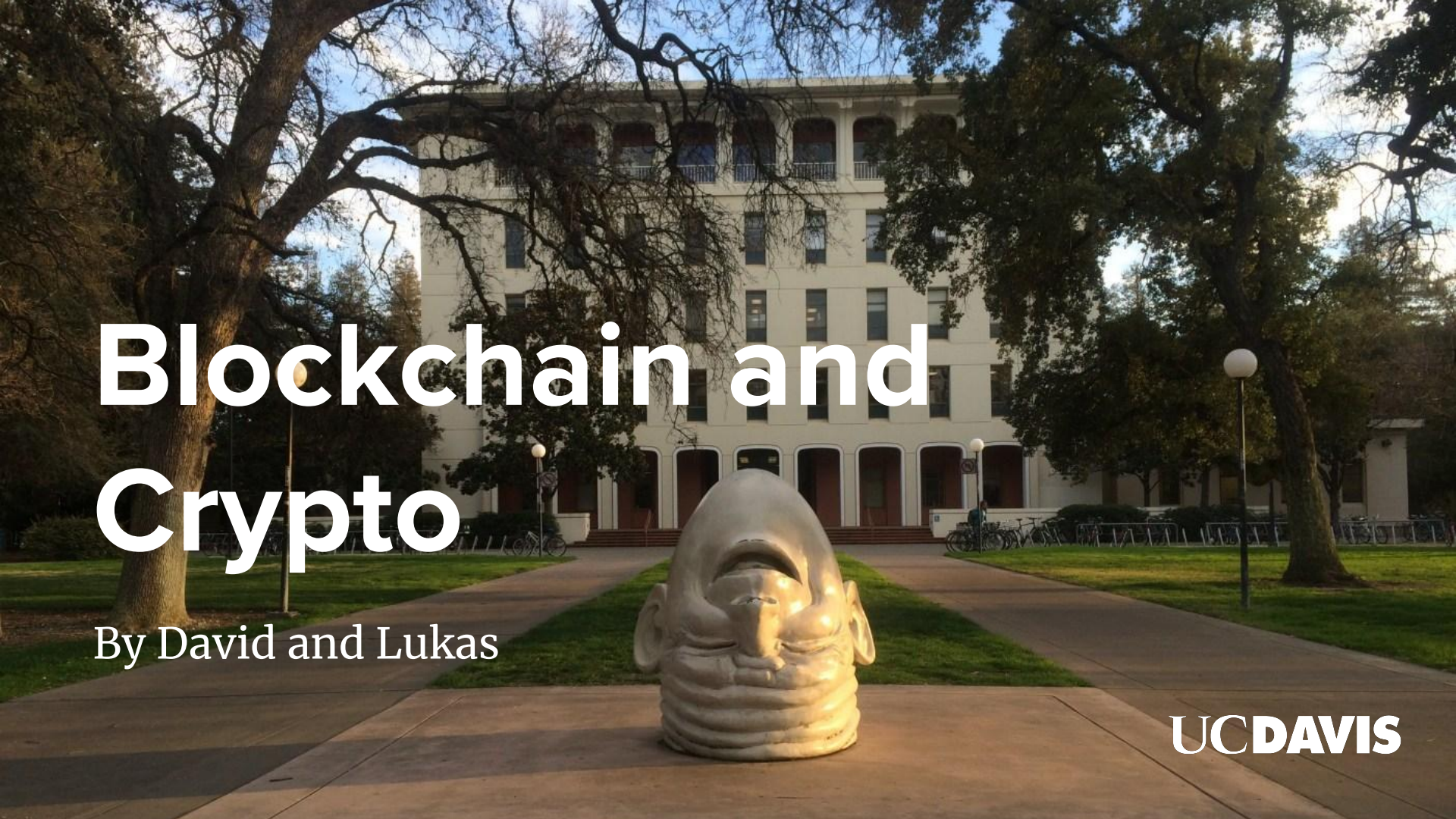


Blockchain and Crypto

By David and Lukas

UCDAVIS

Blockchain and Crypto

By David and Lukas

UCDAVIS
UNIVERSITY OF CALIFORNIA

Topics

- Overview
  - What is Bitcoin?
  - What is a Blockchain?
- Blockchain and Bitcoin In-Depth
  - Transactions
  - New Blocks
  - Forks
- Nakamoto’s Forerunners
- Smart Contracts

Overview

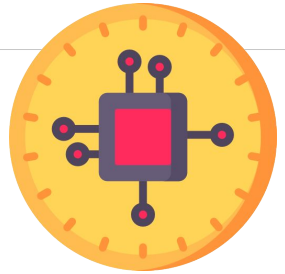
Blockchain & Bitcoin

UCDAVIS

What is Bitcoin?

What is Bitcoin?

