



# Two Sides of the Same (Bit)Coin

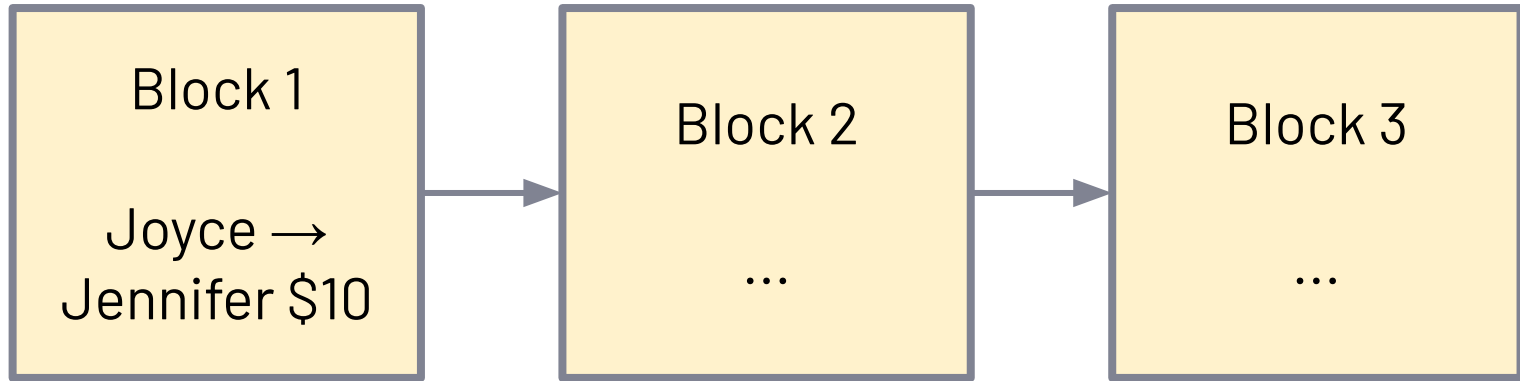
Joyce and Jennifer



# Bitcoin as a Technology

Advanced and secure development

# Bitcoin Technology: The Blockchain



# Open-Sourced Technologies

## Kerckhoffs' Principle

- “A system should be secure even if everything about the system, *except the secret key*, is a public knowledge”

## Security through Obscurity

- To hide the design of the system in order to achieve security

# Decentralisation

**Distributed technologies** are highly valued in recent years.

- **No single point of failure**

[illegible]

### B. Consensus Protocols

In a distributed system comprising of independent and mutually distrusting nodes, having the nodes agree on some data that is crucial for the operation of the system is challenging, even more so in the presence of node failures. An extensive body of research, especially on *distributed consensus protocols*, has been dedicated to address a variety of fault tolerance problems in distributed systems [19, 20]. There are two types of failures a node may undergo, namely *crash failure* and *Byzantine failure*. The former characterizes situation in which a node abruptly stop and does not resume [19], while the latter, which is more disruptive in comparison with the former,

# Cryptographic Primitives

Reduce a complex system to its cryptography

Bitcoin (Elliptic Curve Cryptography) is proven to be existentially unforgeable

Using the chosen message attack we ask the attacker to come up with an **existential MAC forgery**. That is, the attacker need only come up with some *new* valid message-tag pair  $(m, t)$ . By “new”, we mean a message-tag pair that is different from all of the signed pairs. The attacker is free to choose  $m$  arbitrarily; indeed,  $m$  need not have any special format or meaning and can be complete gibberish.

# Bitcoin is...

- (1) Open-Sourced
- (2) Distributed System
- (3) Based on Cryptographic Primitives

**A good, well-designed piece of technology**

# Joining the Bitcoin Network

Bought bitcoins → sold it within 2 months

Didn't understand and feared the fluctuating  
Bitcoin prices





Four thick, dark blue horizontal bars stacked vertically on the left side of the slide.

