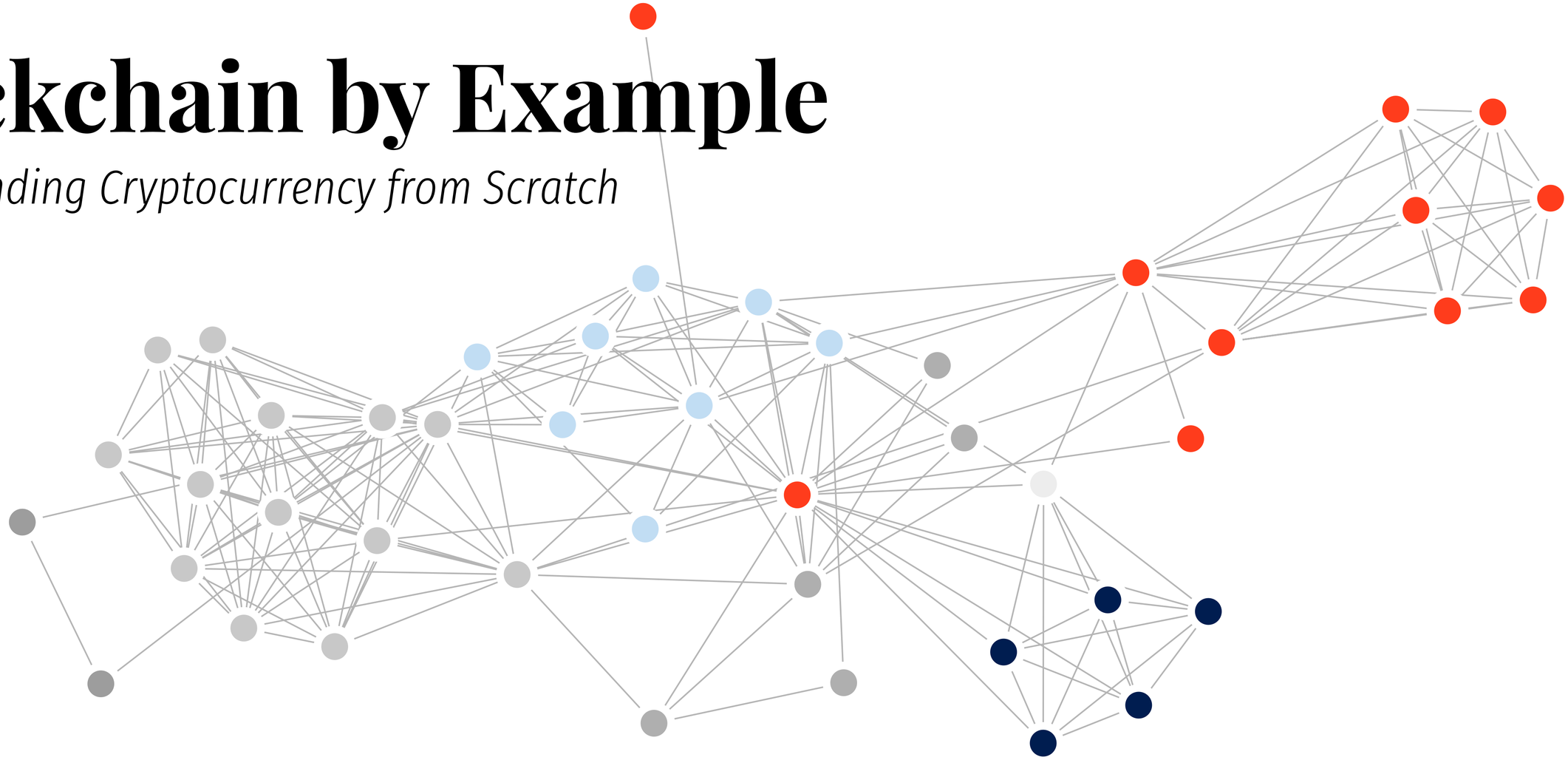
Blockchain by Example

Understanding Cryptocurrency from Scratch



KING'S College LONDON

Moritz Platt, moritz.platt@kcl.ac.uk

PhD student in the Department of Informatics at King's College London

Blockchain

“A blockchain is a **linear collection** of **data elements** called block, where all blocks are linked to form a chain and **secured using cryptography**, and newly generated blocks are continuously chained to the blockchain in an **untrusted environment**.” [Zhang2018]

