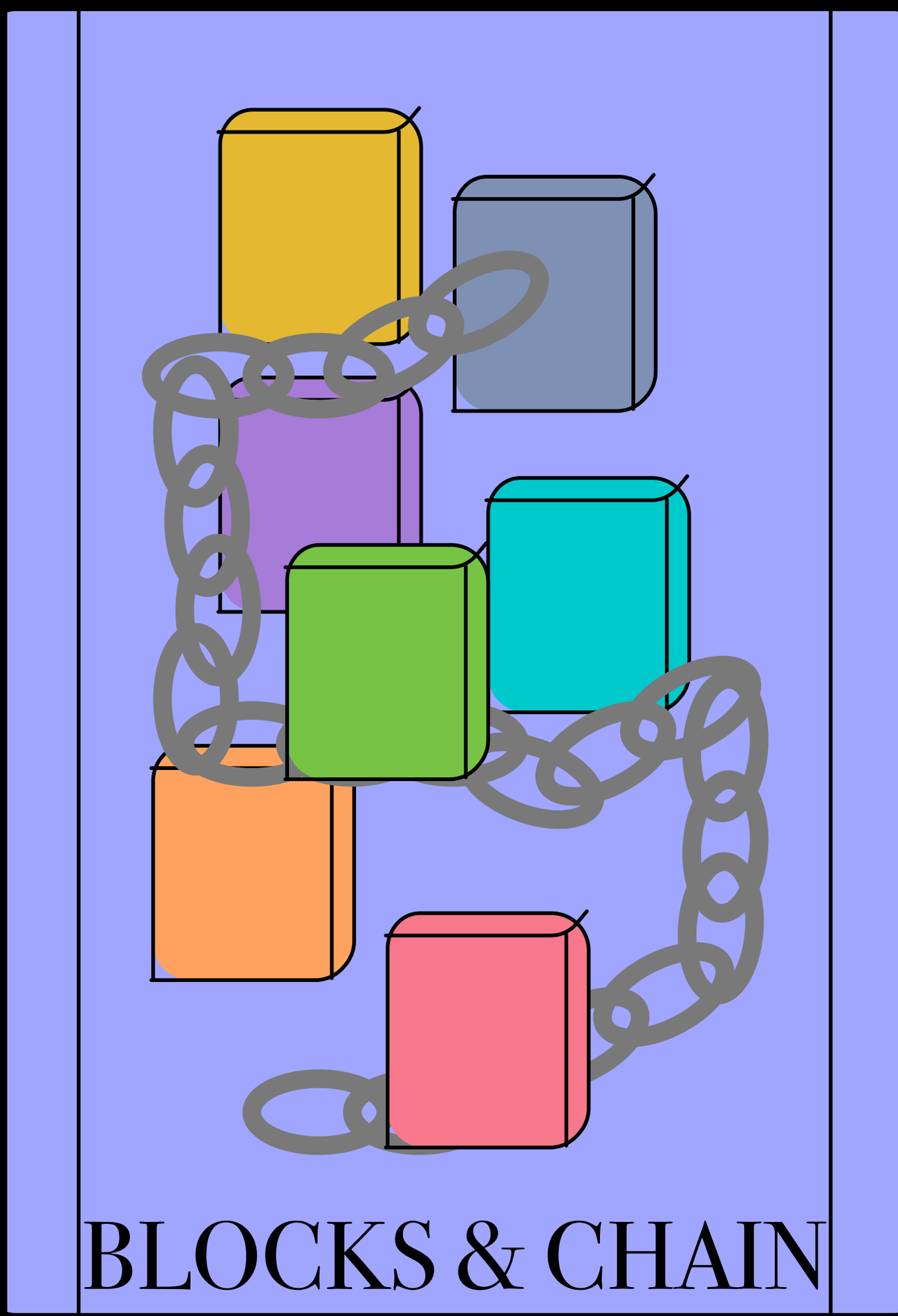
PRASHANT KRISHNAMURTHY

BLOCKCHAINS

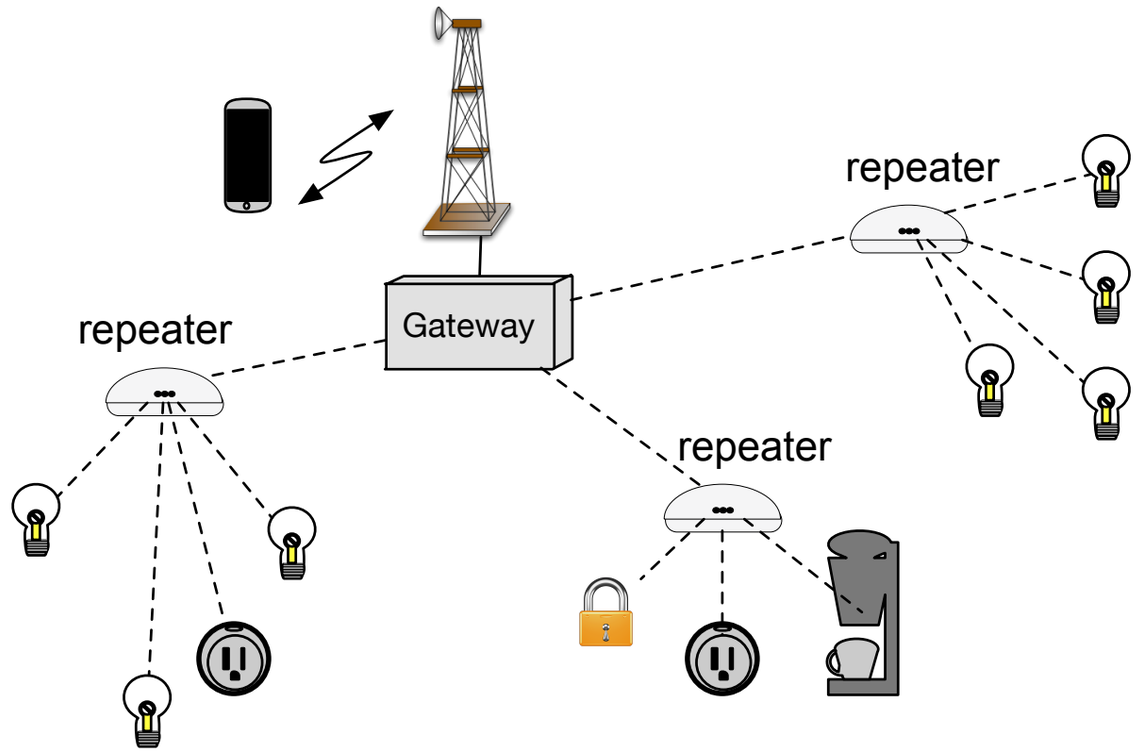
AGENDA

- Introduction
- Some cryptographic concepts
- Chaining and block chaining
- Networks, trust, consensus
- So what…



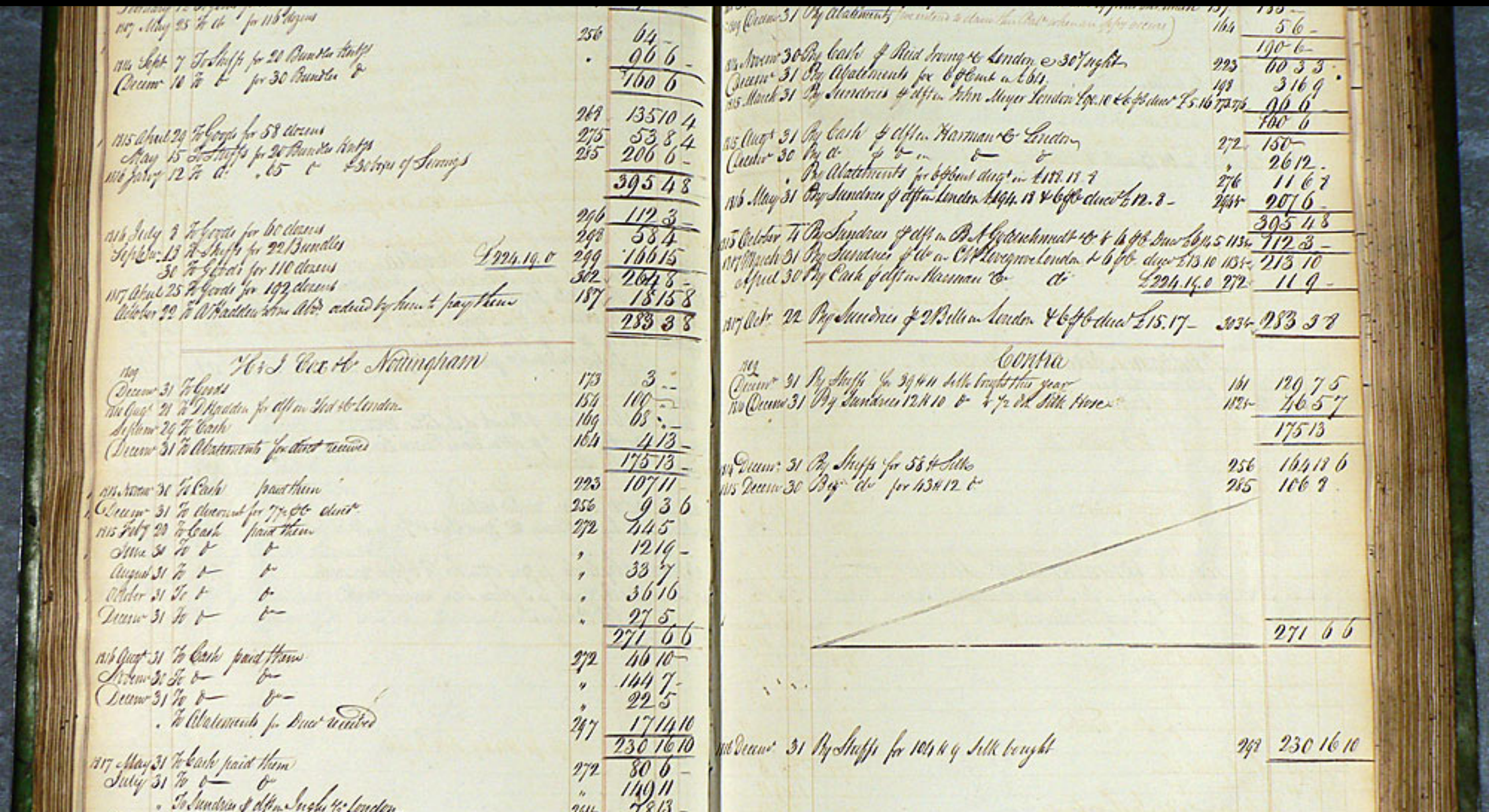
INTRODUCTION

- Bitcoin and Blockchain
    - Other Cryptocurrencies
        - Litecoin, Monero, Ethereum - https://www.coinbase.com/charts
- Potential
    - Financial industry
    - **Internet of Things (IoT)**
    - Credentials
    - Monetizing creative people
    - “Rights” management
- Is “Blockchain Technology” disruptive or not?



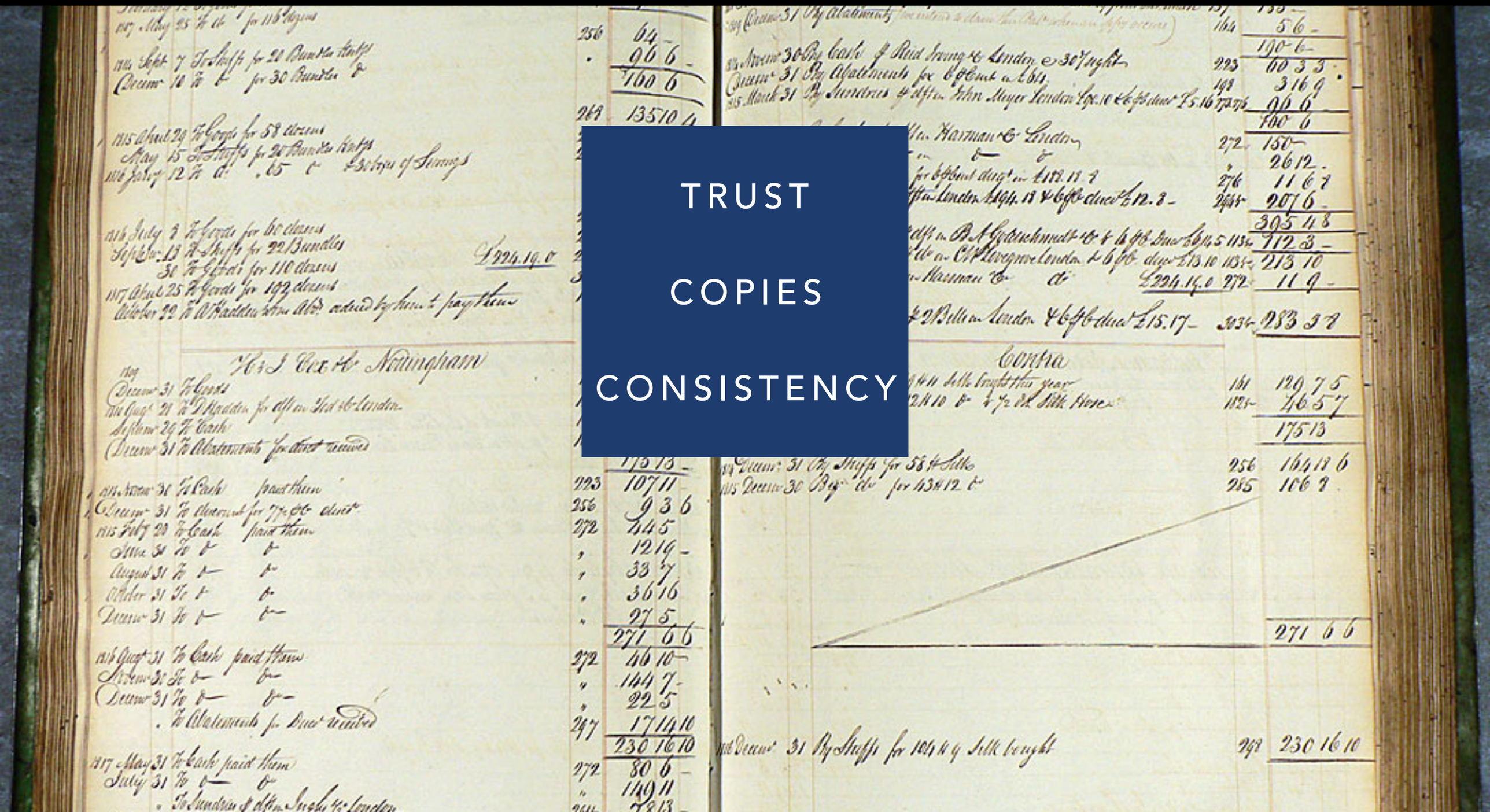
https://bluedotbizblog.files.wordpress.com/2011/06/ledger-book.jpg

TRANSACTIONS AND LEDGERS



https://bluedotbizblog.files.wordpress.com/2011/06/ledger-book.jpg

TRANSACTIONS AND LEDGERS



TRUST

COPIES

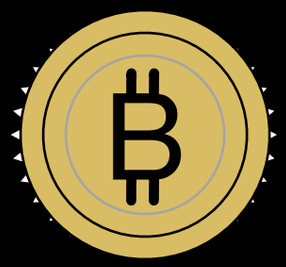
CONSISTENCY

TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

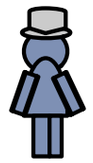
TOKENIZATION

- Physical and digital objects can be “tokenized”
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

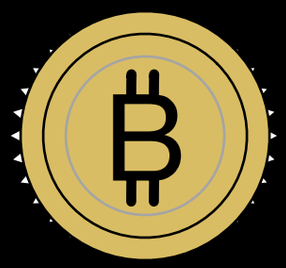


TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

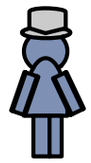


Date/Time
Amount
Place



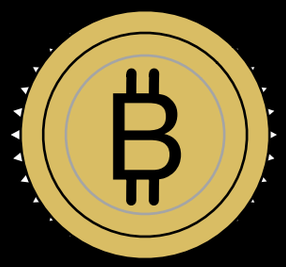
TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?



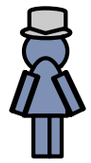
Date/Time
Amount
Place

Creative material
Contributors
Payments



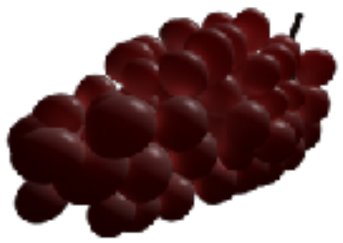
TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?



Date/Time
Amount
Place

Creative material
Contributors
Payments

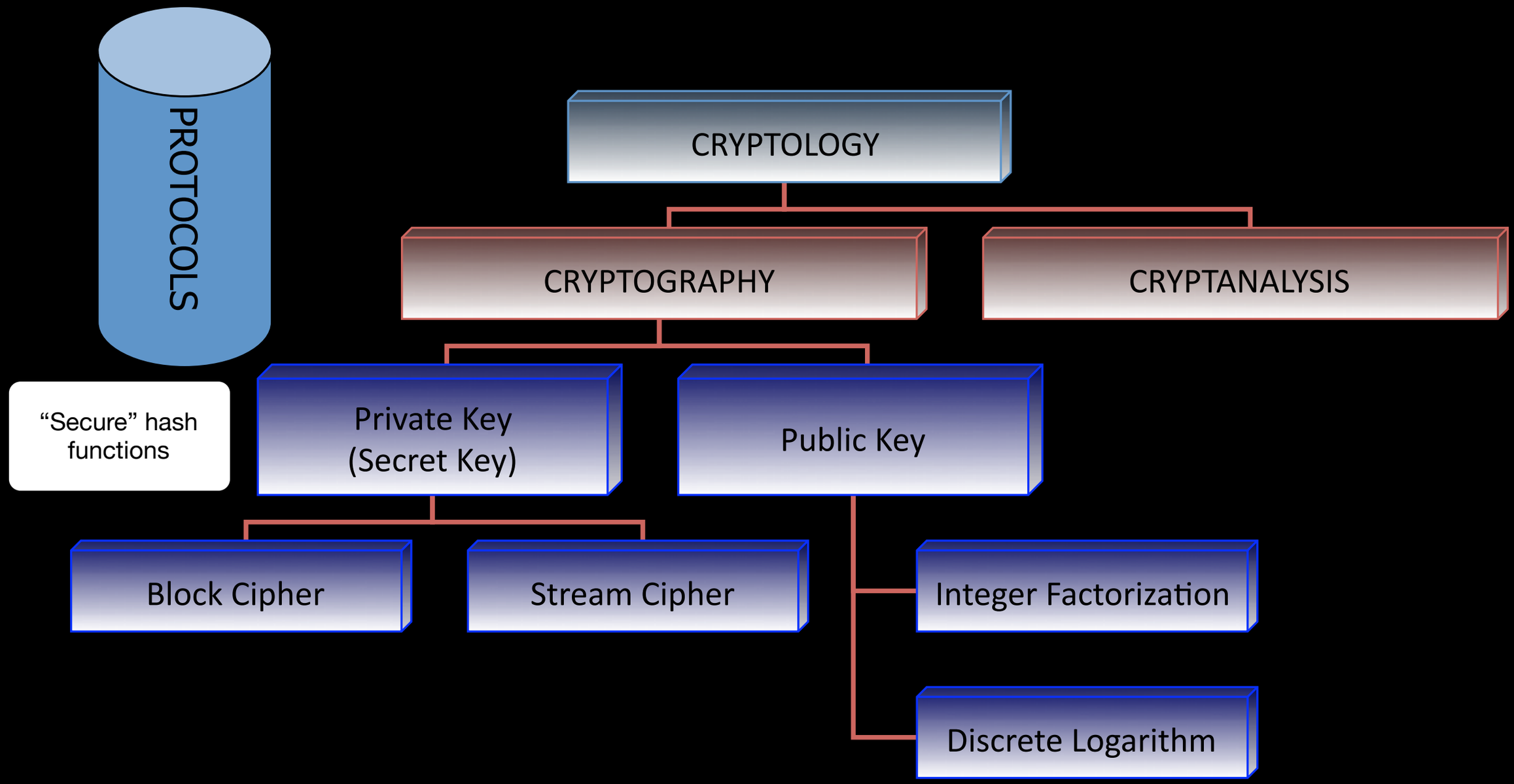


Supply Chain
Producer
Distributor
Locations

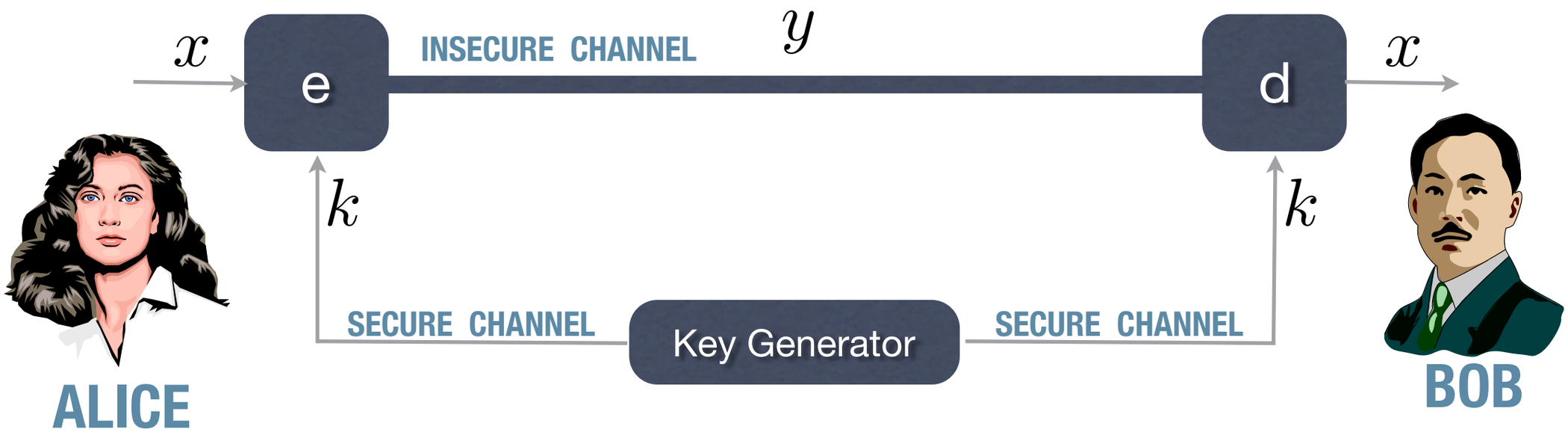
ENABLING TECHNOLOGY

CRYPTOGRAPHY

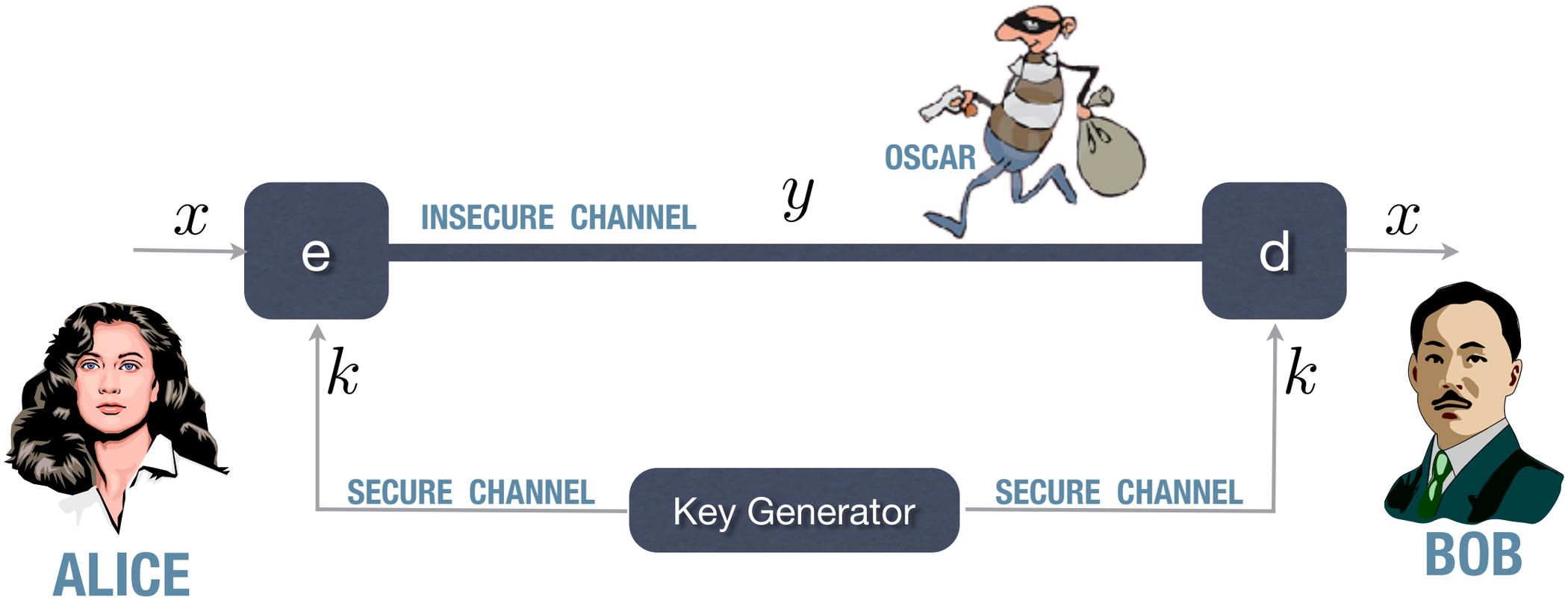
CRYPTOLOGY


PROTOCOLS
CRYPTOLOGY
CRYPTOGRAPHY
CRYPTANALYSIS
"Secure" hash functions
Private Key (Secret Key)
Public Key
Block Cipher
Stream Cipher
Integer Factorization
Discrete Logarithm