2009

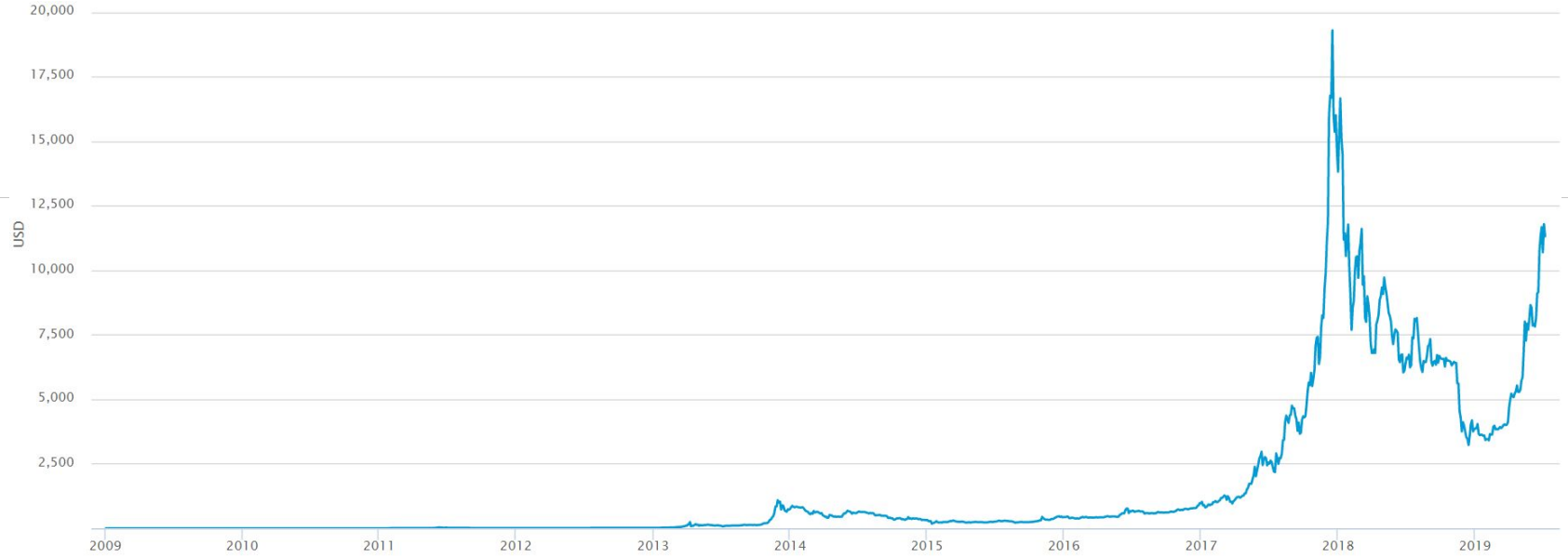


Digital,
Stored in
Bitcoin Wallets

Mining

No centralized
Banking

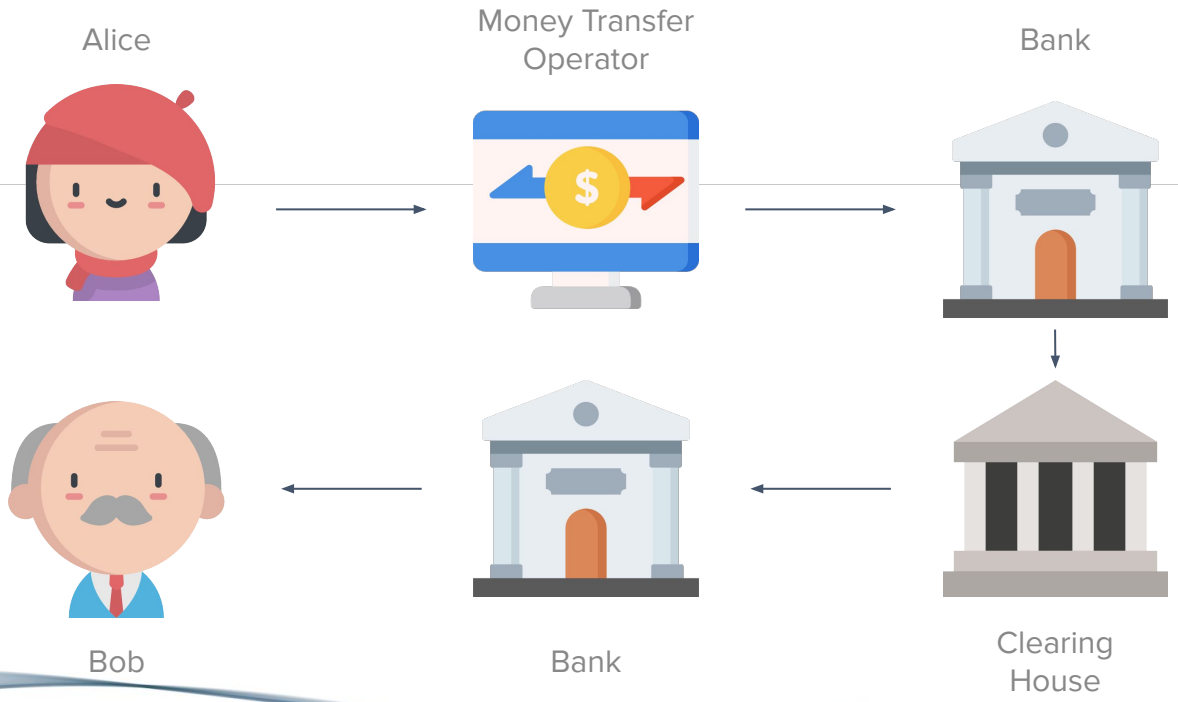
What is Bitcoin?



Source: https://upload.wikimedia.org/wikipedia/commons/0/01/Bitcoin_usd_price.png

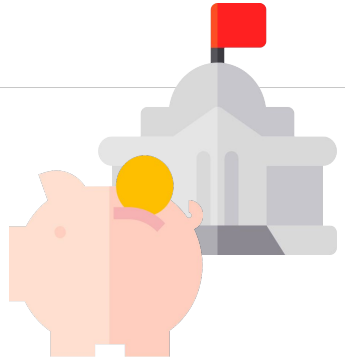
What about traditional banking?

International Bank Transfer

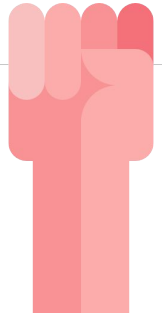


Why bother?

Why bother?

