BLOCKCHAIN TECHNOLOGY

AN OVERVIEW

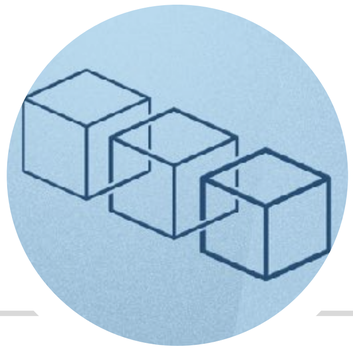
6-JAN-2016

ABOUT ME

Leonard Tan
Digital Consultant

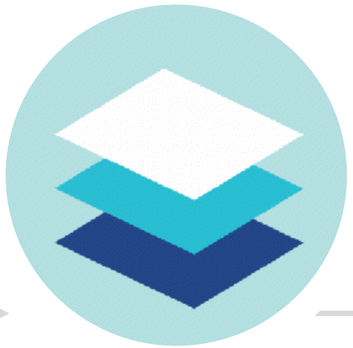
DDP in BSc(Econs) and BBM(Finance) @ SMU
Hack Reactor Graduate
FintechNews & CoinHako

OVERVIEW



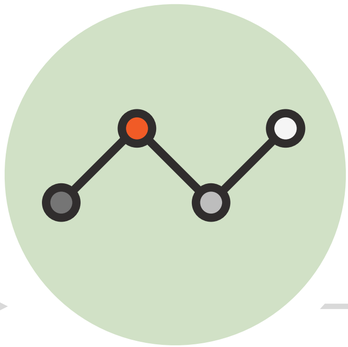
Blockchains
A technical explanation

1. Distributed ledger
2. Blockchain Structure
3. Transaction Structure
4. Nodes
5. Summary



Emerging Technology
Bitcoin 2.0

1. Smart Contracts
2. Anonymous transactions
3. Tokens
4. Off-chain transactions
5. Sidechains



Industry Trends
Risks and responses

1. Scalability
2. Centralisation
3. Regulation
4. Bitcoin vs Altcoins
5. Peripheral services

Future Direction
A blockchain strategy

1. Public vs private blockchains
2. Blockchain consultants
3. Strategic positioning
4. Conclusion

Blockchains

a technical explanation

1. Distributed ledger
2. Blockchain structure
3. Transaction structure
4. Nodes
5. Summary

Distributed Ledgers

- A digital ledger is a digital record of **who** owns **what**
- A **distributed** digital ledger is a ledger that is shared among many nodes
  - The main innovation is the underlying distributed consensus mechanism

- Related to the *Byzantine General's Problem* in computer science
  - Resolved by several algorithms in the past (Coin-flip, Paxos, Chubby, BFT, PBFT)

Distributed Ledgers

- However, besides distributed consensus, blockchains also:
  - **Scale** relatively better than existing consensus algorithms
  - **Compensate** for the costs of verifying and generating consensus
  - **Disincentivise** attacks

- Blockchains work in practice, not theory.