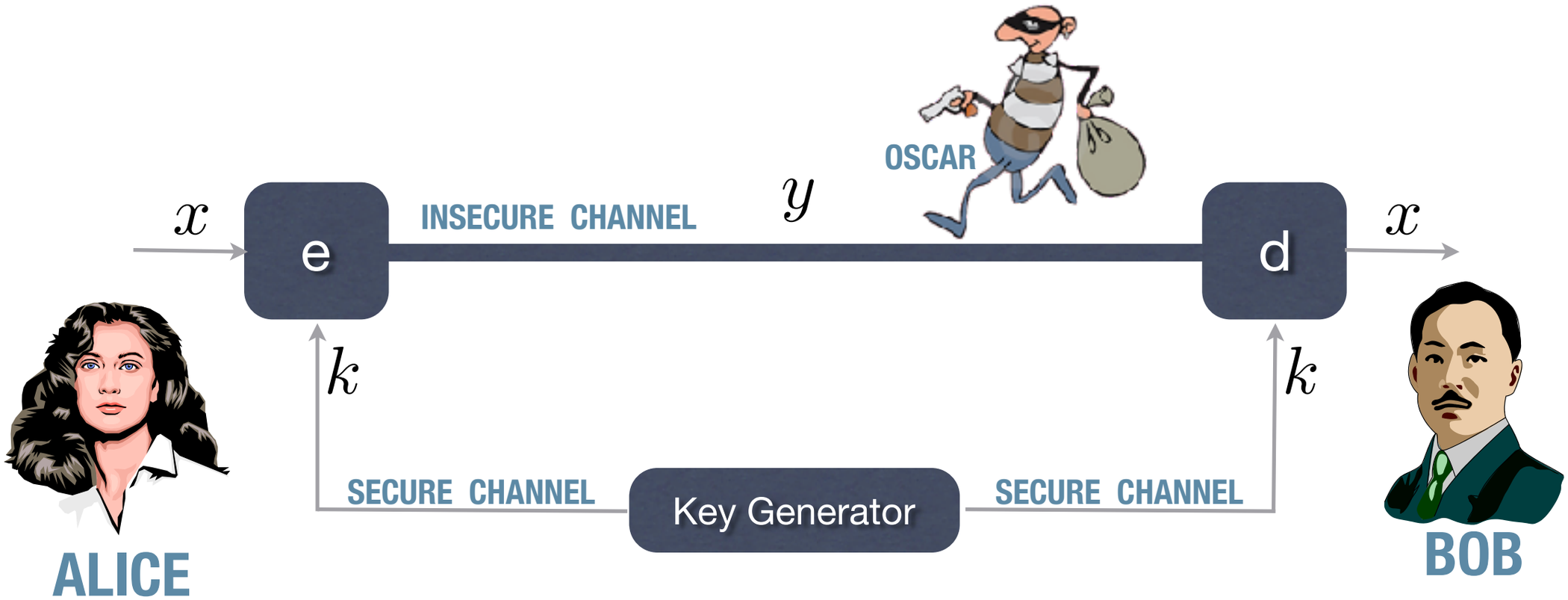
SECRET KEY ENCRYPTION



SECRET KEY ENCRYPTION



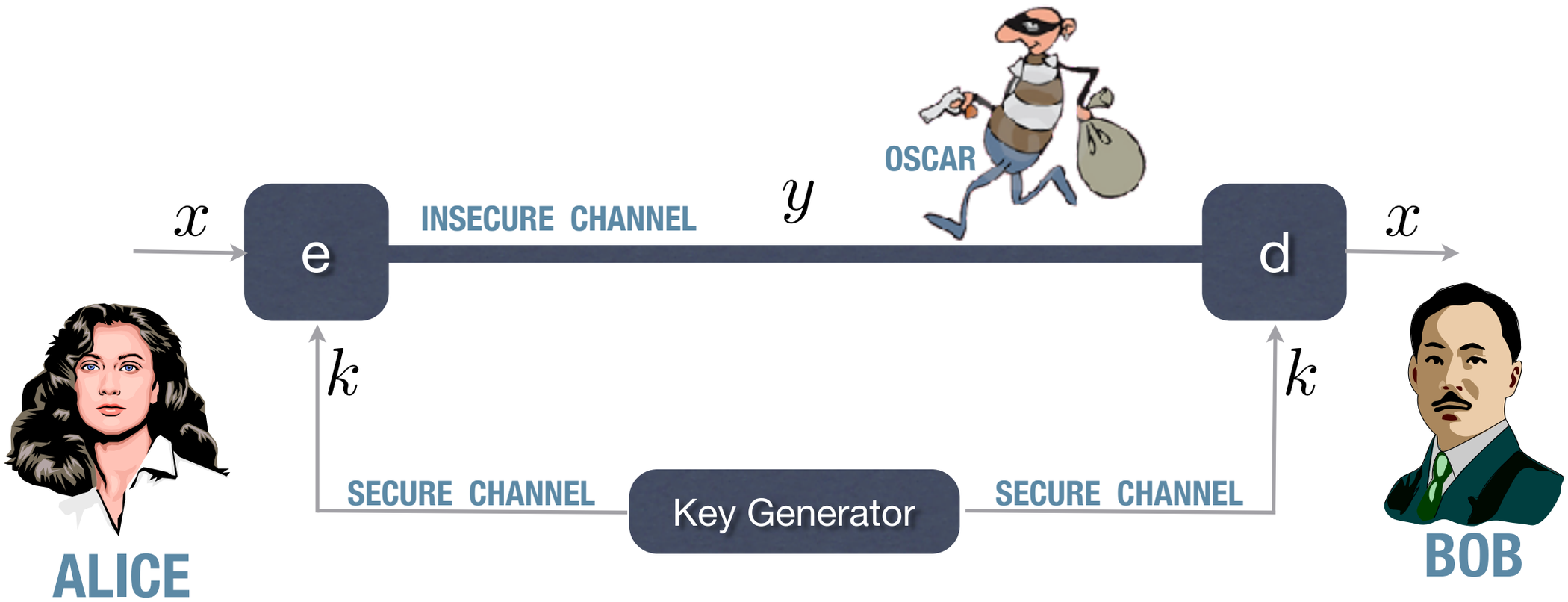
SECRET KEY ENCRYPTION



PLAINTEXT

x

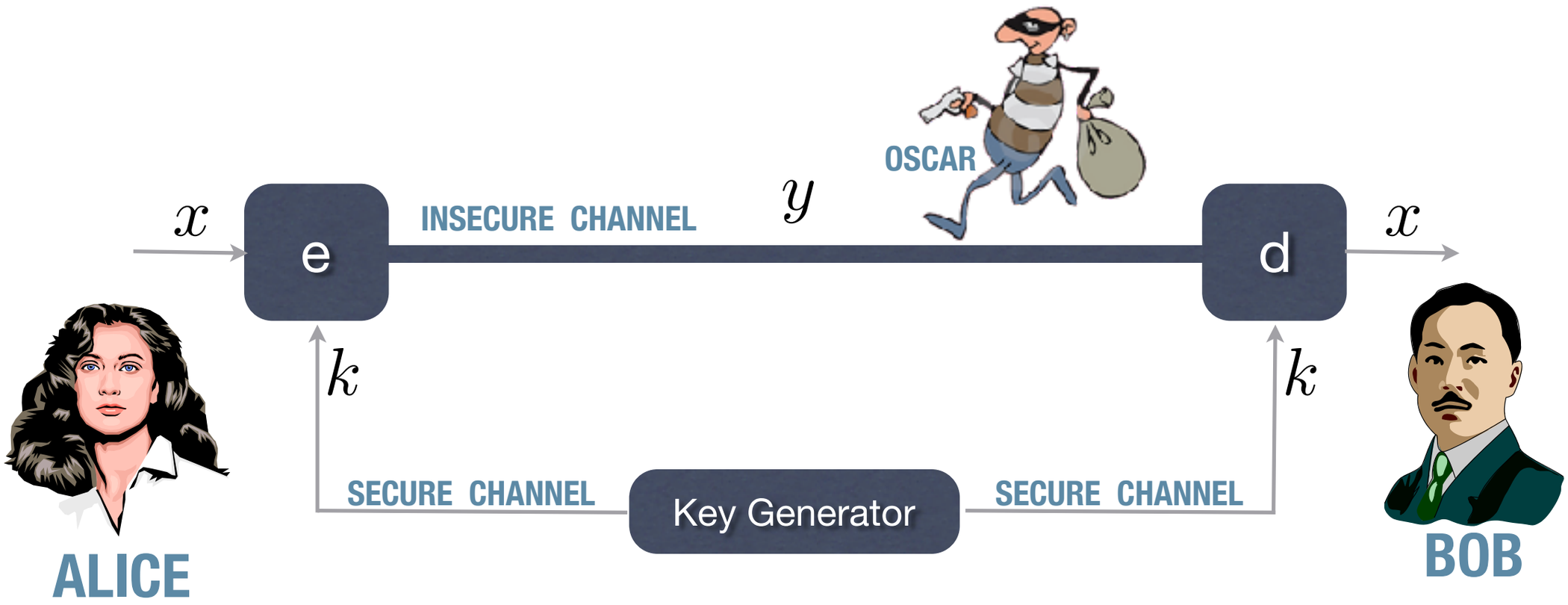
SECRET KEY ENCRYPTION



PLAINTEXT x

CIPHERTEXT y

SECRET KEY ENCRYPTION



ENCRYPTION

$$e_k(x) = y$$

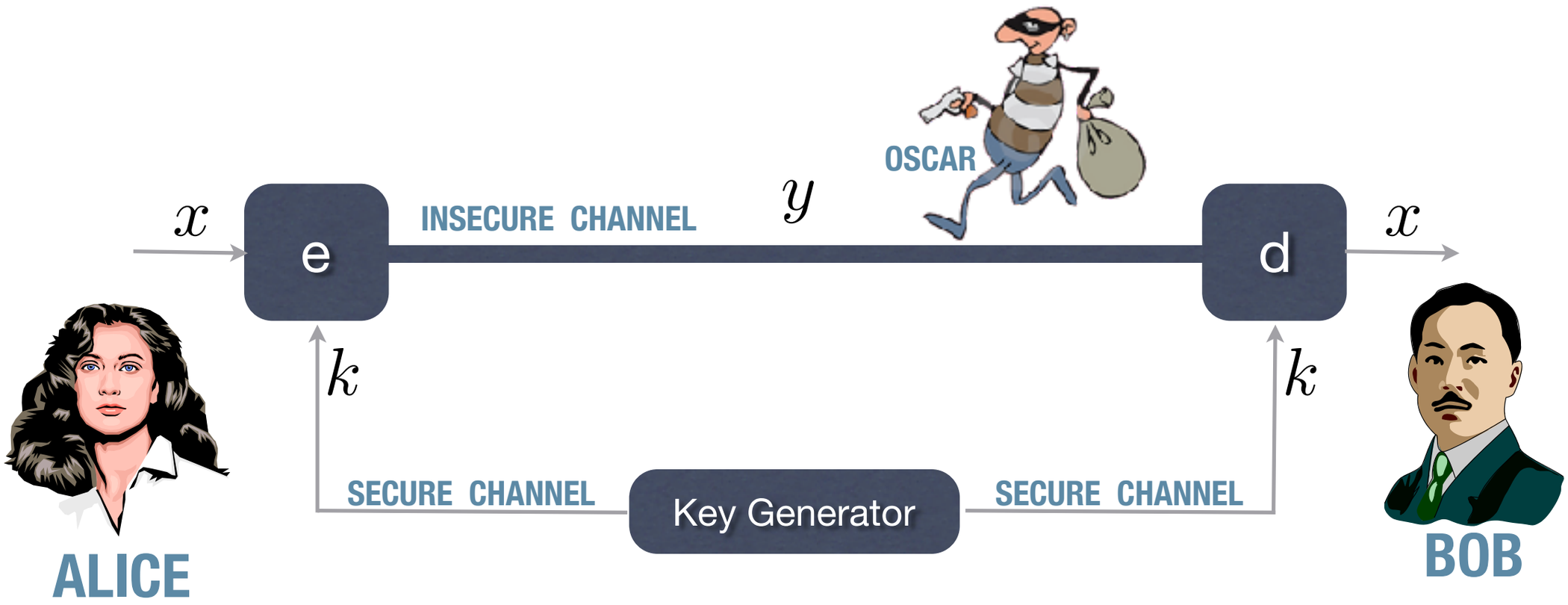
PLAINTEXT

x

CIPHERTEXT

y

SECRET KEY ENCRYPTION



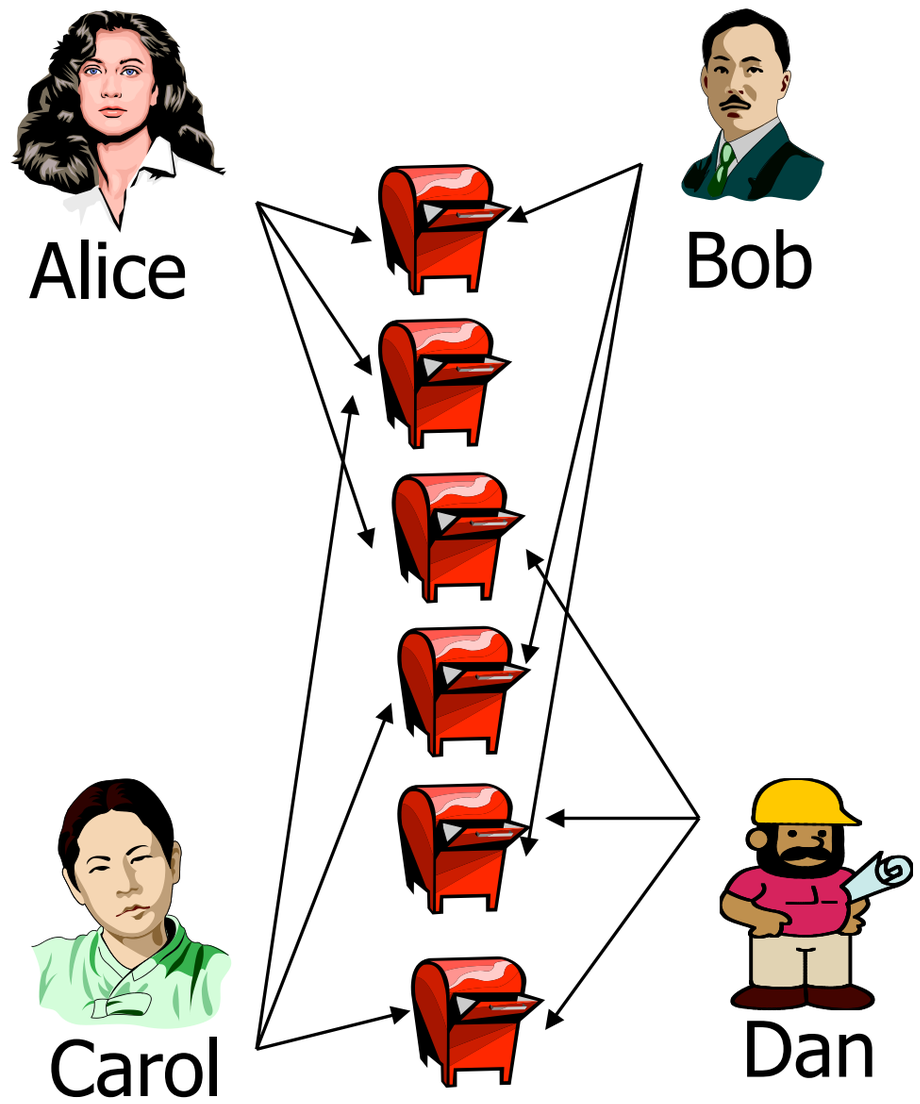
ENCRYPTION	DECRYPTION	PLAINTEXT	CIPHERTEXT
$e_k(x) = y$	$d_k(y) = x$	x	y

WHY AND WHY NOT PUBLIC KEY CRYPTOGRAPHY?

- Key establishment
- Non-repudiation
  - Signatures!
- Computational effort

WHY AND WHY NOT PUBLIC KEY CRYPTOGRAPHY?

- Key establishment
- Non-repudiation
  - Signatures!
- Computational effort

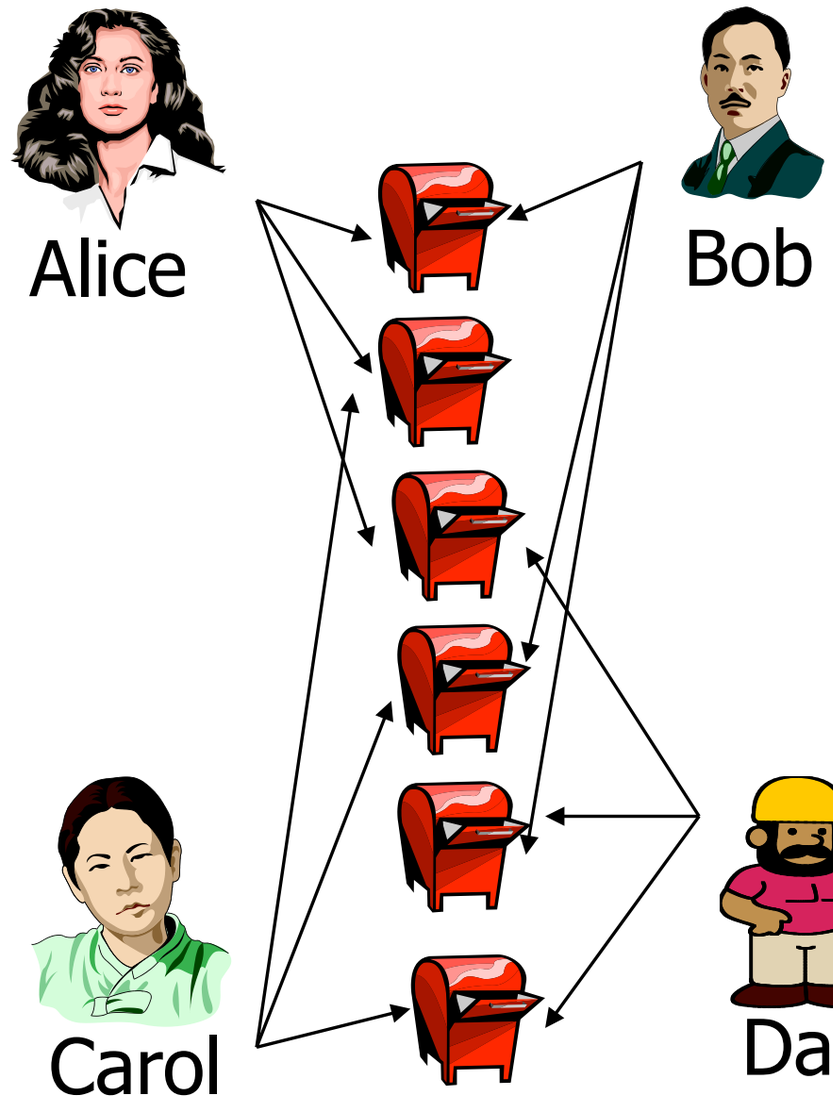


WHY AND WHY NOT PUBLIC KEY CRYPTOGRAPHY?

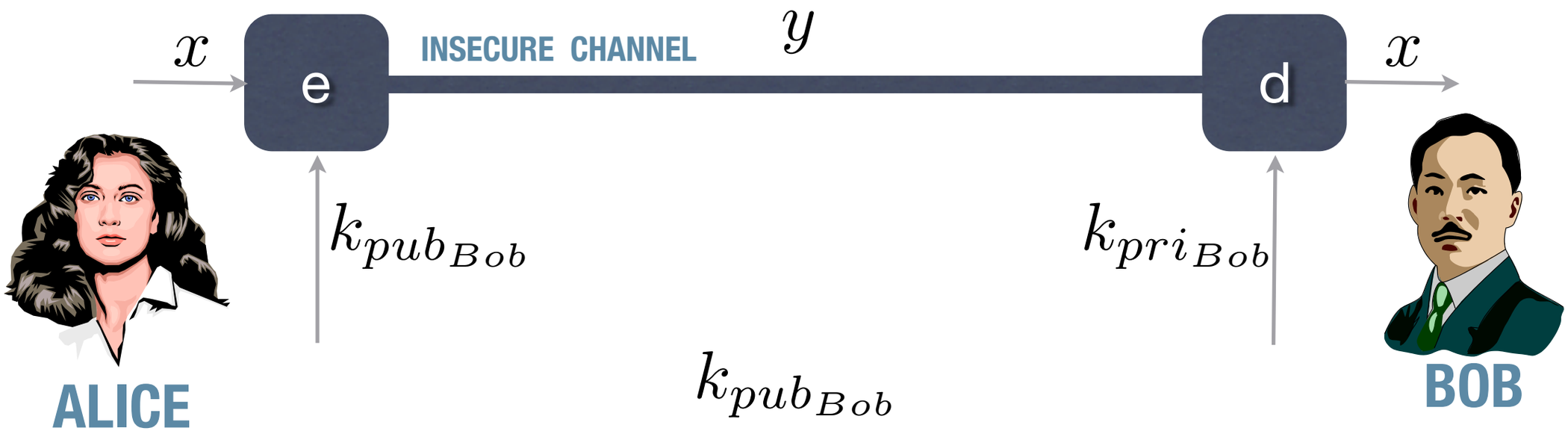
- Key establishment
- Non-repudiation
- Signatures!
- Computational effort


Dear Bob,
I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures. I am writing his letter to show you how we create digital signatures. In fact it is very different from physical signatures.

