RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID:

Protecting Traditional and Blockchain Virtual Economies

Adrian Bednarek

CISO
Overflow Labs, Inc.

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID:

Protecting Traditional and Blockchain Virtual Economies

Adrian Bednarek

CISO
Overflow Labs, Inc.

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID:

Protecting Traditional and Blockchain Virtual Economies

Adrian Bednarek

CISO
Overflow Labs, Inc.

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID:

Protecting Traditional and Blockchain Virtual Economies

Adrian Bednarek

CISO
Overflow Labs, Inc.

Me

- Adrian Bednarek
- CISO@ Overflow Labs
- Into:
  - Breaking and protecting weird stuff
    - Proprietary protocols
    - Obfuscated code
    - Digital assets/Rights management
    - ‘Blockchainy’ things
    - Virtual economies

Agenda

- My background
- Crash course in econ 101 (I'll make it quick)
- Web1, Web2, Web3 economies? What are they?
- Common economic attacks on traditional (web2) economies.
- Deep dive into a web2 economic exploit
- Common attacks on web3 economies
- Summary/Recap

Timeline

1997

2001

2002

2004

+~25 others

2017

2022

OVERFLOWlabs

Virtual Economy Management Platform


The Lord of the Rings Online


Ultima Online


DarkFall
Unholy Wars


Age of Conan


WildStar


Dark Age of Camelot


RIFT


Asheron's Call 2
Fallen Kings


Final Fantasy XIV
Online


The Elder Scrolls
Online


Star Wars
The Old Republic


Shadowbane


World of Warcraft


Lineage


Anarchy Online


Age of Wushu


Final Fantasy XI
Online

RSAConference2022

TLDR/TLDL (Too long didn't listen)

95% of all virtual economies are hackable*

RSAConference2022

Crash Course In Economics

Economy 101

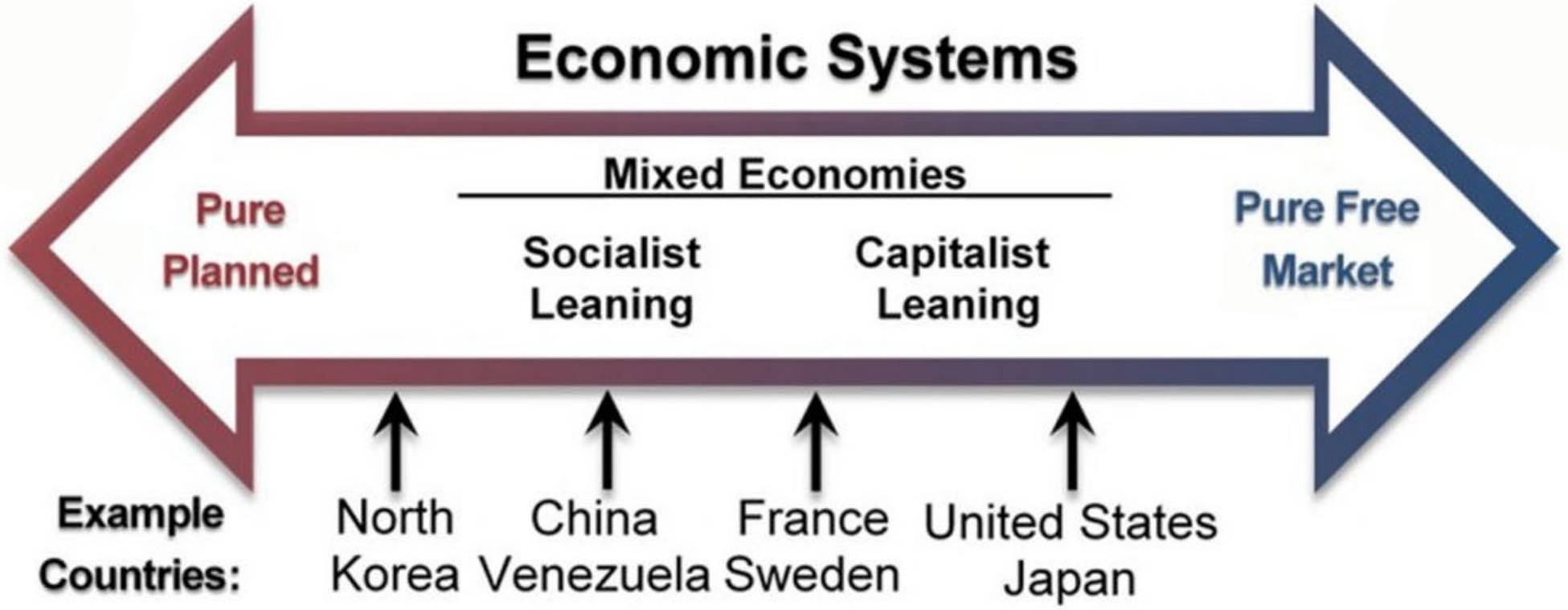
What is an Economy?

- The root of what an economy is both simple and complex
  - In a nutshell an economy is defined by the production and consumption of:
    - Goods
    - Services
  - It gets complicated since both the production and consumption of goods are influenced by:
    - Culture and values
    - Education and technological evolution
    - Social norms
    - Political structure and legal systems
    - Geographic factors and natural resource abundance

Types of Economic Systems

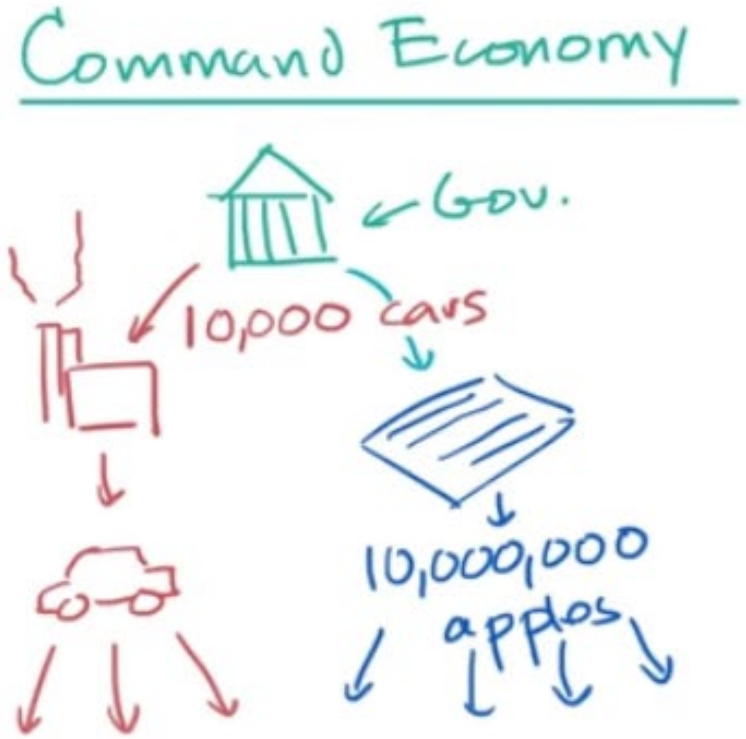
- Four main types
  1. Free Market Economy (Defined by Supply and Demand)
  2. Command Economy (Defined by a Central Government/Entity*)
  3. Traditional Economy (Developing countries, social and custom defined, barter)
  4. Mixed Economy (Typically a hybrid of free market and command)
- Goal: Minimize or control the fluctuation of goods and services availability
  - Stable Markets (prices of goods)
  - Stable Employment Levels
  - Business and Individual Prosperity

