Jaaropening ESAA
31-8-2018

Blockchain in Control, Audit and Oversight

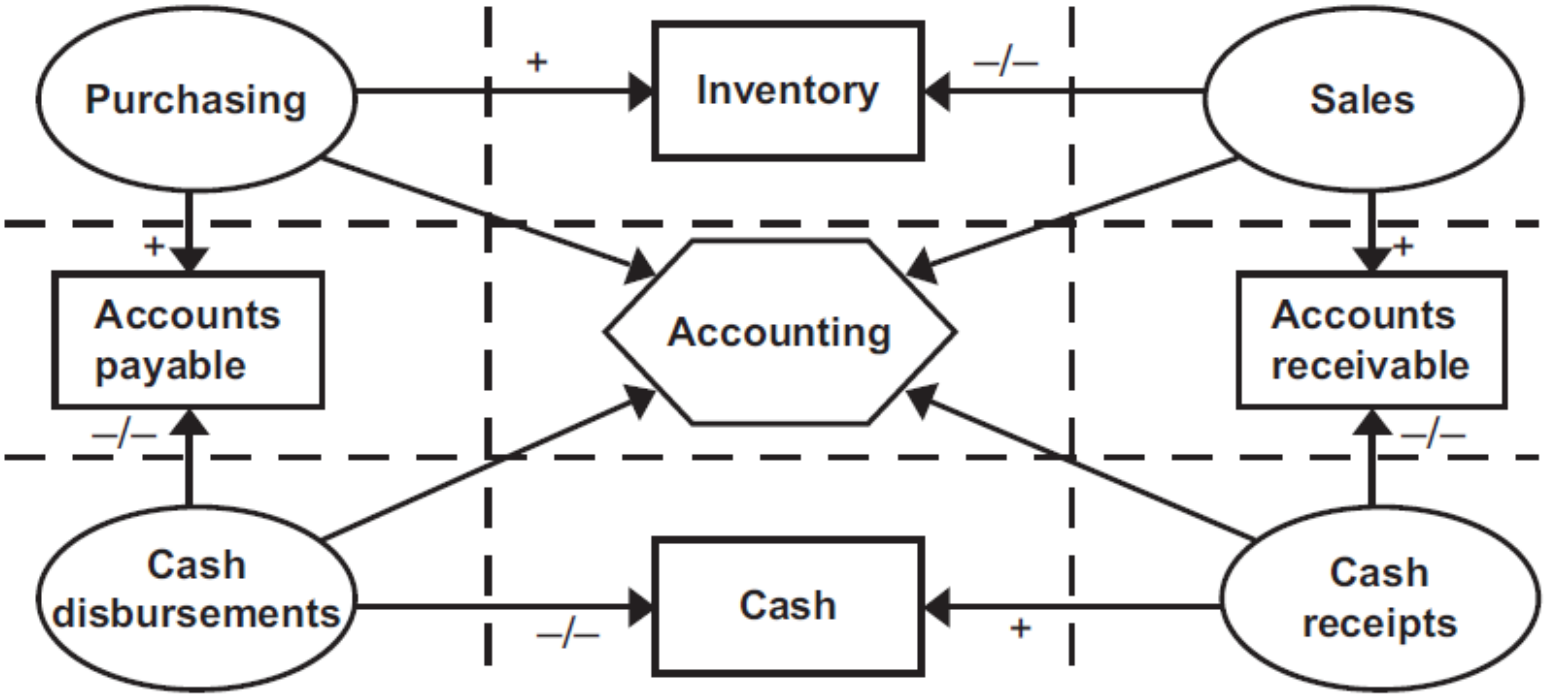
Prof.dr. Eddy Vaassen RA

Tilburg University | Erasmus University | BDO

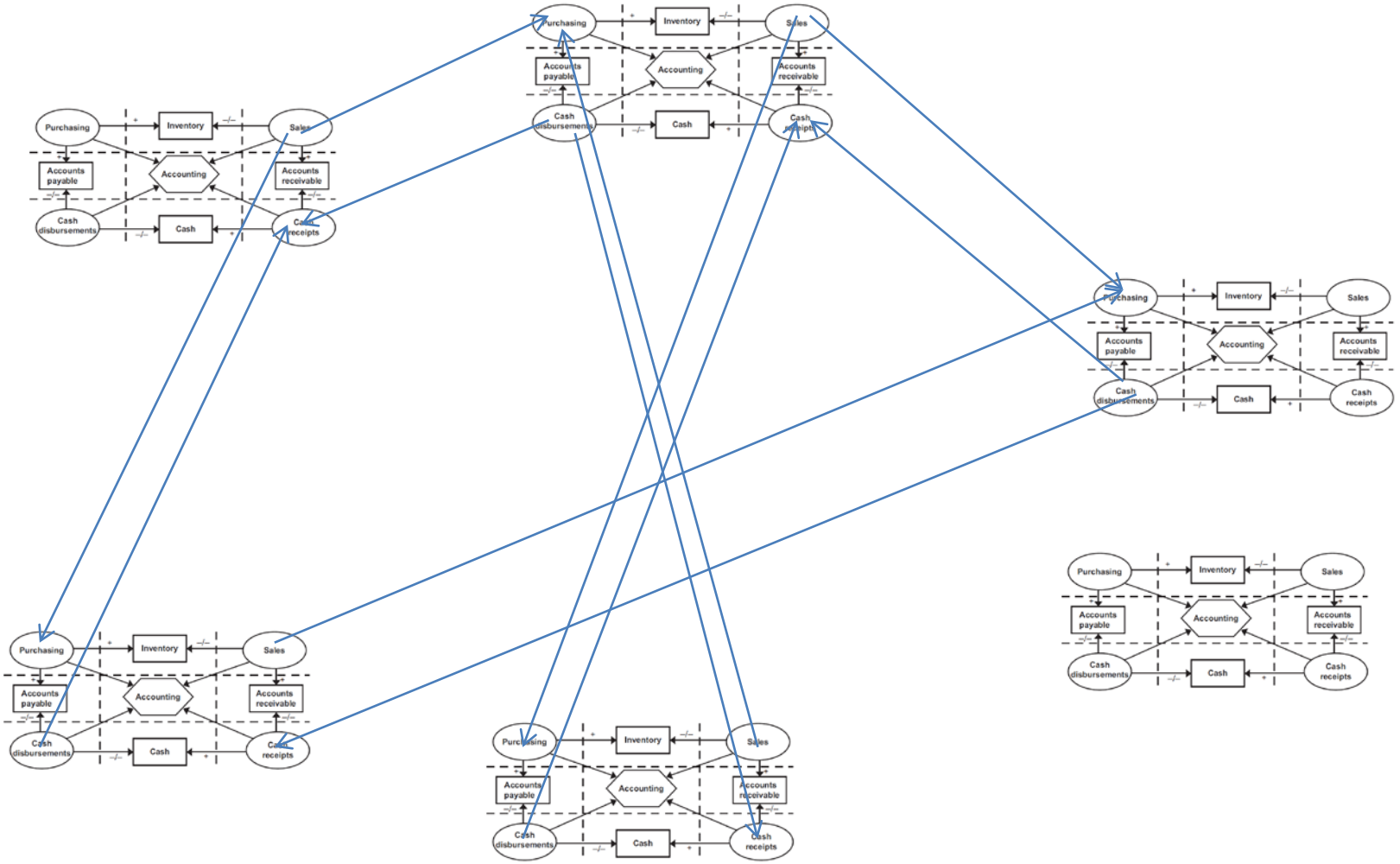
Setting the scene

- Control: realize objectives regarding reliability of information, efficiency, effectiveness, compliance, and safeguarding of assets (including deterring fraud)
- Audit: giving assurance about control goals
- Oversight: inspections on control, audit and management processes