Yours sincerely
Alice Voorhisread
(Alice)

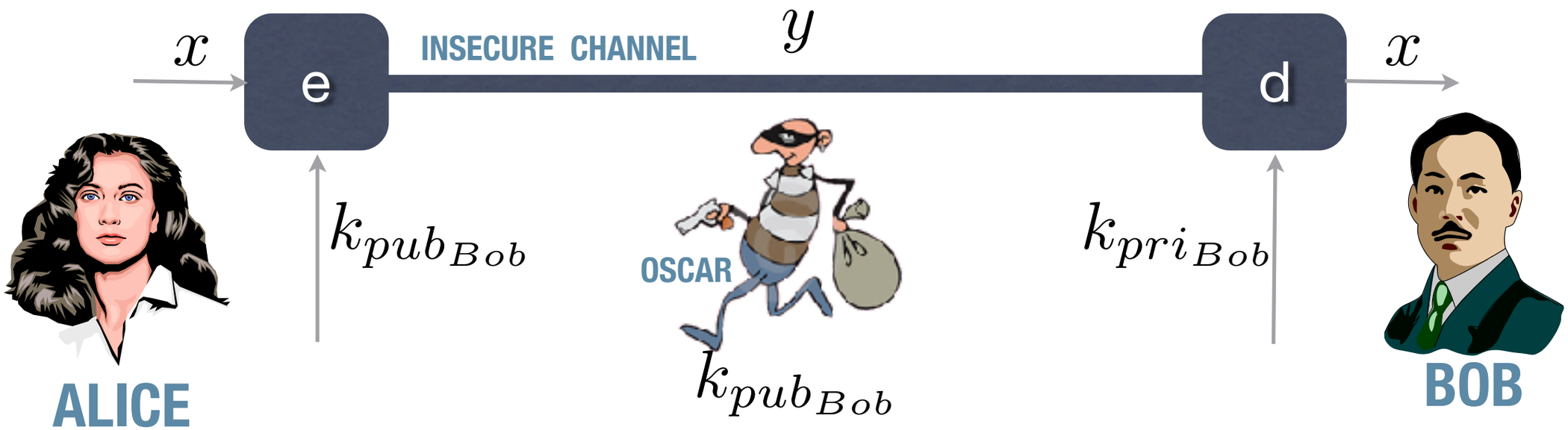


PUBLIC KEY ENCRYPTION



ENCRYPTION	DECRYPTION	PLAINTEXT	CIPHERTEXT
$e_{k_{pub_{Bob}}}(x) = y$	$d_{k_{pri_{Bob}}}(y) = x$	x	y

PUBLIC KEY ENCRYPTION

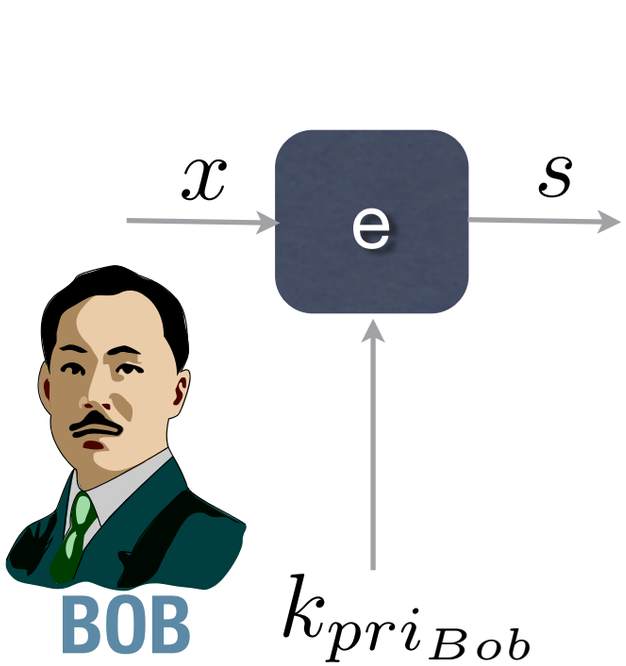


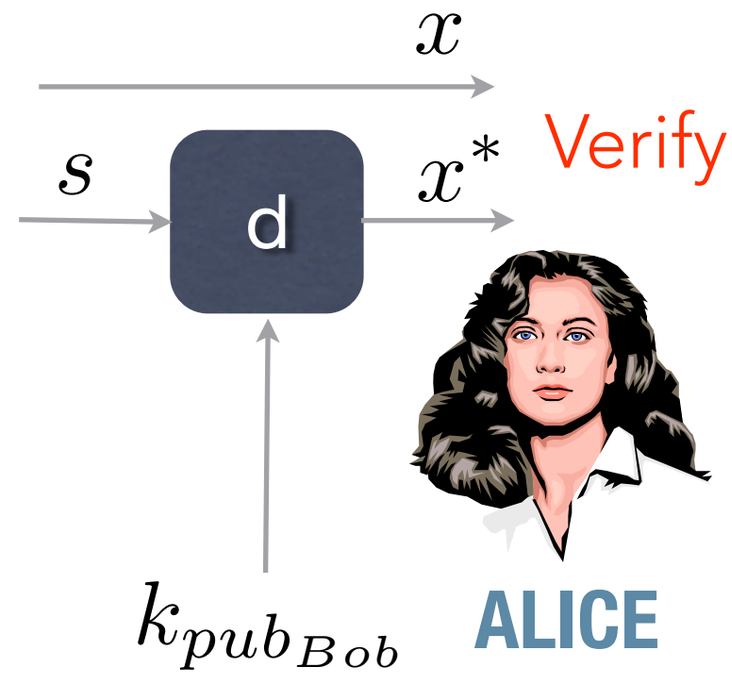
ENCRYPTION	DECRYPTION	PLAINTEXT	CIPHERTEXT
$e_{k_{pub_{Bob}}}(x) = y$	$d_{k_{pri_{Bob}}}(y) = x$	x	y

DIGITAL SIGNATURES

SIGNING	VERIFICATION	PLAINTEXT	SIGNATURE
$e_{k_{pri_{Bob}}}(x) = s$	$d_{k_{pub_{Bob}}}(s) = x$	x	s

DIGITAL SIGNATURES





SIGNING	VERIFICATION	PLAINTEXT	SIGNATURE
$e_{k_{pri_{Bob}}}(x) = s$	$d_{k_{pub_{Bob}}}(s) = x$	x	s

DIGITAL SIGNATURES

BOB

x → e → s

$k_{pri_{Bob}}$

x

ALICE

s → d → x^* Verify

$k_{pub_{Bob}}$

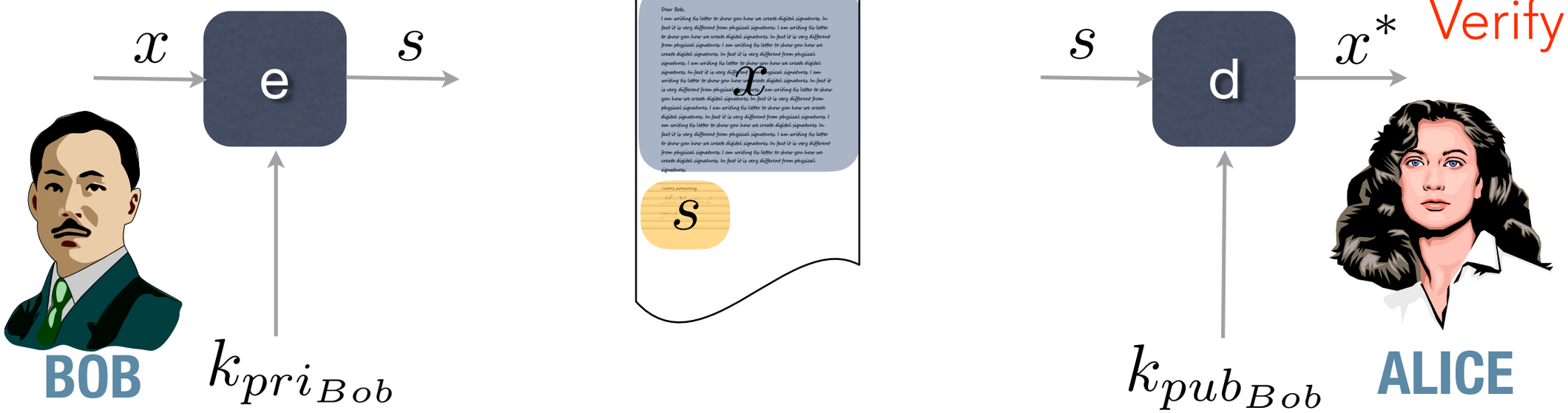
SIGNING $e_{k_{pri_{Bob}}}(x) = s$

VERIFICATION $d_{k_{pub_{Bob}}}(s) = x$

PLAINTEXT x

SIGNATURE s

DIGITAL SIGNATURES



SIGNING

$$e_{k_{pri_{Bob}}}(x) = s$$

VERIFICATION

$$d_{k_{pub_{Bob}}}(s) = x$$

PLAINTEXT

x

SIGNATURE

s

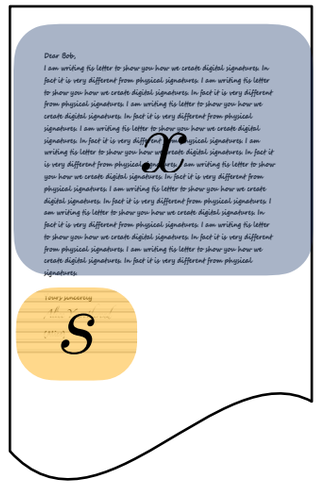
DIGITAL SIGNATURES

$k_{pub_{Bob}}$

BOB

x → e → s

$k_{pri_{Bob}}$



x

s → d → x^* Verify

$k_{pub_{Bob}}$

ALICE

SIGNING	VERIFICATION	PLAINTEXT	SIGNATURE
$e_{k_{pri_{Bob}}}(x) = s$	$d_{k_{pub_{Bob}}}(s) = x$	x	s

KEY SIZES FOR SECURITY

- 80 bit keys are “safe” to use today, but 128 bit keys are recommended
- Common to see 2048-bit RSA
- Elliptic Curve Cryptography is becoming popular for mobile devices

Secret Key	Elliptic Curve	RSA
80	163	1024
128	283	3027
192	409	7680
256	571	15360

The Birthday Paradox

HOW MANY PEOPLE SHOULD YOU LET INTO A ROOM BEFORE TWO OF THEM HAVE THE SAME BIRTH"DAY"?

Source: https://upload.wikimedia.org/wikipedia/commons/thumb/2/2d/Schokoladentorte_Buttercreme_Tulpen_dritter_Geburtstag_001.JPG/1200px-Schokoladentorte_Buttercreme_Tulpen_dritter_Geburtstag_001.JPG

"SECURE" HASH FUNCTIONS

- One-way (random oracle?)
- Takes any arbitrary input and produces a fixed size output
  - 256 bits for security today
    - Show SHA-256: http://passwordsgenerator.net/sha256-hash-generator/
    - Takes ~2^{128} trials to find a collision with probability 0.5
  - What happens if you care only about the first 40 bits?

TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

Date/Time
Amount
Place

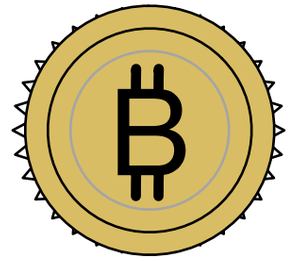
TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

Date/Time
Amount
Place

TOKENIZATION

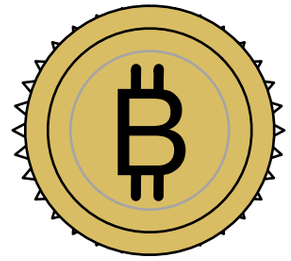
- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?



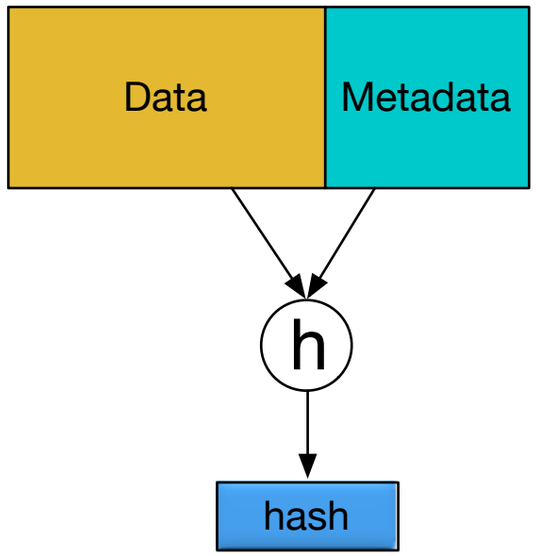
Date/Time
Amount
Place

TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?



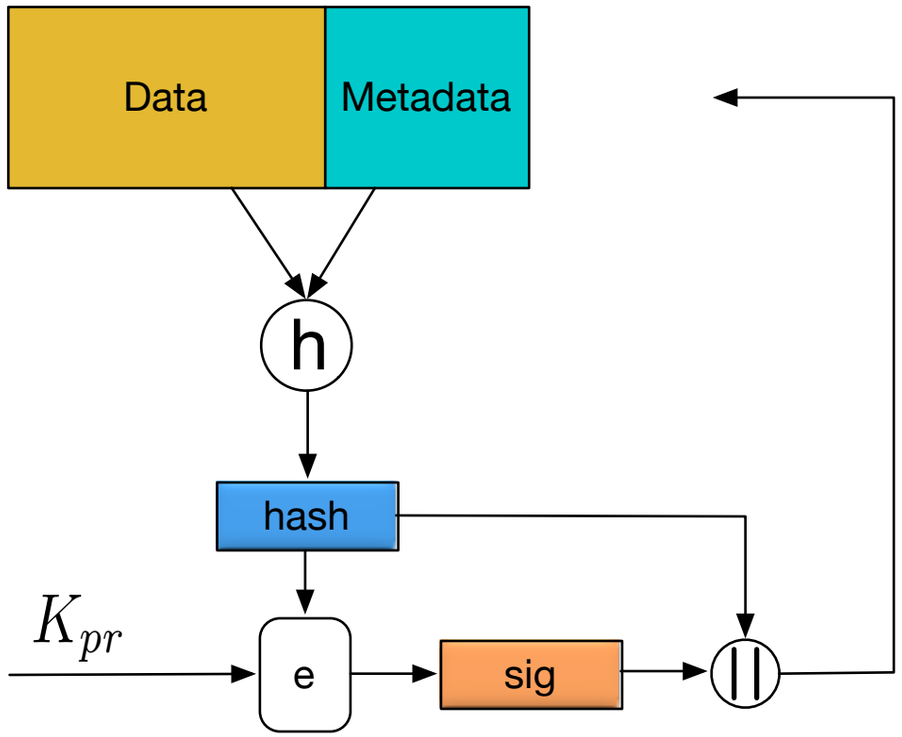
Date/Time
Amount
Place



TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

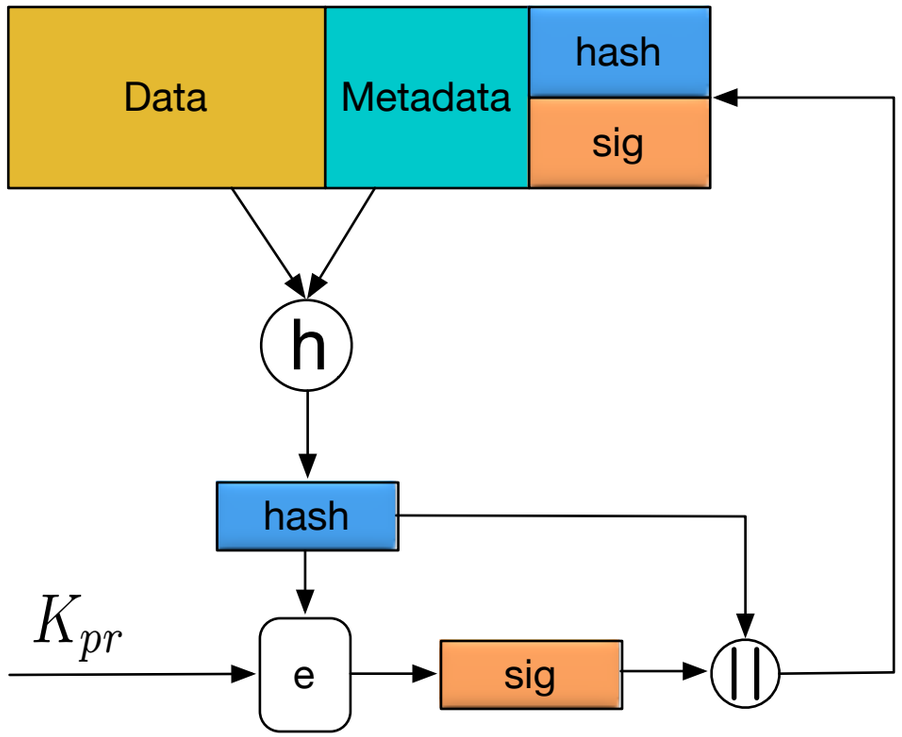
Date/Time
Amount
Place



TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

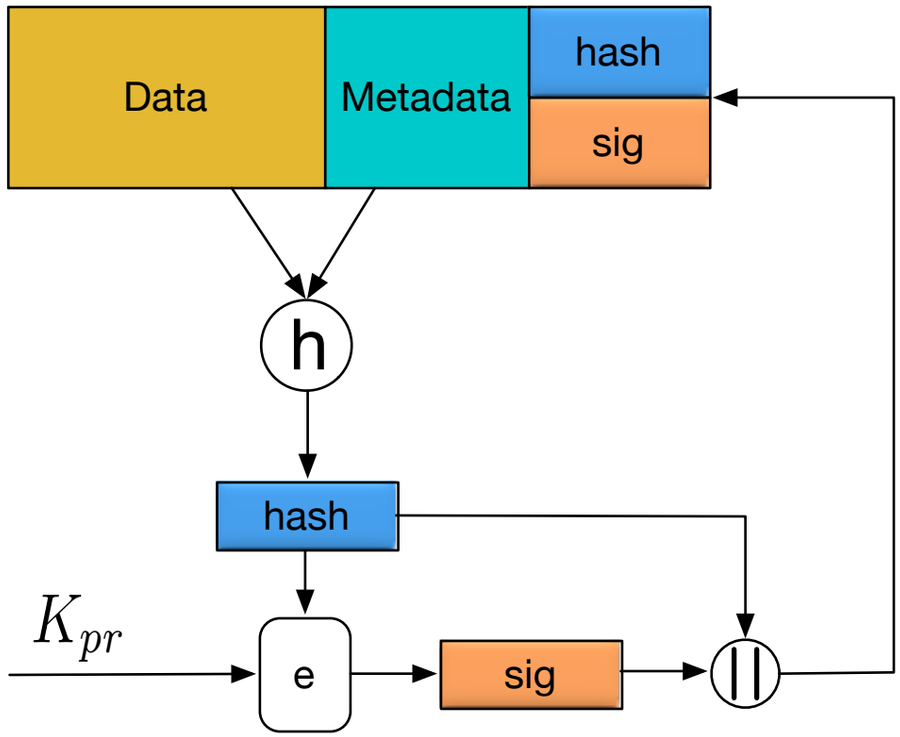
Date/Time
Amount
Place



TOKENIZATION

- Physical and digital objects can be "tokenized"
- Transactions involving such objects can be captured in a database (ledger)
  - Identity
  - Ownership (who owns the object? who owned it previously?)
  - Borrowing/Selling
  - Damages, improvements, you name it
- Forgery?

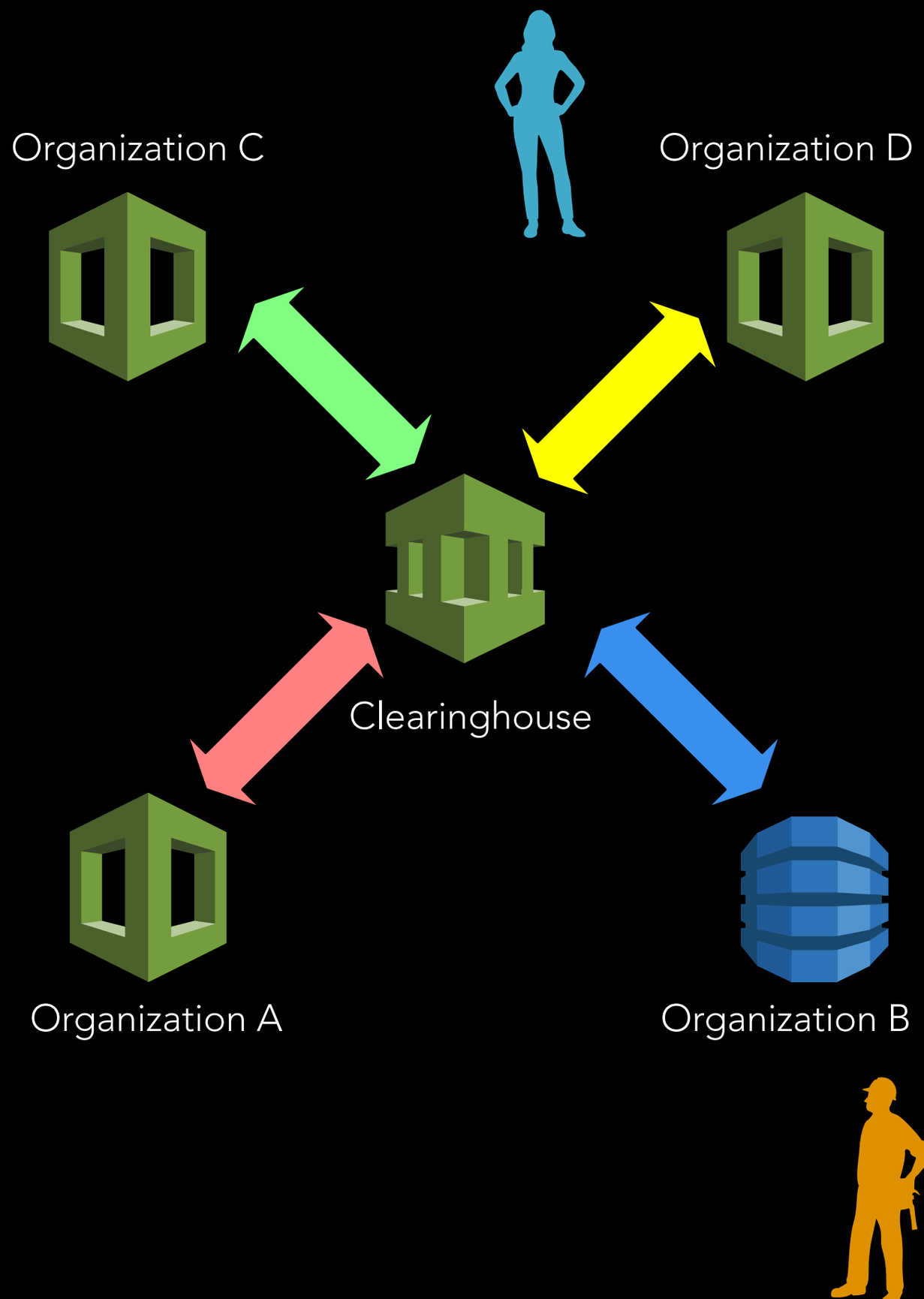
Date/Time
Amount
Place



WHO WRITES? WHO KEEPS? WHO IS RESPONSIBLE FOR INTEGRITY?

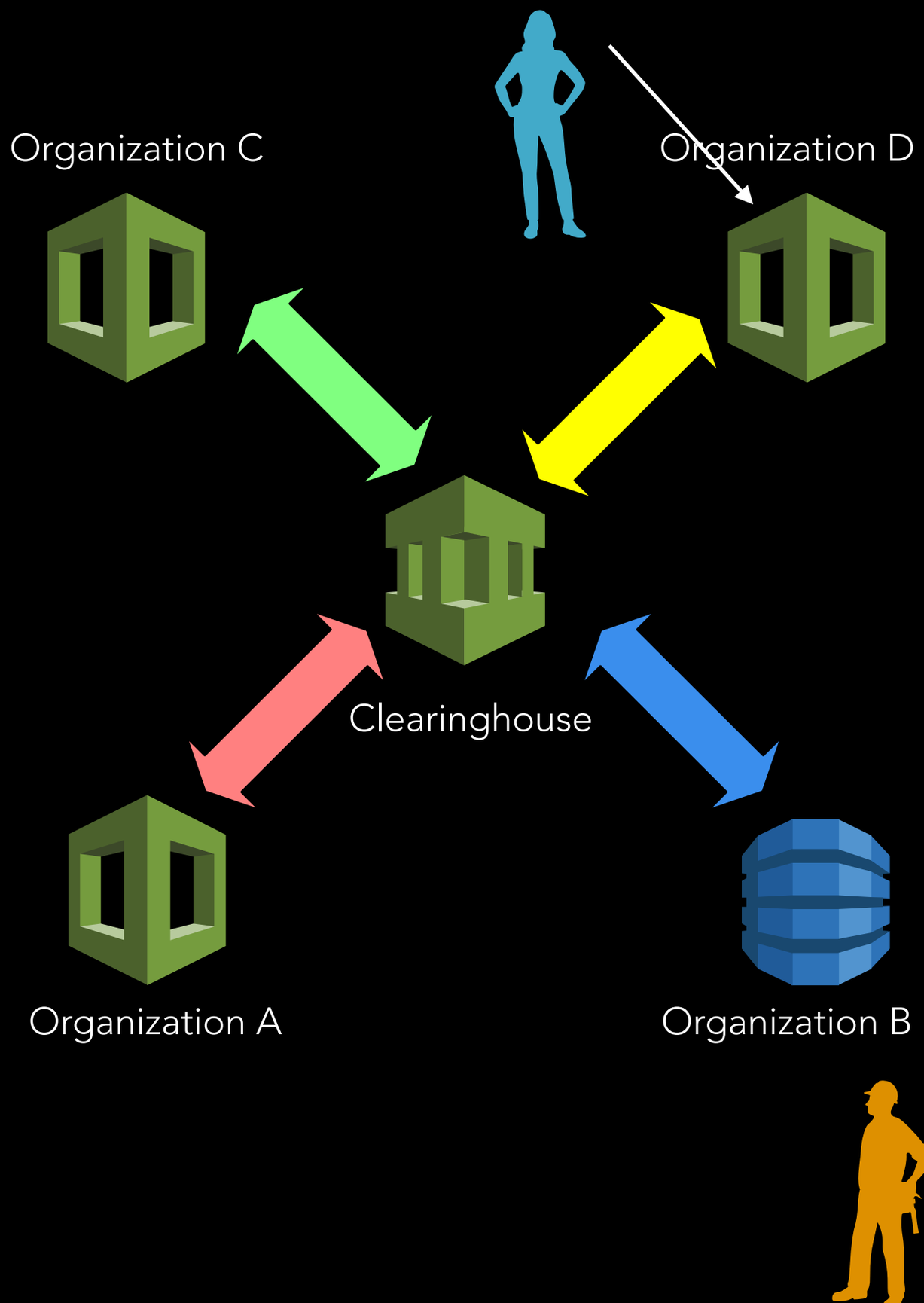
CLEARING-HOUSE

- One central "**trusted third party**" keeps the database
  - Maintains the "final" version
- Everyone sends their data to this third party
- Cost, robustness, and time
- Confidentiality!



