Microsoft Cloud Computing Research Centre

4th Annual Symposium, 12-13 September 2017

The Technologies Underpinning Blockchain / Distributed Ledgers

Professor Jean Bacon, Anwaar Ali, Dave Michels

jmb25@cl.cam.ac.uk, aa980@cam.ac.uk, d.michels@qmul.ac.uk

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London

Centre for Commercial Law Studies

£91 bn.

Blockchain: a digital ledger that records transactions between parties.

1. Creating a blockchain
2. Storing a blockchain
3. Using a blockchain

Two main cryptographic technologies

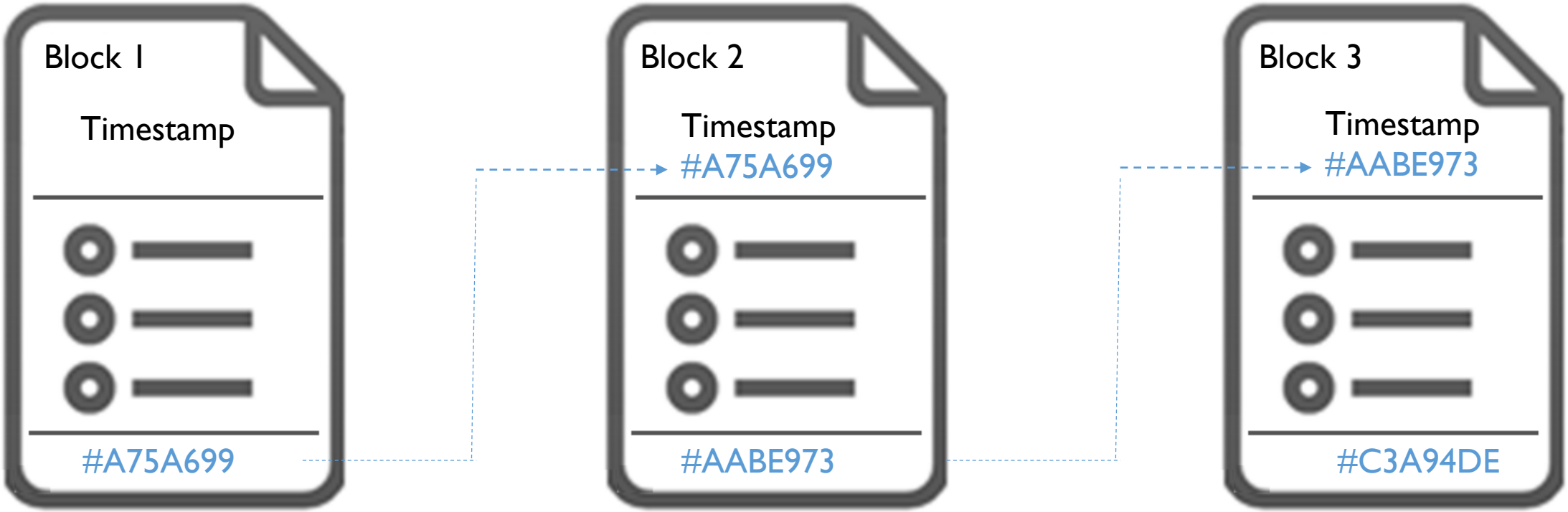
A) Hash functions

B) Public key infrastructure

A) Hash Function

Input	Sing, O goddess, the anger of Achilles son of Peleus, that brought countless ills upon the Achaeans. Many a brave soul did it send hurrying down to Hades, and many a hero did it yield a prey to dogs and vultures, for so was the will of Zeus fulfilled from the day on which the son of Atreus, king of men, and great Achilles, first fell out with one another. And which of the gods was it that set them on to quarrel? It was the son of Zeus and Leto; for he was angry with the king and sent a pestilence upon the host to plague the people, because the son of Atreus had dishonoured Chryses his priest. Now Chryses had come to the ships of the Achaeans to free his daughter, and had brought with him a great ransom: moreover he bore in his hand the scepter of Apollo wreathed with a suppliant's wreath.
Output	AABE9739FA75A699

A) Hash functions link blocks



Demo Time!