Blockchains

a technical explanation

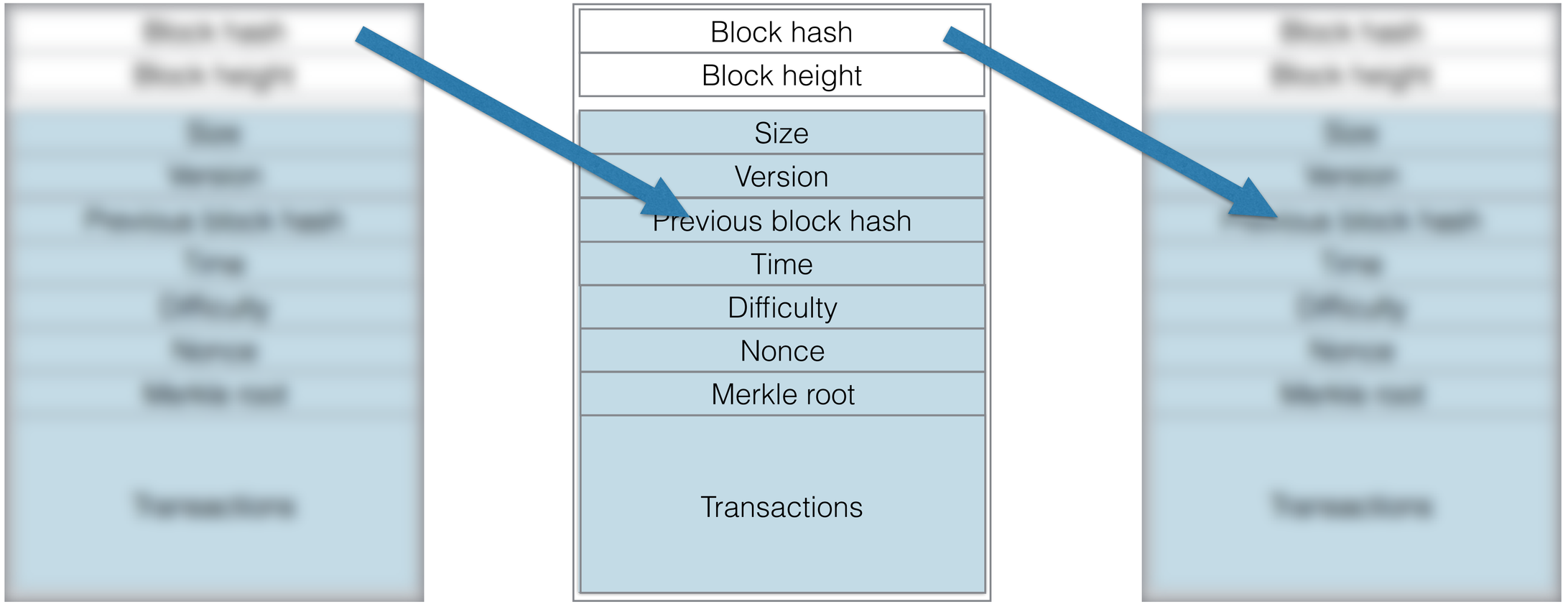
1. Distributed ledger
2. Blockchain structure
3. Transaction structure
4. Nodes
5. Summary