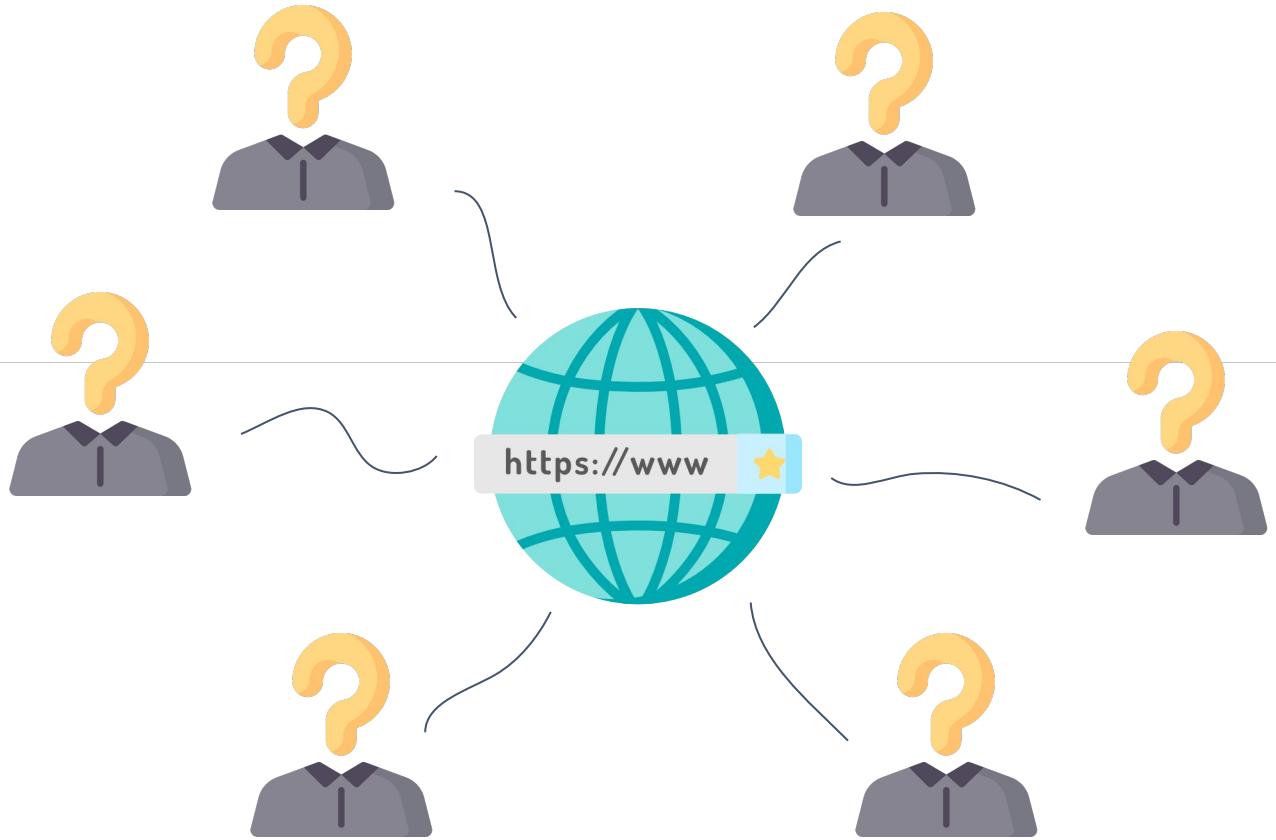


Political Issues



Independence

Availability

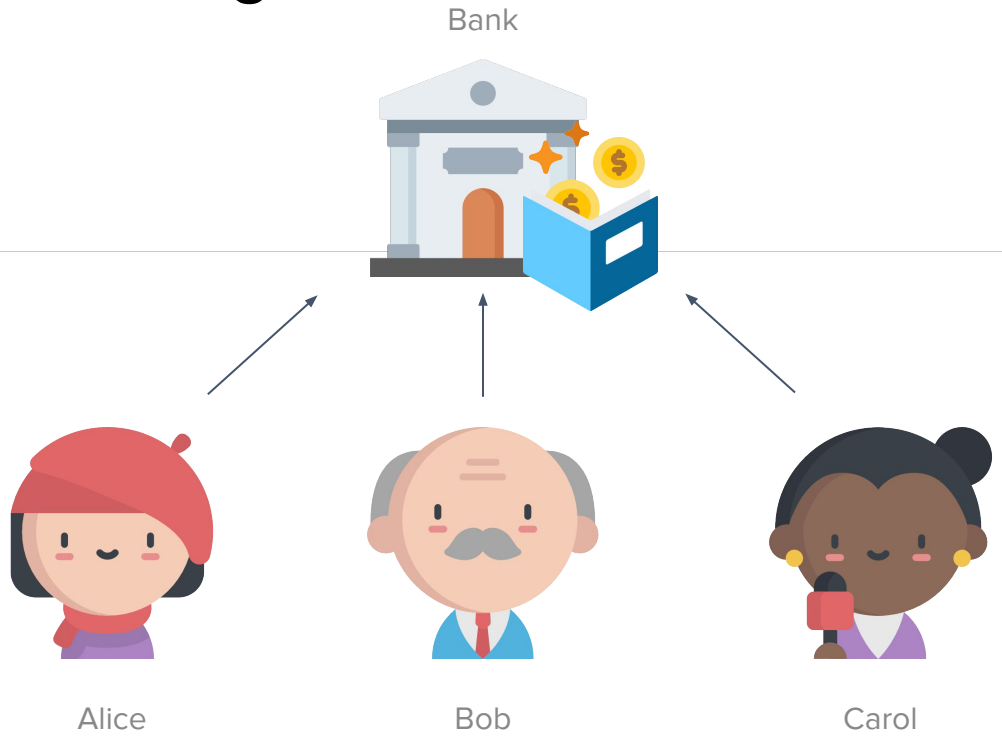

https://www

“On the Internet, nobody knows you’re a dog.”

