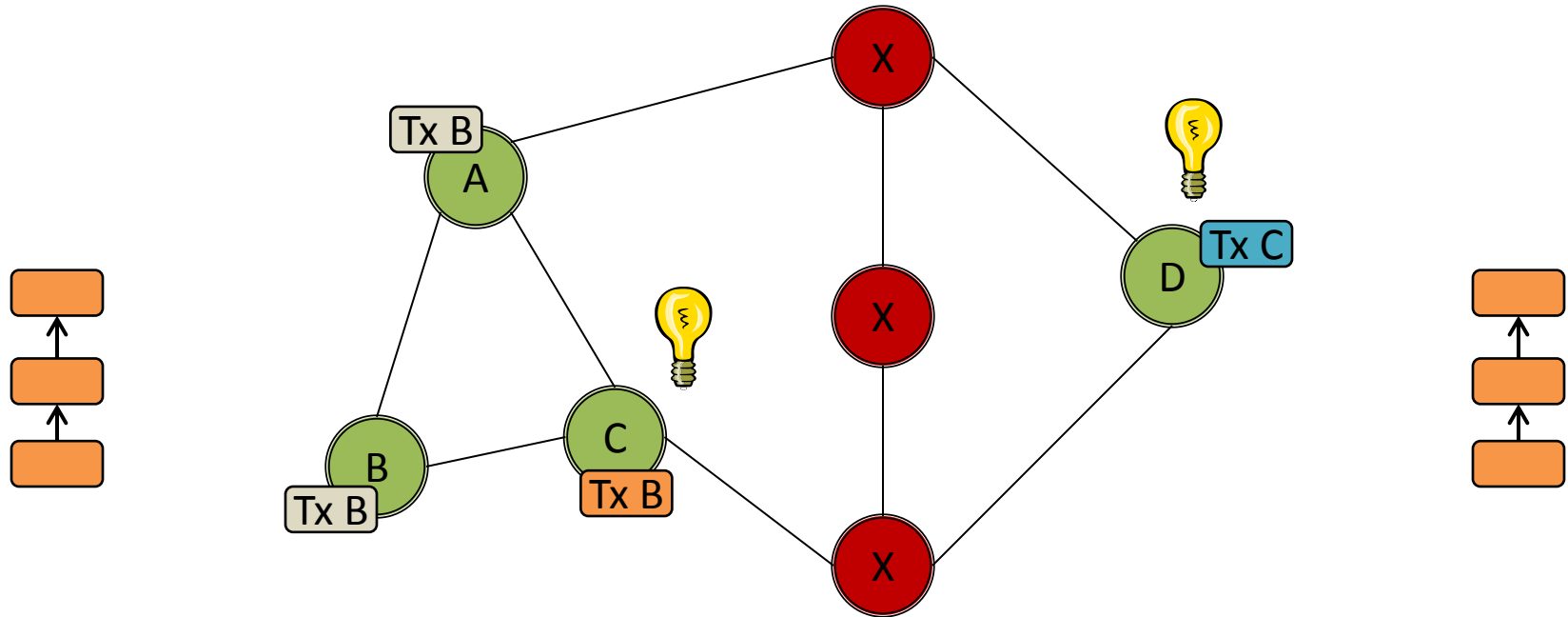
Segmentation example



Segmentation example

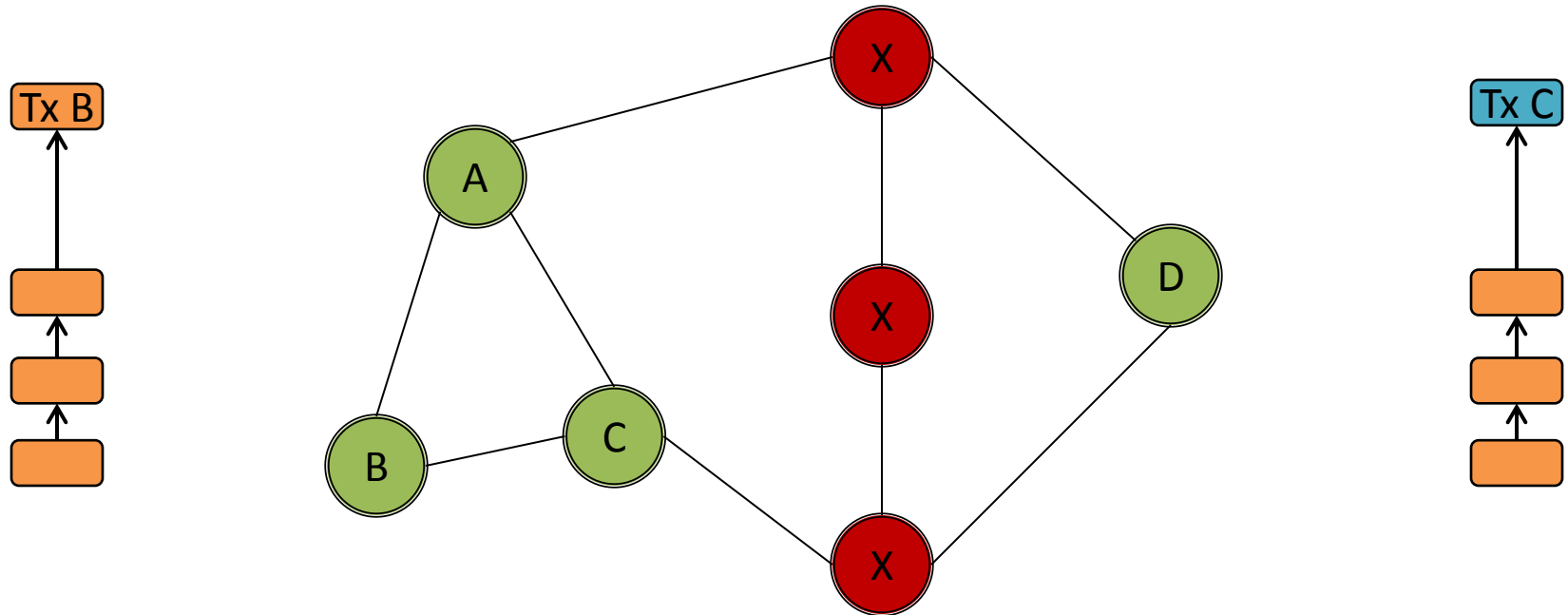


Segmentation example



Segmentation example

- After blocks propagate subgraphs, attacker has double-spent



- Actually feasible? Difficult, but not impossible to surround one or more nodes with attack nodes

Majority power attack

- Attacker can grow whichever branch of the chain he wants, with whatever transactions he wants
 - Trivially breaks Bitcoin for everyone
- Anyone with that much CPU is disincentivized to do this, since they could just gain from acting legitimately

Other concerns

- Denial-of-service
- Anonymity

Denial-of-service

- Follows from segmentation attack
- Trivial for a network attacker
- Bootstrapping process uses no encryption
 - Nodes connect to IRC channel to discover other nodes
- Attacker can connect you to dummy nodes that refuse to broadcast your messages


Denial-of-service

- Follows from segmentation attack
 - Trivial for a network attacker
 - Bootstrapping process uses no encryption
 - Nodes connect to IRC channel to discover other nodes
 - Attacker can connect you to dummy nodes that refuse to broadcast your messages
-
- Not considered a huge problem, just go somewhere else
 - Attacker could cut off all of your other traffic too



Anonymity

- Transactions are anonymous only as long as your public key is never linked to any identifying information
 - Impossible if you buy tangible goods shipped to your home
- Fix (somewhat in progress):
- Never send coins using the same public key twice
 - Every time you receive coins, create a new identity (public key) and send your coins to that new identity through a “mixer”
 - The “mixer” accepts lots of coins from various people and randomly matches source(s) to destination(s)