Agenda

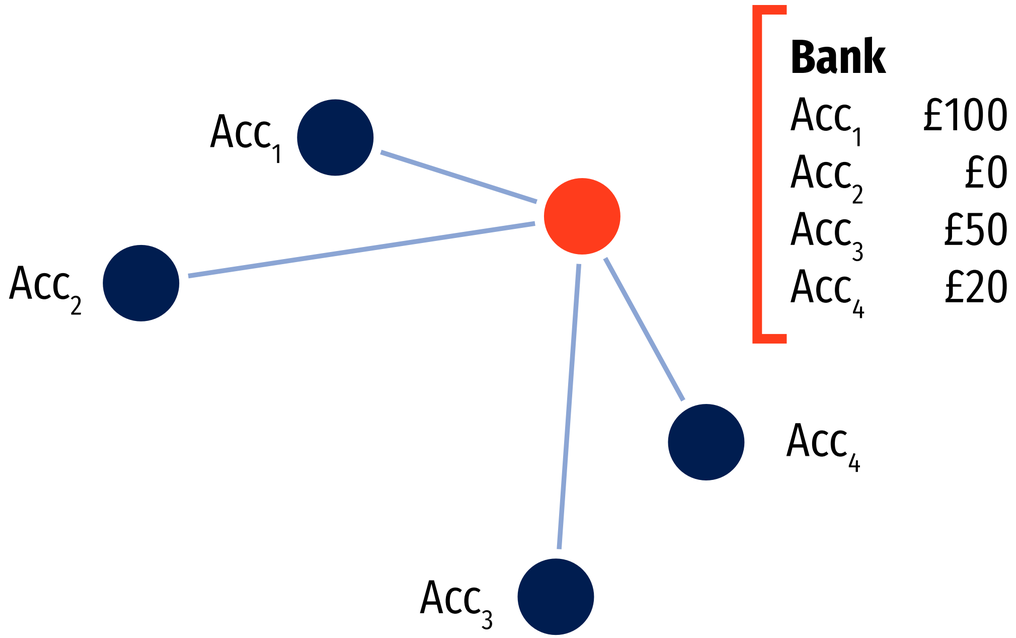
1. **Systemic View:** Properties of both centralized and decentralized architectures in payment systems

2. **Blockchain Components:** Blocks, Consensus and Smart Contracts

3. **Beyond Cryptocurrency:** How the smart contract paradigm can be used beyond the financial sector

Centralized Payment System

- Traditionally, most B2B and B2C systems are centralized
- Single point of authorisation/authentication
- Validation of proposed transactions is done centrally
- In consumer banking, a transaction on behalf of a customer will be exectuted following validation (user identity, account balance, etc.) by the bank



Anatomy of a Payment

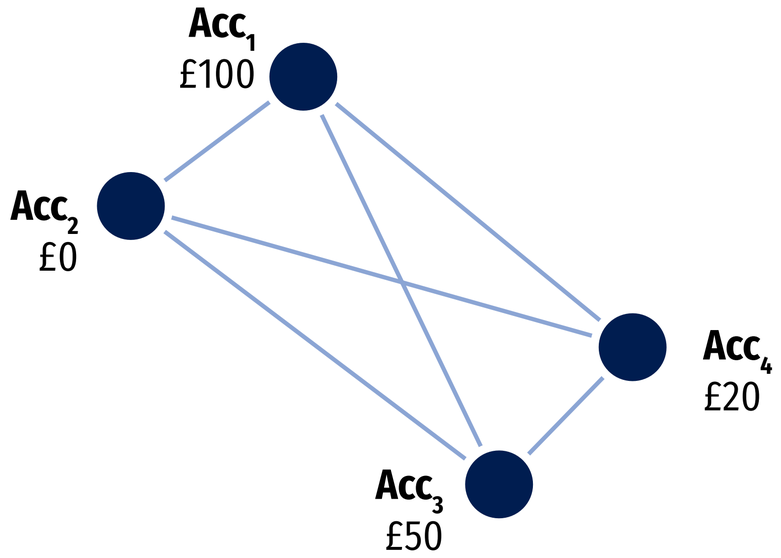
Expressing a transfer of **£30** from **Acc_1** to **Acc_2** on a bank ledger:

Acc	Date	Details	Payment	Deposit	Balance
Acc_1	1 Jan	Opening Balance		£100	£100
Acc_3	1 Jan	Opening Balance		£50	£50
Acc_4	1 Jan	Opening Balance		£20	£20
Acc_1	10 Apr	Transfer to Acc_2	£30		£70
Acc_2	10 Apr	Transfer from Acc_1		£30	£30

The bank ensures the authenticity of the payer's request, sufficient funds on the payer's side, the existence of the recipient's account, the privacy of the payment and it's legality.

A Naïve Distributed System

- Removing any centralized authorithy
- Account holders store balances and execute transactions truthfully and honestly by sending messages to each other
- Each participant holds their own ledger, recording transactions that affect their balance only
- ‘Honour system’ is highly abusable
- No validation of funds
- No validation of authenticity



Anatomy of a Distributed Payment

Expressing a transfer of **£30** from **Acc_1** to **Acc_2** on a naïve distributed ledger:

Led_1

Date	Details	Payment	Deposit	Balance
1 Jan	Opening Balance		£100	£100
10 Apr	Transfer to Acc_2	£30		£70

Led_2

Date	Details	Payment	Deposit	Balance
10 Apr	Transfer from Acc_1		£30	£30

Led_3

Led_4

...

Centralized vs. Naïve Distributed Payments

Function	Centralized	Naïve Distributed
Authenticating Account Holders	Bank	N/A
Keeping Balance Records	Bank	Account Holder
Ensuring Sufficient Funds	Bank	Honour System
Privacy of the Payment	Bank	N/A
Contestability	Legal System	Legal System
Settlement	Bank	N/A

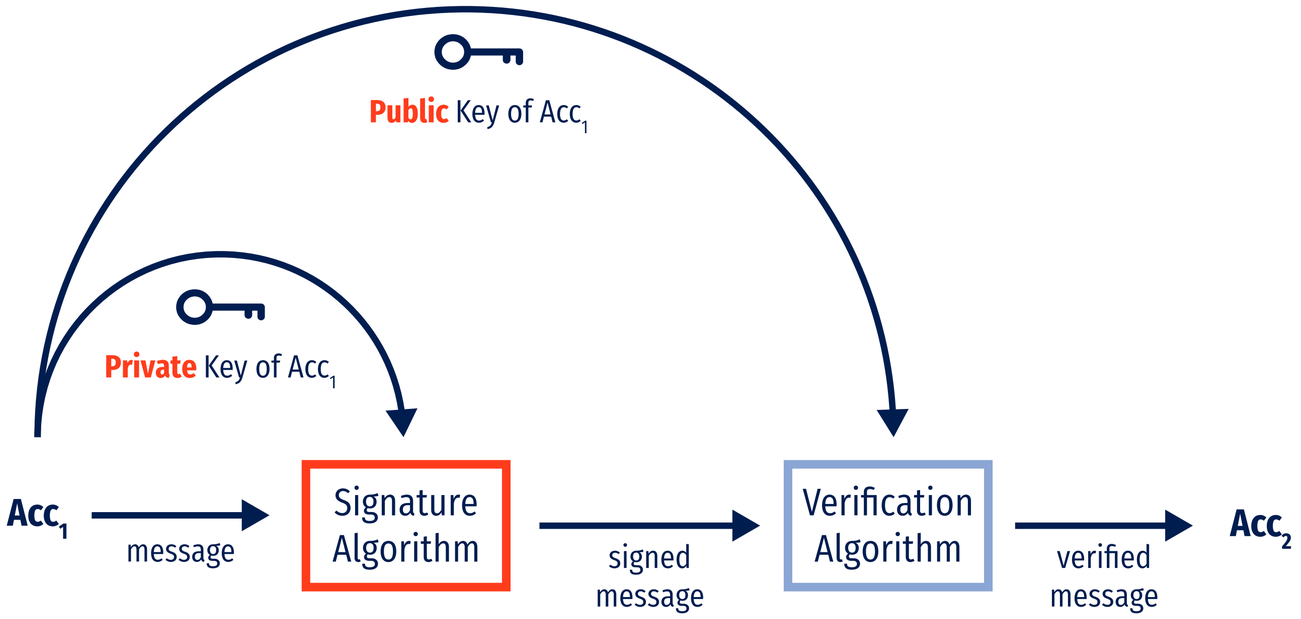
- The distributed approach seems completely unfeasible for any real world applications
- Yet this paradigm is what Cryptocurrencies are founded on