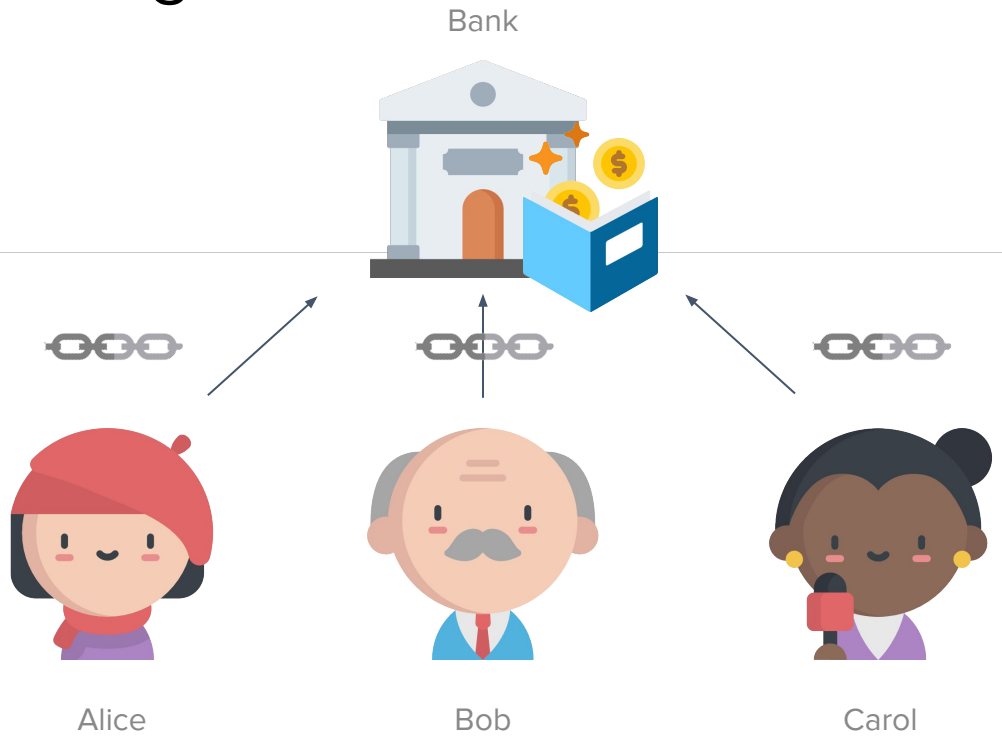
- Peter Steiner, The New Yorker 1993

What is a Blockchain?