Blockchain structure

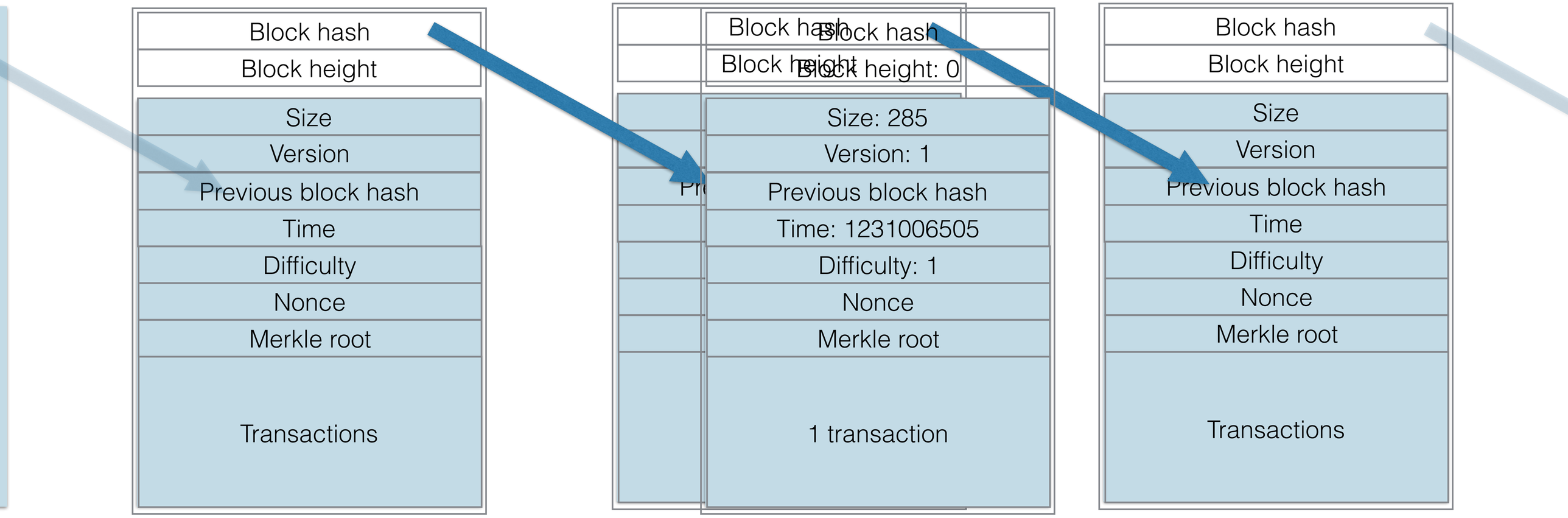
- A typical block looks like this:


```
{
"size" : 43561,
  "version" : 2,
  "previousblockhash" :
      "000000000000000027e7ba6fe7bad39fafdb5a83caed765f05f8a1b71a1632249",
  "merkleroot" :
      "5e049f4030e0ab2debb92378f53c0a6e02348aea083f3ab25e1d94ea1155e29d",
  "time" : 1388185338,
  "difficulty" : 1180923191.25802612,
  "nonce" : 4215439401,
  "tx" : [
      "257e7497fb8bc68491eb2c7b699dbab234831600e7172f0d9e6522c7cf3f6c77",

... transactions omitted ...

      "05cfd38f6ae6aa83674cc99e4d75a1458c1172bab84725eda41d018a09176634"
  ]
}
```

Blockchain structure



Blockchain structure



Blockchain structure

- Properties:
  - Only the longest chain on the network is accepted
    - It has the most “proof-of-work”
    - This can result in competing chains and orphaned blocks
    - Network consensus can only be overcome by a “51% attack”
  - Past blocks are “secure” and cannot be easily modified

Blockchain structure

- Miners get a reward for successfully “mining” a block
  - Difficulty is always adjusted so that mining rate = 1 block / 10 mins
  - The mining reward decreases over time

Note: Since a miner is only incentivised by the block reward of X, they will always try to spend X amount of resources on mining. Increasing mining efficiency will not result in less resources being “wasted” on mining.

