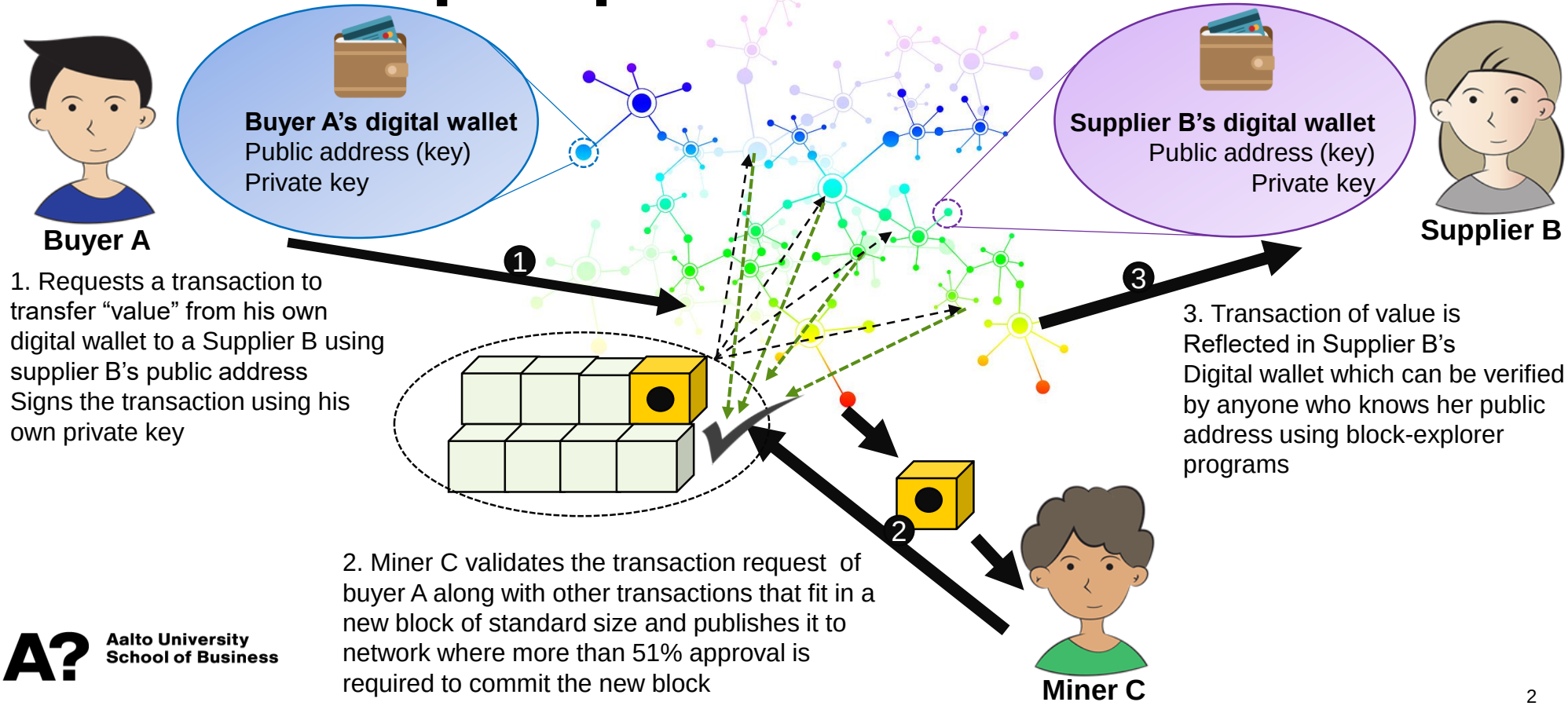
I- Introduction to Blockchain

How does a Blockchain work?: Payment-transaction perspective



1. Requests a transaction to transfer "value" from his own digital wallet to a Supplier B using supplier B's public address
Signs the transaction using his own private key

2. Miner C validates the transaction request of buyer A along with other transactions that fit in a new block of standard size and publishes it to network where more than 51% approval is required to commit the new block

3. Transaction of value is Reflected in Supplier B's Digital wallet which can be verified by anyone who knows her public address using block-explorer programs