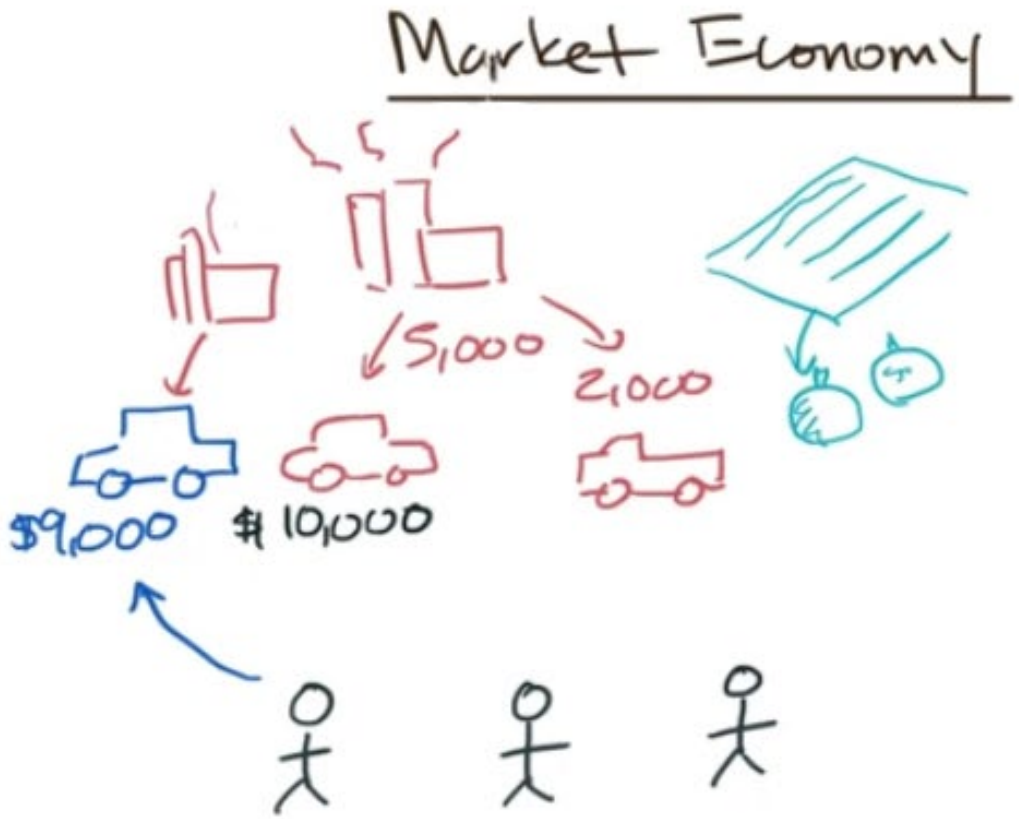
Planned-Free Market Spectrum



*source:https://www.proprofs.com/

Command vs Market Illustrated

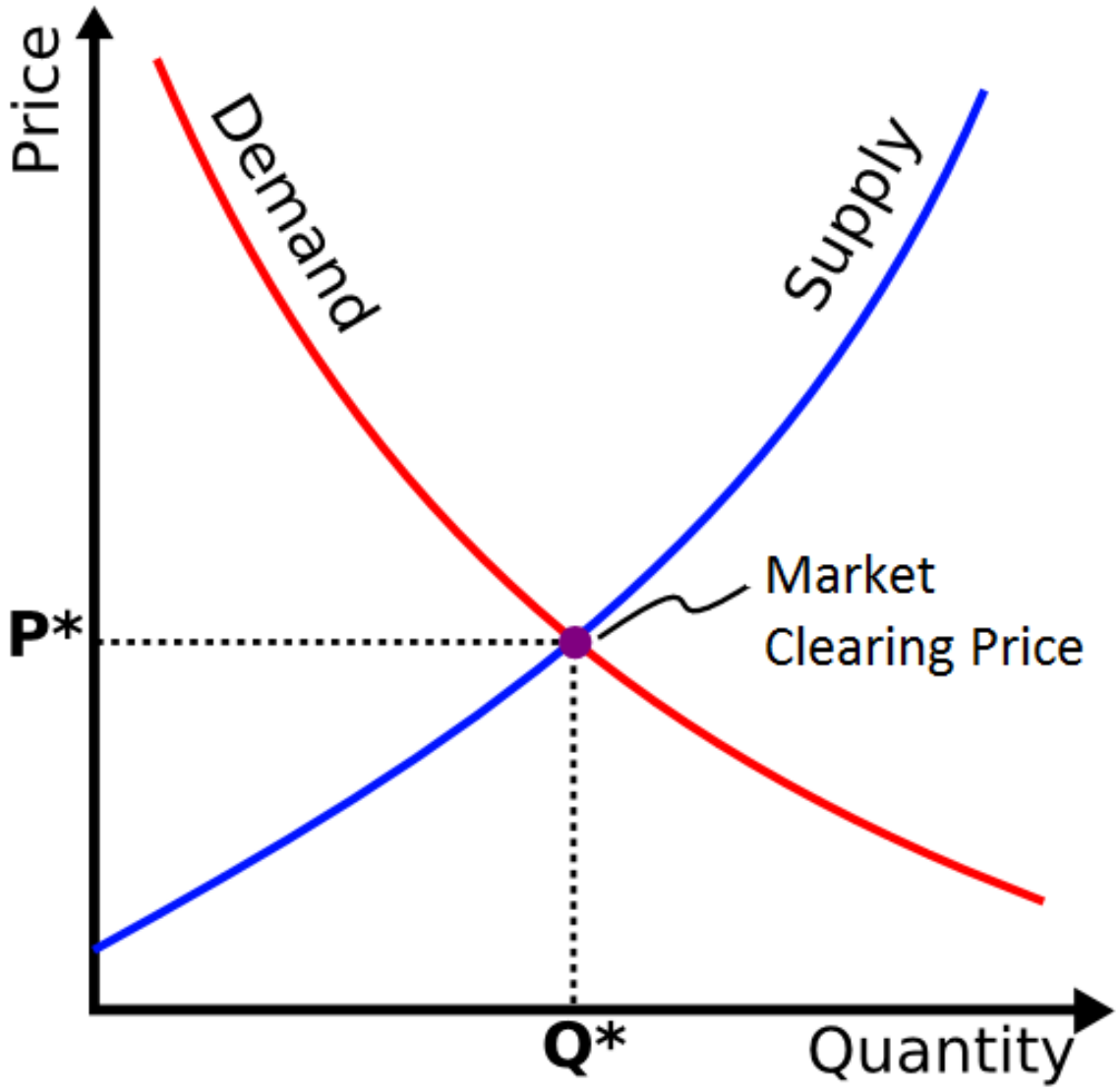




*source: https://www.youtube.com/watch?v=Ve6K10-Yx_M

Supply and Demand

- The entire field of economics is based on the idea of **“Scarcity”**



“Scarcity”