Blockchains

a technical explanation

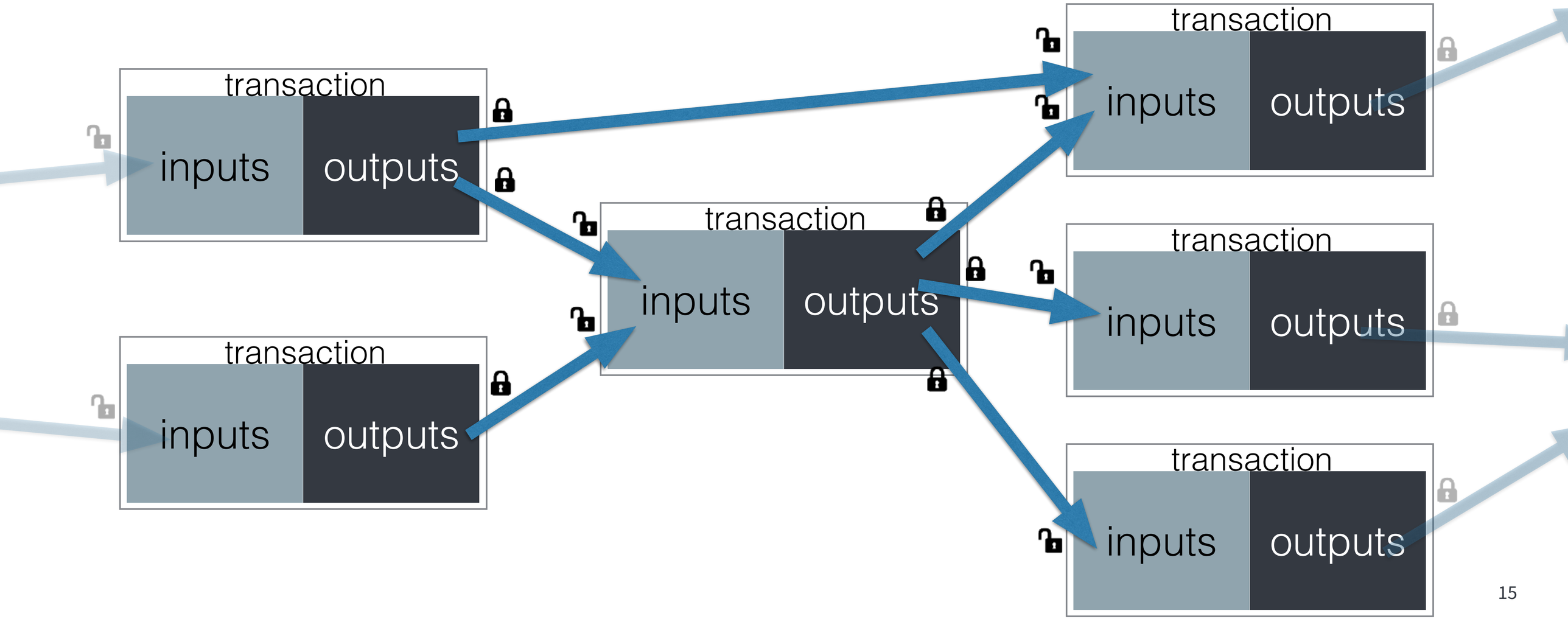
1. Distributed ledger
2. Blockchain structure
3. **Transaction structure**
4. Nodes
5. Summary

Transaction structure

- A transaction is a record that contains **inputs** and **outputs**
  - An input has to reference a previous transaction's output
    - In order to do this successfully, the correct key has to be provided

- Exception: the very first transaction in a block has no inputs and simply generates a set number of bitcoins for the miner (i.e. miner's reward)

Transaction structure



Transaction structure

- Wallet applications build on top of these simple transactions
  - To get your current balance, sum up the UTXOs that your keys can unlock
  - In order to send someone a small input when referencing a large output, create a transaction like this:
    - Large input → 2 partial outputs
      - Send one of the outputs back to yourself
  - Miner fees are implicitly calculated: outputs - inputs

Transaction structure

- These simple transactions act as building blocks to more complex transactions
  - N-of-M multisig
  - Smart contracts (by introducing new opcodes)
  - Crowdfunding

Blockchains

a technical explanation

1. Distributed ledger
2. Blockchain structure
3. Transaction structure
4. Nodes
5. Summary

Nodes

- There are an increasing variety of nodes available
- Mainly 3 different kinds of nodes:
  - Miners
  - Full nodes
  - Light nodes

Nodes

- **Full nodes** are nodes that have a record of the entire blockchain
  - The current size is about 97 GB
- **Light nodes** do not store the blockchain
  - Typically only store a small number of transactions
  - Request transaction hashes from other full nodes

Nodes

- **Miners** are **full nodes** that also try to mine the next block
- In order to successfully mine a block, you need to follow a strict protocol
  - Necessary to have access to the entire blockchain
- In theory, miners only really need access to the UTXO pool for verification
- In practice, most mining software still require miners to have all the blocks

Blockchains

a technical explanation

1. Distributed ledger
2. Blockchain structure
3. Transaction structure
4. Nodes
5. Summary

Summary

- **Transactions** contain inputs and outputs
  - Inputs always reference a previous output by providing the correct key
- **Blocks** contain transactions and a reference to a previous block
  - only accepted by the network if the hash is smaller than the target
  - the chain of blocks is the **blockchain**
- **Nodes** are either **full nodes** or **light nodes**
  - Full nodes hold the entire blockchain, light nodes do not