# Bitcoin as a Currency

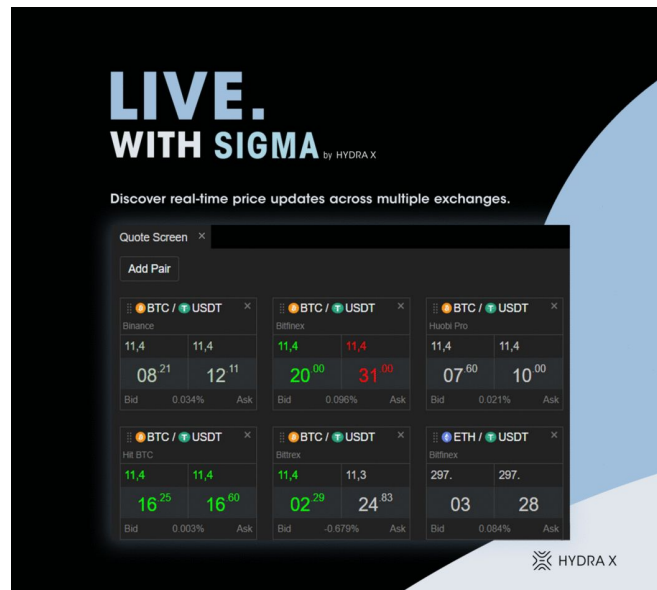
Speculation and Self-Contradictory Design



# Year 2 Summer – Internship


Hydra X – Marketing Intern

- Fintech software startup company
- I was tasked to design a **Cryptocurrency marketing campaign**



# Highly skeptical: Scams, Viruses, Illegal Activities

While scanning through possible marketing channels

Type of Channel	Channel/Group Name/Username	Board	Size of channel	Content Posted
Forum	<a href="https://bitcointalk.org">Bitcointalk.org</a>	Trading Discussion	706841 Posts 27906 Topics	<ul style="list-style-type: none"> <li>1) Tips for local transaction, helpful technical guides for bitcoin transfer, reviews for exchanges</li> <li>2) Serious discussions on trading bitcoin i.e strategies (but not much technical analysis, a lot of speculation from "feel", general advice)</li> <li>3) Scam accusations</li> <li>4) Recommendations for sites for charting, technical analysis, trading bots to practice trading</li> </ul>
		Altcoin Disucssion	2864681 Posts 92261 Topics	<ul style="list-style-type: none"> <li>1) Ways to reduce risk from altcoin investment</li> <li>2) How to be safe from viruses/scams</li> </ul>
	<a href="#">CryptoCurrency: Crypto Trading, ICO, News, Predictions, Bitcoin and Altcoin</a> -		73, 931 members	<ul style="list-style-type: none"> <li>1) Posts seeking opinions e.g. What do you think will increase adoption of cryptocurrencies / do you think this dip will last etc</li> <li>2) Memes galore: <ul style="list-style-type: none"> <li>- Memes reacting to market and prices, sharing common trading problems e.g. not sleeping enough; or egging for alts to rise</li> <li>- Memes that mock lower-skill traders e.g. those who panic-sell after a small dip, which the better traders will rush in to buy at a lower price</li> <li>- Memes that recall the heydays of Bitcoin when it was at its peak + memes that place hope in BTC that the best is yet to come</li> <li>- Memes about crypto's superiority over fiat/certain tokens' superiority</li> </ul>  </li> <li>3) News updates e.g. scam exchanges that made away with many people's savings</li> <li>4) Posts asking if something is a scam because there are scammers in the group</li> </ul>

# Highly skeptical: Scams, Viruses, Illegal Activities

While scanning through possible marketing channels

## 3) Scam accusations

1) Ways to reduce risk from altcoin investment

2) How to be safe from viruses/scams

3) News updates e.g. scam exchanges that made away with many people's savings

4) Posts asking if something is a scam because there are scammers in the group

# Highly skeptical: Speculation, Cult-like Behaviour

FOMO (Fear of Missing Out), FUD (Fear, Uncertainty and Doubt)