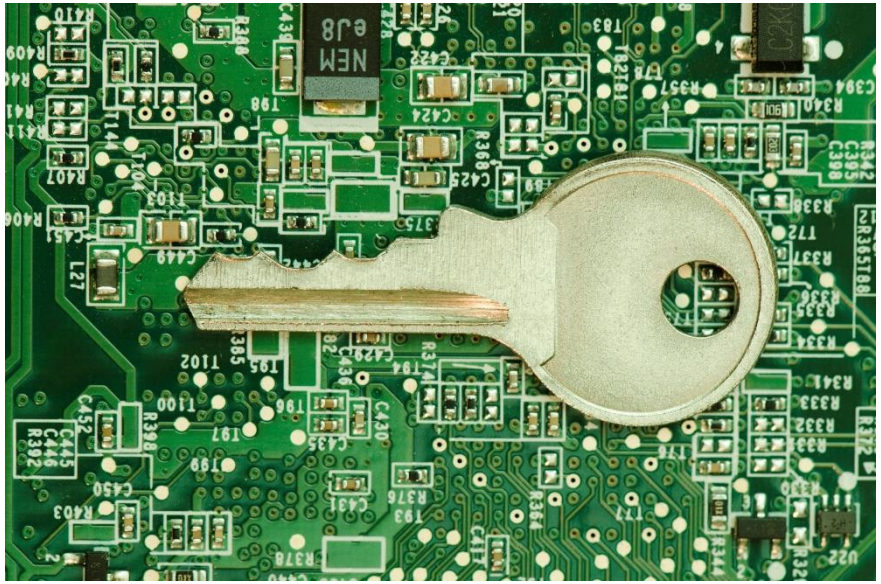
Two main cryptographic technologies

A) Hash functions

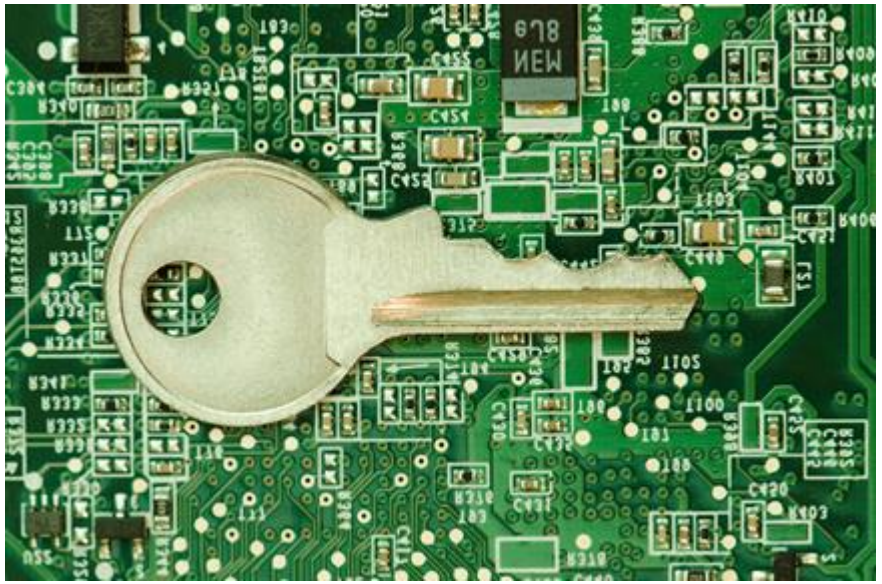
B) Public key infrastructure

B) Public key infrastructure

Public Key



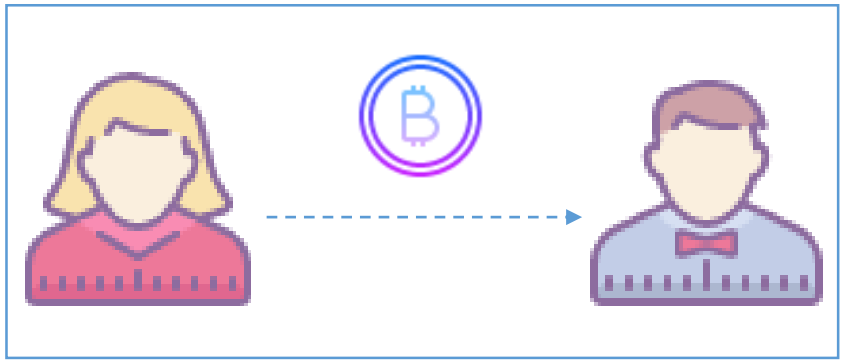
Private Key

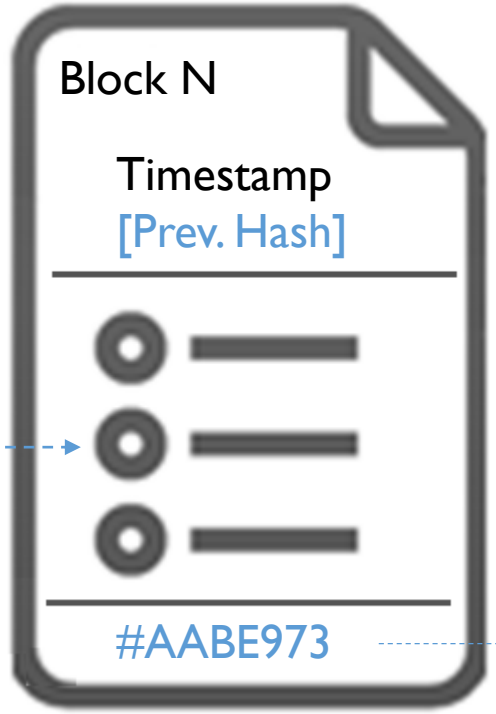


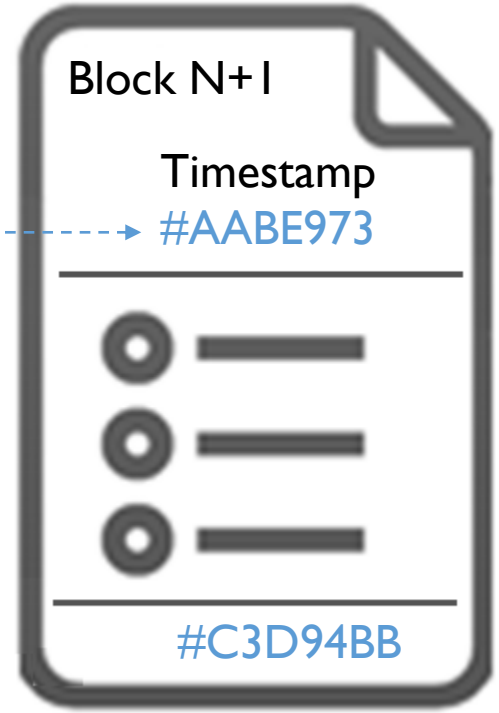
Demo Time!