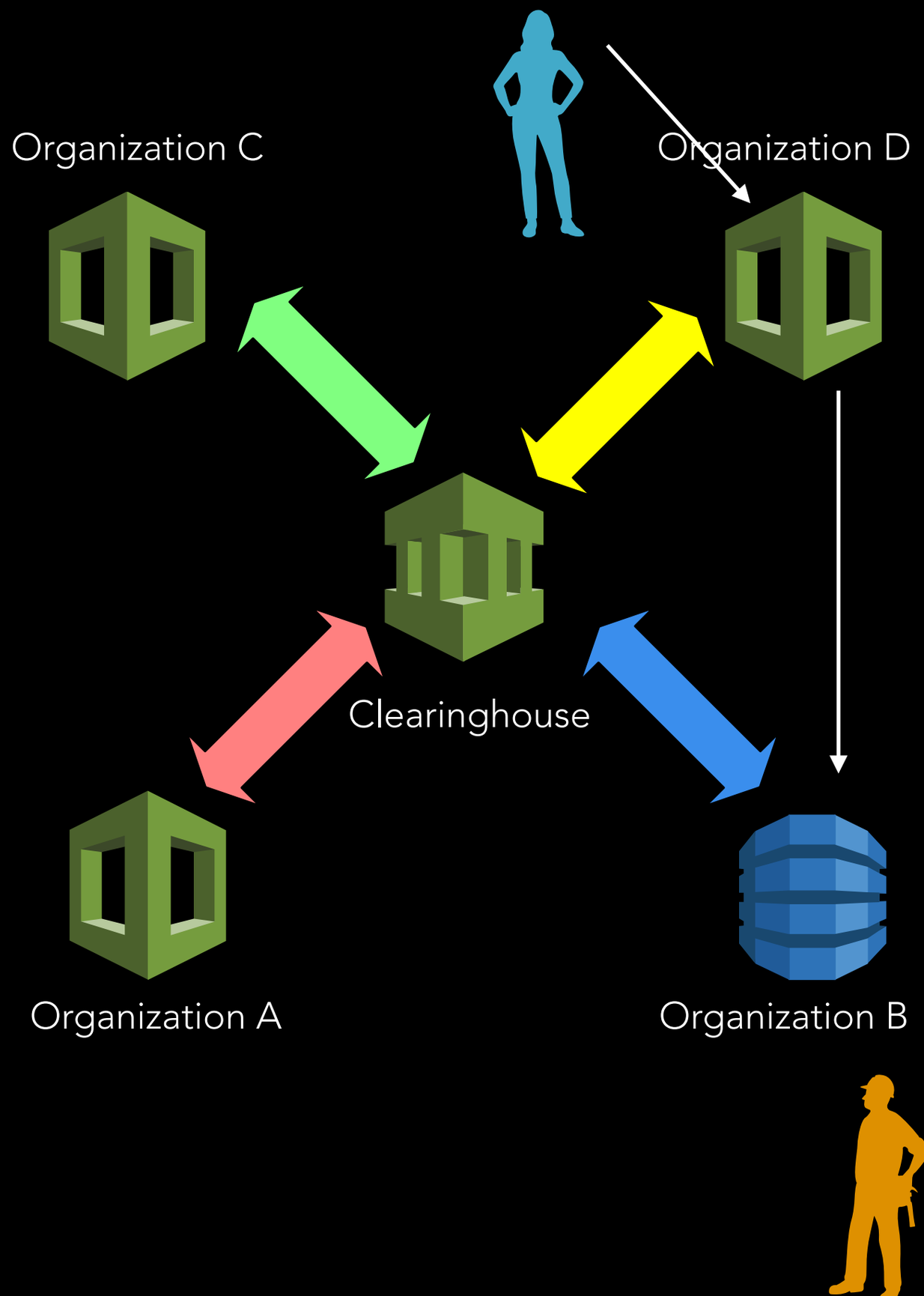
CLEARING-HOUSE

- One central "**trusted third party**" keeps the database
  - Maintains the "final" version
- Everyone sends their data to this third party
- Cost, robustness, and time
- Confidentiality!



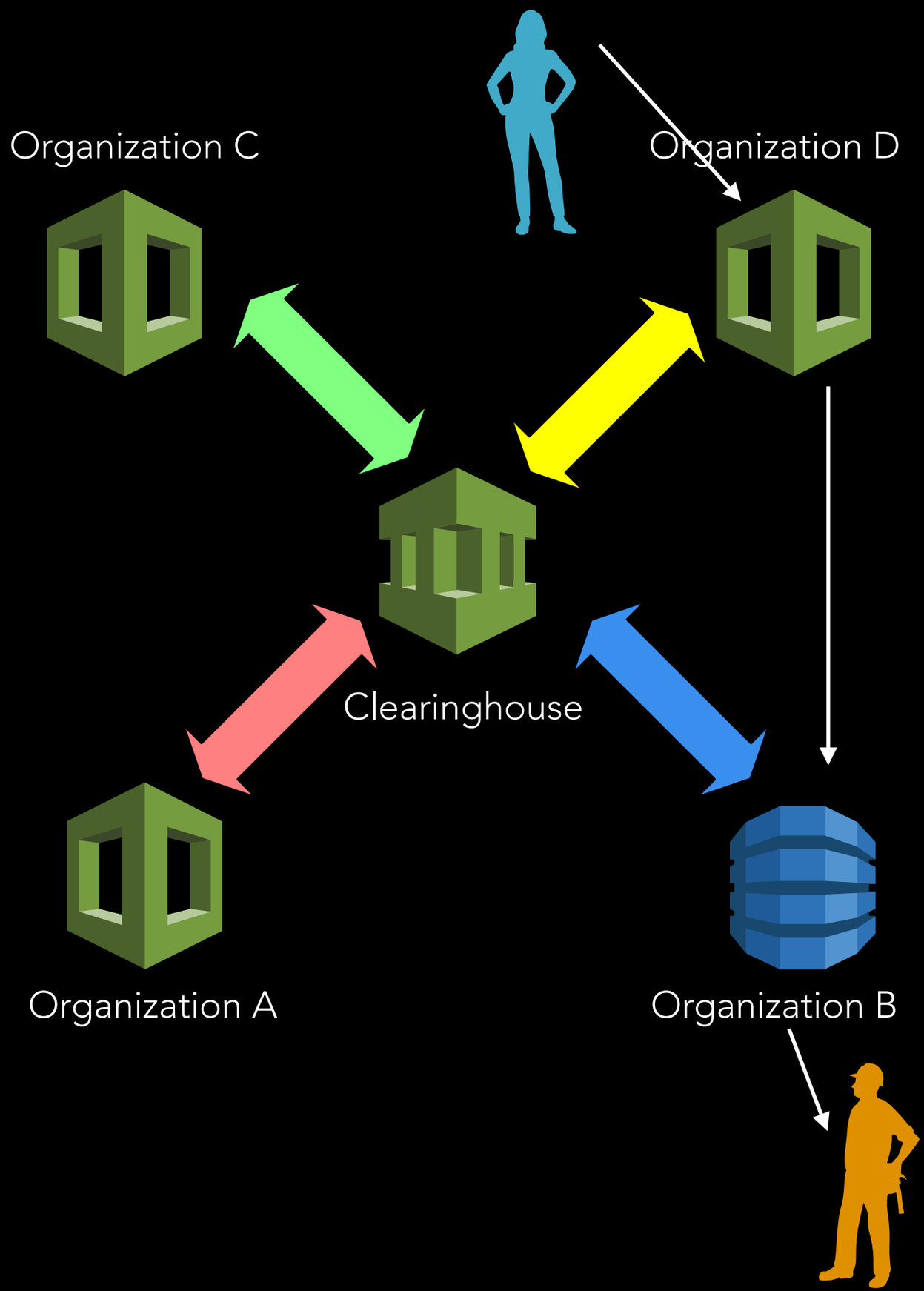
CLEARING-HOUSE

- One central "**trusted third party**" keeps the database
  - Maintains the "final" version
- Everyone sends their data to this third party
- Cost, robustness, and time
- Confidentiality!



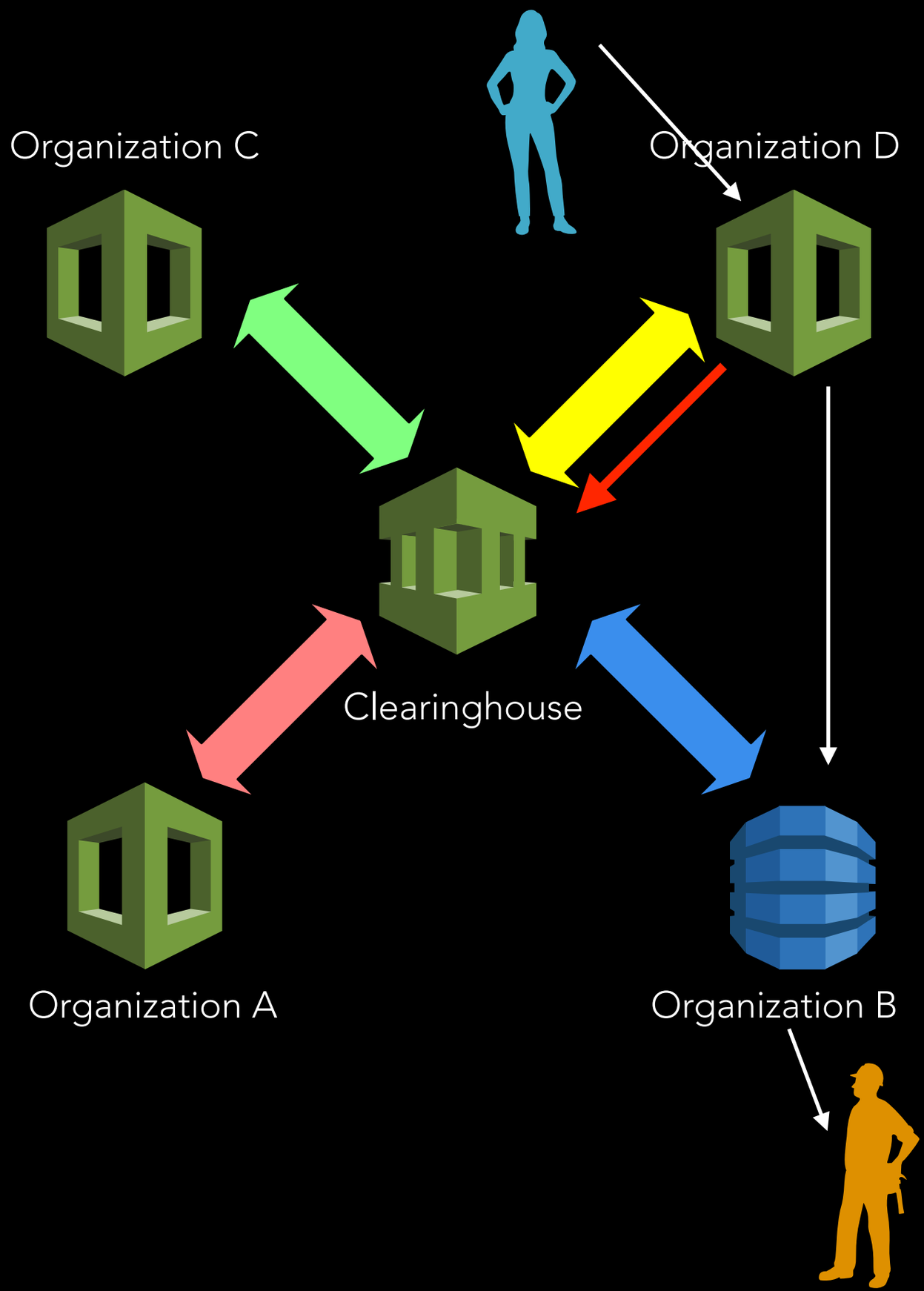
CLEARING-HOUSE

- One central "**trusted third party**" keeps the database
  - Maintains the "final" version
- Everyone sends their data to this third party
- Cost, robustness, and time
- Confidentiality!



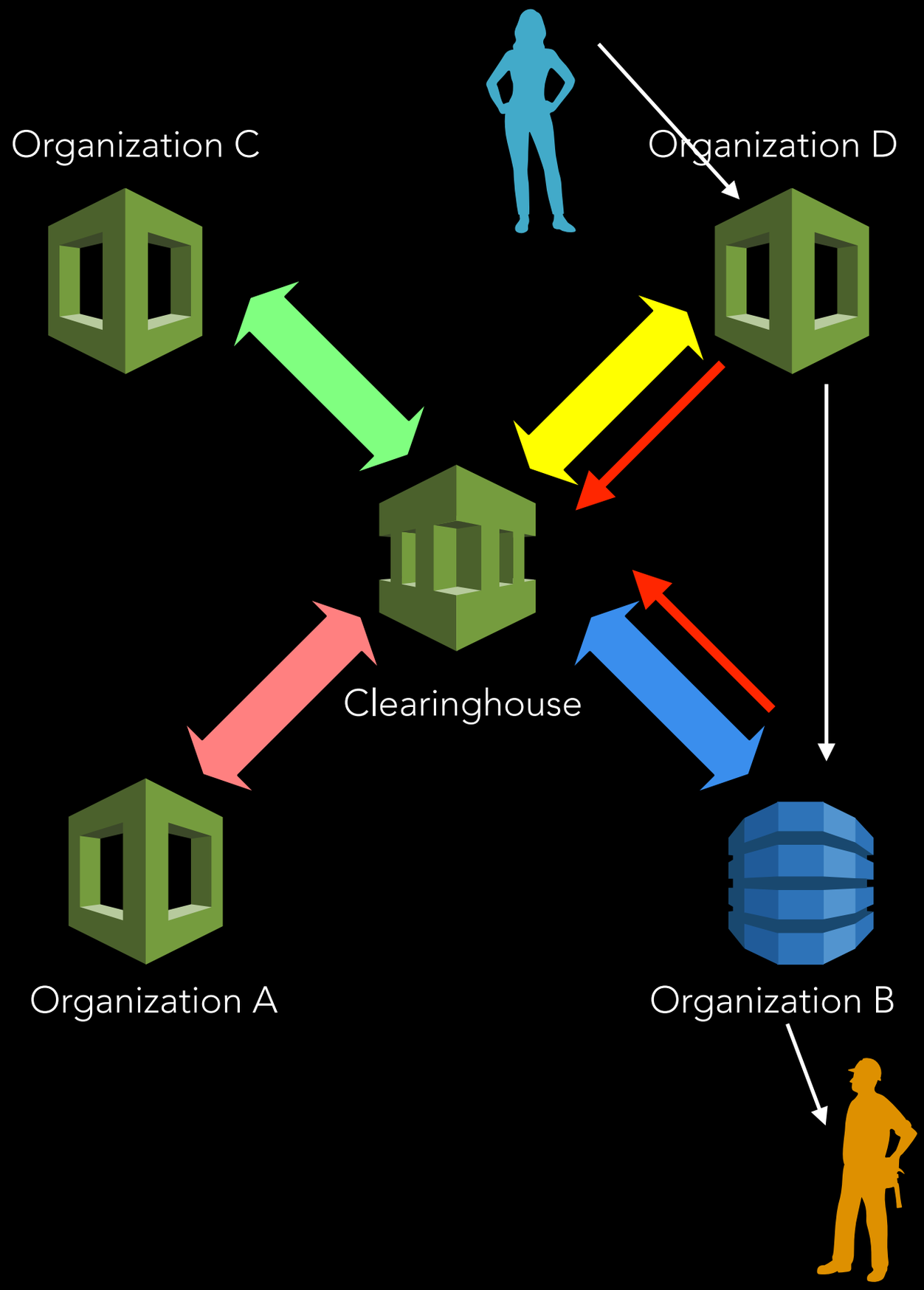
CLEARING-HOUSE

- One central "**trusted third party**" keeps the database
  - Maintains the "final" version
- Everyone sends their data to this third party
- Cost, robustness, and time
- Confidentiality!



CLEARING-HOUSE

- One central "**trusted third party**" keeps the database
  - Maintains the "final" version
- Everyone sends their data to this third party
- Cost, robustness, and time
- Confidentiality!



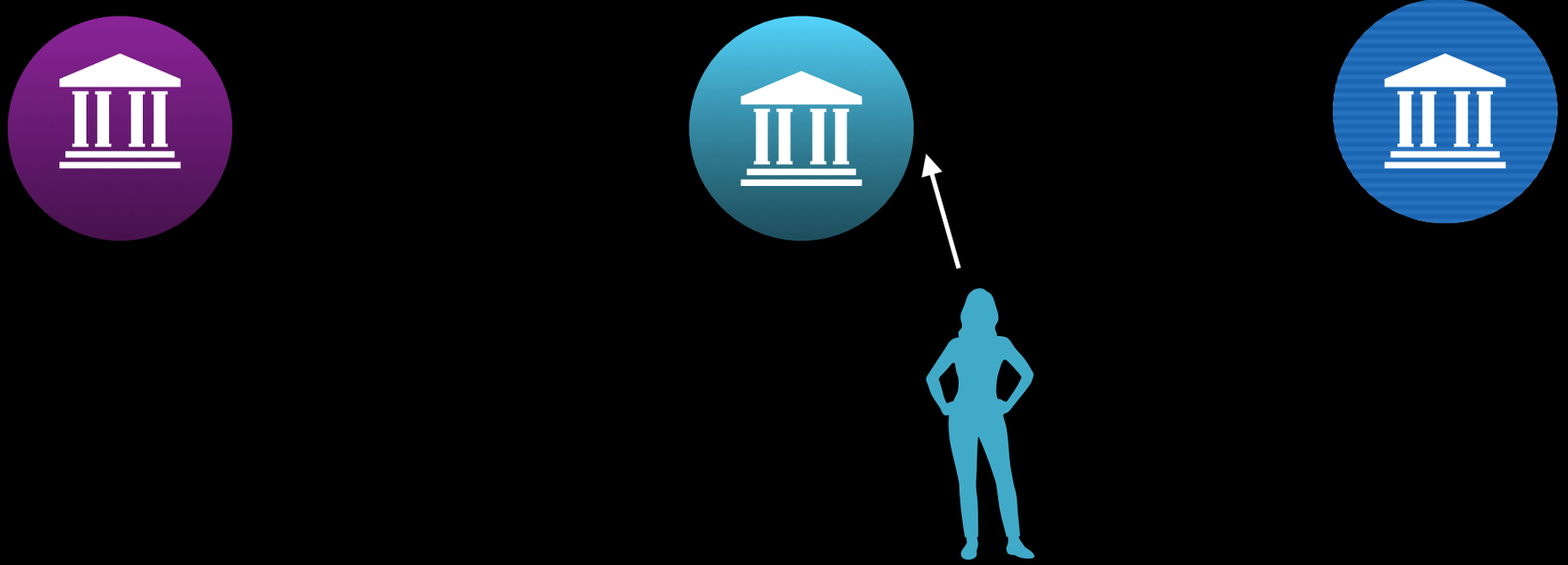
DISINTERMEDIATION

- “reduction in the use of intermediaries between producers and consumers, for example by investing directly in the securities market rather than through a bank.”
- Mac OS X Dictionary

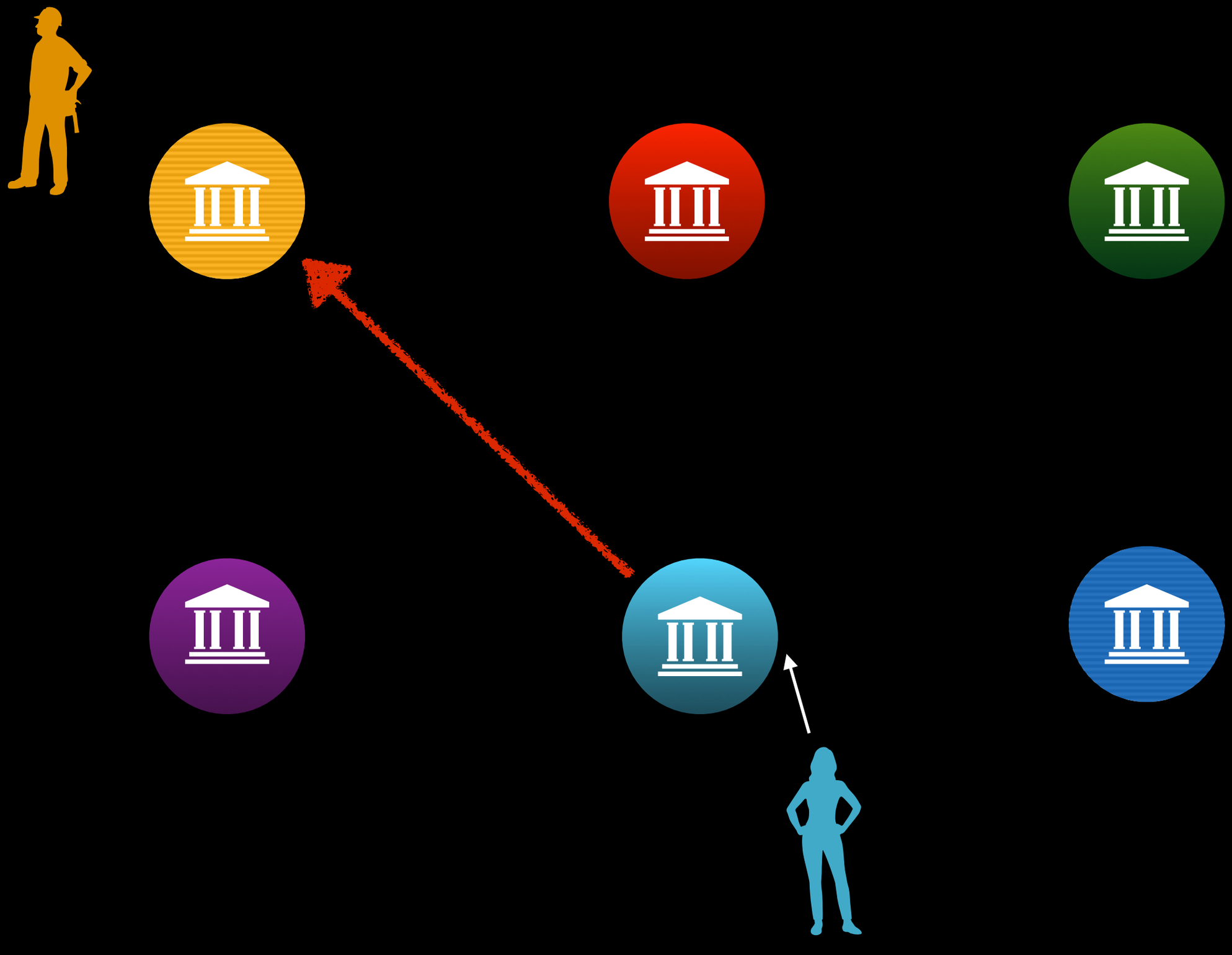
Source: http://blog.omnipress.com/wp-content/uploads/2015/07/Middleman-Sm.jpg