Bitcoin adoption

[Contact Us](#) | [Help](#) | [Shopping Cart](#) | [Order Status](#)

SEARCH



Shop By System

- Gameboy Advanced
- Gameboy Color
- Gamecube
- NES
- Nintendo 64
- Nintendo DS
- Playstation
- Playstation 2
- Playstation 3
- Sega Dreamcast
- Sega Genesis
- Super Nintendo
- Wii
- Xbox
- Xbox 360

Bitcoin Payment

What is Bitcoin?

Bitcoin is a digital commodity that can be used, like a currency, to pay for goods and services. It's created and managed by a [peer-to-peer network](#) without a central bank. JJGames.com offers a **2% discount** on orders paid for with Bitcoin.

How to Pay with Bitcoin

- Add products to your shopping cart, as usual
- During checkout, click **Have a Promo Code**, below the Secure Checkout button
- Enter the code: **bitcoin**. You'll see your **2% discount** appear in the shopping cart.
- Proceed through checkout to **enter your shipping details**.
- Send Bitcoin payment** to the address indicated
- Click **I've Sent Payment**
- Within seconds, your payment is confirmed and you receive your order number

Demo Video

Using Bitcoin on JJGames





Silk Road

anonymous marketplace

Log in:

[create a username and password](#)

Shop by category:

- Marijuana (3)
- Shrooms (7)
- Ecstasy (3)
- LSD (7)
- Cocaine (0)
- Prescription (6)
- Other (12)
- Weapons (0)



5 grams of shrooms
Price: 29 BTC



1 hit of LSD (blotter)
Price: 18 BTC



500 mg of pure MDMA
Price: 60 BTC

Step-by-step:

- Get **anonymous money**
- Buy something here
- Enjoy it when it arrives!

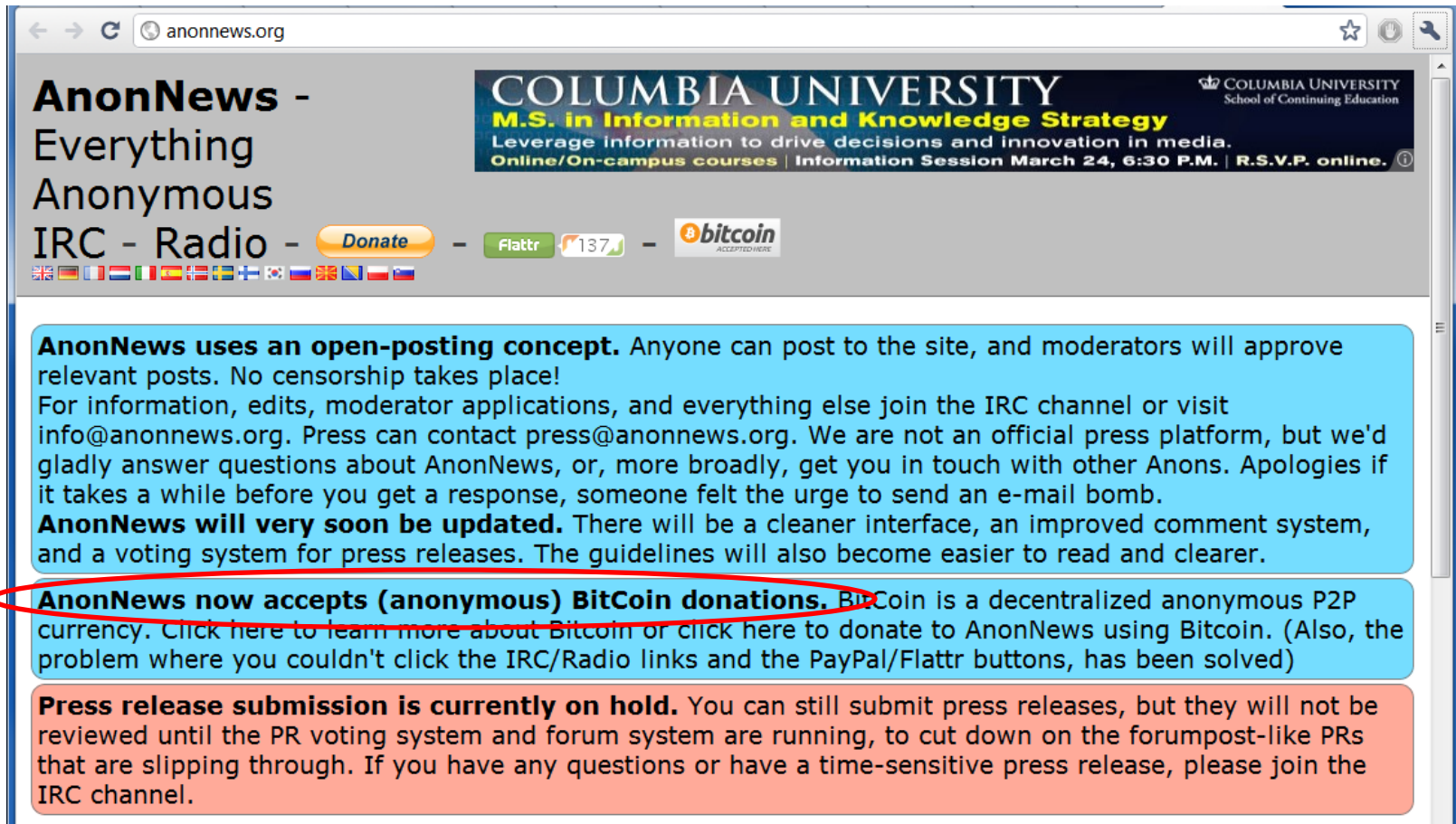
Become a seller!