Traditional Banking

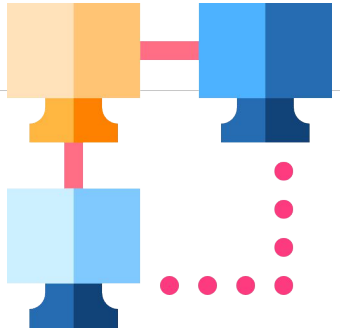


Distributed Ledger



Blockchain Attributes

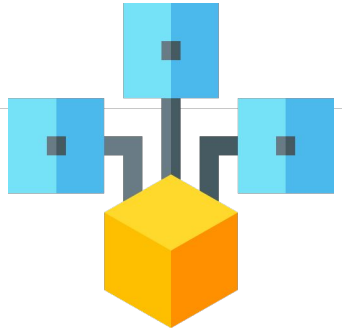
Immutable



Distributed

Consensus

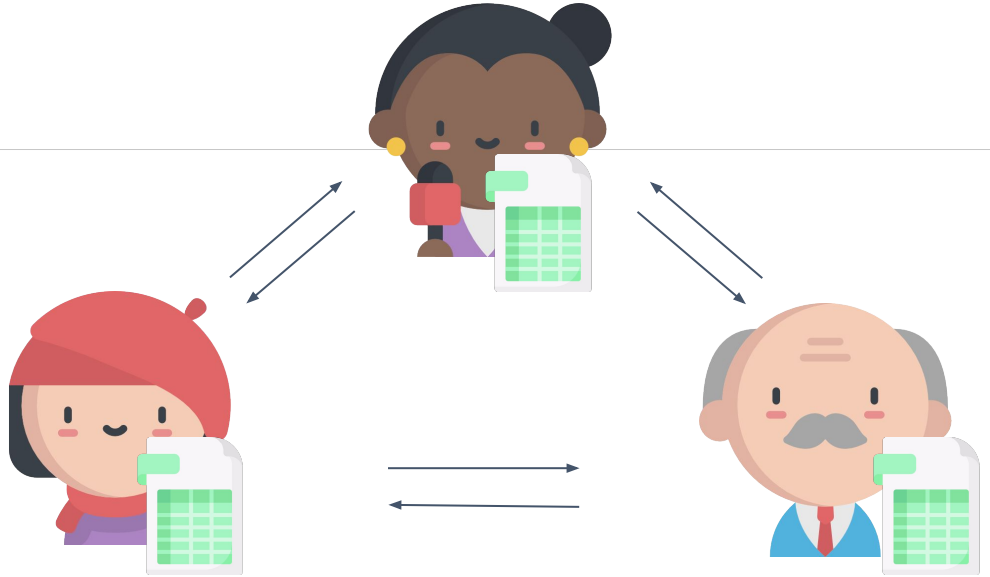
Blockchain Attributes



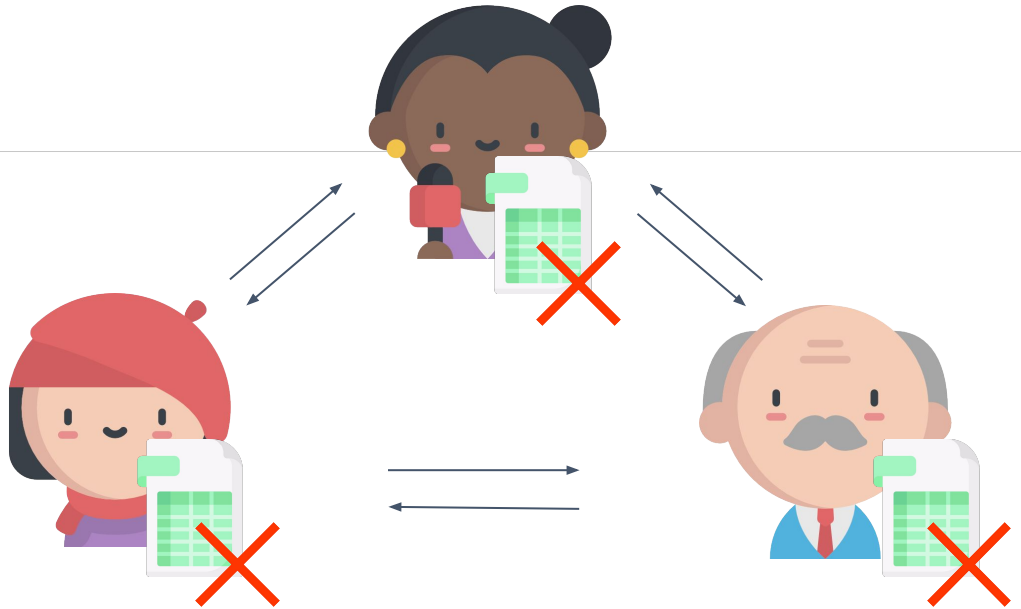
Peer-To-Peer

Cryptographically Secured

Shared Ledger

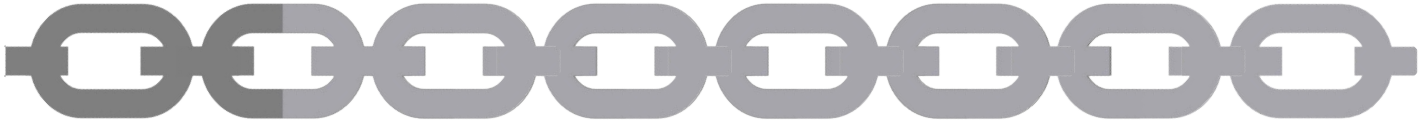


Shared Ledger



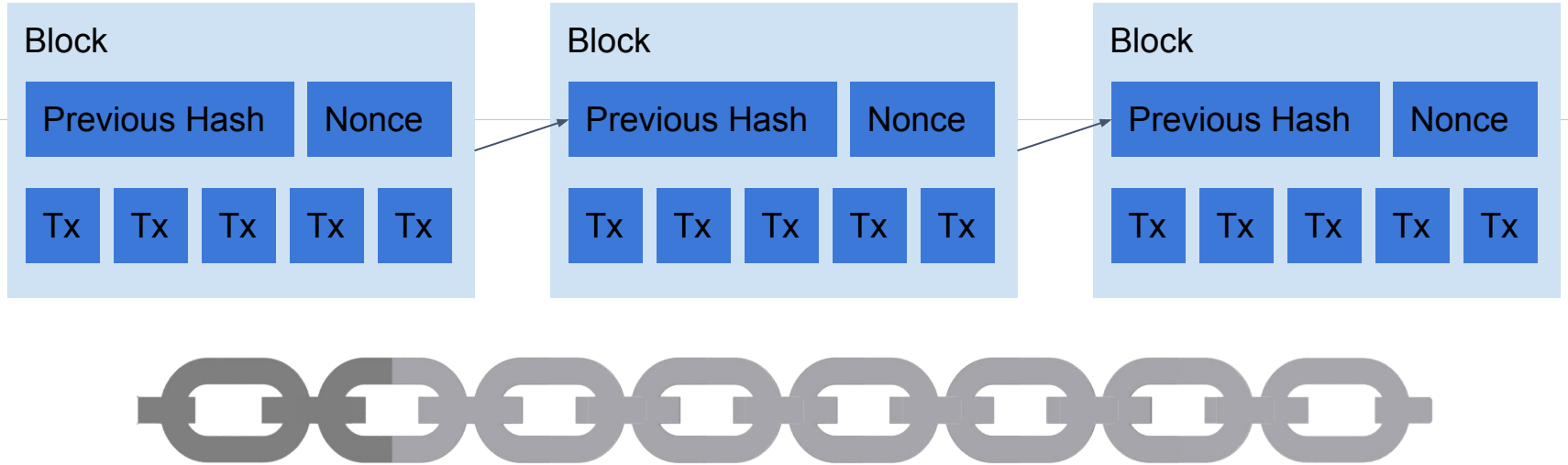
How does it work?

How does a Blockchain work?