8L Banff Air

~~$32.00~~ **$25.00**

OVERFLOW labs

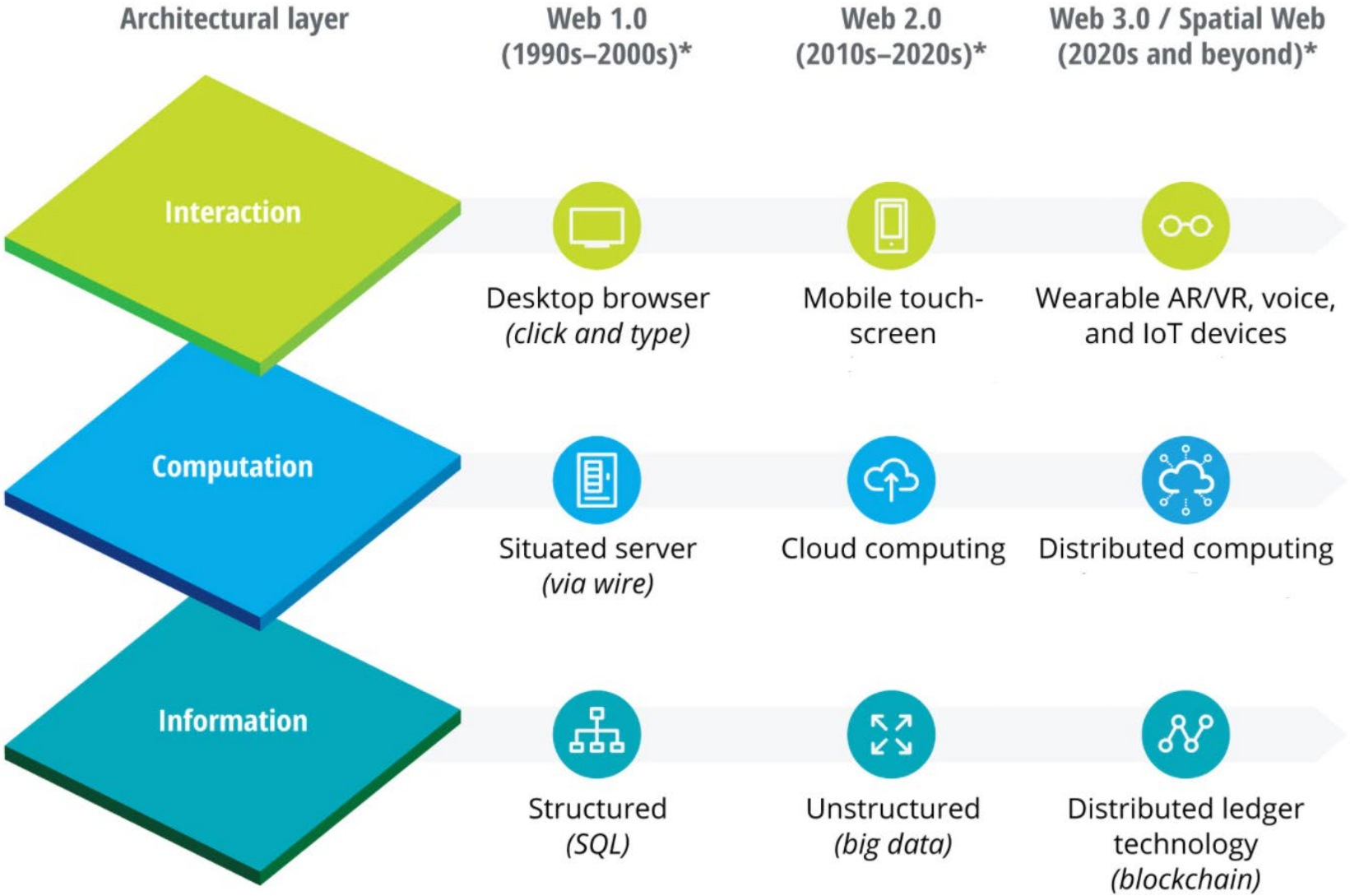
Recap

- In a free-market people vote with their money on what goods and services should be provided
- In a command top-down designed economy a group of people in leadership mandate what goods and services should be provided
- The concept of **Scarcity** is central to economic activity
  - Scarcity must be protected?

RSAConference2022

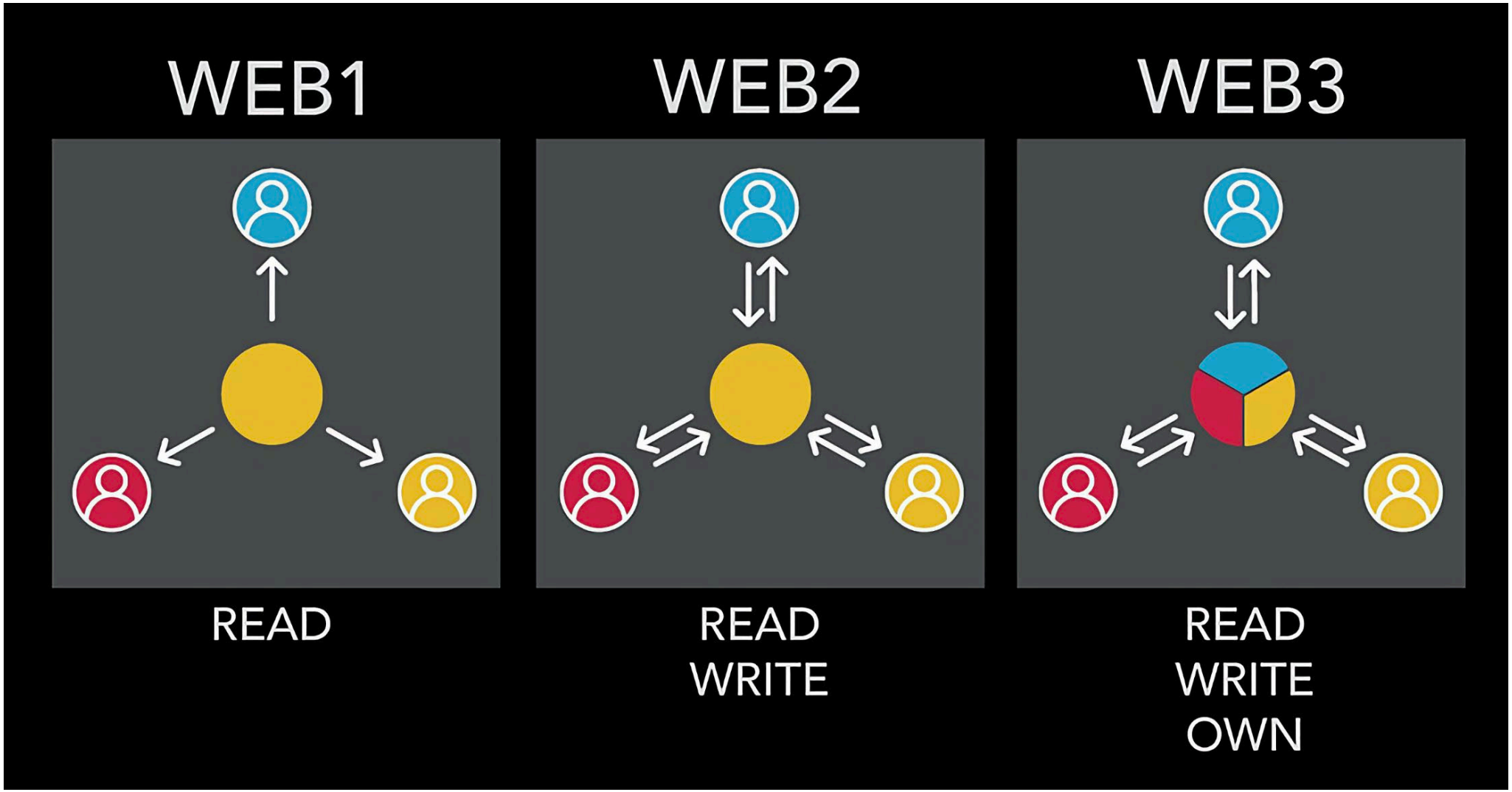
Virtual Economies

What is web1/web2, and web3?



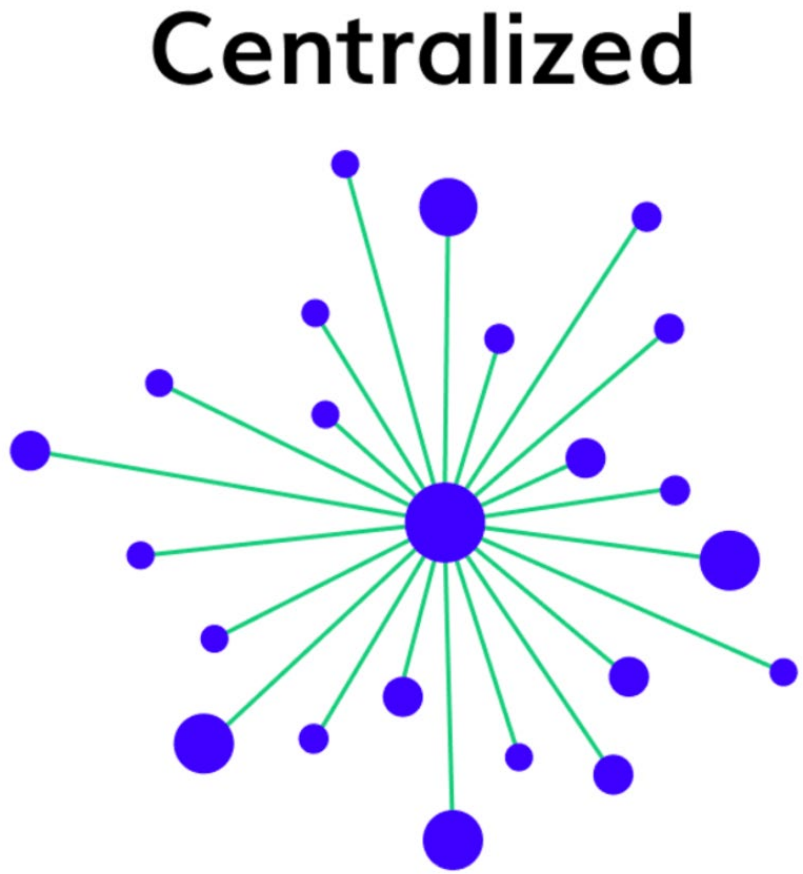
*Source:Artivatic.ai

In a Nutshell



Protecting Web 2 Economies

- Centralized data ownership issues:
  - Trust of maintainers
  - Trust of codebase
  - Trust of infrastructure
- Exploit classes:
  - OWASP TOP 10
  - Infrastructure configuration
  - Business logic
- Why? – Protect Scarcity