NETWORKS OF PEERS

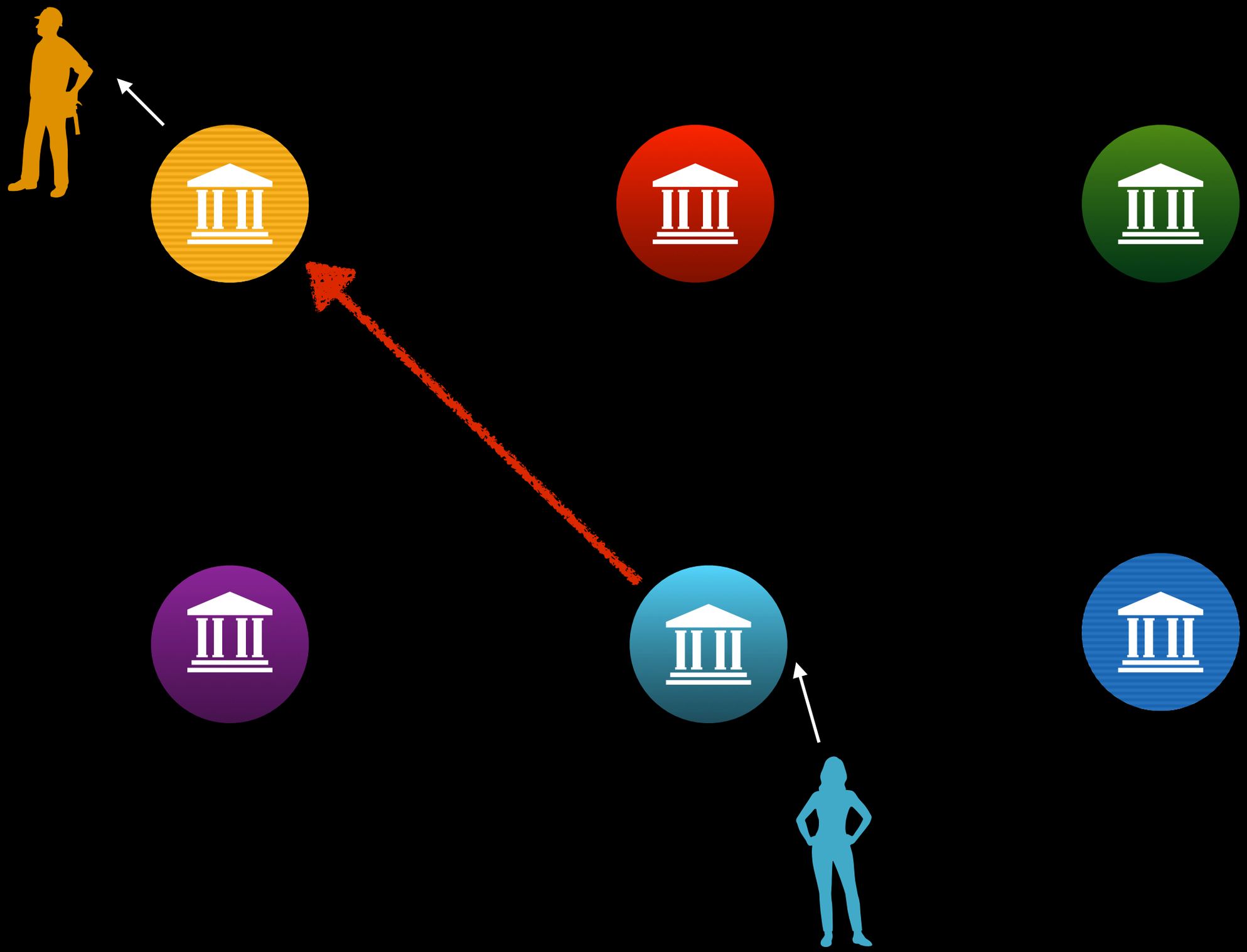
NETWORKS OF PEERS



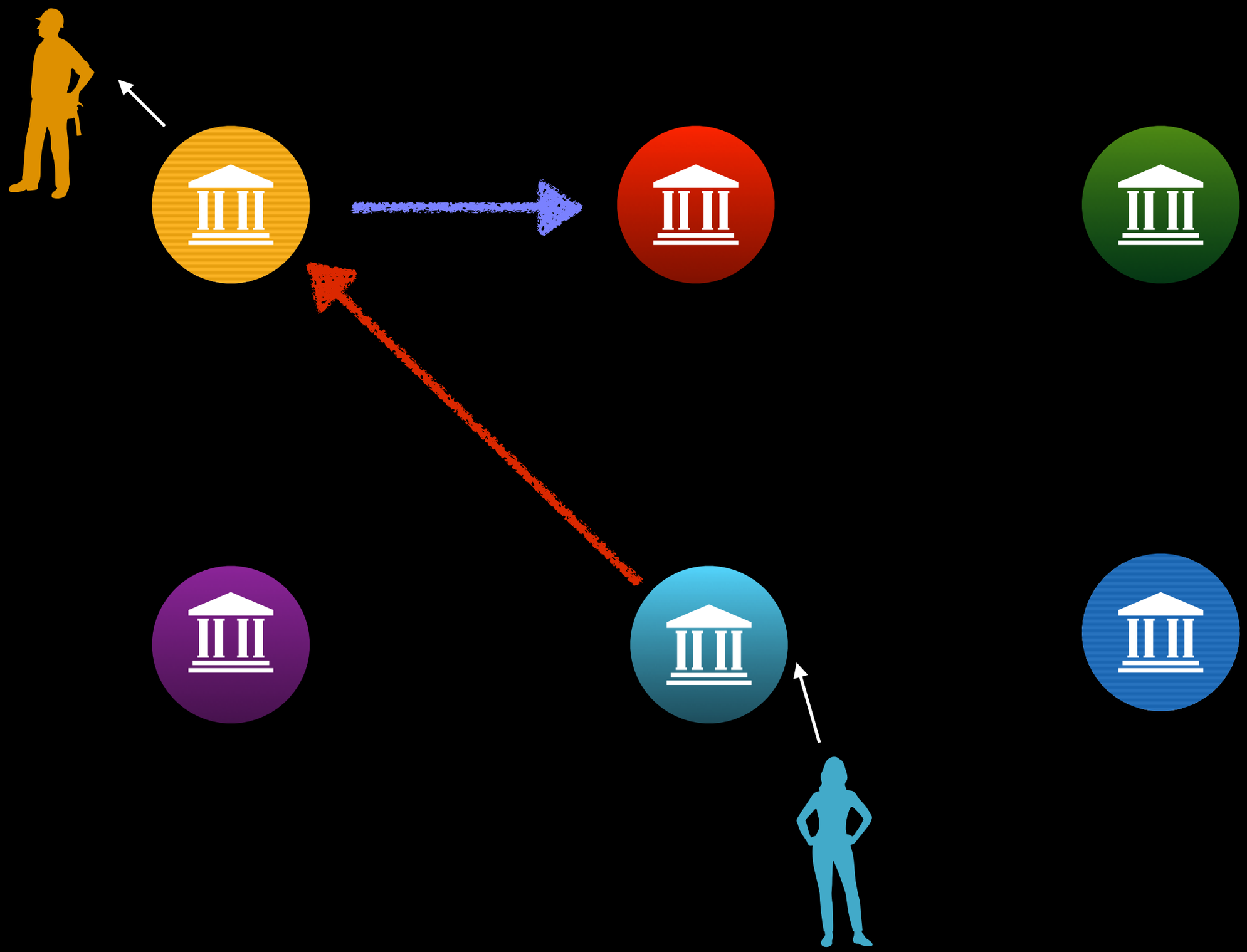
NETWORKS OF PEERS



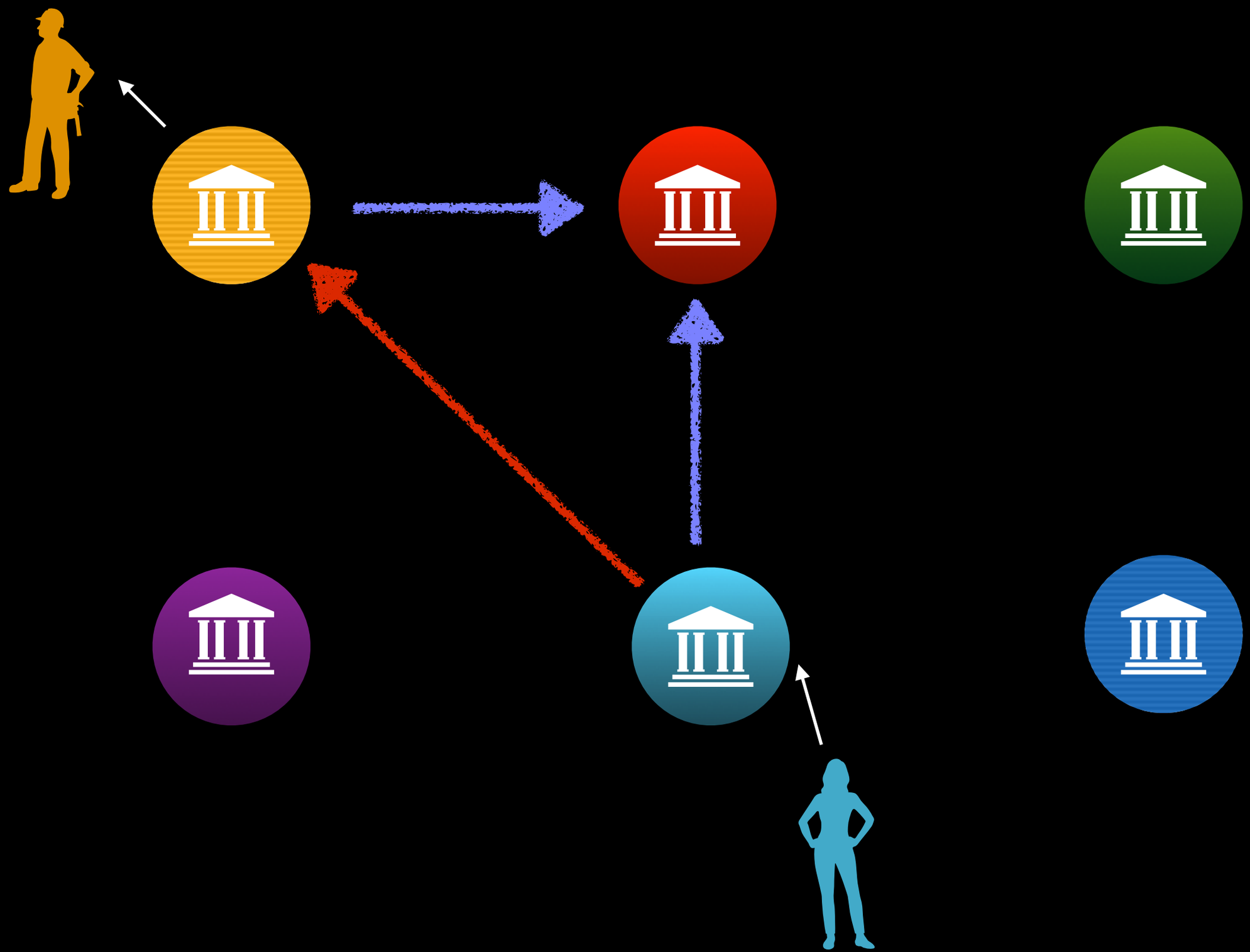
NETWORKS OF PEERS



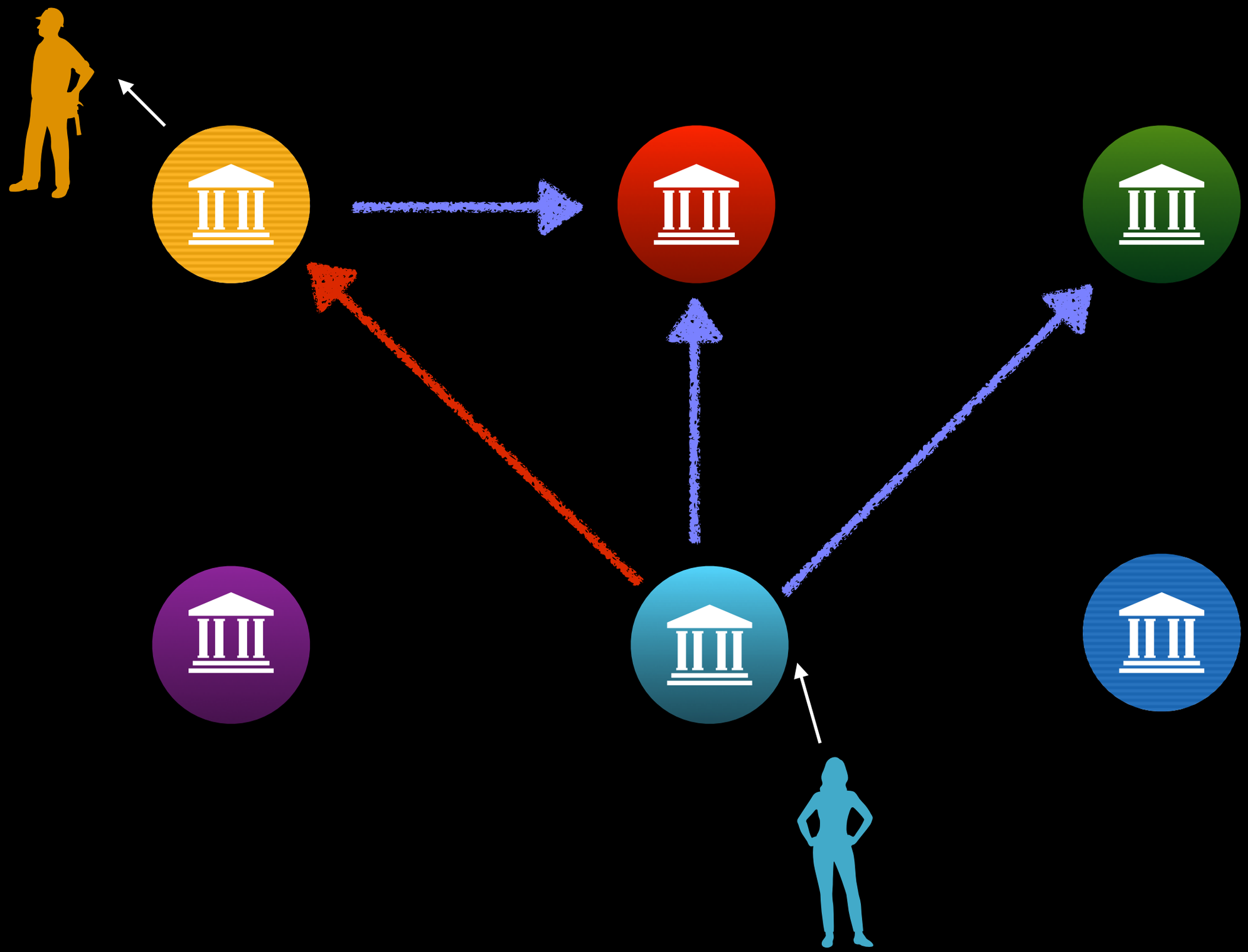
NETWORKS OF PEERS



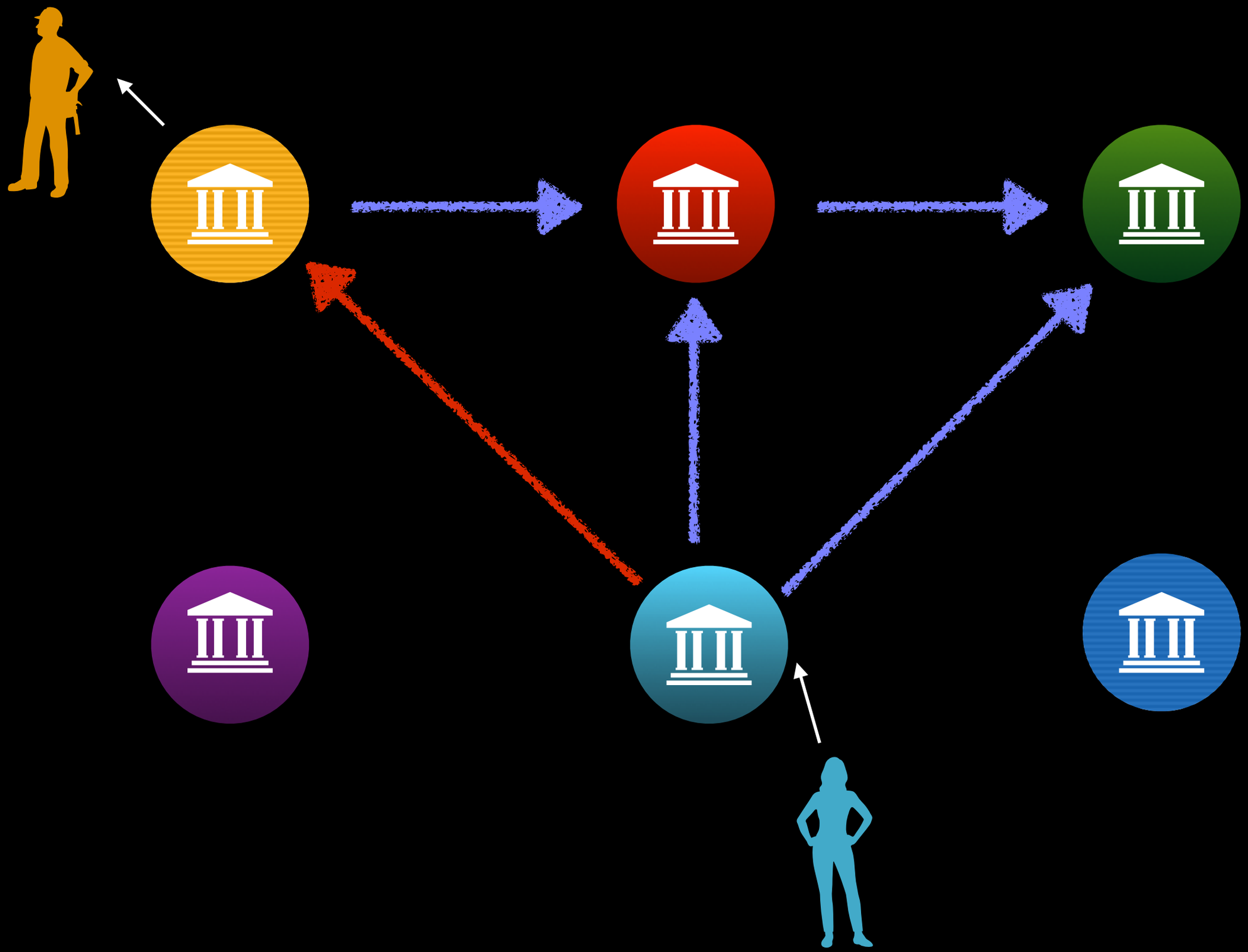
NETWORKS OF PEERS



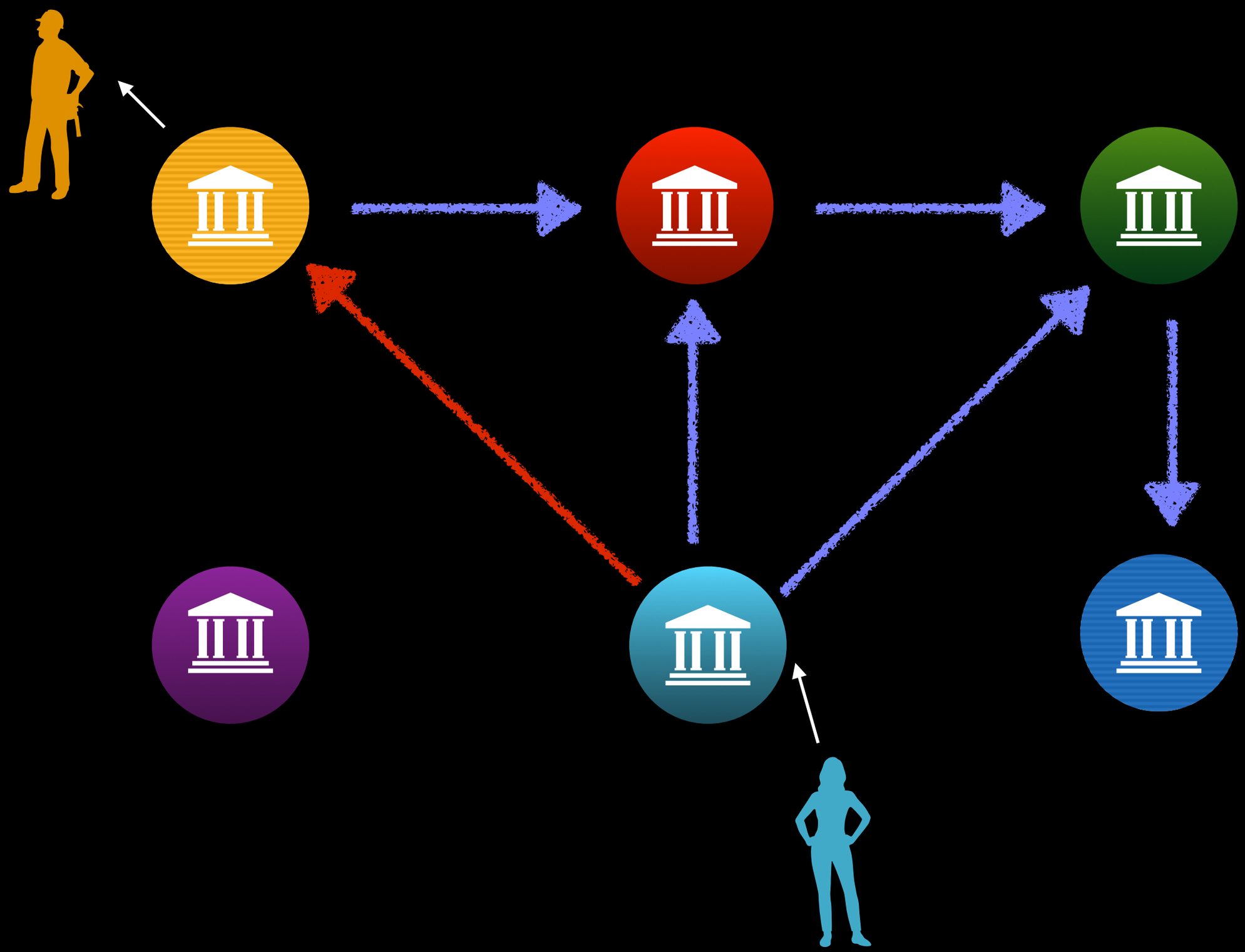
NETWORKS OF PEERS



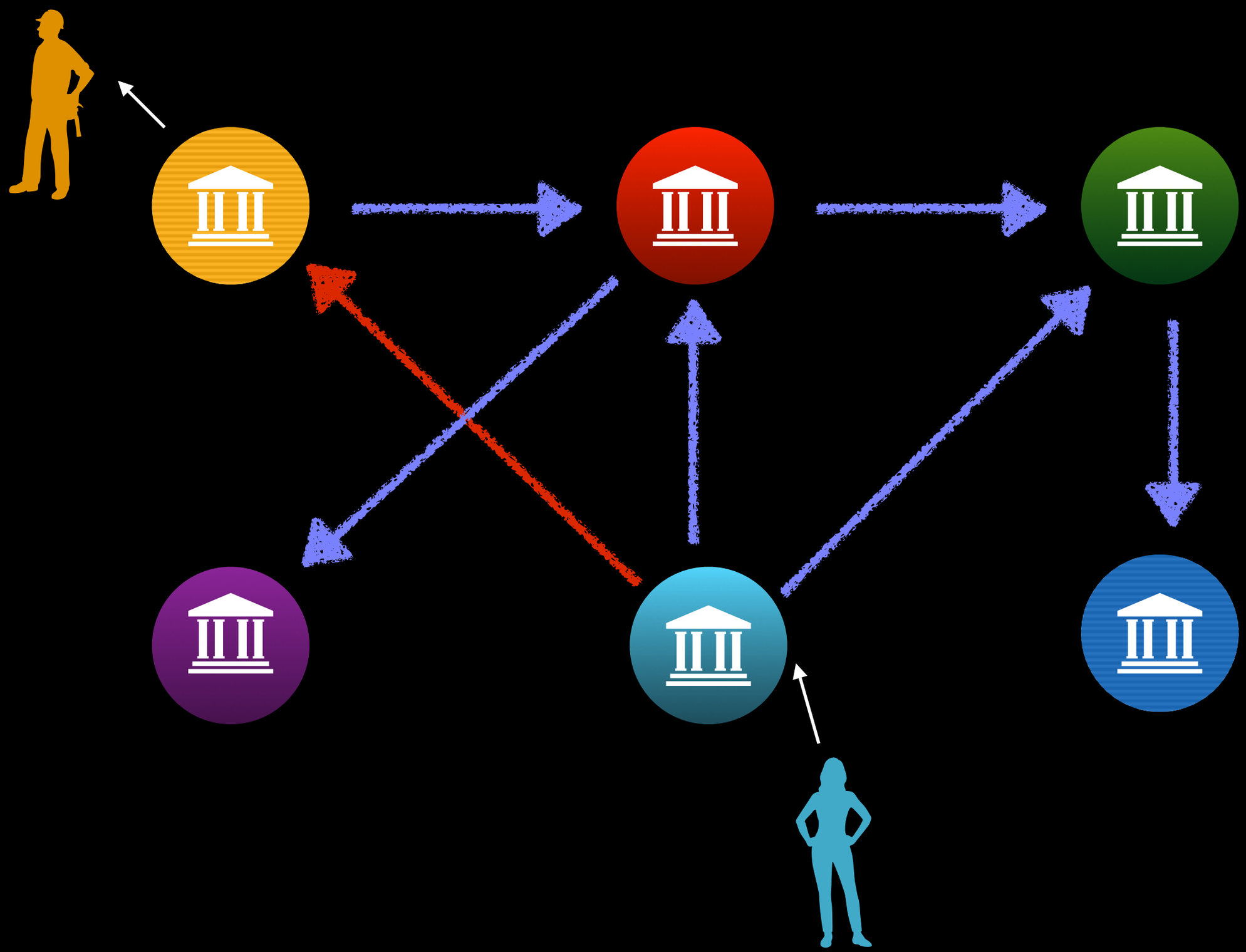
NETWORKS OF PEERS



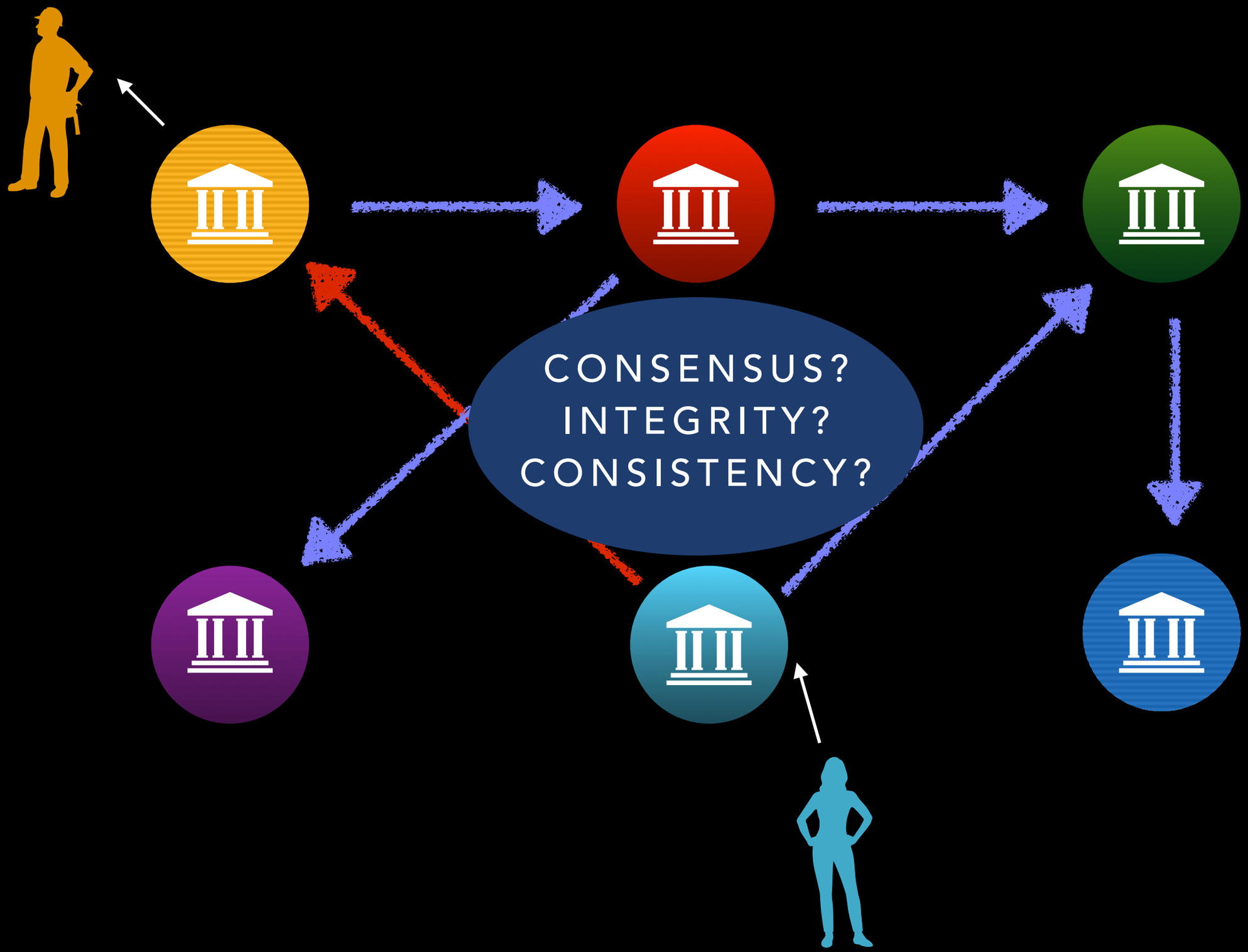
NETWORKS OF PEERS



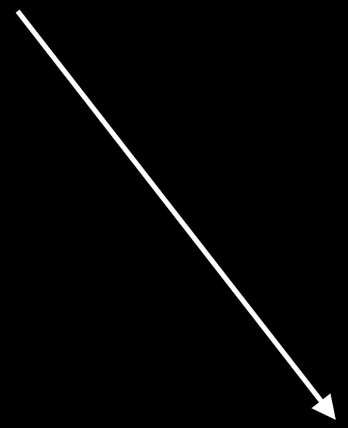
NETWORKS OF PEERS



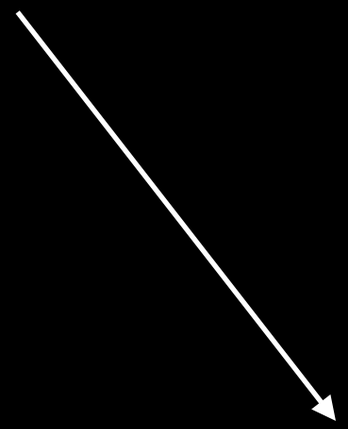
NETWORKS OF PEERS



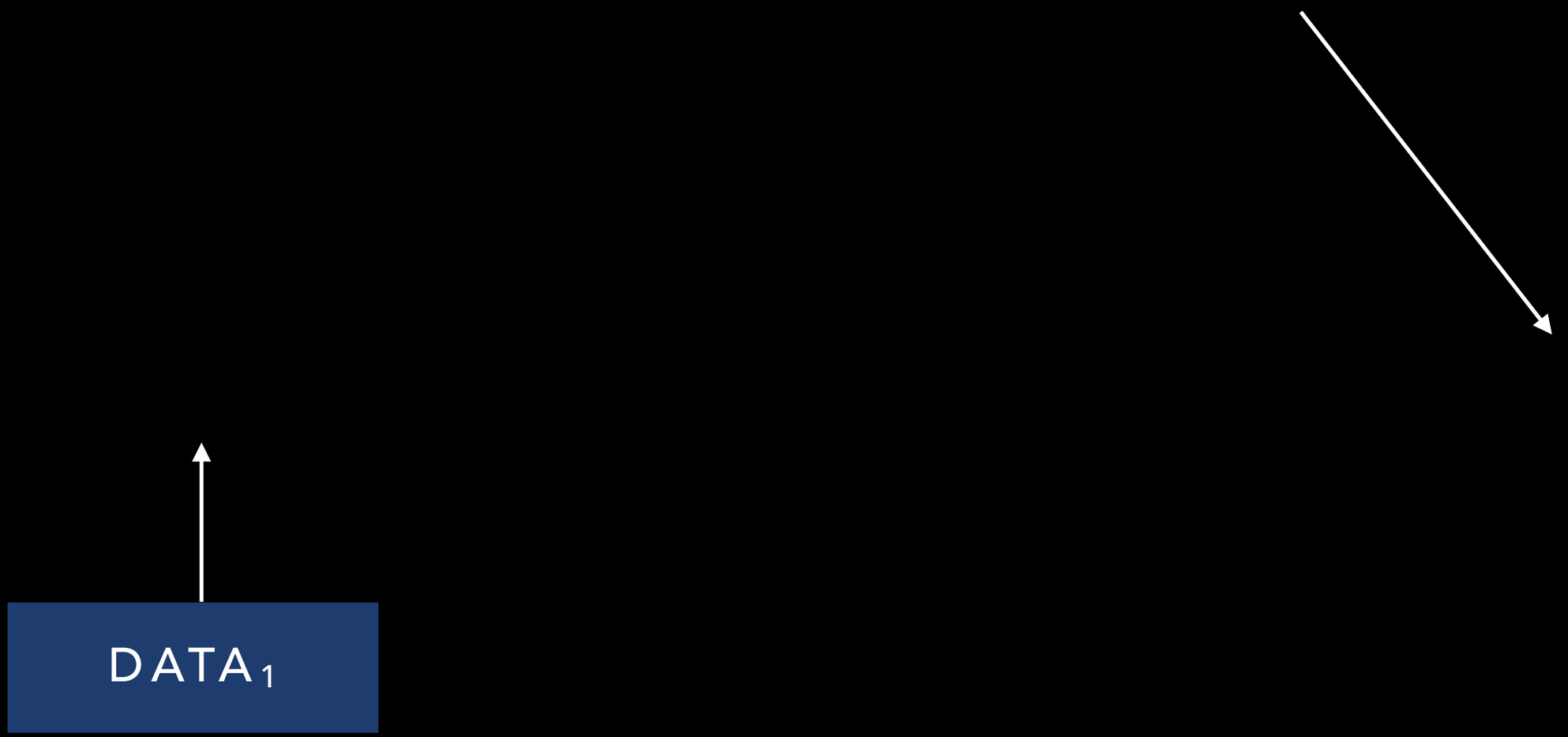
CHAINING AND BLOCK CHAINING



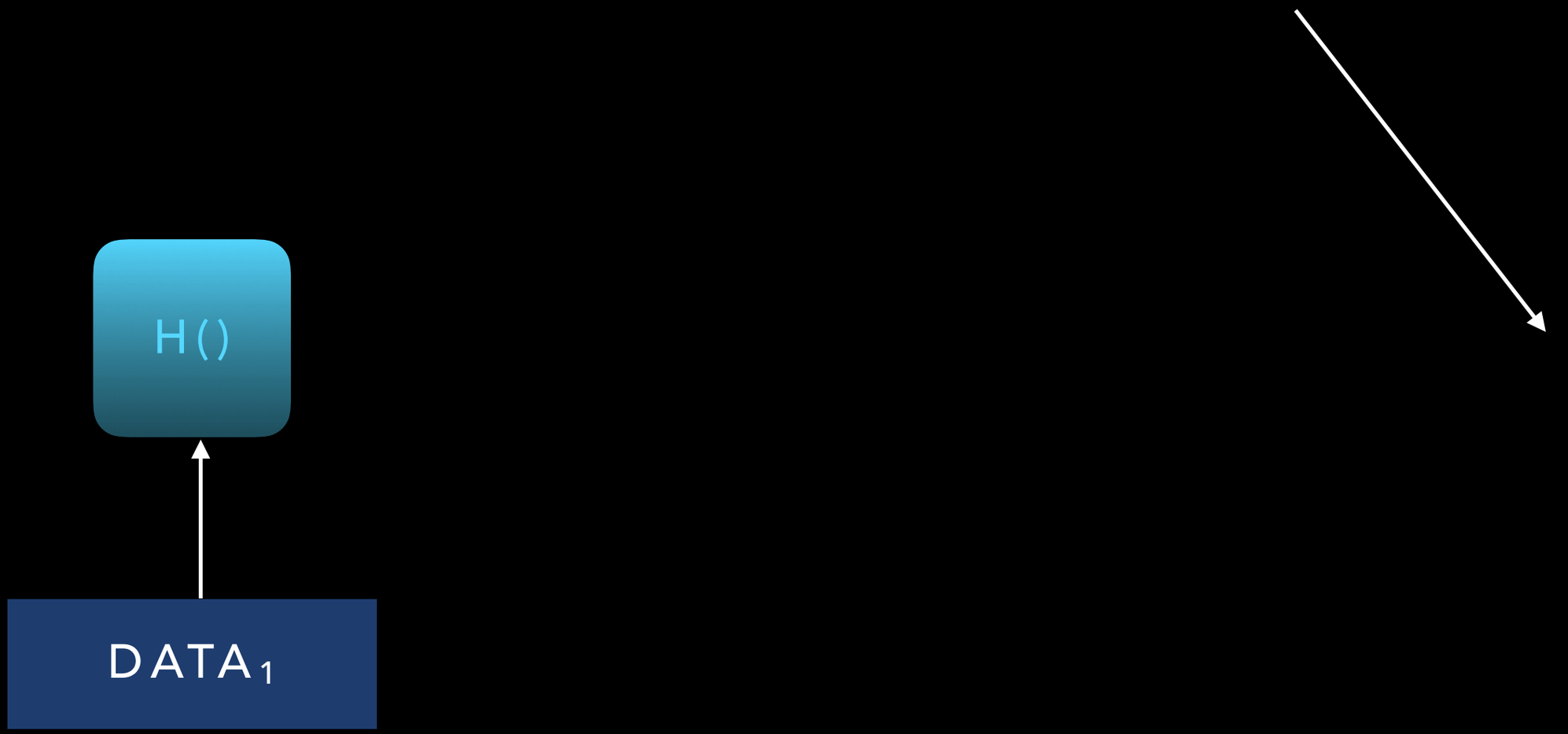
CHAINING AND BLOCK CHAINING



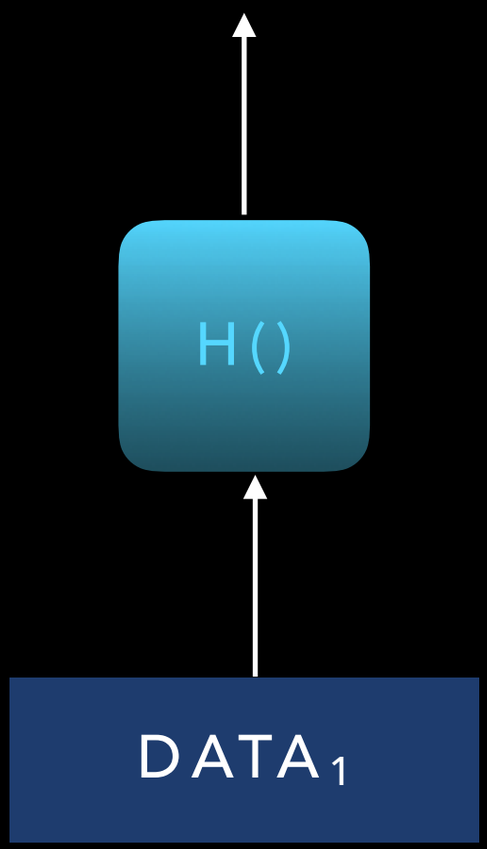
CHAINING AND BLOCK CHAINING



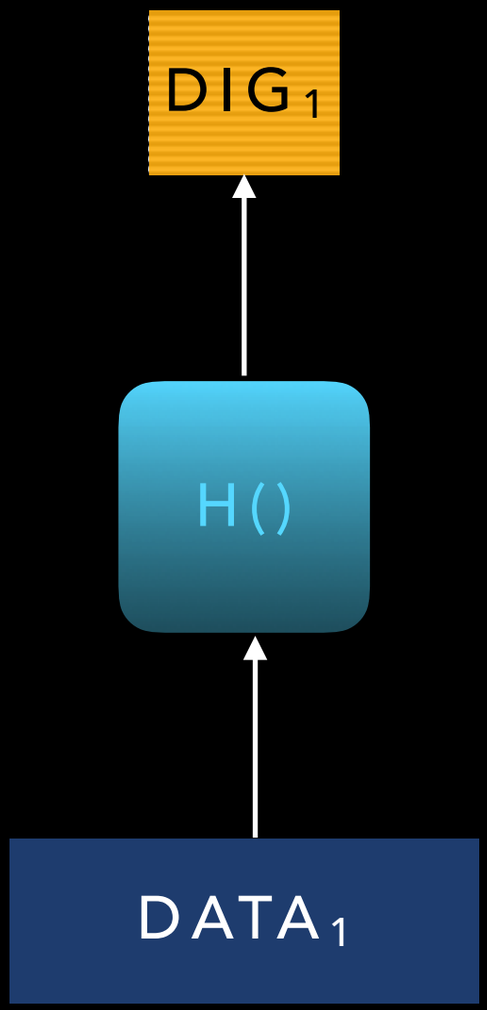
CHAINING AND BLOCK CHAINING



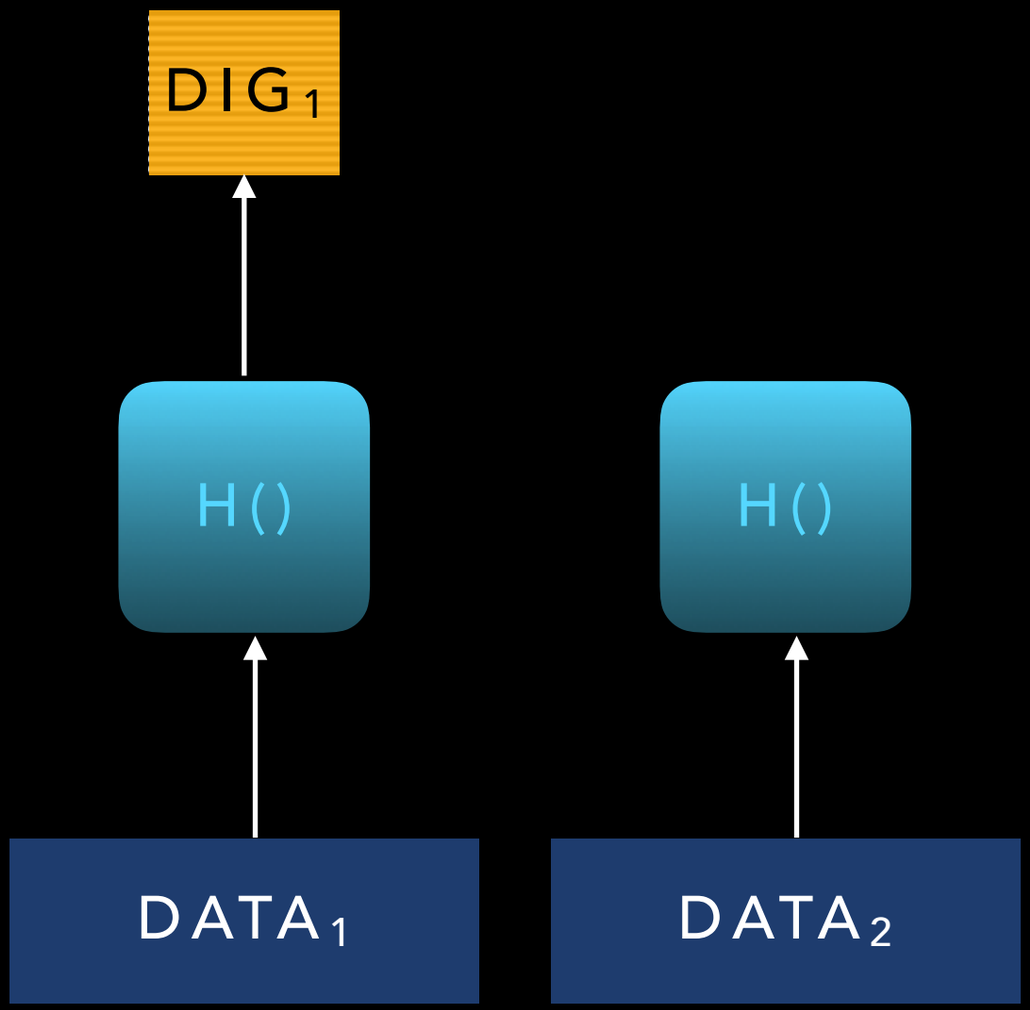
CHAINING AND BLOCK CHAINING



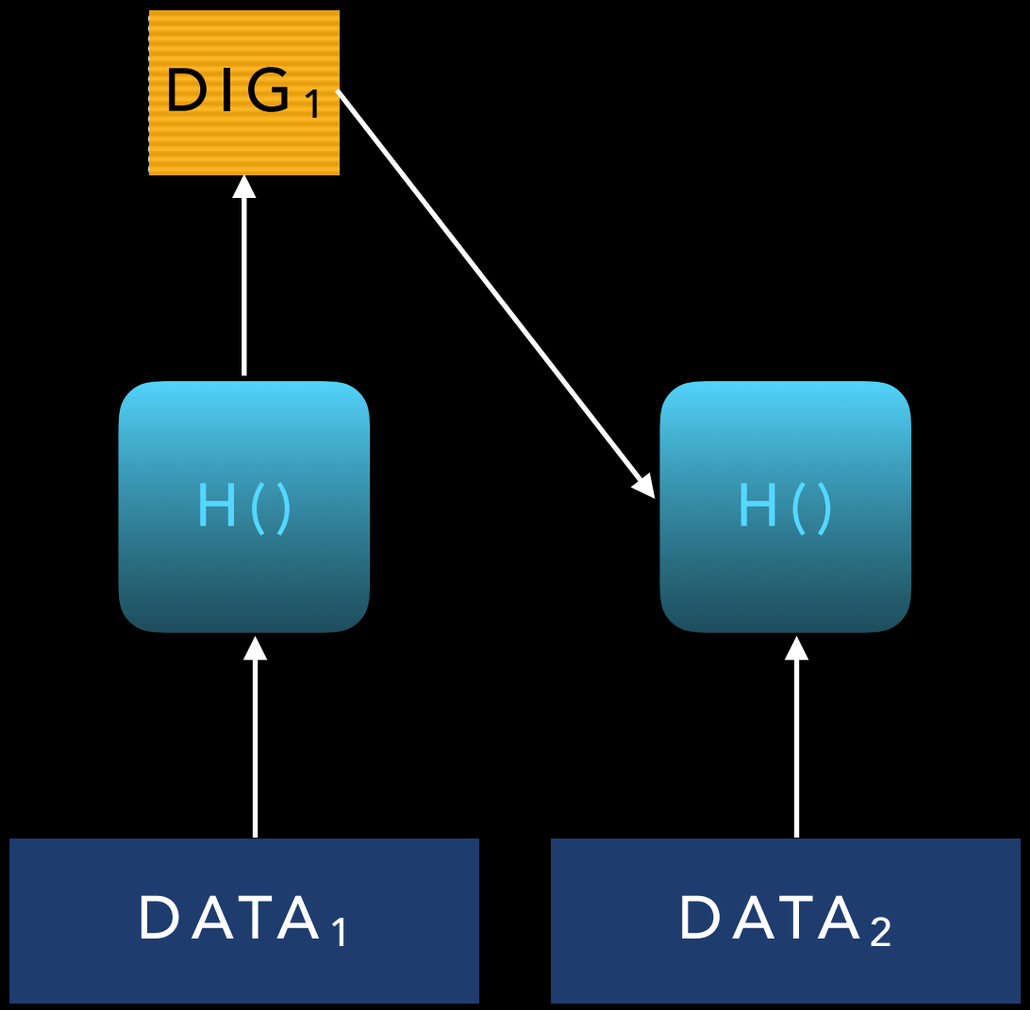
CHAINING AND BLOCK CHAINING



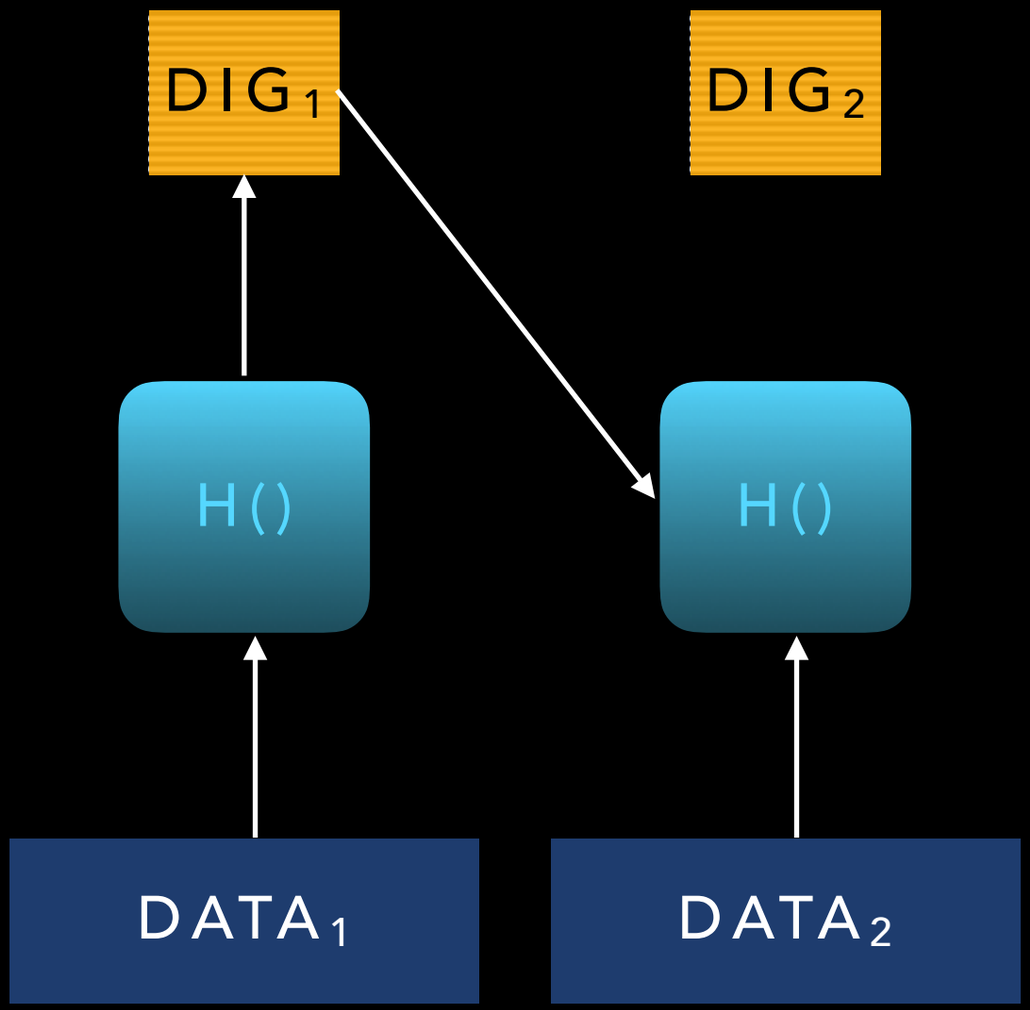
CHAINING AND BLOCK CHAINING



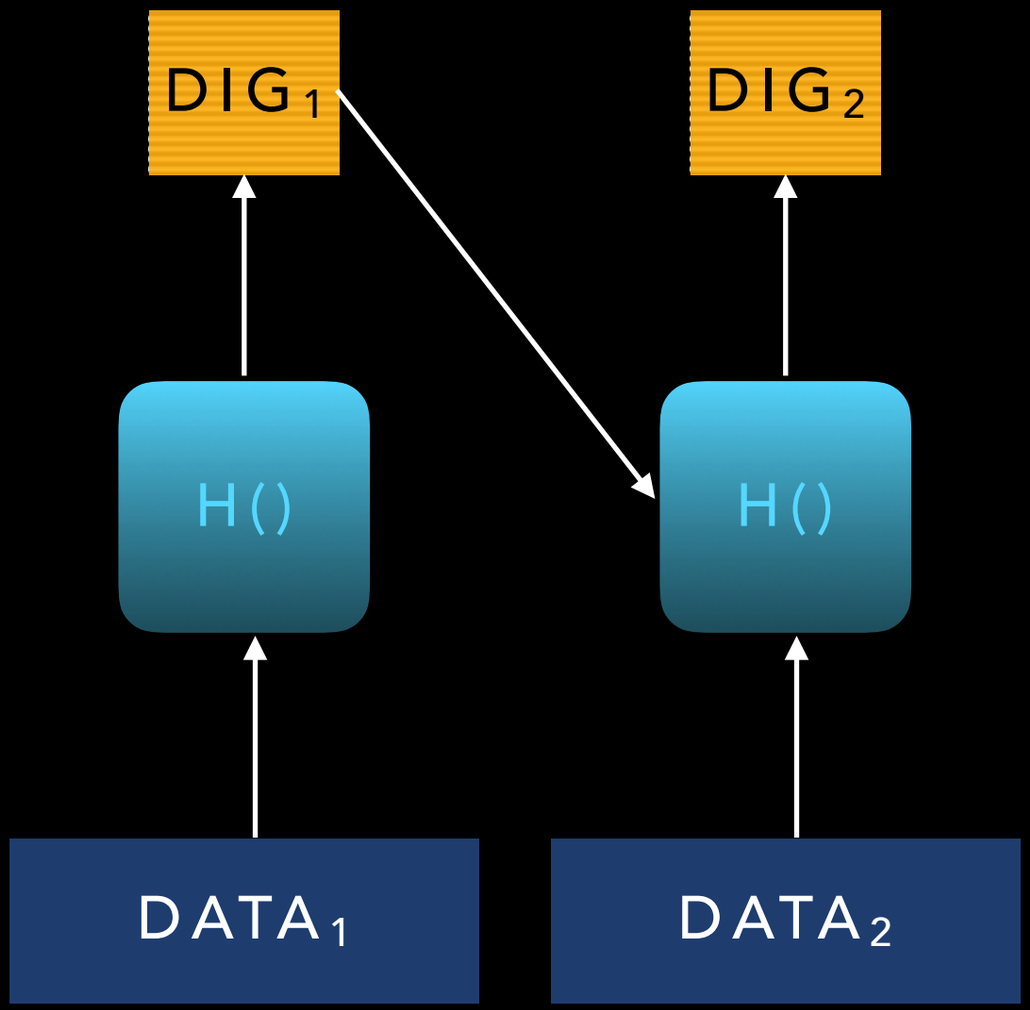
CHAINING AND BLOCK CHAINING



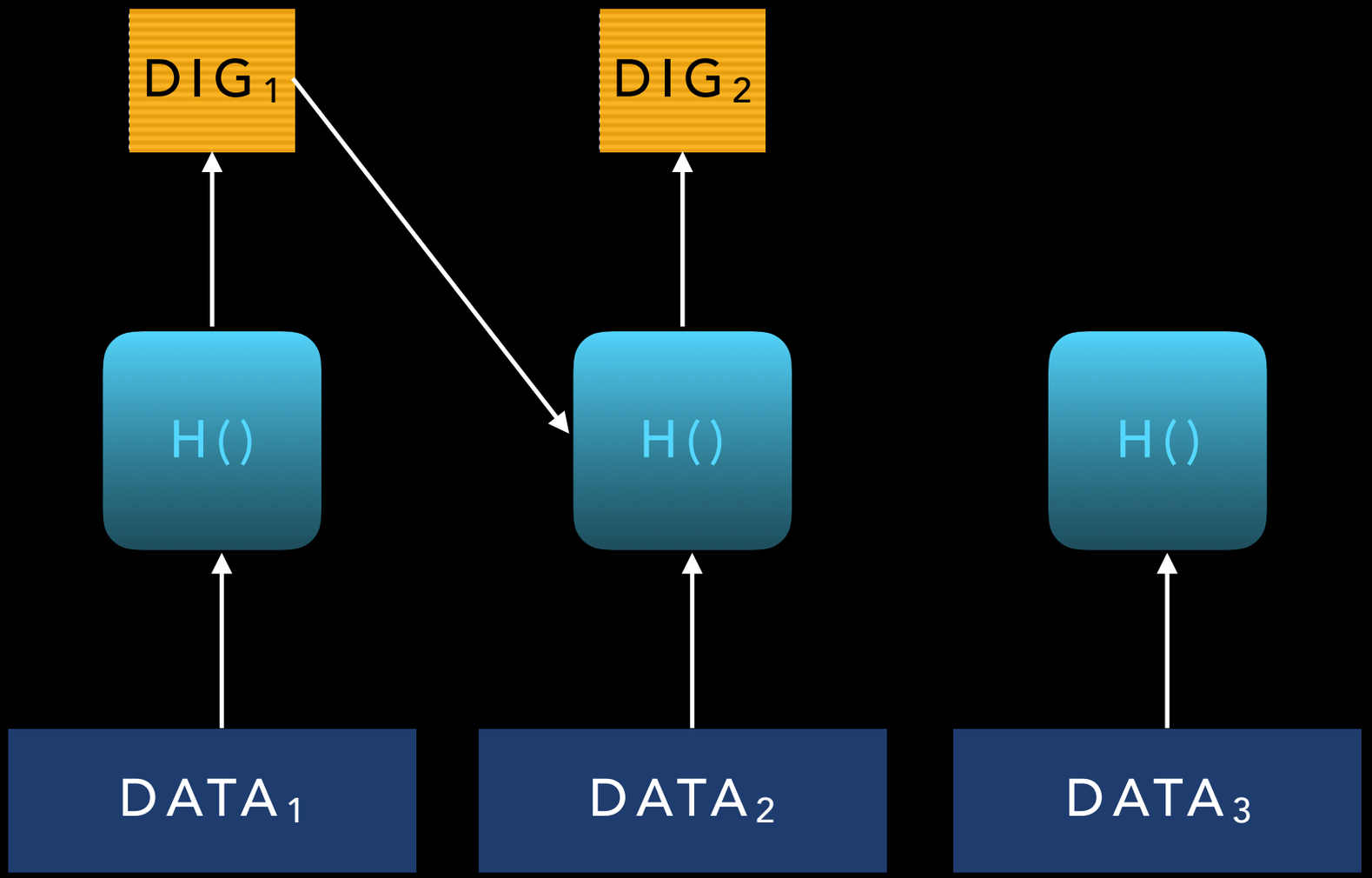