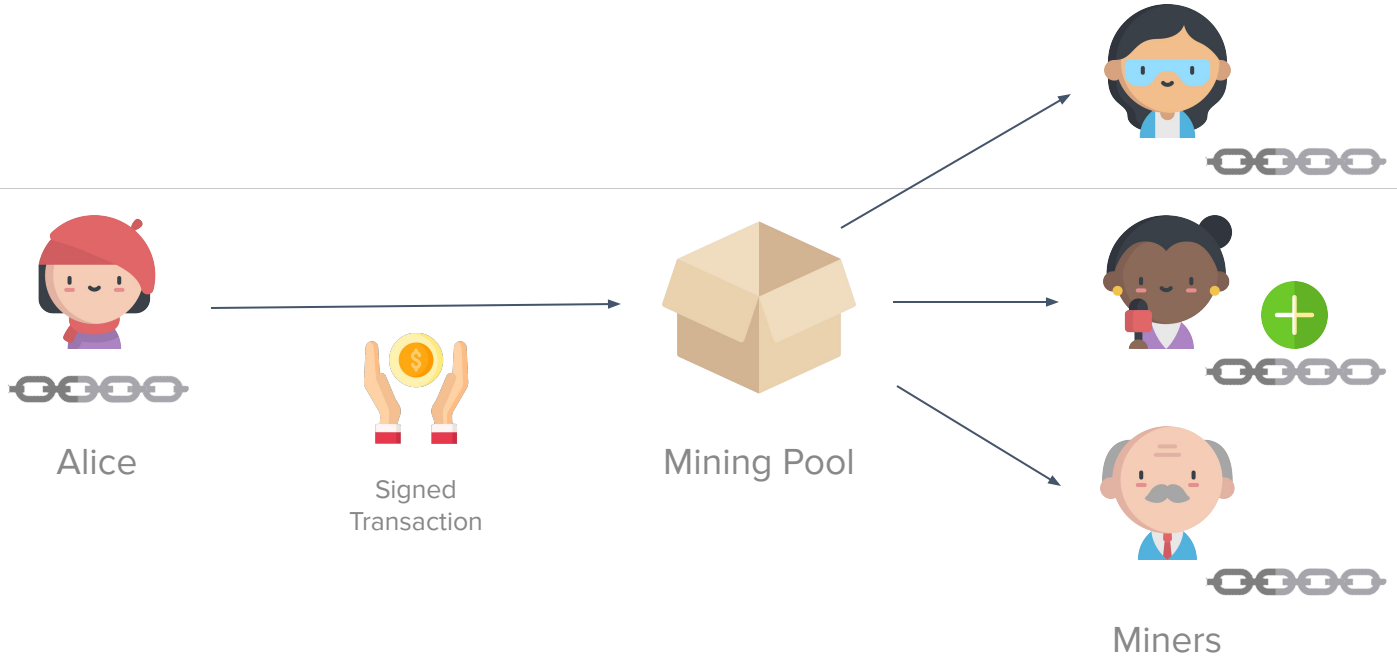


Genesis
Block

How does a Blockchain work?



How does a transaction work?



Blockchain and Bitcoin

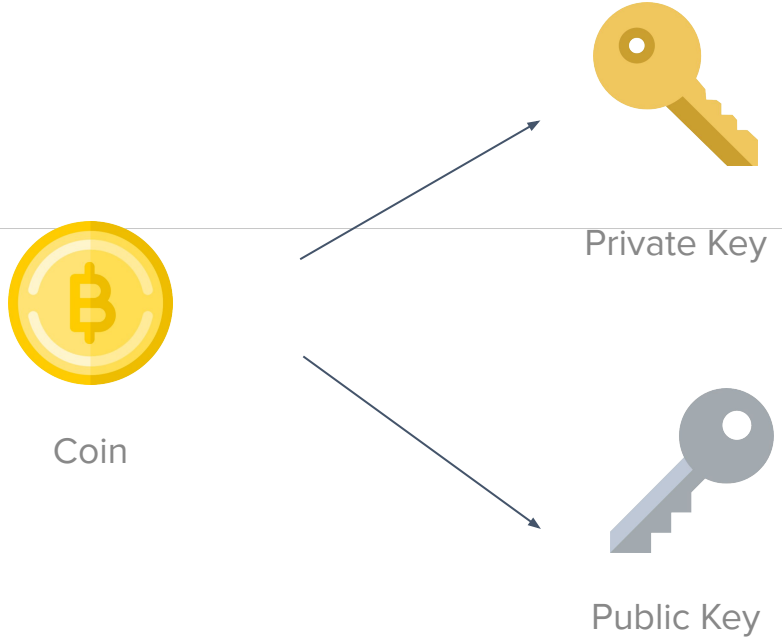
A closer Look

UCDAVIS

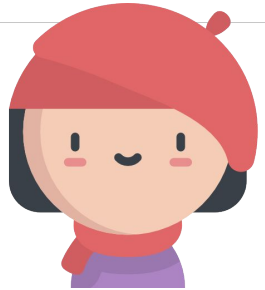
Transactions

Private Key: Signature
Knowledge confers Ownership

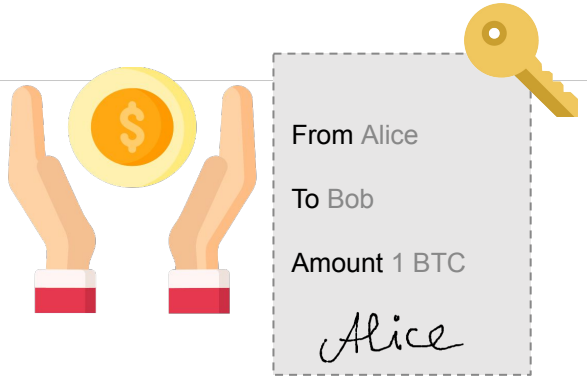
Public Key: Verification
Proof of Ownership