B) PKI for a blockchain

C) Combining the two technologies



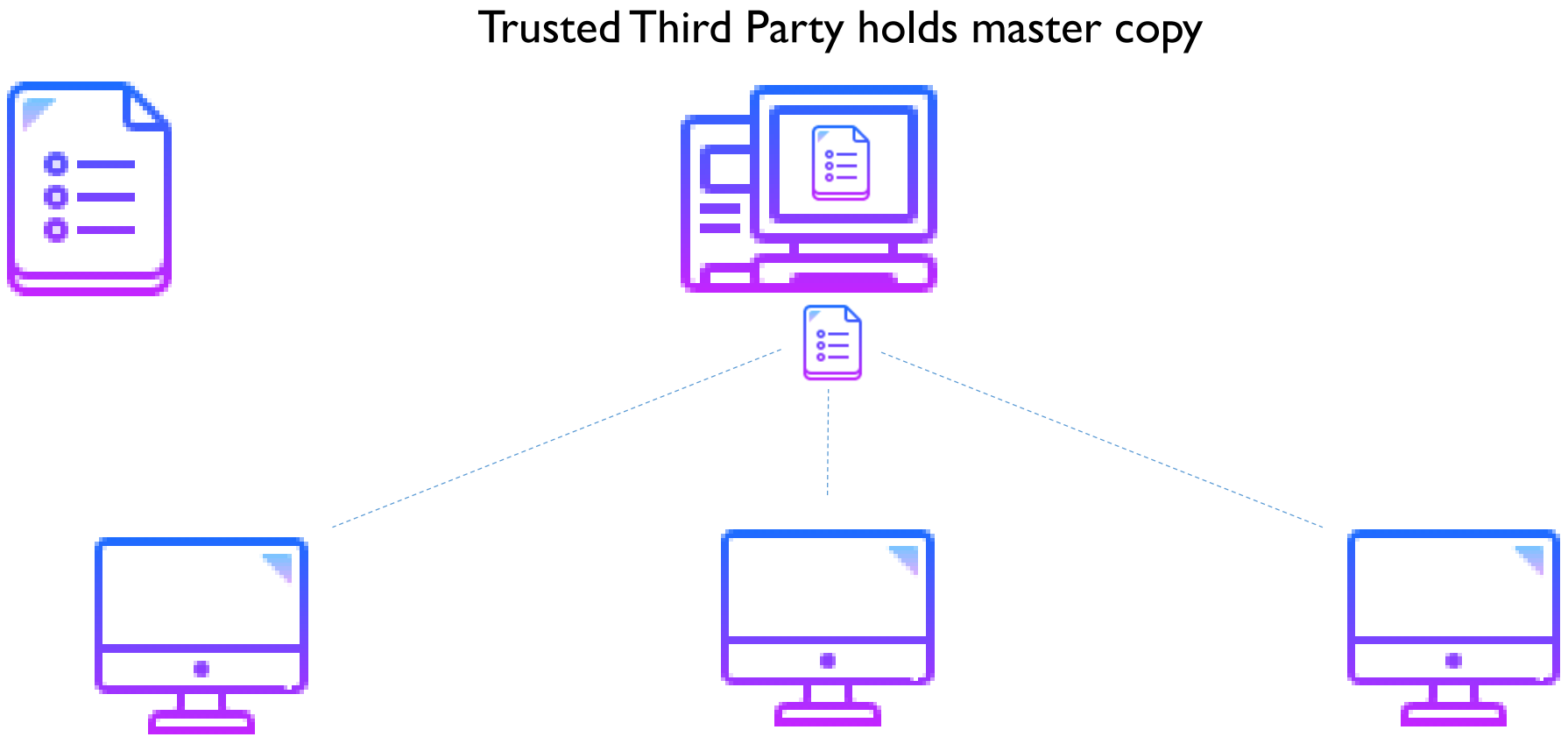