Emerging Technology

Bitcoin 2.0

1. Smart contracts
2. Anonymous transactions
3. Tokens
4. Off-chain transactions
5. Sidechains

Smart contracts

- Smart contracts are **conditional payments**
  - If <Event A is true> then <output is valid>
  - More complex conditions can be created using
    - Timestamps
    - Oracles
    - References to other contracts
    - Outputs that are contracts

Smart contracts

- Ethereum is a cryptocurrency with **Turing-complete** smart contracts
  - They are capable of doing any computation
  - Costs of calculation are fuelled by “gas”
  - Examples: Augur, DAO

Smart contracts

- How is this different from traditional contract settlement?
  - No central point of control
  - Increased transparency
  - Decreased costs of verification
  - Increased flexibility

Smart contracts

- Blockchains have no built-in way of incorporating external information
- Limits the variety of smart contracts
- Solution: Oracles
  - A trusted third party supplies external information
    - Augur’s rating system
    - Intel’s SoftwareGuard Extensions enabled hardware
      - Town crier

Emerging Technology

Bitcoin 2.0

1. Smart contracts
2. Anonymous transactions
3. Tokens
4. Off-chain transactions
5. Sidechains

Anonymous transactions

- Since every transaction needs to reference a previous transaction, bitcoins leave a **transaction trail**
- Using graph analysis, it is possible to associate people with transactions
- Especially because of “change” outputs
- Solution: Bitcoin laundries
  - CoinJoin/ZeroCash

Emerging Technology

Bitcoin 2.0

1. Smart contracts
2. Anonymous transactions
3. Tokens
4. Off-chain transactions
5. Sidechains

Tokens

- A token is a bitcoin that also represents some other resource
  - The value of that resource is more than its value in bitcoin
  - Used for trading and managing real-world assets
- Leverages normal bitcoin transactions by adding some metadata
- Requires a trusted third party to verify assets
- Requires a special node to make sense of token transactions

Tokens

- 3 step process:
  - Creation transaction
  - Transfer transaction
  - Proof-of-burn (redemption)
- Examples: **Colored coins/CounterParty**