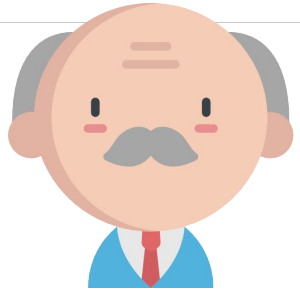


Transactions



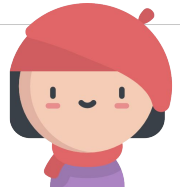
Alice





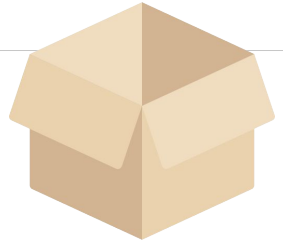
Bob

Transactions



Alice

Signed
Transaction



Mining Pool

Transactions

Value (Coins) represented by Key Pairs

Sender creates transaction message

Message signed and verifiable

Package stored in Mining Pool

Eventually, Transaction added to the Blockchain

Adding new Blocks

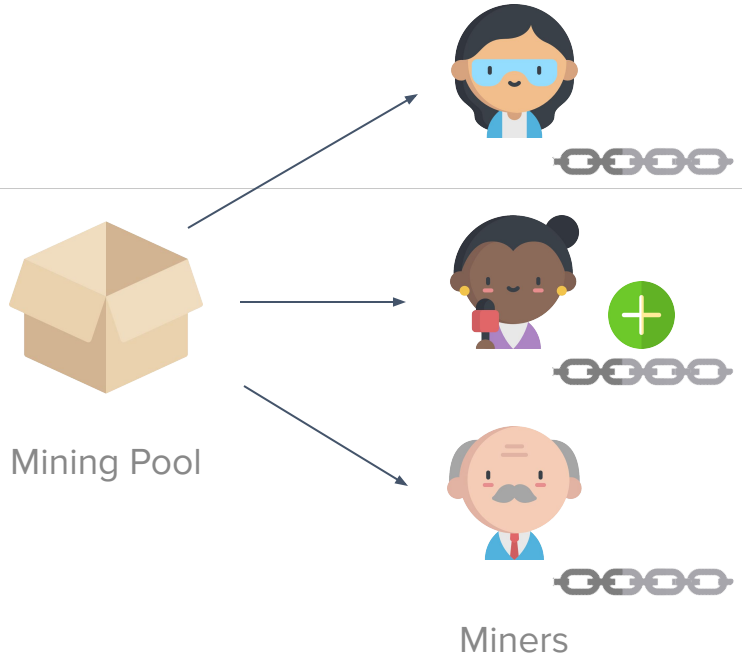
Mining: Proof of Work (PoW)

Work: Computing Hashes

Goal: Find specific Hash

Incentive (BFT): Reward

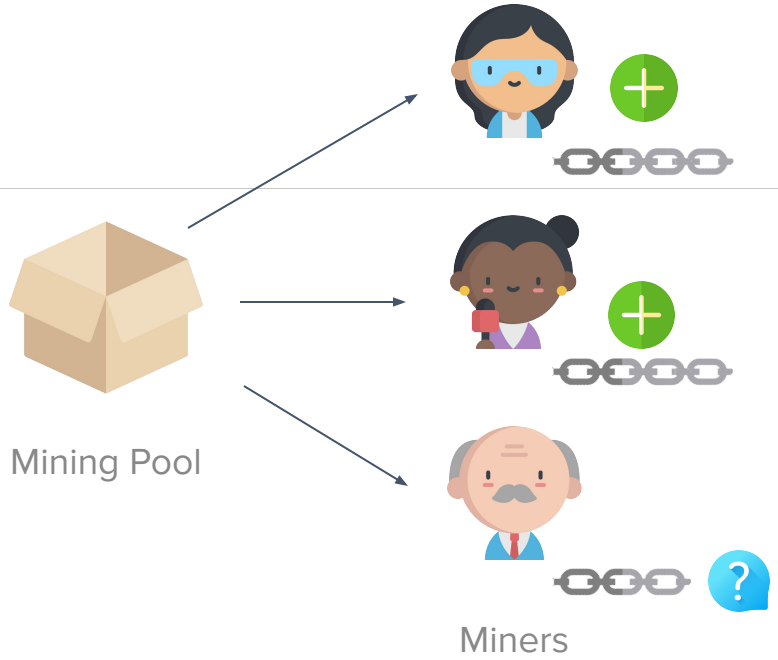
Winner publishes new block on the blockchain and is rewarded with BTC



Forks

Two Miners solve simultaneously:
chain is forked

Approaches: longest chain wins, etc.