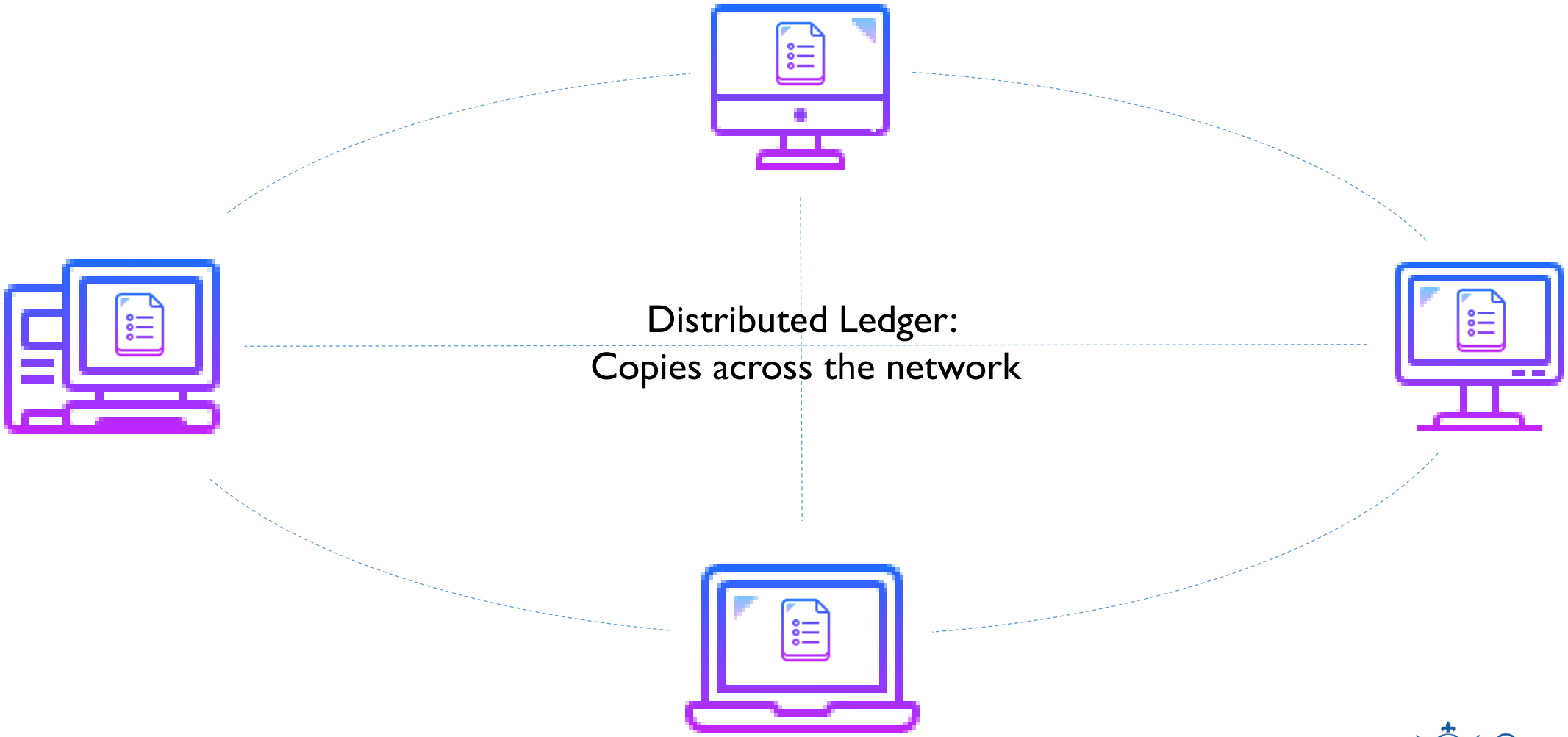
Blockchain: a digital ledger that records transactions between parties.