Persona[ptorea]	Desc	Backgrounds	Say	Do	Think & Feel	Read	Feel	Pains
Complete beginners	Completely new to trading market	New to trading and jumping into cryptocurrency market due to its associated high profits	"What exchanges do you use?" "What's a good token to buy?" "what's a good trading strategy"	Place trades in small amounts, practice trading first before investing in a lot of capital	Scared to take large risks, shocked when see prices fluctuate so much	Forums, Reddit, Investopedia, social media	Some level of uncertainty, FOMO, etc	Scams security
FOMO group	Essentially followers. People who buy in certain ideas/tradings strategies due to trend.	People who are interested to earn a quick buck but don't have the technical expertise for high-commitment trading, they make up large majority of Crypto community	"I bought (token) at (higher price level) :(" "When are you guys selling?" "Is it ok to sell at \$___?" "Why is BTC falling?" "Will BTC keep falling?"	High-frequency transactions  More prone to panic selling, very reactive to slight market movements	When BTC drops however little, they tend to panic more Tend to do as the crowd does	Forums, Reddit, Twitter, the more general ones, big threads like r/bitcoin Follow opinion-leaders	Fear when prices fall so rapidly	Market fluctuations, sensitive to market prices, Fear, uncertainty and doubt (FUD)  When the community (websites with opinion leaders/influencers) recommends it
I-want-the-freebies group	People who collect any digital token/ cryptocurrency for low cost in the event that they will rise in value in the future	Often don't have a strong understanding of what they are investing in. They just anyhow throw the fishing net in the sea hoping to catch at least one fish.	They would only spread the word if you have something to gain from it	Collect all digital tokens, even if they ulu ulu	Very excited when there are giveaways. Will snatch for it.	Forums, Facebook groups	To get returns, an investment must be made	Winning free things  Free.



# Highly skeptical: Speculation, Cult-like Behaviour

FOMO (Fear of Missing Out), FUD (Fear, Uncertainty and Doubt)

Essentially followers. People who buy in certain ideas/tradings strategies due to trend.

People who are interested to earn a quick buck but don't have the technical expertise for high-commitment trading, they make up large majority of Crypto community



# Highly skeptical: Speculation, Cult-like Behaviour

## Dogecoin soars to record high as Elon Musk fires off new tweet

NEW YORK (BLOOMBERG) - Dogecoin rose to all-time high on Sunday (Feb 7) as Tesla co-founder Elon Musk tweeted "Who let the Doge out" amid the rally.

The Shiba Inu-themed digital coin surpassed 8 cents for the first time, just a week after crashing to 2.5 cents and sparking an outcry on Reddit. It rose 53 per cent in the last 24 hours to 8.2 cents as of 5:45pm in New York on Sunday, according to CoinMarketCap data, breezing through its recent record of 7.8 cents posted in late January.



# Year 3 Sem 1 – ISM

Increasing  
centralization  
as miners pool  
resources  
together to  
share risk

## MINING POOLS



**20**

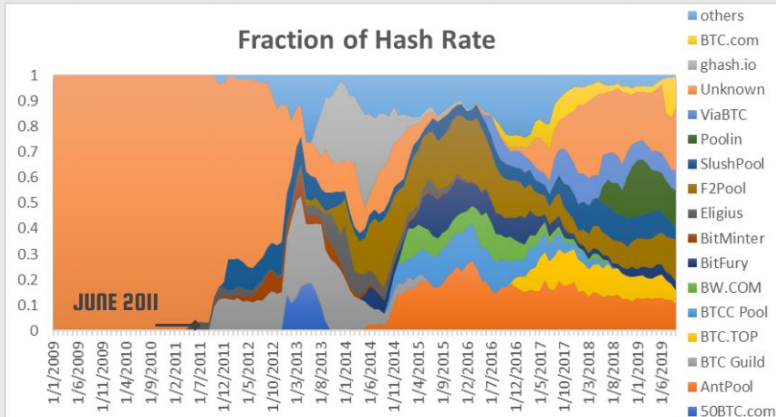
Major Mining Pools



**81%**

Controlled by Chinese pools

Fraction of Hash Rate





# Highly Skeptical: Self-Contradictory Design

Mining pool

- 1) Same returns
- 2) Lower risk

## MINING POOL

$$\pi_{solo} (\text{in USD}) = x * p_{win} * \sum_{i=1}^Q (B + \tau_i) - (a(T) + b(T) * Q), \quad p_{win} = \frac{\text{Miner's } T}{\text{Total } T}$$

$$\pi_{pool} (\text{in USD}) = x * p_{win} * \frac{\text{Miner's } T}{\text{Pool's } T} * \sum_{i=1}^Q (B + \tau_i) - (a(T) + b(T) * Q), \quad p_{win} = \frac{\text{Pool's } T}{\text{Total } T}$$

$$\pi_{pool} (\text{in USD}) = x * \frac{\cancel{\text{Pool's } T}}{\text{Total } T} * \frac{\text{Miner's } T}{\cancel{\text{Pool's } T}} * \sum_{i=1}^Q (B + \tau_i) - (a(T) + b(T) * Q)$$



Mathematically equivalent

# Dismissive of Financial “Innovation”

**A giant Ponzi scheme, money created out of “thin air”**

Worried for disastrous real economic consequences

- The mismanagement of mortgage-backed securities was what resulted in the 2008 Global Financial Crisis

Could Bitcoin be the next trigger?