Ledger

Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

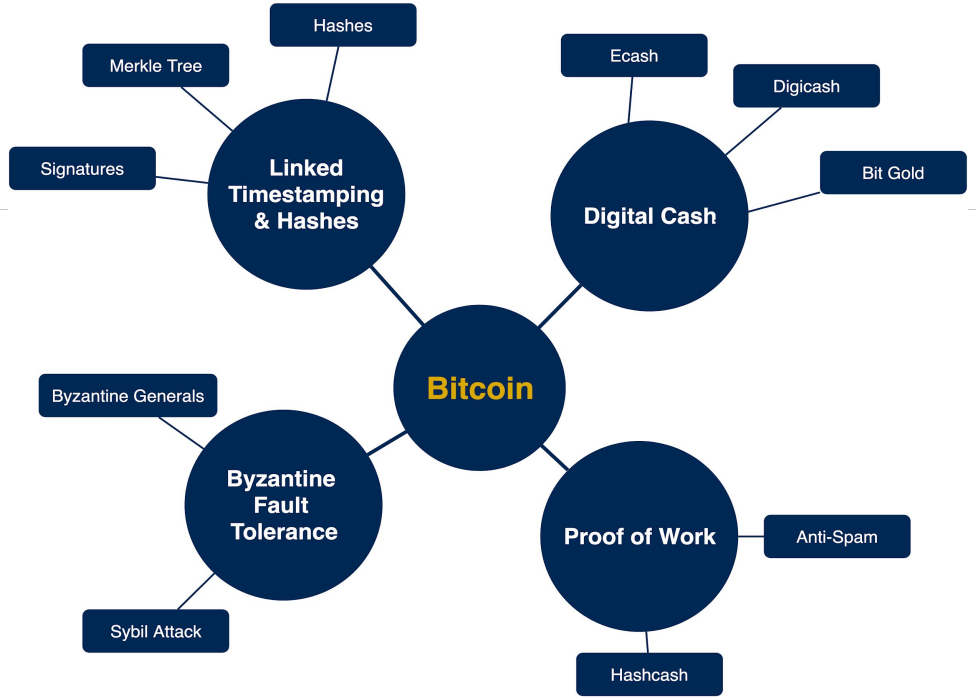
Carol

Nakamoto’s Forerunners

Bitcoin and its Academic Roots

UCDAVIS

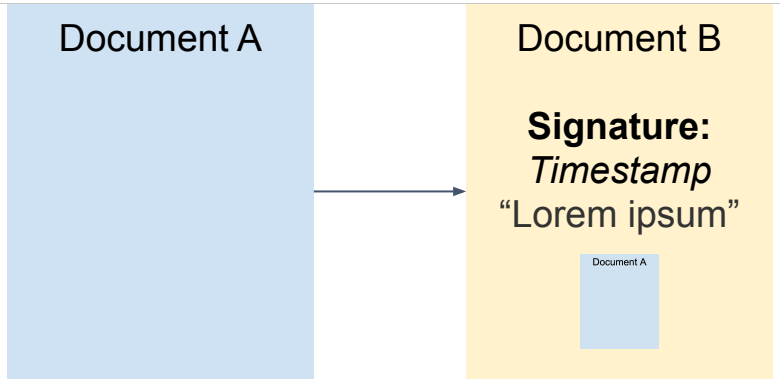
Bitcoin's Roots in Academia



Linked Timestamps & Hashes

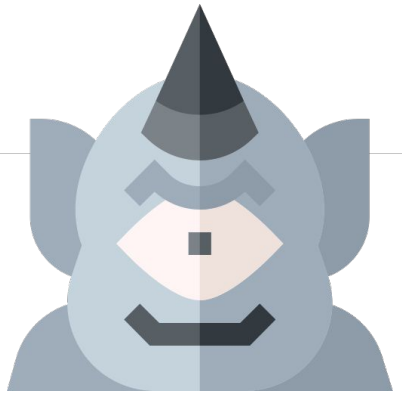
Original Idea: Signatures

Simplification: Hashing



How to timestamp a Digital Document
Haber & Stornetta 1991

Byzantine Fault Tolerance



How can we handle faulty or deviant members in a distributed system?

Byzantine Fault Tolerance

There will be a WHOLE talk on this topic 🤯

Lots of research and no definitive consensus

Notable work: The Byzantine Generals Problem, Lampert

Nakamoto solves this using **Proof of Work**

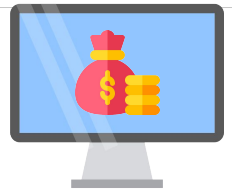
Proof of Work

Avoid Spam Mail through PoW
Work: Signature
Dwork & Naor 1992

Hashcash
Work: Hash-Functions
Back 1997

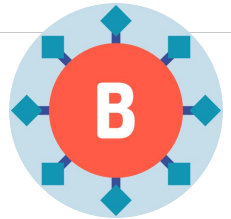
Digital Cash

There are several precursors of Bitcoin!

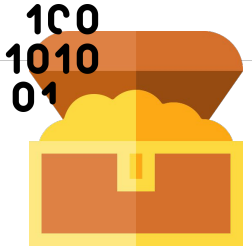


Ecash
Chaum 1983

Hashcash
Back 1997



B-Money
Dai 1998



Bit Gold
Szabo 2008

Smart Contracts

Distributed Software on Blockchain

UCDAVIS

Smart Contracts

Instead of simple transactions, just run code on the blockchain!

Contracts: small programs

Deployed to the blockchain (immutable)

Peers can interact with the contract via transactions

Lots of possibilities

Thanks.

Feel free to ask and discuss!

UCDAVIS
UNIVERSITY OF CALIFORNIA

References

Presentation Template: “UC Davis Presentation Template - 8/17/2018” from Google Drive

Title image: https://i0.wp.com/www.dailycal.org/assets/uploads/2016/02/IMG_5721.jpg?w=1404&ssl=1

“UC Davis” Logos and Marks: http://marketingtoolbox.ucdavis.edu/docs/logo-files/UC_Davis_Wordmarks.zip

Icons: All Icons made by Freepik from www.flaticon.com

Video: https://www.youtube.com/watch?time_continue=1&v=I9jOJk30eQs

Literature:

Arvind Narayanan and Jeremy Clark. 2017. Bitcoin's academic pedigree. Commun. ACM 60, 12 (November 2017), 36-45. DOI: https://doi.org/10.1145/3132259

Maurice Herlihy. 2019. Blockchains from a distributed computing perspective. Commun. ACM 62, 2 (January 2019), 78-85. DOI: https://doi.org/10.1145/3209623

UCDAVIS

Additional Information

Questions asked during class

Additional Information

Q1) How to keep honest miners from adding fake/no/wrong transactions to the blockchain?

Q2) If the blockchain forks are nodes separated into two groups and do they stay part of the same node network?

Q3) Where in the peer network are smart contracts executed?

Q1) How to keep miners in check

We used this article to find the answer:

https://bitcoin.stackexchange.com/questions/67768/how-does-the-protocol-prevent-miners-from-building-off-of-a-fraudulent-blockchai

The gist of it is that miners who would produce wrong/malicious blocks or add wrong or no transactions will just be ignored by the honest nodes in the network (the block won't validate). Thus, the incorrect block will not be published throughout the network.

Q2) How nodes react to chain forks

We used this article to find the answer:

https://bitcoin.stackexchange.com/questions/75394/how-do-the-nodes-divide-after-a-hard-fork-soft-fork

There are hard and soft forks. When we speak of hard forks it really means that the disagreeing nodes split into two separate networks. If the systems experiences a soft fork it makes sure that the new fork is backwards compatible and transactions are valid in both chains.

For accidental forks, the rule of the longest chain still applies.

Q3) Where smart contracts are executed

We used this article to find the answer:

https://ethereum.stackexchange.com/questions/20781/at-which-point-the-smart-contracts-get-executed

Basically, the mining node executes the contract code and adds any output to the next block it mines.
The code is then re-executed by every validating node in the network.