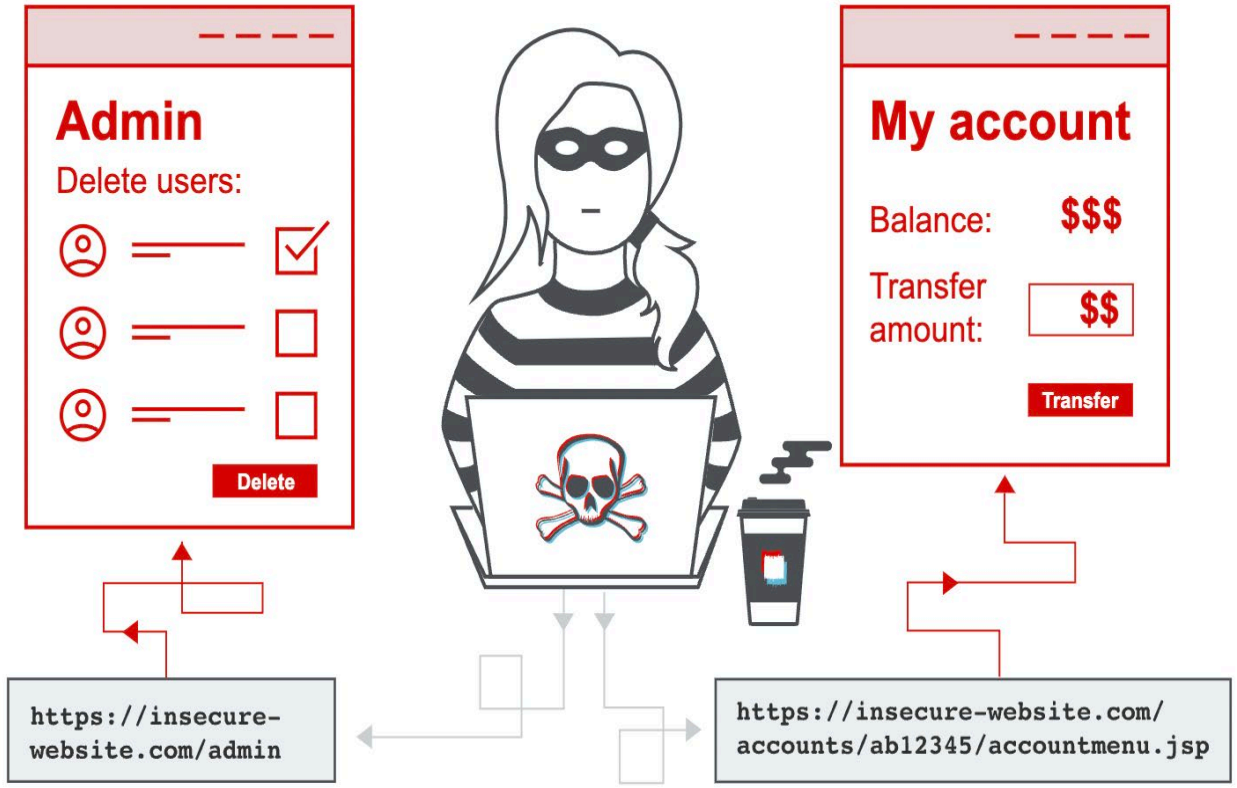
RSAConference2022

Common Types of Attacks

Integer/Data Race/Access/Authorization Issues

Access/Authorization Issues

- Insufficient access checks or enforcement



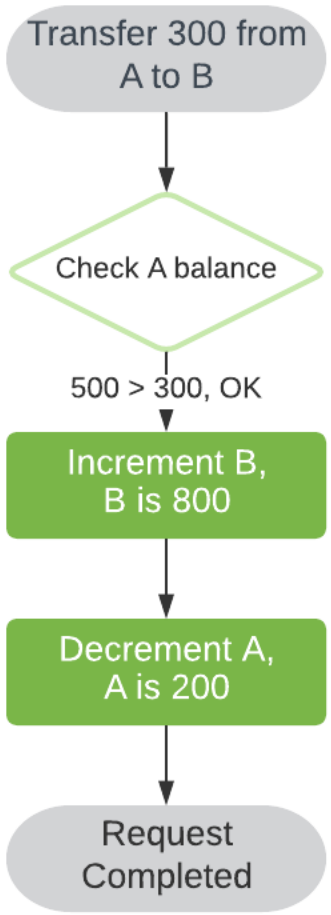
*Source: portswigger.net

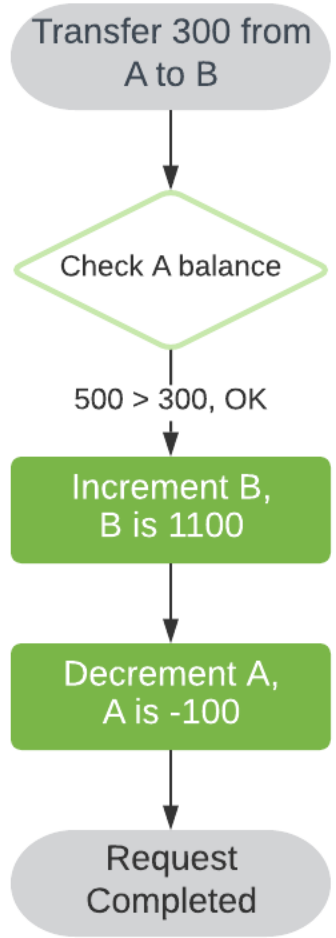
Integer Exploits

- Simpsons did it!

Race Conditions

- Complicated
- Frequent in multithreaded systems/distributed computing





*Source: baeldung.com

RSAConference2022

Case Study

Guild Wars 2 – a ‘web 2’ era ecosystem

Guild Wars 2

- WoW type clone
- Player to player trading
- Popular
- Large feature set
  - crafting, guild banks, personal banks, auction house, vendors.. etc
- large attack surface + popular game + in game commerce


Black Lion Trading Company
Trading Post [0]
112 76 91
GET MORE GOLD
Home
Buy Items
Sell Items
My Transactions
pearl rod
Search : pearl rod
Only Show Available
Armor
Weapons
Upgrade Components
Skins
Crafting Material
Other
Inventory Bags
Delivery Box
Items: 0
Funds: 0
When you buy or sell on the Trading Post the items and funds will show up here. Speak to a Black Lion Trading Company NPC to pick them up.
Qty.
Item
Level
Price
10650 Pearl 0 1 94
27 Rodgort 80 1,974 99
202 Dire Pearl Rod 80 1 75 27
206 Rabid Pearl Rod 80 94 73
250 Magi's Pearl Rod 80 89 99
40 Giver's Pearl Rod 80 3 88 99
270 Carrion Pearl Rod 80 1 22 1


Dire Pearl Rod
Vendor Value: 2 64
Quantity: 1
Max. Price 1 75 27
Total Price: 1 75 27
Buy Instantly
Cancel
Current Buyers
Ordered
Price per Unit
2 Ordered 81 40
3 Ordered 81 39
2 Ordered 81 38
4 Ordered 81 37
2 Ordered 81 33
Current Sellers
Available
Price per Unit
Buying 1/2 1 75 27
2 Available 1 75 28
1 Available 1 81 29
1 Available 1 81 30
1 Available 1 83 33


Current Sellers
Available
Price per Unit
Buying 1/2
1 75 27
2 Available
1 75 28
1 Available
1 81 29
1 Available
1 81 30
1 Available
1 83 33
2 Available
2 4 91

AH – BUYING STUFF (via GUI)

- Listed:

2 @ 1 g 75 s 27 c

2 @ 1 g 75 s 28 c

- To buy 3 the price would be:

2* 1g 75s 27c (17527)

+ 1* 1g 75s 28c (17528)

= (17527*2) + (17528*1)

= 52582 or 5 Gold 25 silver 82 coper

AH – BUYING STUFF (INTERNALS)

- RESTFUL API – JSON
- Example buy request:

{"protocol":"Game.gw2.Trade",

"command":"Buy",

"body":{"offers":[{"UnitPrice":17527,"Quantity":2},{"UnitPrice":17528,"Quantity":1}]},"headers":{"t":"$45977","m":“<CHARID/SESSIONTOKEN GUID"},"type":"One"}

45977 is item id (https://www.gw2spidy.com/item/45977)

TLDR; The Exploit

Original Request

- *Item Number*
- "t":"$45977"
- *Array of purchase requests*

[{"UnitPrice":17527,"Quantity":2},

{"UnitPrice":17528,"Quantity":1}]

- Buyer spends 5g 25s 82c and gets all 3 items.
- The Seller gets the full 5g 25s 82c!