Aalto University
School of Business

Blocks & Blockchain database

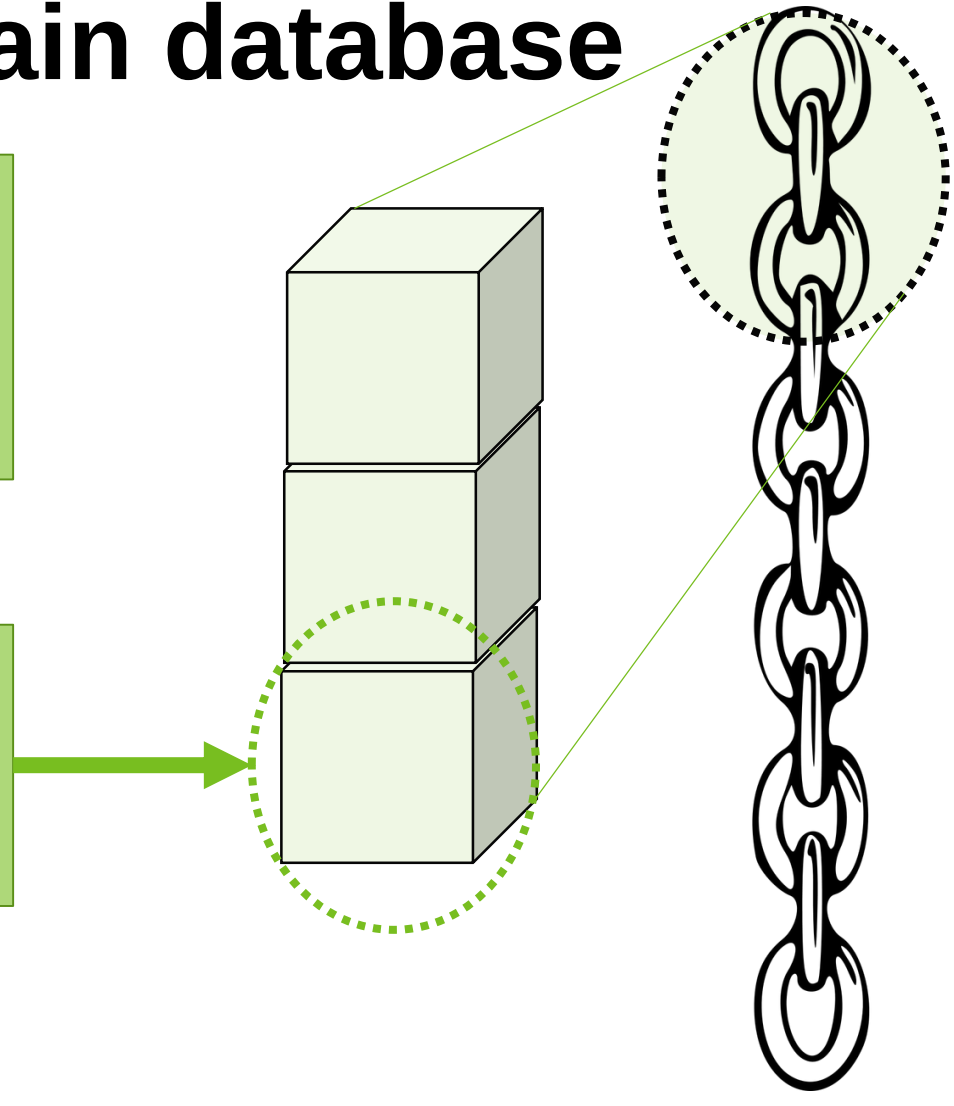
Open block explorers to see the information about blocks

https://etherscan.io/
https://blockexplorer.one/btc/mainnet
https://btc.com/

Hash of the previous block

Hash: fingerprint of the block

A block of Transactions with time stamps



Consensus Algorithm

Byzantine Fault Tolerance

- A reliable distributed system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked – namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed as the Byzantine Fault Tolerance.

Proof of work

- A piece of data that requires significant computation to find. In the case of bitcoin, miners must find a nonce (numeric solution) to the SHA256 algorithm that meets a network

Proof of Stake

- Is a method by which a Blockchain network aims to achieve distributed consensus. Proof of Stake requires users to provide certain amount of currency as stake.

Source: Antonopoulos, A.M., (2017) Mastering Bitcoin: Programming the open Blockchain

Forking

Hard fork

- Major protocol upgrade
- Disagreement in the network on the Blockchain protocol or state of blocks leading to two different asset creation

Soft fork

- Majority of network participants forcing (minor) protocol or code changes that support new transaction types that most of the participants accept
- Compatible with previously validated blocks of data

What constitutes a Blockchain? 1 of 2

	Elements of a Blockchain	Example from Ehtereum Blockchain
1	A **peer-to-peer (P2P)** network connecting participants and propagating transactions and blocks of verified transactions, based on a standardized “gossip” protocol	Ethereum runs on the Ethereum main network, which is addressable on TCP port 30303, and runs a protocol called DEVp2p
2	One or more open source software implementations of the above (“**clients**”)	Ethereum has several interoperable implementations of the client software, the most prominent of which are Go-Ethereum (Geth) and Parity.
3	**Messages**, in the form of transactions, representing state transitions	Ethereum transactions are network messages that include (among other things) a sender, recipient, value, and data payload.
4	A set of **consensus rules**, governing what constitutes a transaction and what makes for a valid state transition	Ethereum’s consensus rules are defined in the reference specification
5	A **chain of cryptographically secured blocks** that acts as a journal of all the verified and accepted state transitions	Ethereum’s state is stored locally on each node as a database (usually Google’s LevelDB), which contains the transactions and system state in a serialized hashed data structure called a Merkle Patricia Tree.

Source: Antonopoulos, A.M., Wood Gavin (2019) Mastering Ehtereum: Building Smart Contracts and Dapps,

What constitutes a Blockchain? 2 of 2

	Elements of a blockchain	Example from Ehtereum blockchain
6	A **consensus algorithm** that decentralizes control over the blockchain, by forcing participants to cooperate in the enforcement of the consensus rules	Ethereum uses Bitcoin's consensus model, Nakamoto Consensus, which uses sequential single-signature blocks, weighted in importance by Proof of Work (PoW) to determine the longest chain and therefore the current state. However, there are plans to move to a Proof of Stake (PoS) weighted voting system, codenamed Casper, in the near future.
7	A game-theoretically sound **incentivization scheme** (e.g., proof-of-work costs plus block rewards) to economically secure the state machine in an open environment	Ethereum currently uses a PoW algorithm called Ethash, but this will eventually be dropped with the move to PoS at some point in the future.
8	A **state machine** that processes transactions according to the consensus rules	Ethereum state transitions are processed by the Ethereum Virtual Machine (EVM), a stack-based virtual machine that executes bytecode (machine-language instructions). EVM programs, called "smart contracts," are written in high-level languages (e.g., Solidity) and compiled to bytecode for execution on the EVM.

Source: Antonopoulos, A.M., Wood Gavin (2019) Mastering Ehtereum: Building Smart Contracts and Dapps,