Emerging Technology

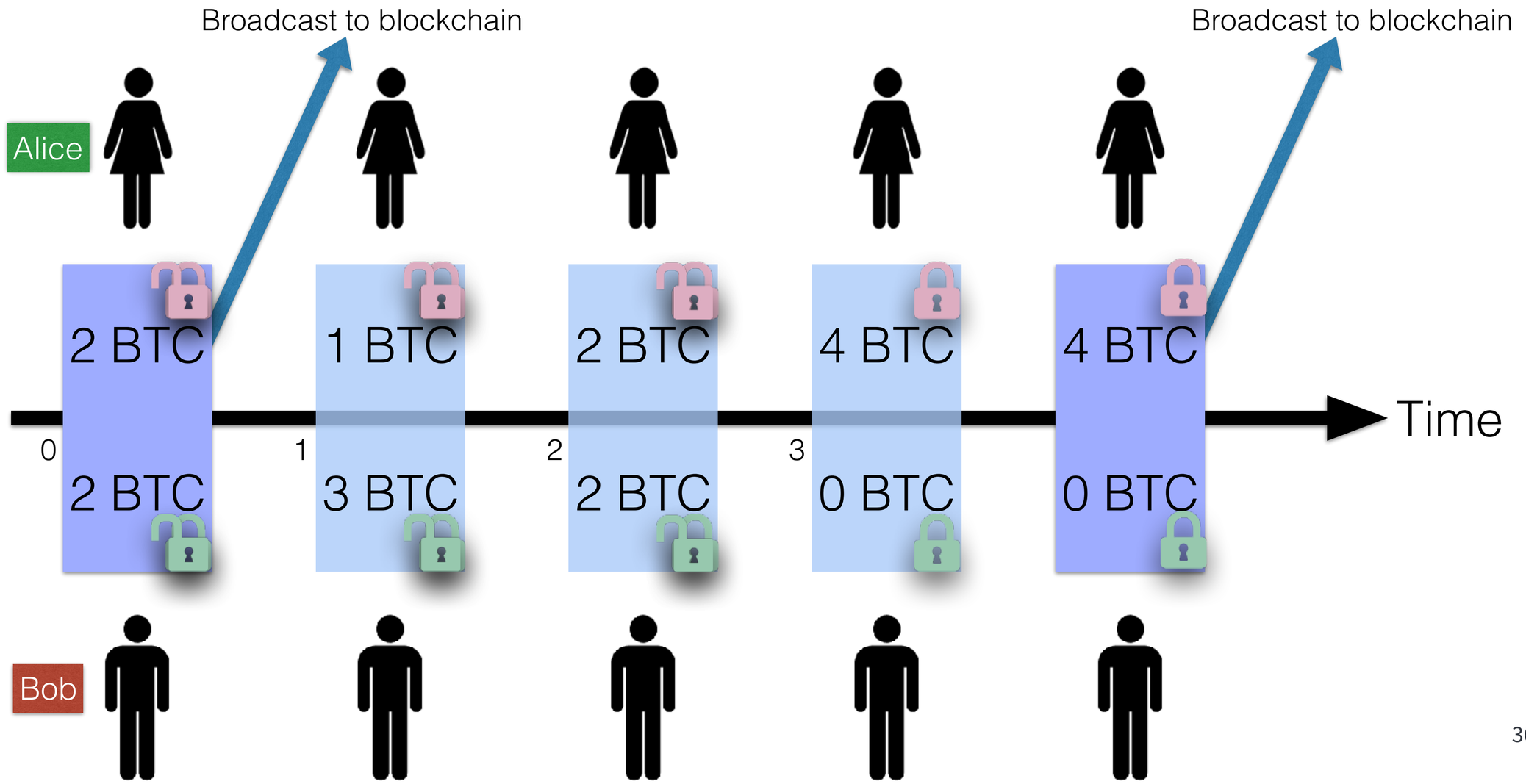
Bitcoin 2.0

1. Smart contracts
2. Anonymous transactions
3. Tokens
4. Off-chain transactions
5. Sidechains

Off-chain transactions

- In order to scale the volume of bitcoin transactions, some people are advocating the use of **off-chain transactions**
  - Transactions that happen off the blockchain, but are still secured
- Requires some new protocols to be effective (Segwit), but are theoretically feasible today.
  - **Lightning Network**

Off-chain transactions



Emerging Technology

Bitcoin 2.0

1. Smart contracts
2. Anonymous transactions
3. Tokens
4. Off-chain transactions
5. Sidechains

Sidechains

- As we have seen in off-chain transactions, you can create side-channels by freezing a set number of bitcoins
  - Using this feature, we can trade between two blockchains
  - **2-way peg**
  - Examples: **Elements Project, Hivemind**

Sidechains

- Allows future experimentation without affecting the major blockchain’s protocols
  - Potentially allows for the merging of private blockchains
  - Will increase the variety of applications and speed of development

BREAK TIME

15 MINUTES

Industry Trends

Risks and responses

1. Scalability
2. Centralisation
3. Regulations
4. Bitcoin vs Altcoins
5. Peripheral services

Scalability

- VISA handles ~2000 transactions per second (can handle up to 56000 tps)
  - Bitcoin handles 7 transactions per second
  - Ethereum can handle 25 transactions per second
- Block limits are artificial and can be raised to accommodate more transactions, in theory. However:
  - The community is divided for many reasons
  - There are still bandwidth limitations
    - In order reach VISA-scale, each block would need to be 8GB

Scalability

- More likely that we will see off-chain solutions in the near future
  - Lightning Network/Sidechains
- We might also make use of other cryptocurrencies for smaller exchanges of currency
- Scalability is the biggest problem that needs to be addressed for cryptocurrency’s viability