Modified Request

- *Item Number*
- "t":"$45977"
- *Array of purchase requests*

[{"UnitPrice":17527,"Quantity":2},

{"UnitPrice":1,"Quantity":1}]

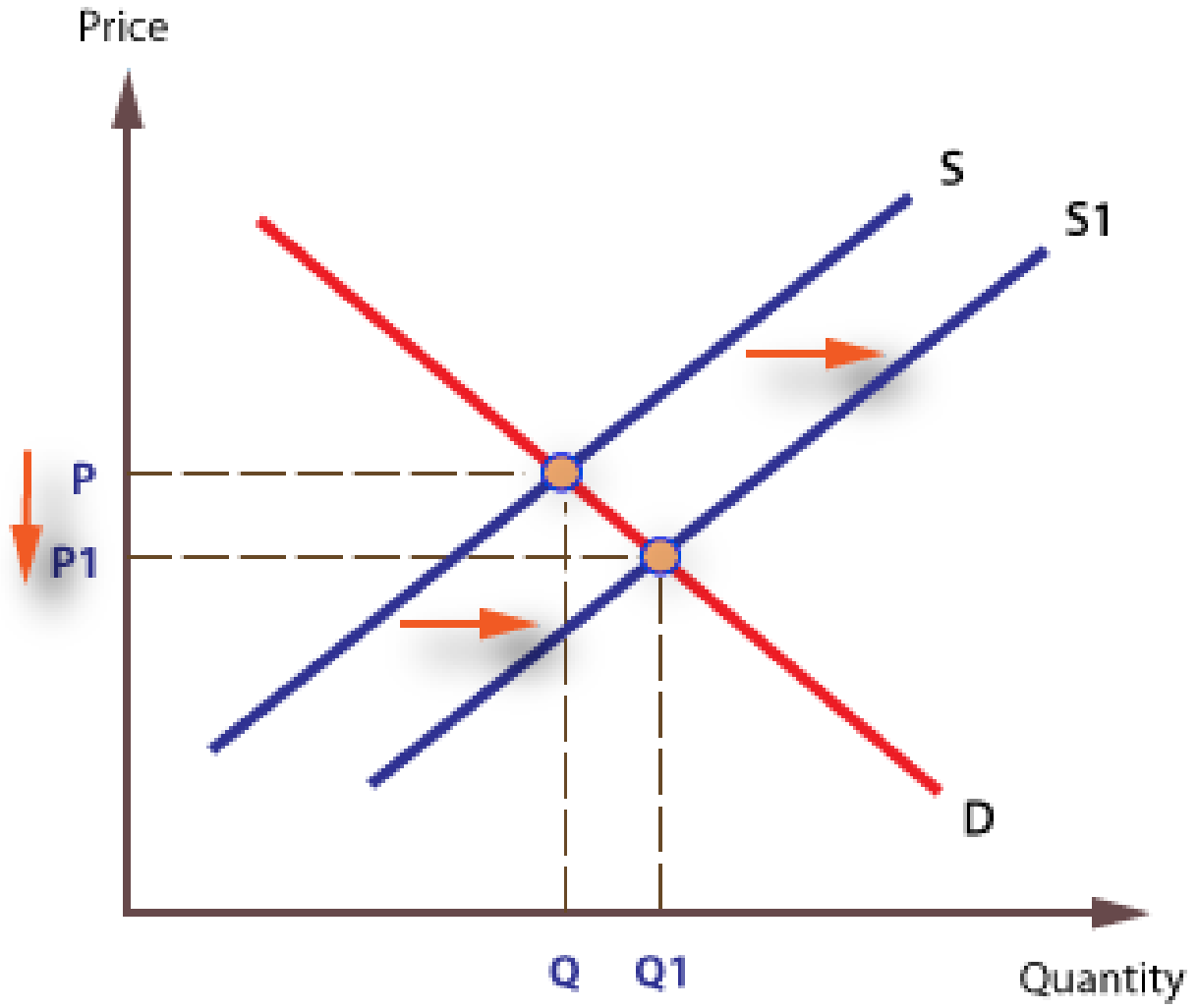
- Buyer spends 3g 50s 54c and gets all 3 items.
- The Seller gets the full 5g 25s 82c!

TLDR; The Exploit

- The buyer and seller can be the same account!
- What does this mean?
- Account 1 Lists 10 items up for sale at 1,000 gold per item
- Account 1 Buys 1 item at 1,000 gold and 9 at 1 copper in the same request:
- Account 1 now has all 10 items
- Account 1 now has a net gain of 10,000 – 1,000 gold = **9000 gold profit!** (rinse and repeat!)
- **Illusion of ”Scarcity” is at risk – if abused then the economy will be broken**