1. Creating a blockchain
2. Storing a blockchain
3. Using a blockchain

A) Centralised storage



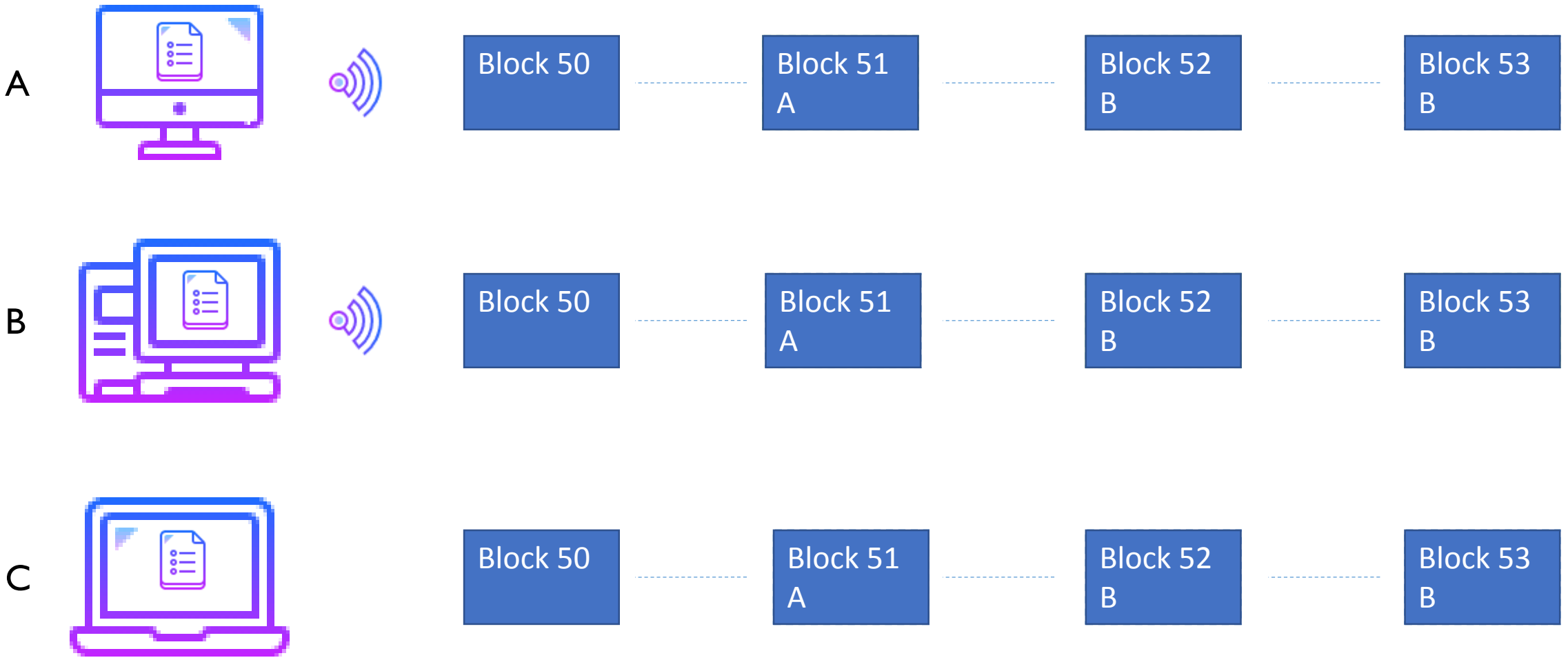
B) Decentralised storage



B) Consensus Protocol

Demo Time!

B) Consensus: example



Blockchain: a digital ledger that records transactions between parties.

1. Creating a blockchain
2. Storing a blockchain
3. Using a blockchain

	Early applications	Future applications
1. What?	On-chain assets	Off-chain assets
2. Who?	Open, permission-less	Closed, permissioned
	Pseudonyms	Real-world identities

Summary

1. Creating a blockchain

A) Hash values link blocks
B) Public key infrastructure

2. Storing a blockchain

A) Centrally: Trusted Third Party
B) Decentrally: Peer-to-Peer Network

3. Using a blockchain

A) What to track?
B) Who will participate?

Thank you!

All icons courtesy of Icons8.com under creative commons licence.