Industry Trends

Risks and responses

1. Scalability
2. **Centralisation**
3. Regulations
4. Bitcoin vs Altcoins
5. Peripheral services

Centralisation

- Decentralisation is one of the main advantages of blockchain technology and cryptocurrency
- However, most cryptocurrencies are still centralised in some way:
  - Small group of privileged developers
    - Reference client
  - Mining pools
    - Specialised hardware
    - Cheap electricity
    - Government funding

Centralisation

- Many of the arguments against certain scaling proposals bring up the idea of unnecessary centralisation
  - If nodes are allowed to be high-performance, they are no longer accessible to the masses
  - Off-chain transactions incentivise a hub-and-spoke model of creating channels
    - Everyone wants to be connected with the most connected person
- Not necessarily a bad thing, with the right incentive structures

Industry Trends

Risks and responses

1. Scalability
2. Centralisation
3. **Regulations**
4. Bitcoin vs Altcoins
5. Peripheral services

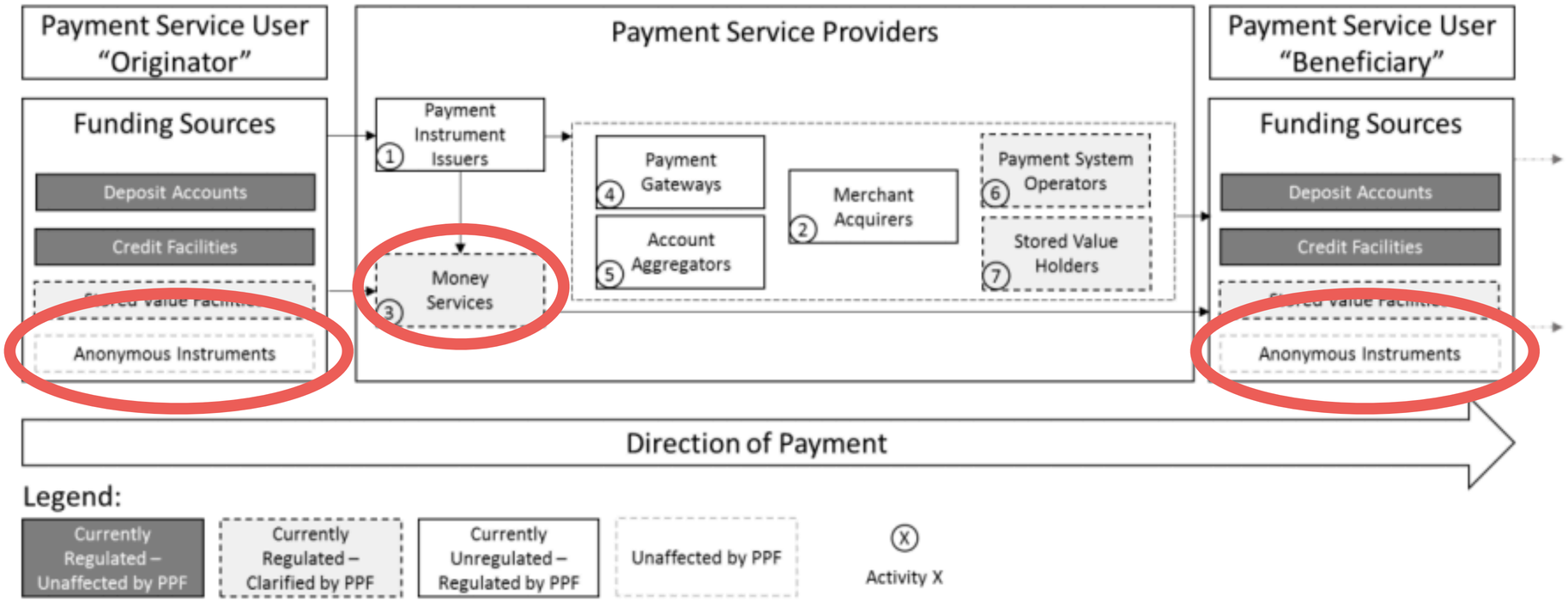
Regulations

- Is it a currency, or is it an asset?
  - *Hashfast Technologies LLC vs Lowe - asset*
  - MAS doesn’t specify that it is a currency - asset?
- Should cryptocurrency companies be subject to financial institution regulations (KYC/AML)?
  - MAS has announced that they want to regulate virtual currency intermediaries for AML and terrorism financing