Illusion of Scarcity at Risk

- Supply shift possible
  - Worst case: to infinity



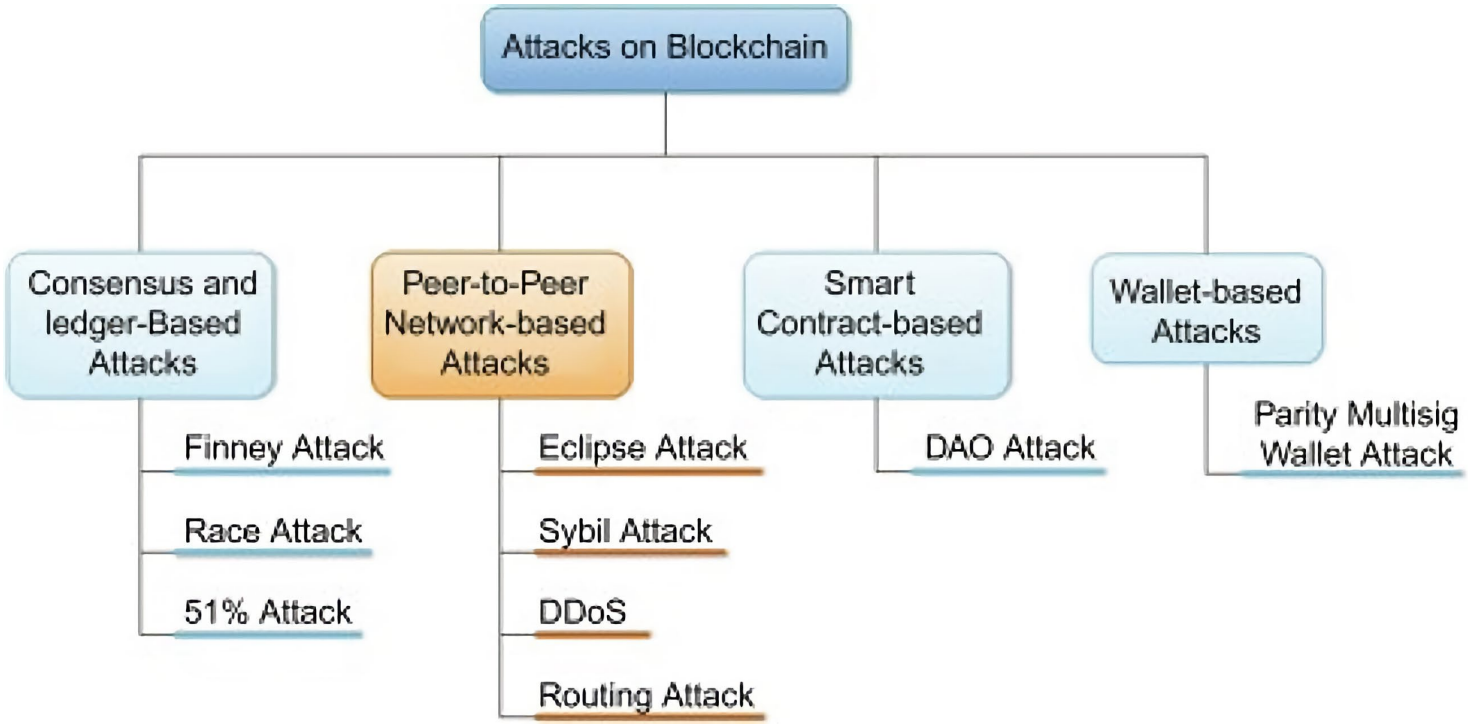
RSAConference2022

Blockchain Economy

3-10 Billion USD lost/stolen in 2019/2020/2021

Threats against blockchain economies

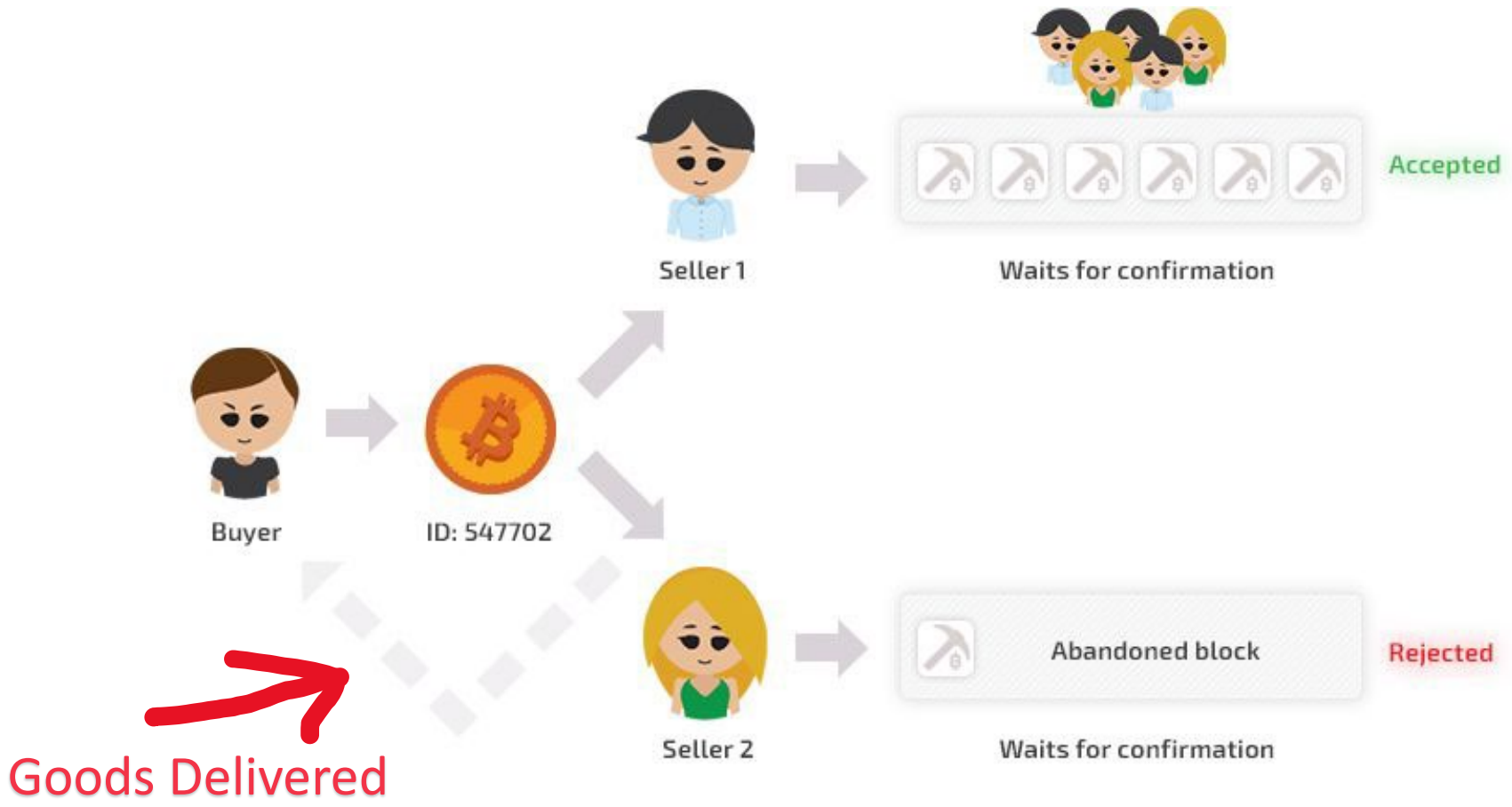
- Blockchain network itself
- User wallet attacks
- Smart contract attacks
- Cryptographic failures



Finney Attacks and Race Attacks

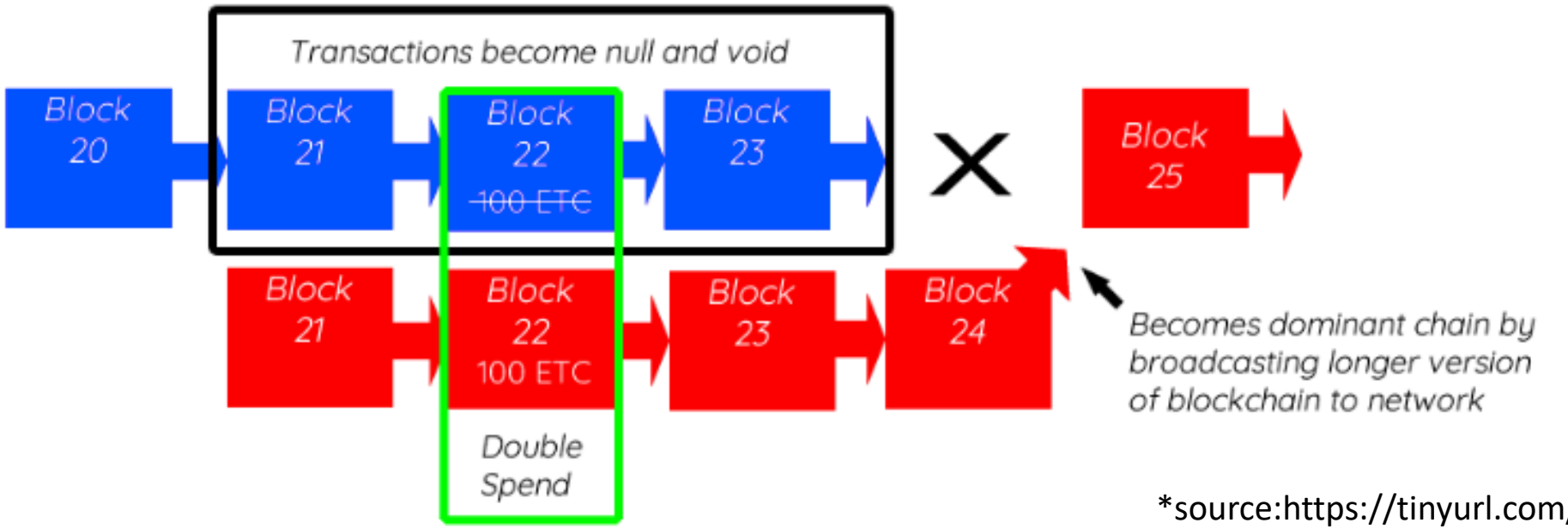
- Double Spend Attack

*source:https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors



51% Attack (Blockchain Unique)

- Goal is to
  - 1: Spend Virtual Currency and Receive Goods
  - 2: Reject the transaction that spent the virtual currency