CHAINING AND BLOCK CHAINING



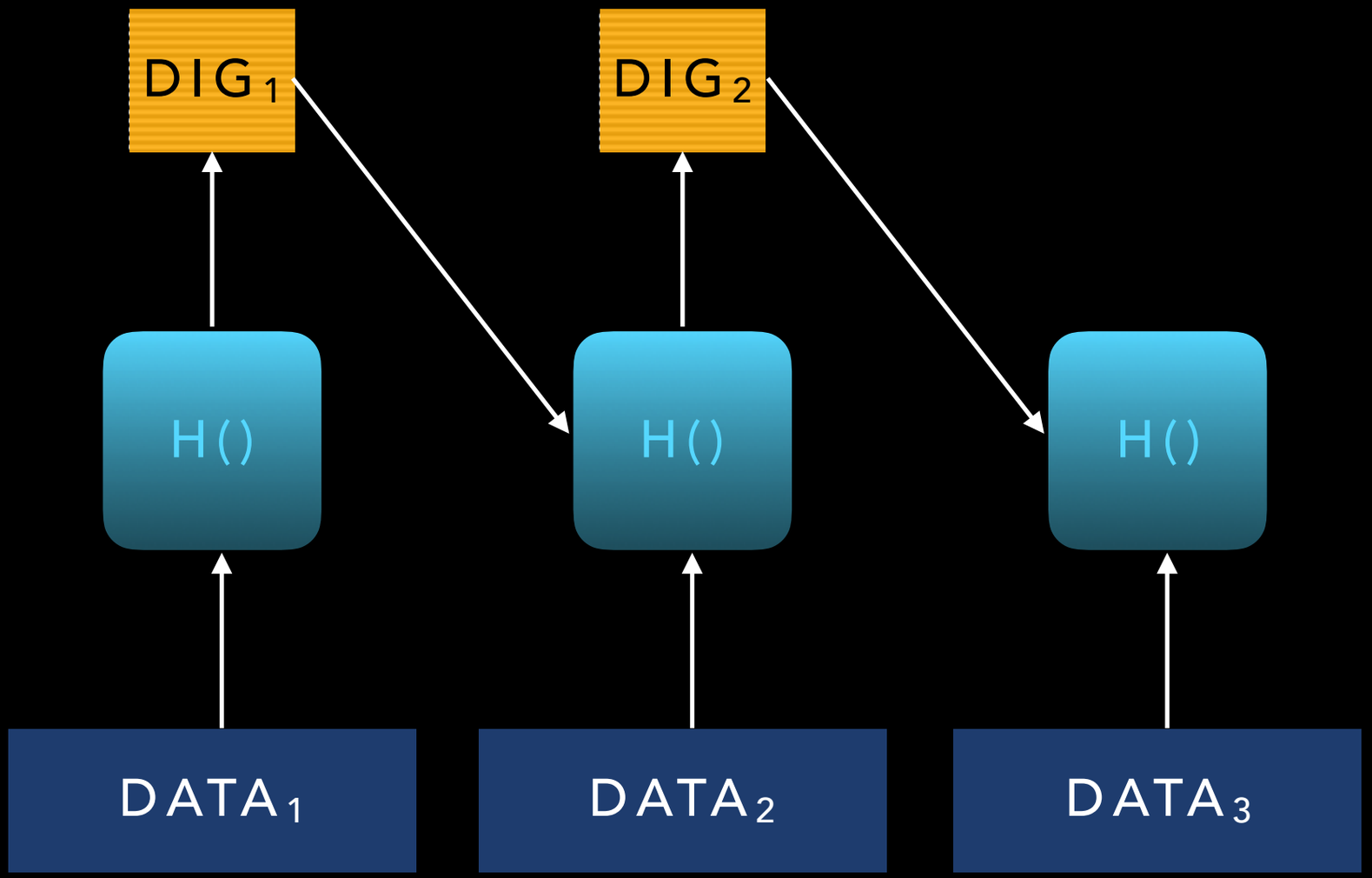
CHAINING AND BLOCK CHAINING



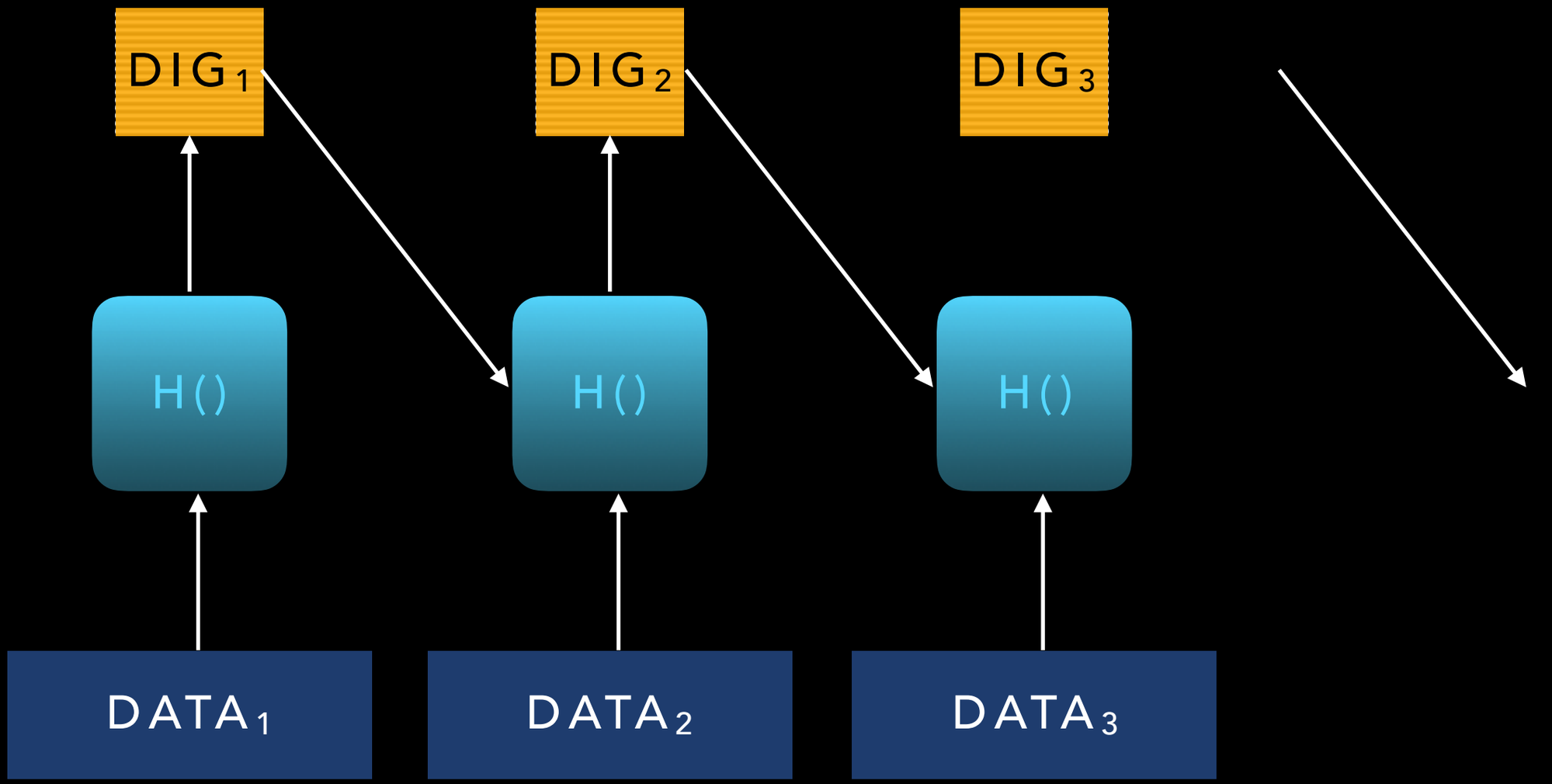
CHAINING AND BLOCK CHAINING



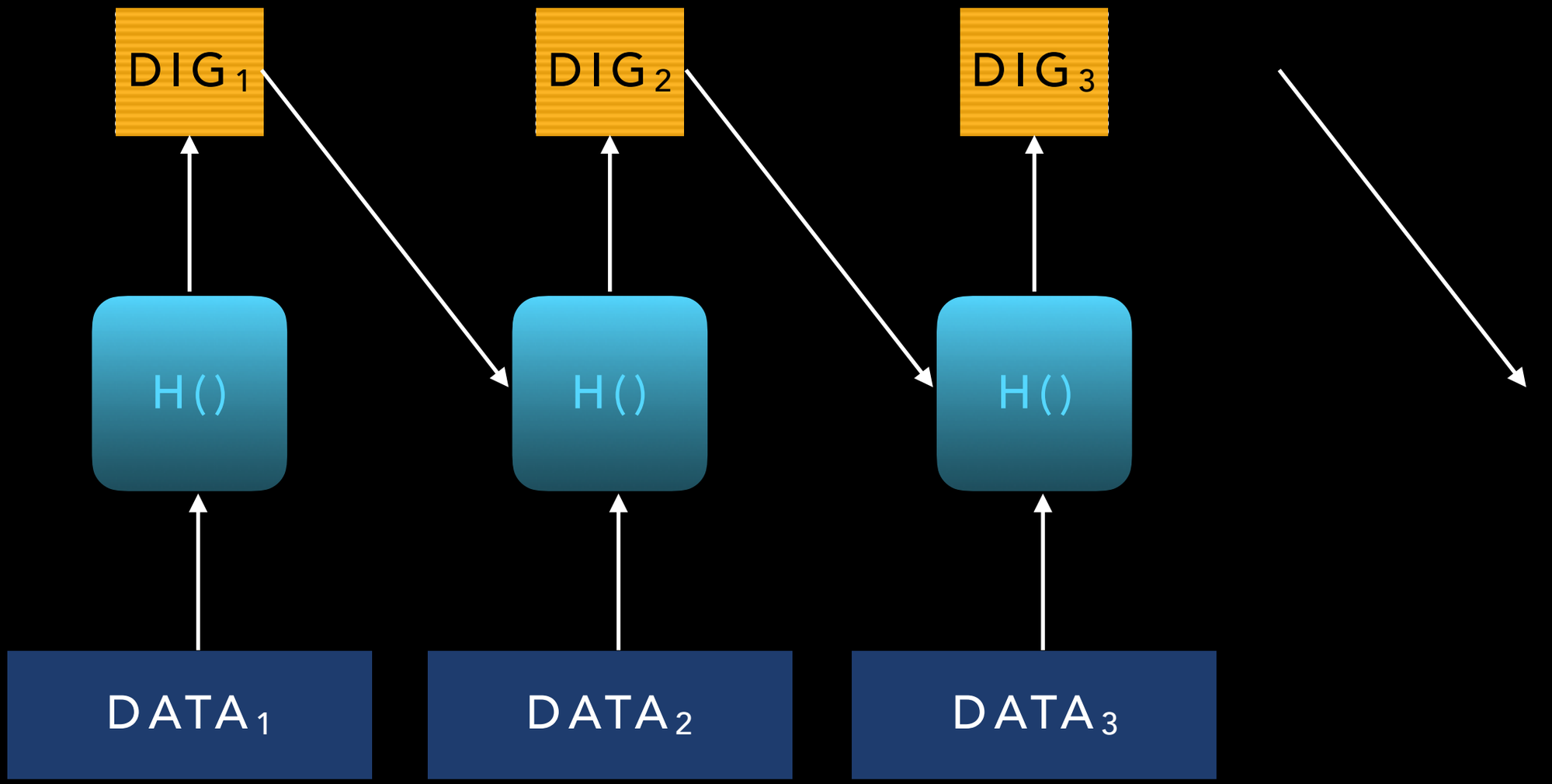
CHAINING AND BLOCK CHAINING



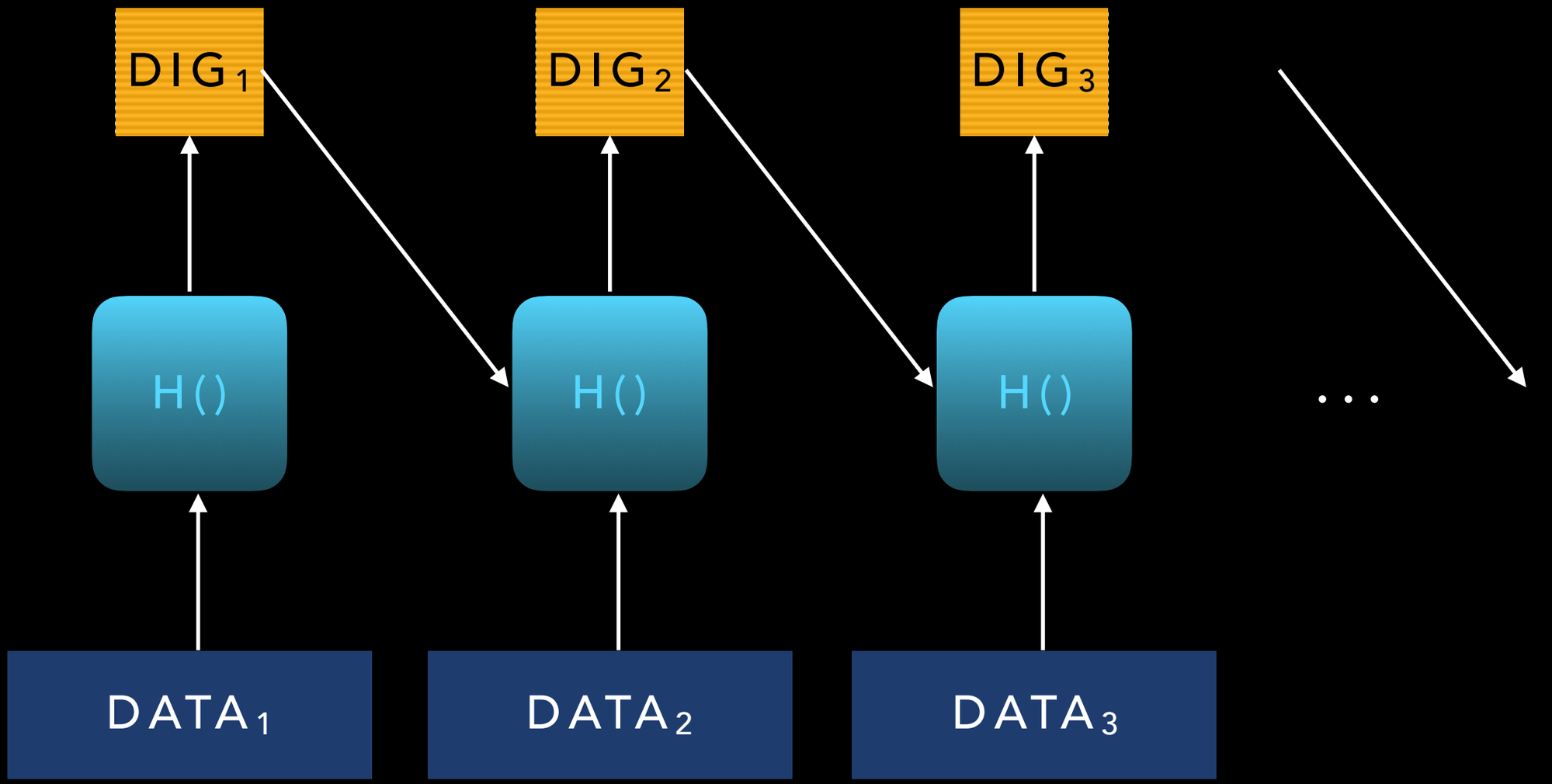
CHAINING AND BLOCK CHAINING



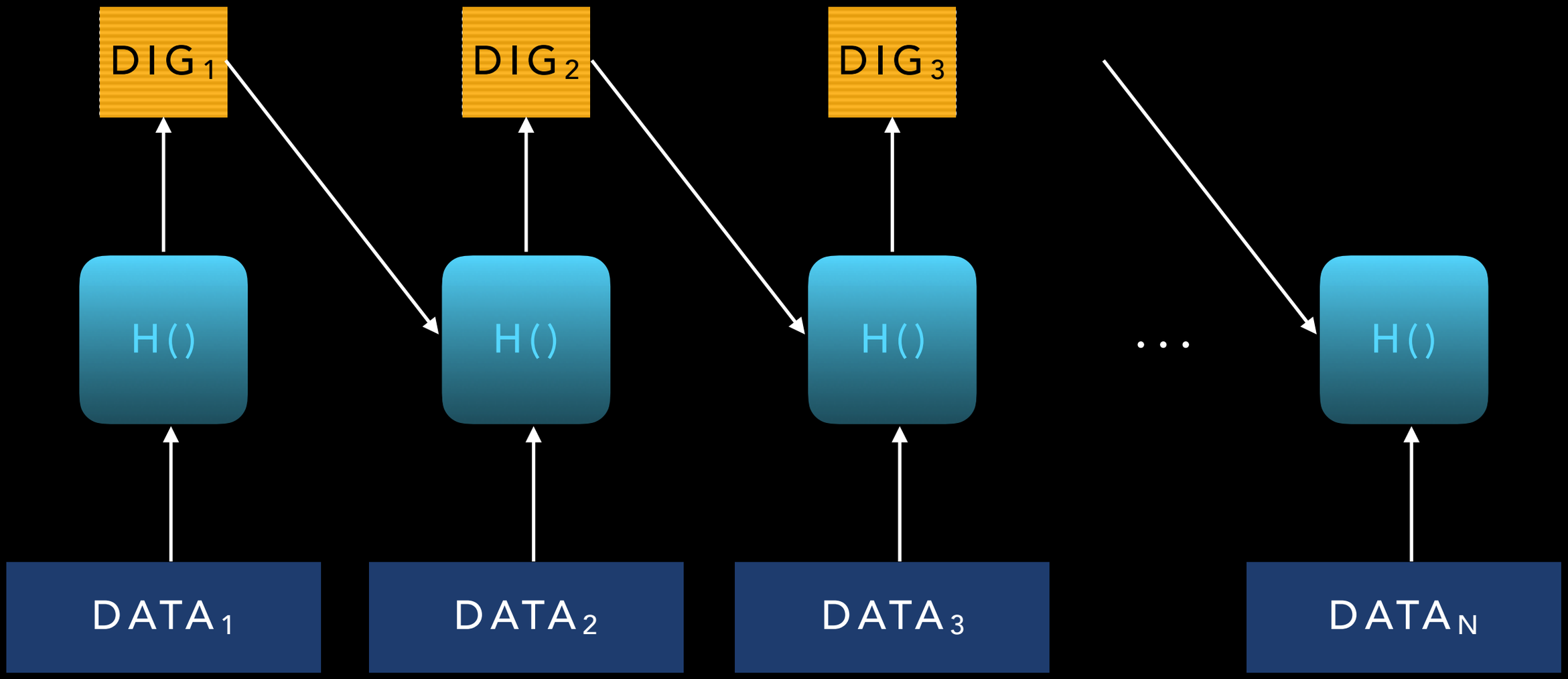
CHAINING AND BLOCK CHAINING



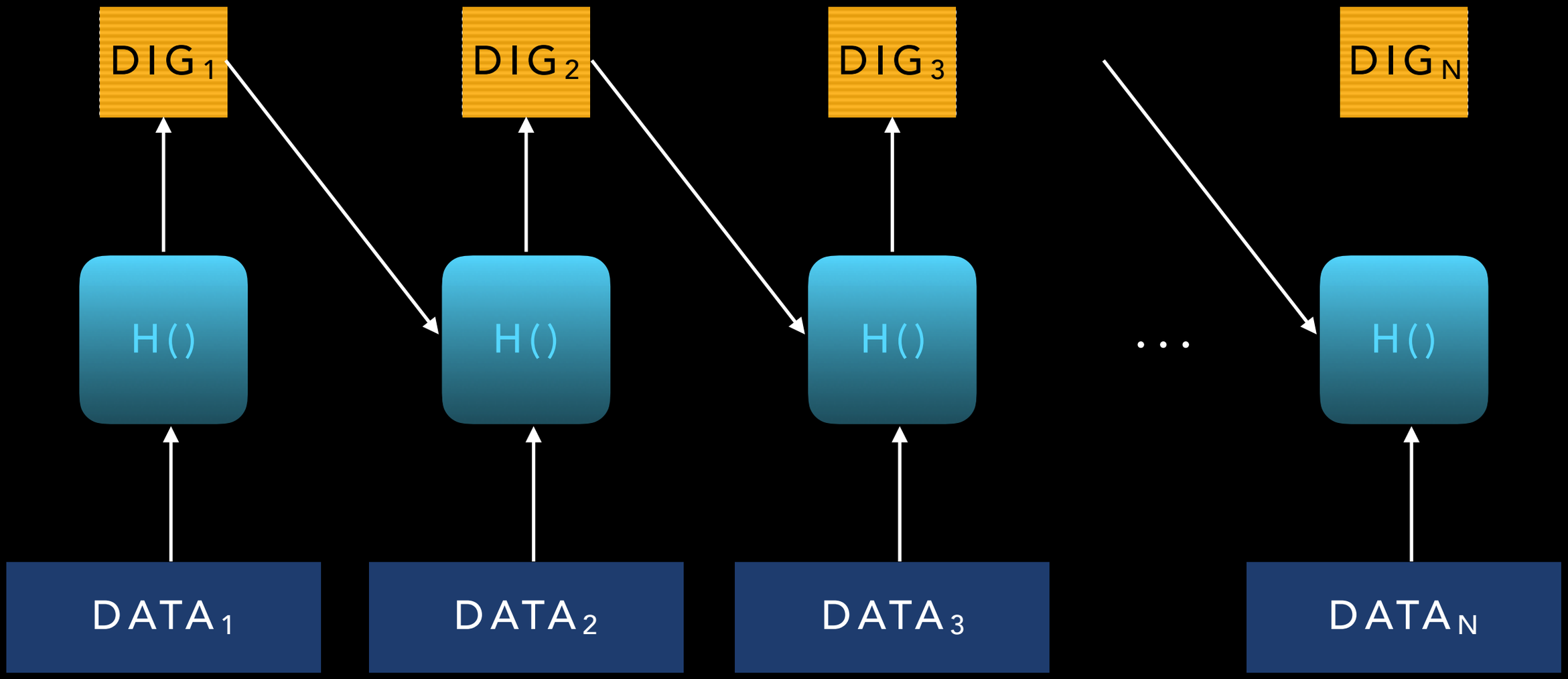
CHAINING AND BLOCK CHAINING



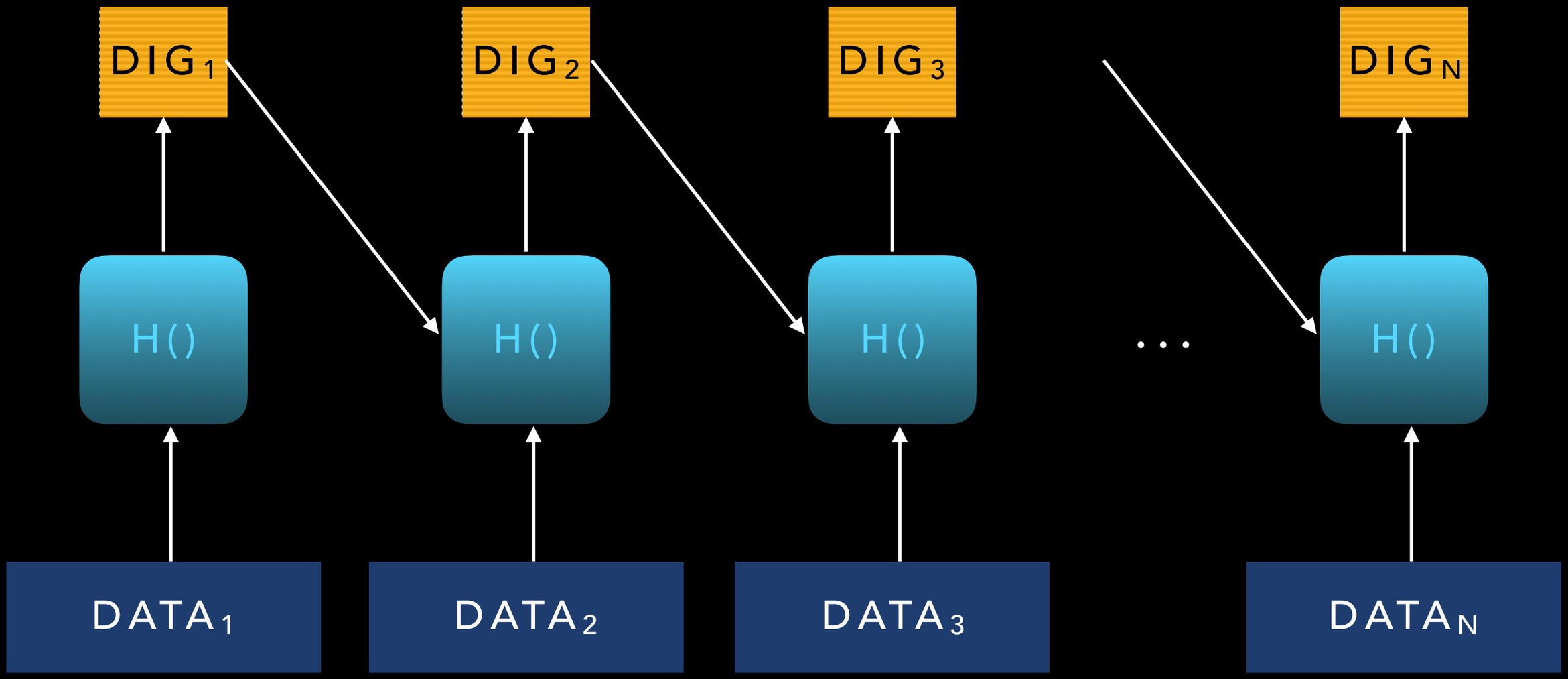
CHAINING AND BLOCK CHAINING



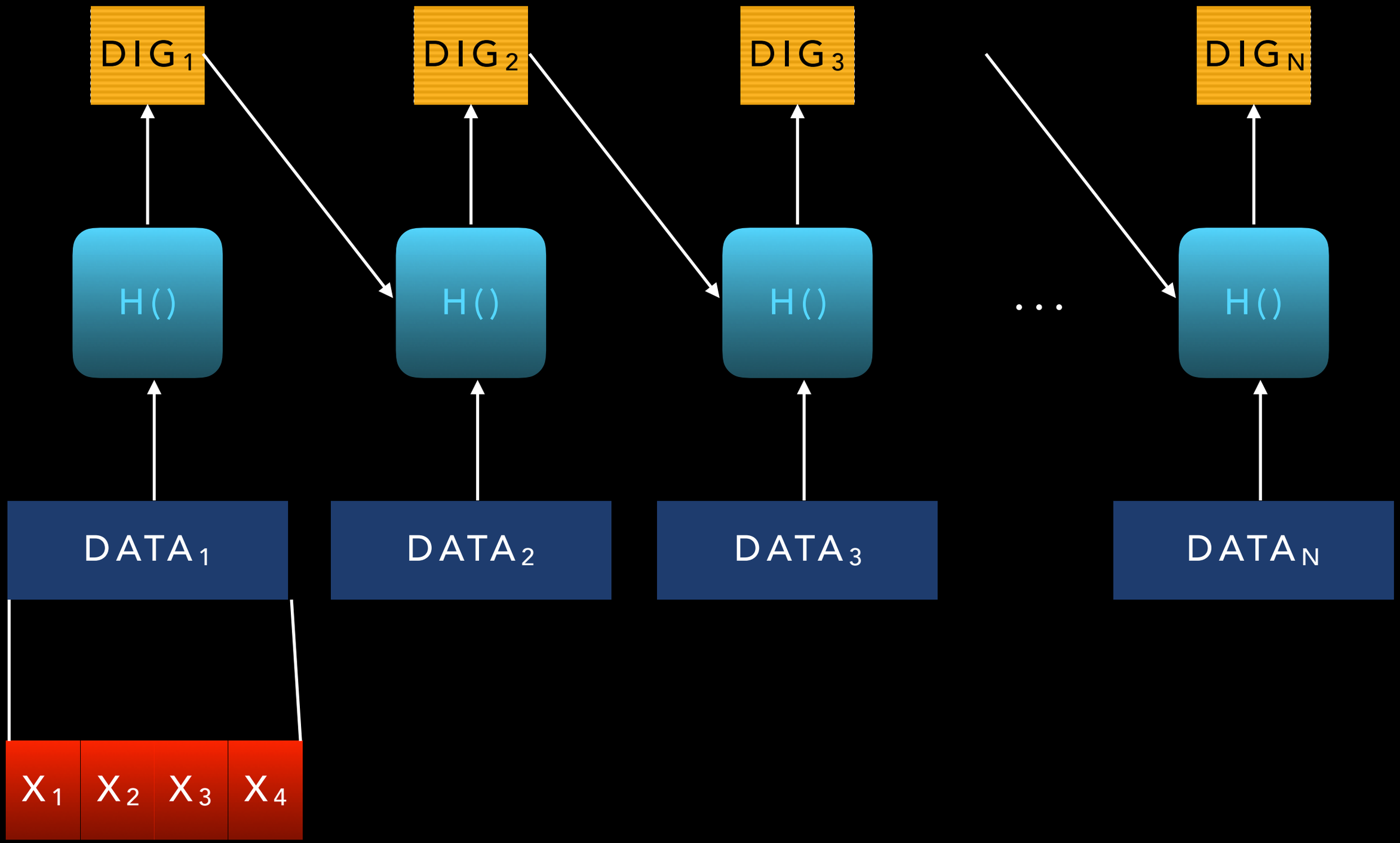
CHAINING AND BLOCK CHAINING



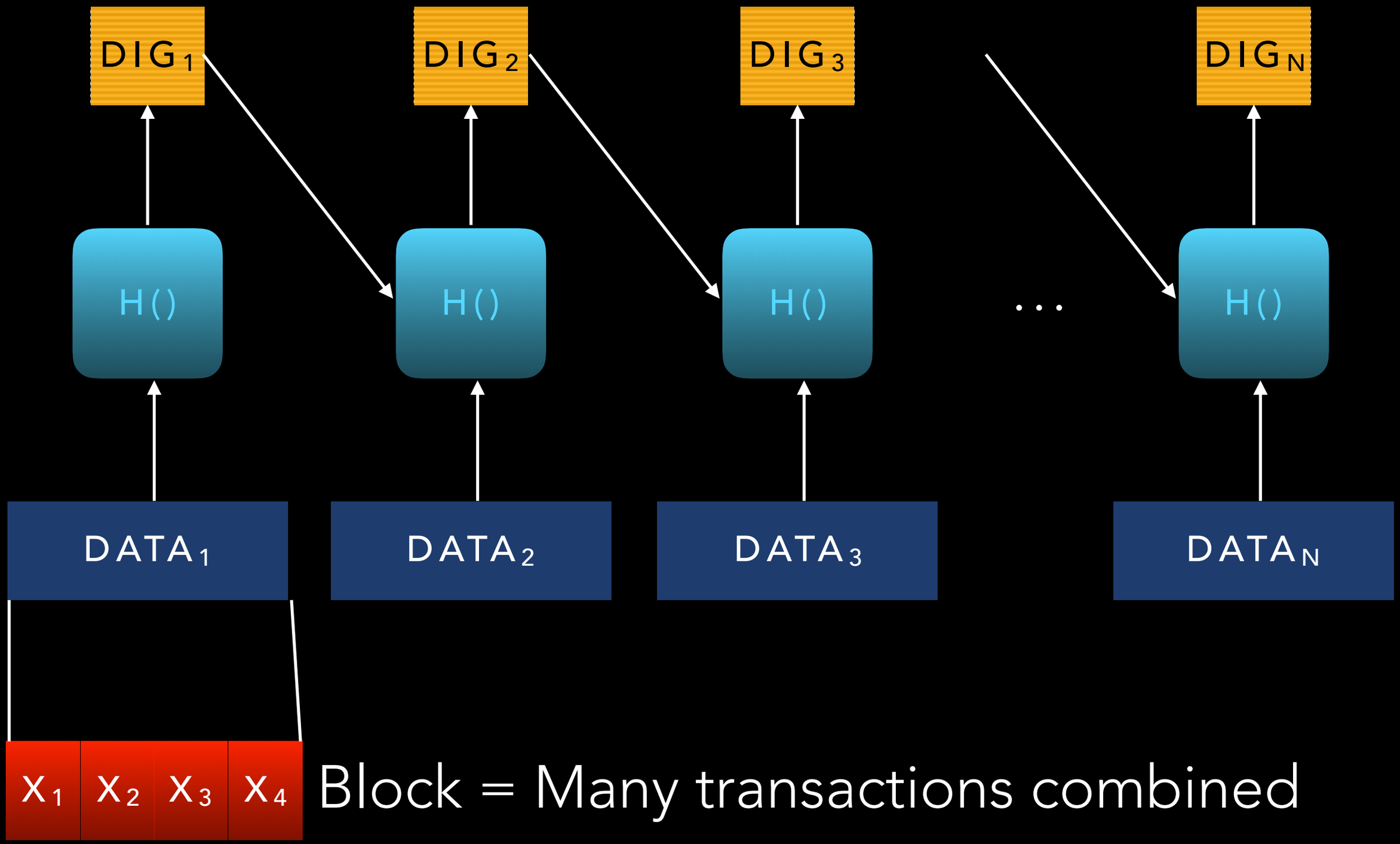
CHAINING AND BLOCK CHAINING



CHAINING AND BLOCK CHAINING

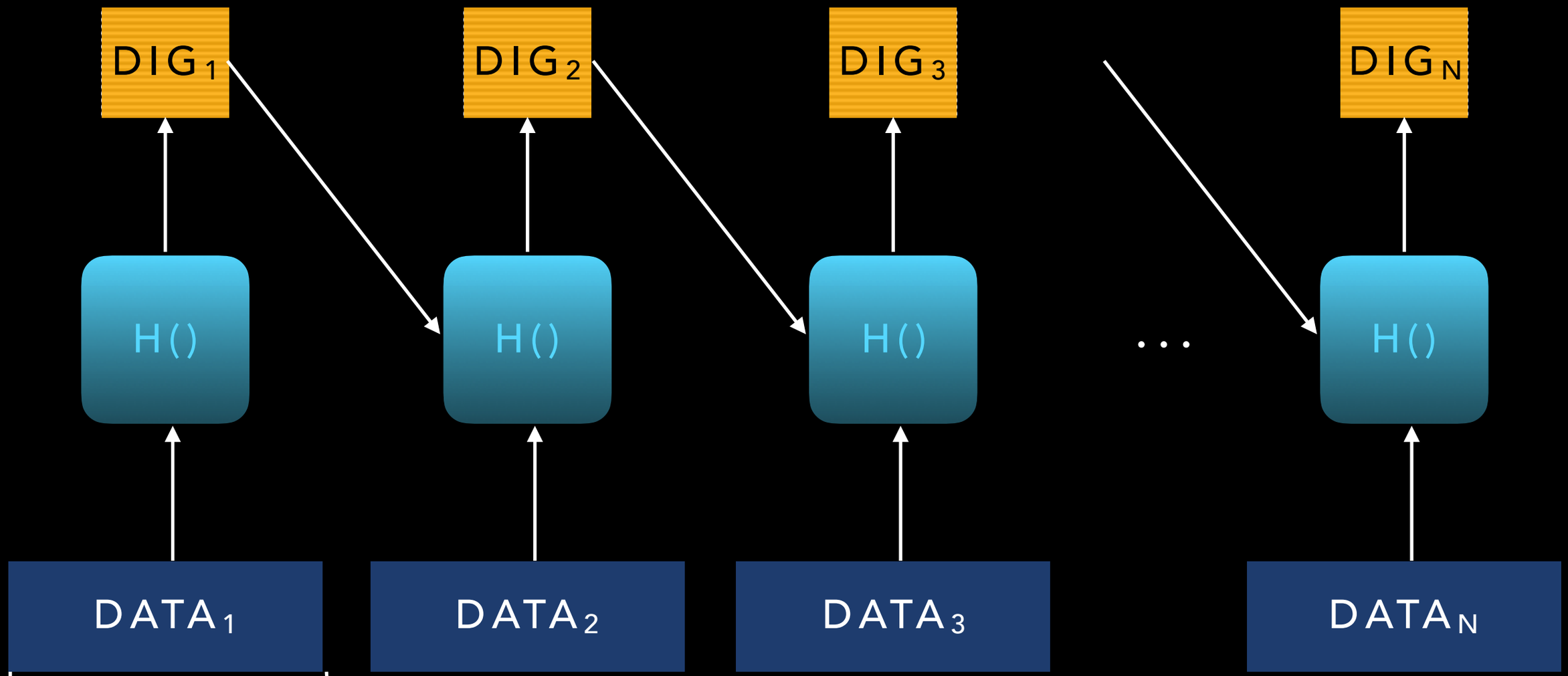


CHAINING AND BLOCK CHAINING



Block = Many transactions combined

CHAINING AND BLOCK CHAINING



Block = Many transactions combined

Forgery or Fraud becomes very hard

WHO ARE THE PEERS?

- Anyone? - Public Blockchain
  - Example: Bitcoin - identity of peers is unknown
  - No one is trusted, anyone can view records
- Only validated users - Private or Permission-ed Blockchain
  - Explored by the financial industry
  - Partially trusted (have skin in the game), may have limitations on access to records