# Changed Perspectives

Bitcoin - A technological force, but an economic controversy

## A more nuanced perspective of Bitcoin

Jennifer: More **appreciative** of tech behind innovations

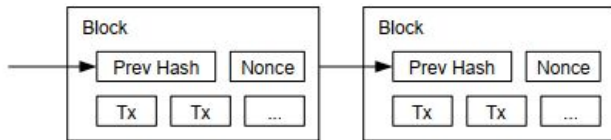
Joyce: Designing tech cannot be an **isolated endeavour**.

# A more nuanced perspective of Bitcoin

## 4. Proof-of-Work

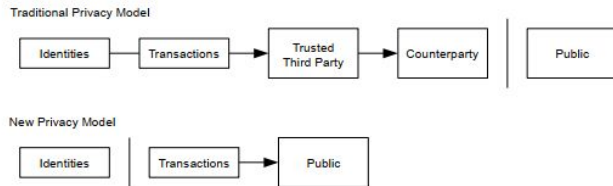
To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



## 10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.



# Meta-Reflection



The Dual Nature of a Specialisation +  
Multidisciplinary Education



## Put the disciplinary in multidisciplinary

Depth of perspectives formed from **systemic thinking reinforced by our majors**

Breadth + **depth** of discussion

1. Specialisation
2. Communication between specialisations

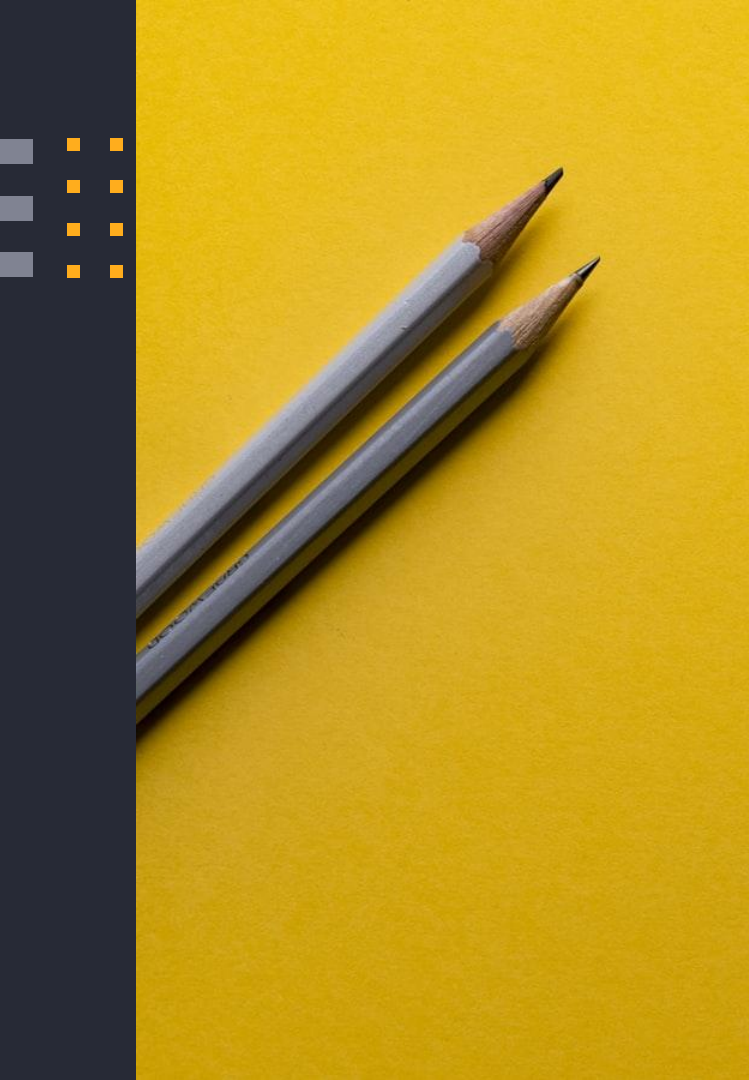
# Multidisciplinary Collaboration

**Extracting key ideas**

**Reducing the jargon**







# Thanks!

Any questions?