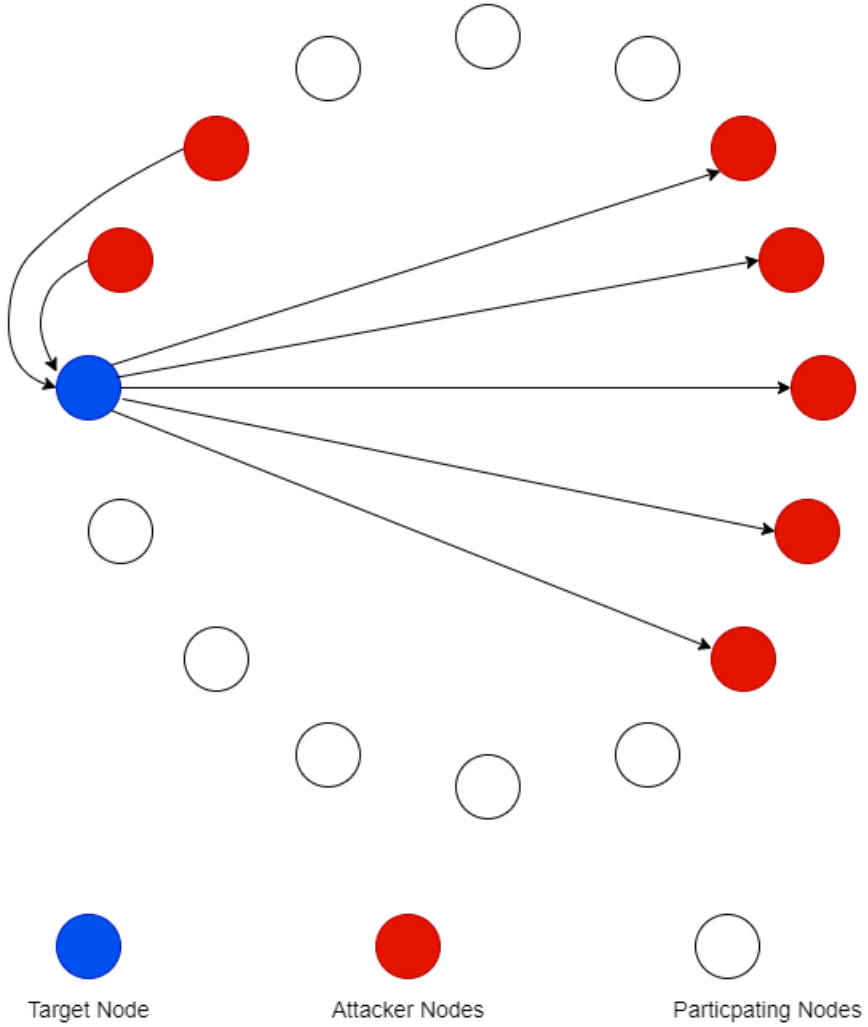


*source:https://tinyurl.com/ykj6jv29

Eclipse/Sybil/Routing Attacks

- Goal is to influence a node to fetch an alternate view of the blockchain from other attacker-controlled nodes
- This allows an attacker to:
  - Double spend to steal goods and services
  - Disrupt a blockchain network
    - Miners
    - Reputation

*source:https://www.geeksforgeeks.org/what-is-an-eclipse-attack/



DAO attacks

- What is a DAO?
  - Decentralized Autonomous Corporation
  - An entity defined by code?
  - I like to think of it as a vending machine in the cloud
    - Participants can interact with it
    - Participants can govern and alter its behavior through voting
- Popular DAO example:

UNISWAP

Wallet Attacks

- Wallets are defined by private keys
  - If someone get your private key, they can:
    - See your virtual currency balance
    - Transfer all your virtual currencies
- Popular attack vectors
  - Malware
  - Phishing
  - Fake wallet hardware and/or software

RSAConference2022

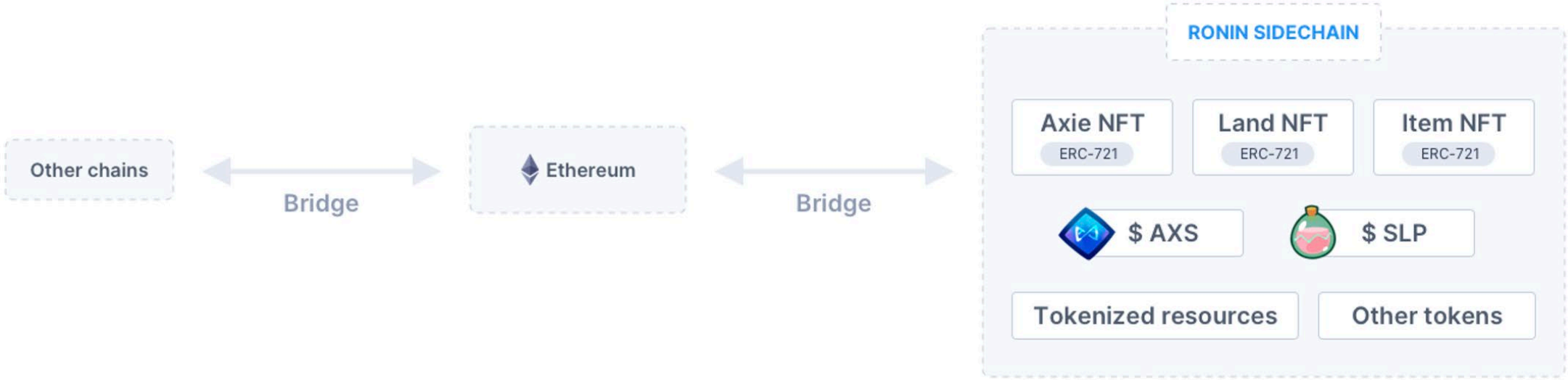
Case Study

Axie Infinity

- Blockchain game
- Has its own currency ”AXS”
  - Tradeable for Ethereum

Axie Infinity

- Sidechain structure with an Ethereum bridge
- Ethereum wallet compromised
  - Social engineering attack to steal private keys
- Result: 600,000,000$ Lost



RSAConference2022

Web2/Web3 Summary

Web 2 Incidents

MMO	Launched	Integer	Access	Data Race
Ultima Online	1997	✓	✓	✓
Asherons Call	1999			✓
Dark Age of Camelot	2001	✓	✓	✓
Anarchy Online	2001	✓	✓	
Final Fantasy Online (XI)	2002	✓	✓	✓
Asherons Call 2	2002			✓
Shadowbane	2003	✓	✓	✓
Lineage 2	2003	✓	✓	
World of Warcraft	2004	✓	✓	
Lord of The Rings Online	2007	✓	✓	

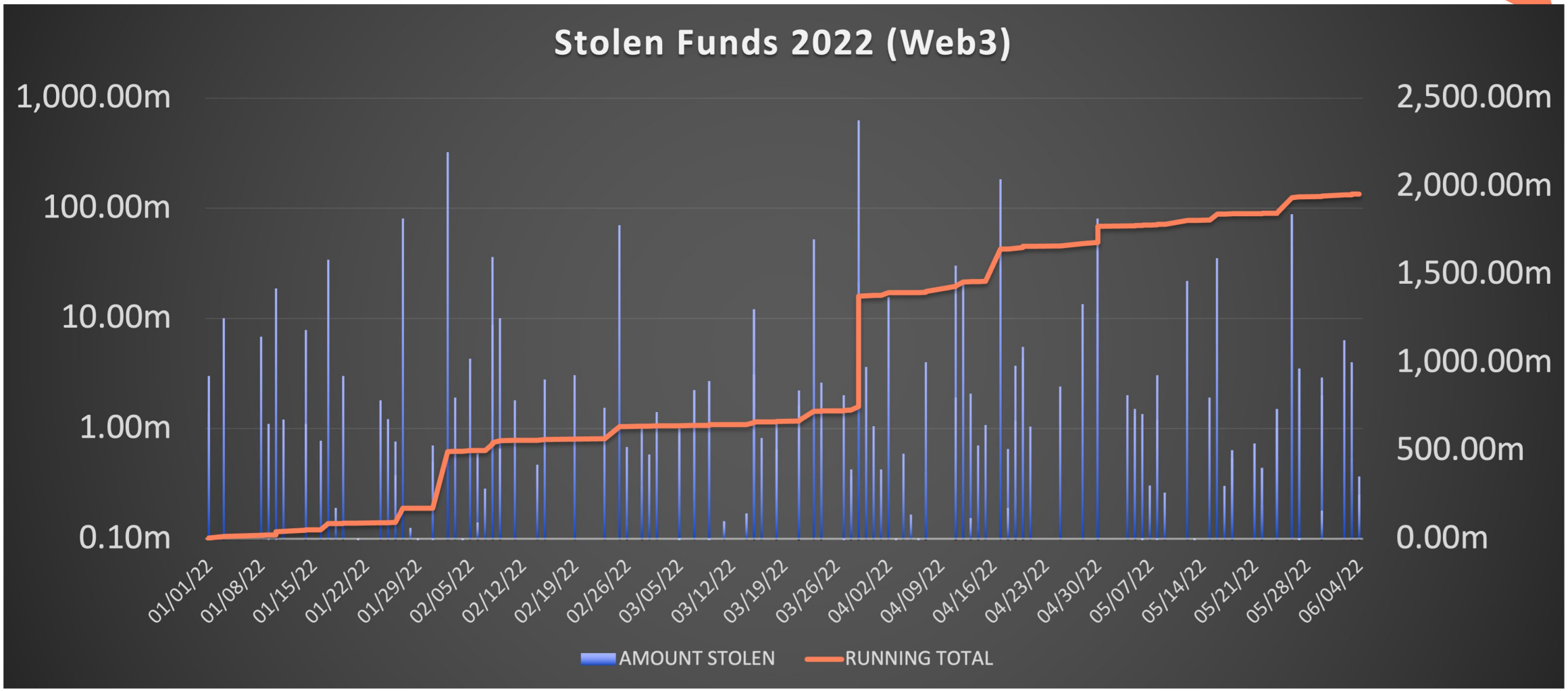
Web 2 Incidents

MMO	Launched	Integer	Access	Data Race
Age of Conan	2008	✓	✓	
Darkfall: Unholy Wars	2009	✓	✓	
Final Fantasy Online (XIV)	2010	✓	✓	✓
Star Wars the Old Republic	2011	✓	✓	
Rift Online	2011	✓		
Guild Wars 2	2012	✓	✓	
Age of Wushu	2013	✓		
Wildstar	2014	✓	✓	
Elder Scrolls Online	2014	✓	✓	