PROOF OF WORK

- How do you decide the most current “state” of the blockchain?
  - How do you add a transaction?
- Show “work” (= skin in the game)
  - Find a digest that has so many leading zeros (2^{20} computations?)
    - Cost to anyone who tries to attack the blockchain
- Estimate: Bitcoin network consumes as much energy as Denmark!!
  - (source: https://arstechnica.com/tech-policy/2017/12/bitcoins-insane-energy-consumption-explained/)

PROOF OF STAKE

- Stakeholders place “bets” on the blockchain status
  - “I say this transaction is valid by posting a bond of $100”
- Reputation of validated users
- Validated users have tokens they can use to add a transaction to the blockchain
- Faster, but works in a controlled environment

WHEN TO USE A BLOCKCHAIN

- Why not an authenticated database?
  - Everyone is equal
  - Robustness
  - Automated audit trail?
- Why a central database?
  - Can a blockchain be maintained by one entity?
  - We want transactions to be hidden. Why should Chloe know how much Bob paid for Alice's antique?

INEFFICIENCY
COST
SPEED

MAY BE A PROBLEM IN ANY SYSTEM

ISSUES

- Confidentiality of usage
  - Authentication to access blockchains
  - Control of what is visible (proof of age, but not address)
- Robustness
  - If one or even a few nodes in the “network” are down, others still have the blockchain

SO…?

- No one knows if blockchains will make it big
- IBM, Microsoft, many others are invested in this
- See
  - Azure & Blockchains: https://github.com/Azure/azure-blockchain-projects/blob/master/bletchley/bletchley-whitepaper.md
  - IBM's Platform built on Hyperledger: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/

SOURCES (1)

- NY Times, March 4, 2017: Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?

- WSJ: Steve Norton, CIO Explainer: What Is Blockchain?

- Steve Cheng and others, “Using blockchain to improve data management in the public sector,” McKinsey, February 2017

- Ryo Takahashi, “How can creative industries benefit from blockchain?,” McKinsey, August 2017

SOURCES(2)

- Video: Gideon Greenspan, “What is the difference between a Blockchain and a database?” https://www.youtube.com/watch?v=NK5Fz3w-H4o

- Animation: http://bitbonkers.com

- Animation: http://bitlisten.com

- Video: Blockchain explained: Jerry Cuomo and Oscar Roque answer the internet's top blockchain questions at: https://www.youtube.com/watch?v=O-j4pBi0gFk

https://youtu.be/lD9KAnkZUjU

WHAT CAN BLOCKCHAINS DO FOR YOU?