Distributed Ledgers

- ‘Public’ blockchain protocols (e.g. *Bitcoin*) follow the exact same approach with the difference that *all* updates to the ledger are visible to all participants, not only the individual
- Ledger updates (i.e. payments and deposits) are distributed to all participants
- Participants gain understanding of all individual account balances by calculating the sum of all payments and deposits that occured so far

Cryptographic Signatures: Ensuring Message Authenticity

- Public key cryptography is a method to encrypt messages using a non-secret key.
- In a public key signature scheme, knowledge of the key used to verify a signature does not allow one to derive the key to sign messages.
- Therefore a verification key can be made public without endangering the security of the signing key. [Sako2011]
- These properties can be used to ensure a message was *actually* sent by a participant even if it is sent over an untrusted network.



[Stallings1995]

Public Keys Serve as Unique Identifiers

- Public keys can be self-generated by any user on a blockchain
- In addition to enabling message authenticity, public keys can be used as individual addresses (or ‘account numbers’) on a blockchain
- They are unique and are difficult to guess
- These two properties allow for the following:
  - Address a message to a certain address (‘account number’)
  - Assert that a message claiming to come from a certain address actually originated at this address
- Thinking back to the example, these properties can solve the first problem:
  How to authenticate individual account holders.

Ensuring Sufficient Funds: Smart Contracts

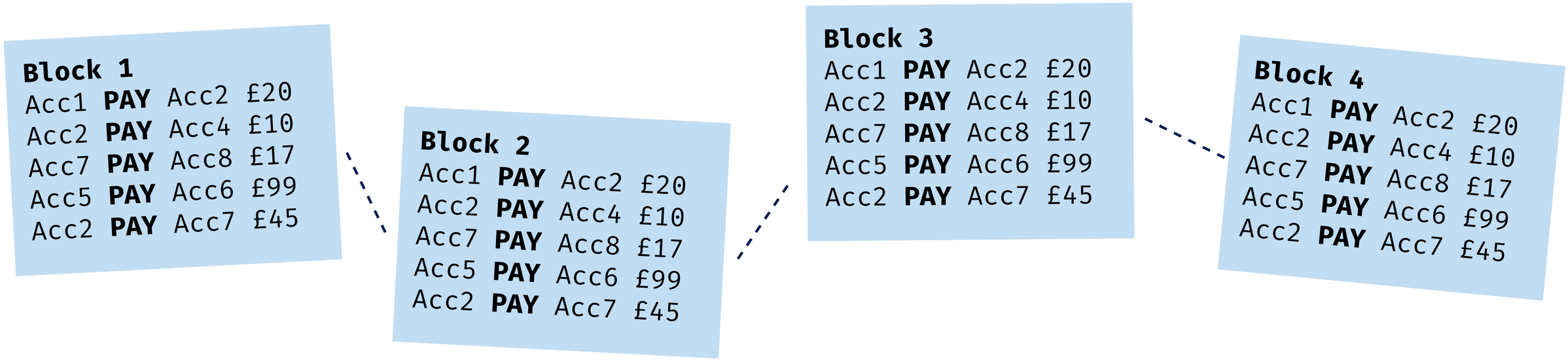
- To prevent overspending and other problematic transactions, rules—so called Smart Contracts—need to be executed on the ledger:

```
if PAYER_BALANCE is greater than or equal to PAYMENT_AMOUNT
   decrease PAYER_BALANCE by PAYMENT_AMOUNT and
   increase PAYEE_BALANCE by PAYMENT_AMOUNT
else
   fail
```

- These are correctness checks that are agreed on by the participants of the transaction
- They can be excercised by all participants on the ledger, not only the payer/payee