Regulations

- “For clarity, cash and other anonymous instruments, having no identifiable issuer that opens and maintains accounts for users, will not be considered as regulated funding sources or payment instruments.”

— MAS Consultation Paper: Proposed Activity-based Payments Framework and Establishment of a National Payments Council



Industry Trends

Risks and responses

1. Scalability
2. Centralisation
3. Regulations
4. Bitcoin vs Altcoins
5. Peripheral services

Bitcoin vs Altcoins

- Two points of view
  1. Multiple altcoins represent decentralisation and diversity of choice
  2. Multiple altcoins serve to weaken network effects
- Bitcoin XT vs Bitcoin Unlimited vs Bitcoin Core
- Ethereum Classic vs Ethereum Core
- Litecoin, Dogecoin, Peercoin …
  - Merged mining

Industry Trends

Risks and responses

1. Scalability
2. Centralisation
3. Regulations
4. Bitcoin vs Altcoins
5. Peripheral services

Peripheral services

- Blockchain-as-a-Service
  - Microsoft Azure, IBM Blockchain, Deloitte Rubix
- Cryptocurrency exchanges/Wallets
  - CoinHako, Coinbase, itBit, Kraken
- Blockchain consulting
  - PwC, Accenture, Chainsmiths

Future Direction

A blockchain strategy

1. Public vs private blockchains
2. Blockchain consultants
3. Strategic positioning
4. Conclusion

Public vs private blockchains

- Public blockchains
  - Open source
  - Higher hashing power
  - Usually associated with a currency of value
- Private blockchains
  - Proprietary
  - Some aren’t even blockchains, just distributed ledgers (eg. Hyperledger)

Future Direction

A blockchain strategy

1. Public vs private blockchains
2. **Blockchain consultants**
3. Strategic positioning
4. Conclusion

Blockchain consultants

- Blockchain technology is still nascent
  - New developments every day; several theoretical topics discussed here are whitepapers and have not made it to peer-reviewed scientific journals.
- Unpredictable nature means that consultants cannot give you a clear guideline on what needs to be done
  - Their primary goal is to help you to develop a blockchain strategy
    - Allow room for exploration
    - Minimise risks

Future Direction

A blockchain strategy

1. Public vs private blockchains
2. Blockchain consultants
3. Strategic positioning
4. Conclusion

Strategic positioning

- Although it’s not possible to make perfect predictions, we can still get an edge over the competition.
- Position yourself relatively better than peers to take advantage of improvements in blockchain technology
  - Acquire clients that rely on blockchain services
  - Keep up to date with government regulations about cryptocurrency for Singapore as well as for trading partners
  - Joining a consortium

Future Direction

A blockchain strategy

1. Public vs private blockchains
2. Blockchain consultants
3. Complementary services
4. Conclusion

Conclusion

- Cryptocurrencies and blockchains are very new technologies
  - Like all new technologies, they are uncertain and potentially disruptive
- Over the next few years, we are likely to see more global standards being adopted as regulatory frameworks start to catch up

Conclusion

- My own opinions:
  - Public blockchains are more likely to dominate over private ones
  - Tiered protocol layers are likely to emerge and be widely adopted
  - Still undergoing rapid development
    - Makes more sense to build up expertise and prepare for opportunities than to invest in building your own blockchain solution
  - Key players are governments, miners, and protocol developers
    - What they do will shape the future direction of blockchains and cryptocurrencies

Q&A

Hashing

Public Key Cryptography