How does it work?
Contact us
Community forums

151 registered users | 38 current listings | 28 transactions to date

* This site runs on the **Tor anonymity network**.
It can be expected to run slowly and occasionally drop connections.

Bitcoin adoption



The screenshot shows the website anonnews.org. The header includes the site name "AnonNews - Everything Anonymous IRC - Radio" with a "Donate" button, a "Flattr" button with a "137" count, and a "bitcoin" logo with the text "ACCEPTED HERE". A banner for Columbia University is also visible. The main content area contains three text blocks: a blue box explaining the open-posting concept, a blue box announcing Bitcoin donations (circled in red), and an orange box stating that press release submissions are on hold.

AnonNews - Everything Anonymous IRC - Radio - [Donate](#) - [Flattr](#) 137 - [bitcoin](#) ACCEPTED HERE

AnonNews uses an open-posting concept. Anyone can post to the site, and moderators will approve relevant posts. No censorship takes place!
For information, edits, moderator applications, and everything else join the IRC channel or visit info@anonnews.org. Press can contact press@anonnews.org. We are not an official press platform, but we'd gladly answer questions about AnonNews, or, more broadly, get you in touch with other Anons. Apologies if it takes a while before you get a response, someone felt the urge to send an e-mail bomb.

AnonNews will very soon be updated. There will be a cleaner interface, an improved comment system, and a voting system for press releases. The guidelines will also become easier to read and clearer.

AnonNews now accepts (anonymous) BitCoin donations. BitCoin is a decentralized anonymous P2P currency. [Click here to learn more about Bitcoin](#) or [click here to donate to AnonNews using Bitcoin](#). (Also, the problem where you couldn't click the IRC/Radio links and the PayPal/Flattr buttons, has been solved)

Press release submission is currently on hold. You can still submit press releases, but they will not be reviewed until the PR voting system and forum system are running, to cut down on the forumpost-like PRs that are slipping through. If you have any questions or have a time-sensitive press release, please join the IRC channel.