Bundling Transactions: Putting the *Block* in Blockchain

- All transactions (i.e. every single payment) need to be propagated to all network participants
- Distributing all transactions one-by-one over the network introduces ordering and timing problems
- The solution: Bundling transactions in *blocks*



Bundling Transactions: Putting the *Block* in Blockchain

- ⊞ Easier transmission over the network
- ⊞ Bulk validation of transactions
- ☐ Assume initial balance £20 for Acc_1 and Acc_2:

Block 1_A
Acc1 **PAY** Acc2 £10 S9C8
Acc1 **PAY** Acc3 £10 S179
Acc2 **PAY** Acc4 £15 S026

Valid Block

Block 1_B
Acc1 **PAY** Acc2 £19 S8CC
Acc1 **PAY** Acc3 £10 SE98
Acc2 **PAY** Acc4 £15 SF9E

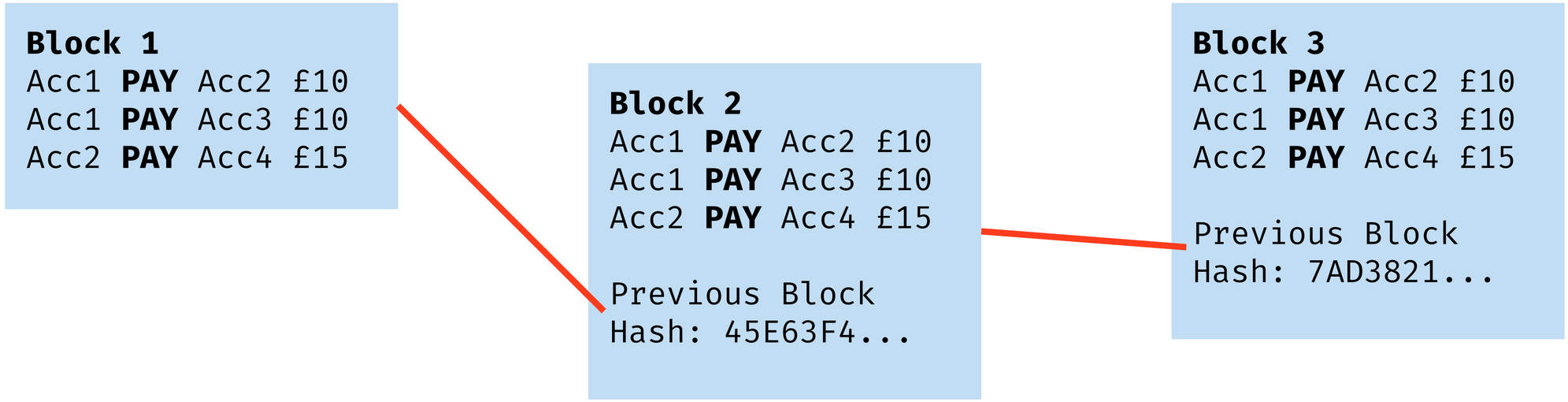
Invalid Block! Acc_1 overspent (£29)

Stopping Transactions that Violate Contracts

- Whoever creates new blocks is economically incentivized to check that no transaction violates their contract
- They will refuse to add transactions that are incorrect
- Different blockchains use different protocols to solve this problem
- Incentivizing block creation usually means giving a ‘reward’ to the user who created new blocks and thereby attested for the correctness of the data in the block
- Adding transactions to new blocks is often called ‘mining’

Linking Transactions: Putting the *Chain* in Blockchain

- The blockchain evolves by adding new blocks to it
- New blocks are added through the mining process
- There is no temporal relationship between transactions *within* one block but a linear relationship between blocks (i.e. one block occurs after another block)



Linking Transactions: Putting the *Chain* in Blockchain

- Since a reference to the previous block is encoded in the respective successor, tampering with the contents of a previous block is not possible without rendering the cryptographic properties of the blockchain invalid

Piecing it all Together

- Alice wants to send £10 to Bob.
- Her public key is `A6789...`
- Alice knows Bob's public key: `B1234...`
- Alice has sufficient balance in her account
- Alice builds a transaction that captures her intent:

  ```
  A6789... PAY B1234... £10
  ```

- Alice signs the transaction, where `S5678...` is her signature of the message, producing the following output:

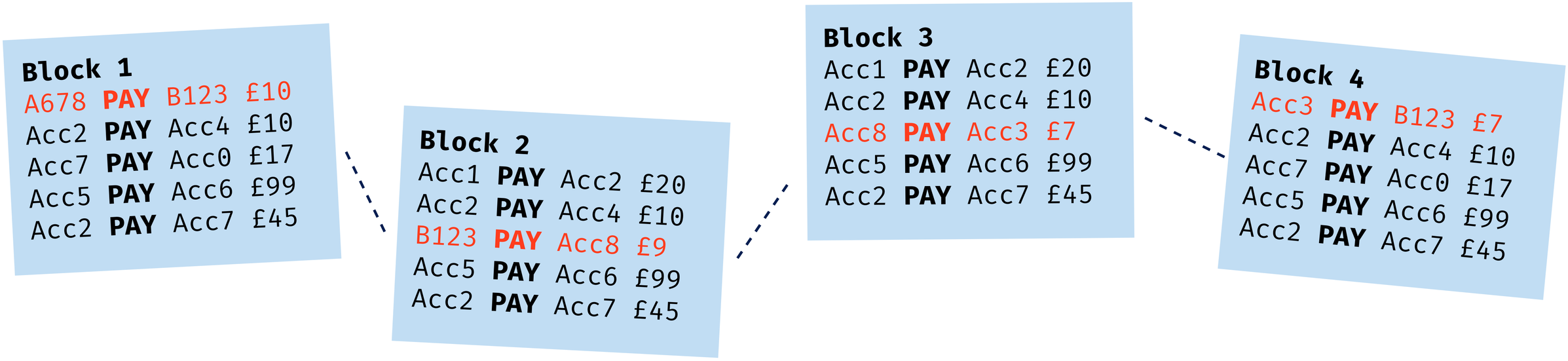
  ```
  A6789... PAY B1234... £10 S5678...
  ```

Piecing it all Together

- Alice submits her message `A6789… PAY B1234… £10 S5678…` to a ‘miner’ so it can be included in the following block
- The miner validates that the message was actually authored by Alice by checking the signature using her private key
- The ‘miner’ validates the transaction against the ‘smart contract’ for the payment
- To ensure Alice actually has sufficient balance, the miner has to take into account all payments Alice was ever part in (both as payer and as payee) to determine her true balance
- This calculation shows her balance is larger than £10.
- The transaction is bundled with other (non-conflicting and valid) transactions and written to the next block
- The block is distributed to other participants in the blockchain

Piecing it all Together

- Both Alice's and Bob's balances are now *implicitely* updated since the details of the transaction are made public on the ledger



- Assuming Bob (B123), Acc_8 and Acc_3 all had a balance of £0 initially, their balances at the time of Block 4 are Bob=8; Acc_8=2; Acc_3=0

Piecing it all Together

Function	Centralized	Distributed
Authenticating Account Holders	Bank	Public/Private Key Cryptography
Keeping Balance Records	Bank	Blockchain
Ensuring Sufficient Funds	Bank	Smart Contracts
Privacy of the Payment	Bank	**limited**
Contestability	Legal System	**unfeasible**
Settlement	Bank	Exchanges

- Transactions on ‘public’ blockchains are visible to all participants by definition
- Regulation of blockchain technology is emerging

Beyond Cryptocurrency

- The smart contract paradigm is applicable beyond cryptocurrency
  - Digital Identity
  - Tax Records
  - Insurance
  - Real Estate and Land Titles Recording
  - Supply Chain
  - IoT
  - Authorship and Intellectual Property Rights

Bibliography

InBook (Zhang2018)
Zhang, Y.
Shen, X. (S.; Lin, X. & Zhang, K. (Eds.)
Blockchain
Encyclopedia of Wireless Networks, Springer International Publishing, **2018**, 1-4

InBook (Sako2011)
Sako, K.
van Tilborg, H. C. A. & Jajodia, S. (Eds.)
Public Key Cryptography
Encyclopedia of Cryptography and Security, Springer US, **2011**, 996-997

Book (Stallings1995)
Stallings, W.
Network and Internetwork Security: Principles and Practice
Prentice-Hall, Inc., **1995**