Web 2 Summary (1997-2017)

- This is from my perspective
- ~180 economic exploits found in total
- ~5-10 economy breaking exploits per game
  - Average lifespan for an exploit before detection ~2 months
    - Some have run for multiple years. (12 years for one)
- Interesting sidenote:
  - The more an economic system relied on ‘bolt-on’ anti cheat detection the more likely it was to have critical exploits

Web 3 Incidents 2022 (144 as of June 5)



*Data Source: https://web3isgoinggreat.com/

Web 3 Incidents 2022 Summary

- Average attack yield 13,580,000$
- On average there is an Attack every 26 hours
- Total value lost in 2022 ~ 2 Billion*
  - About 42 Billion if Terra/Luna is included

Protecting the Virtual Economy

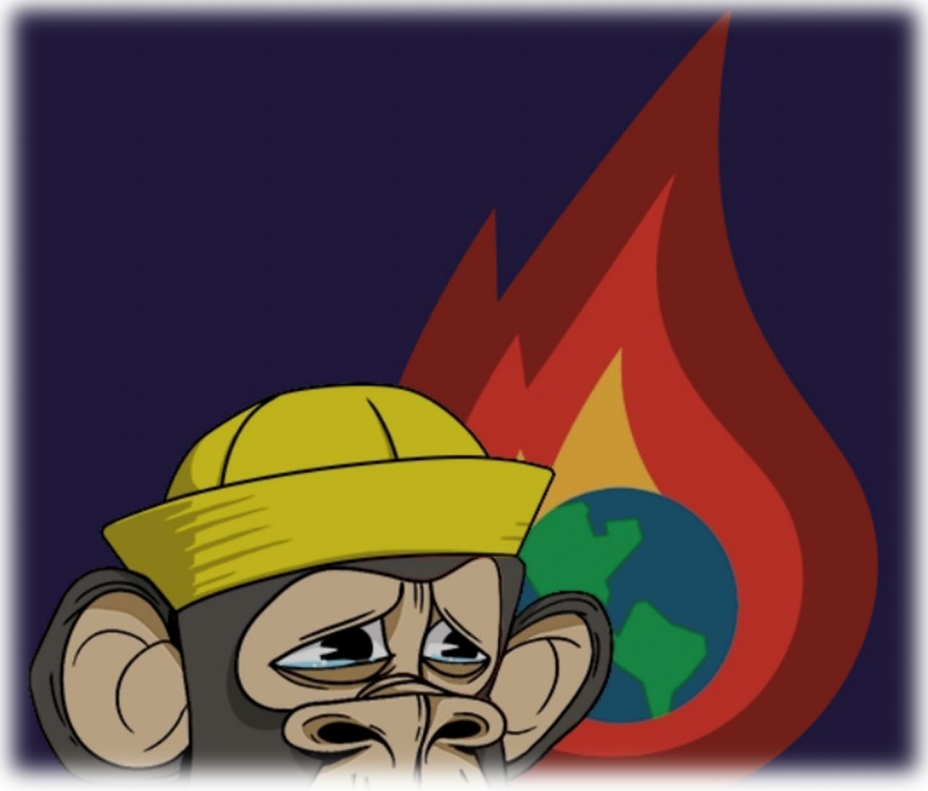
- Web 3 economic scarcity has to be maintained
- Web 2 ‘illusion of scarcity’ has to be maintained
- Violation of scarcity will lead to price crash and abandonment of economic participation by individuals

Apply What You Have Learned Today

- Next week you should:
  - Identify present or future workflows that may have interactions with internal or external virtual economies
- In the first three months following this presentation you should:
  - Catalog virtual economy items:
    - Scarce assets
    - Sources of assets and define security controls around them. Who can generate assets, how are asset generation controls enforced?
- Within six months you should:
  - Threat model and define steps to test security guarantees provided by systems that interact with ‘scarce’ assets

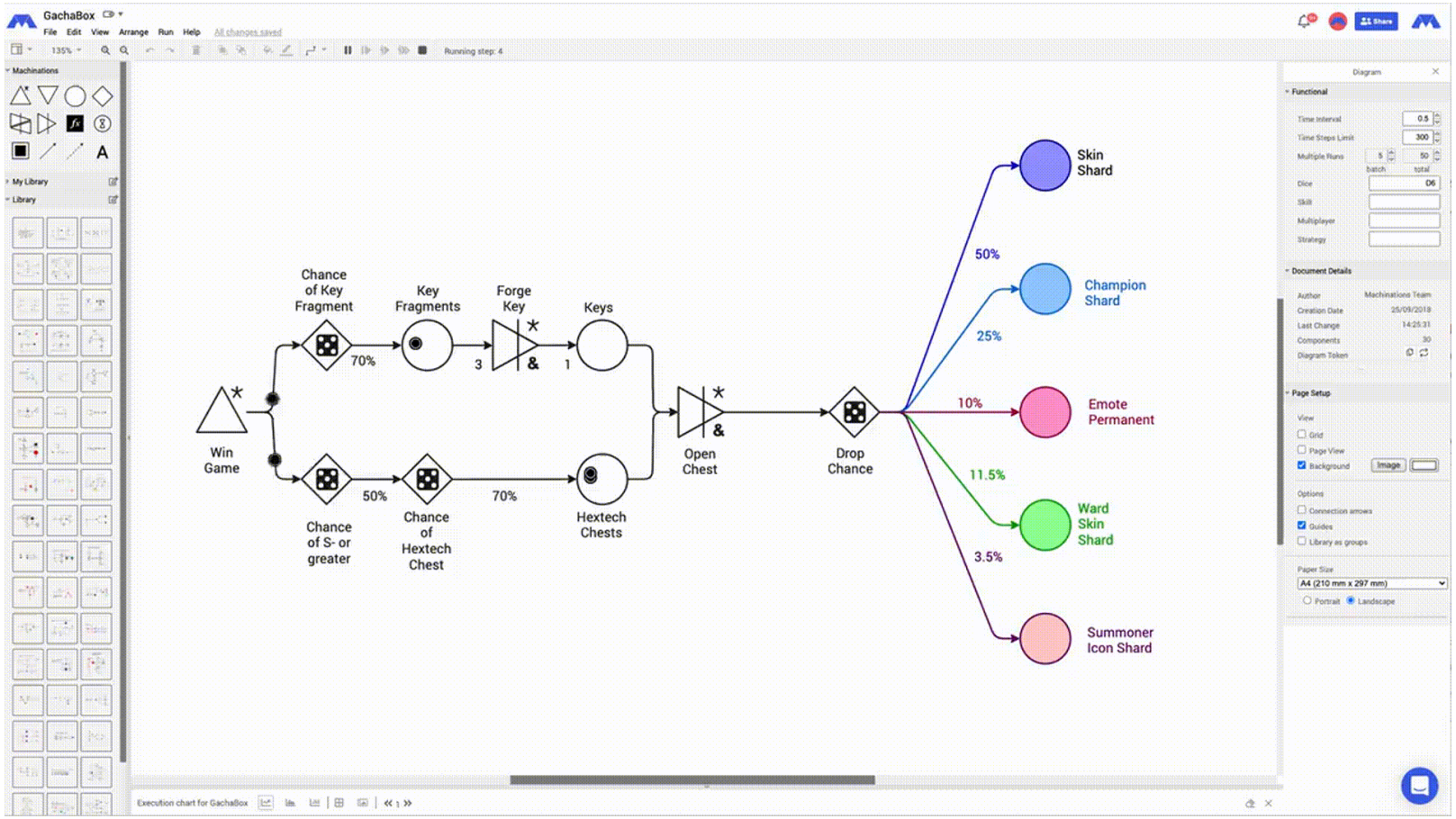
Additional Resources

- https://web3isgoinggreat.com/
- Seems like satire but its not
  - Covers the struggles of web3 as it matures



Additional Resources

- https://machinations.io/ -- Economic Modeling



RSAConference2022

Thank You!

Adrian Bednarek

https://www.linkedin.com/in/adrianbksd/