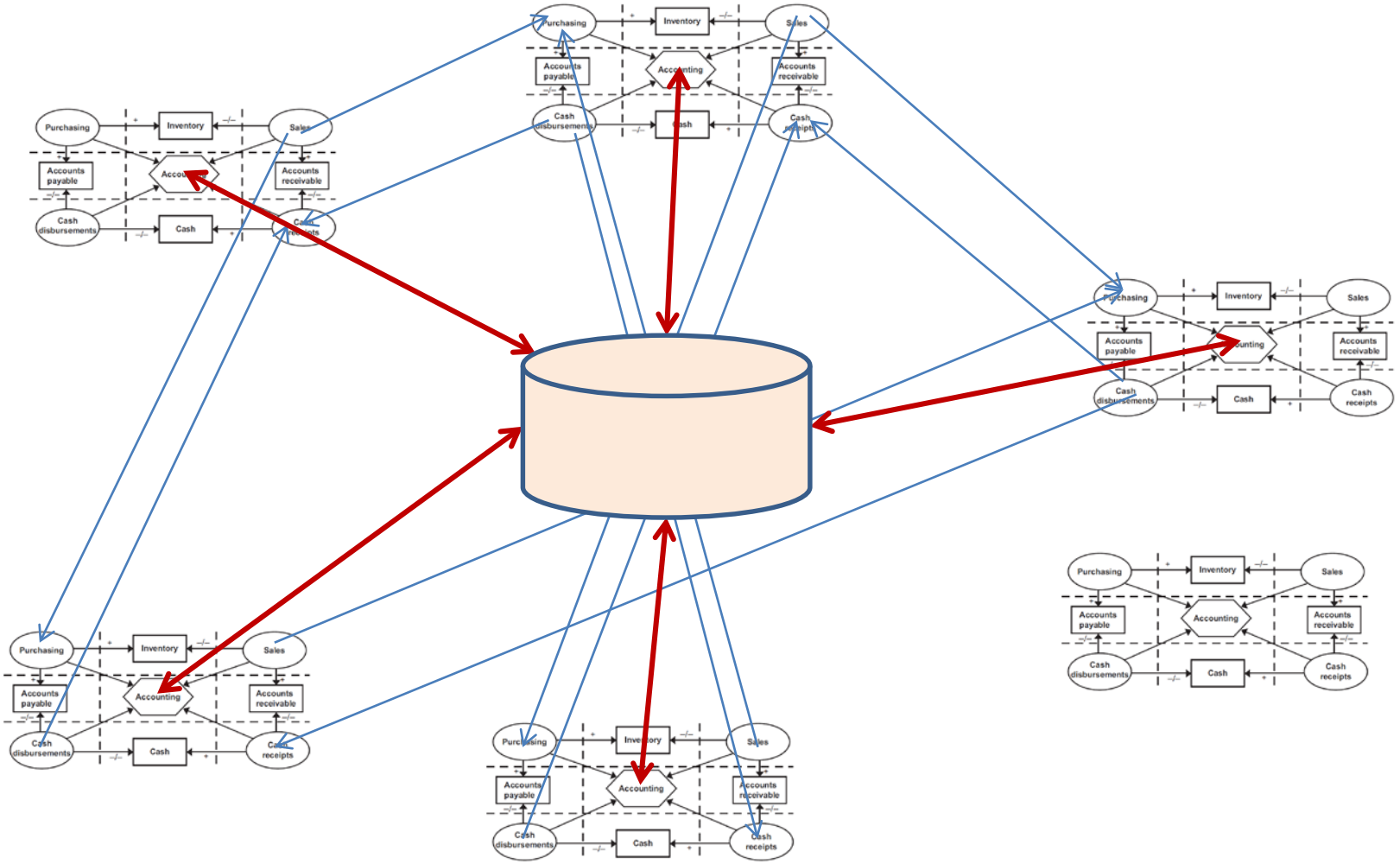
Example: Value cycle



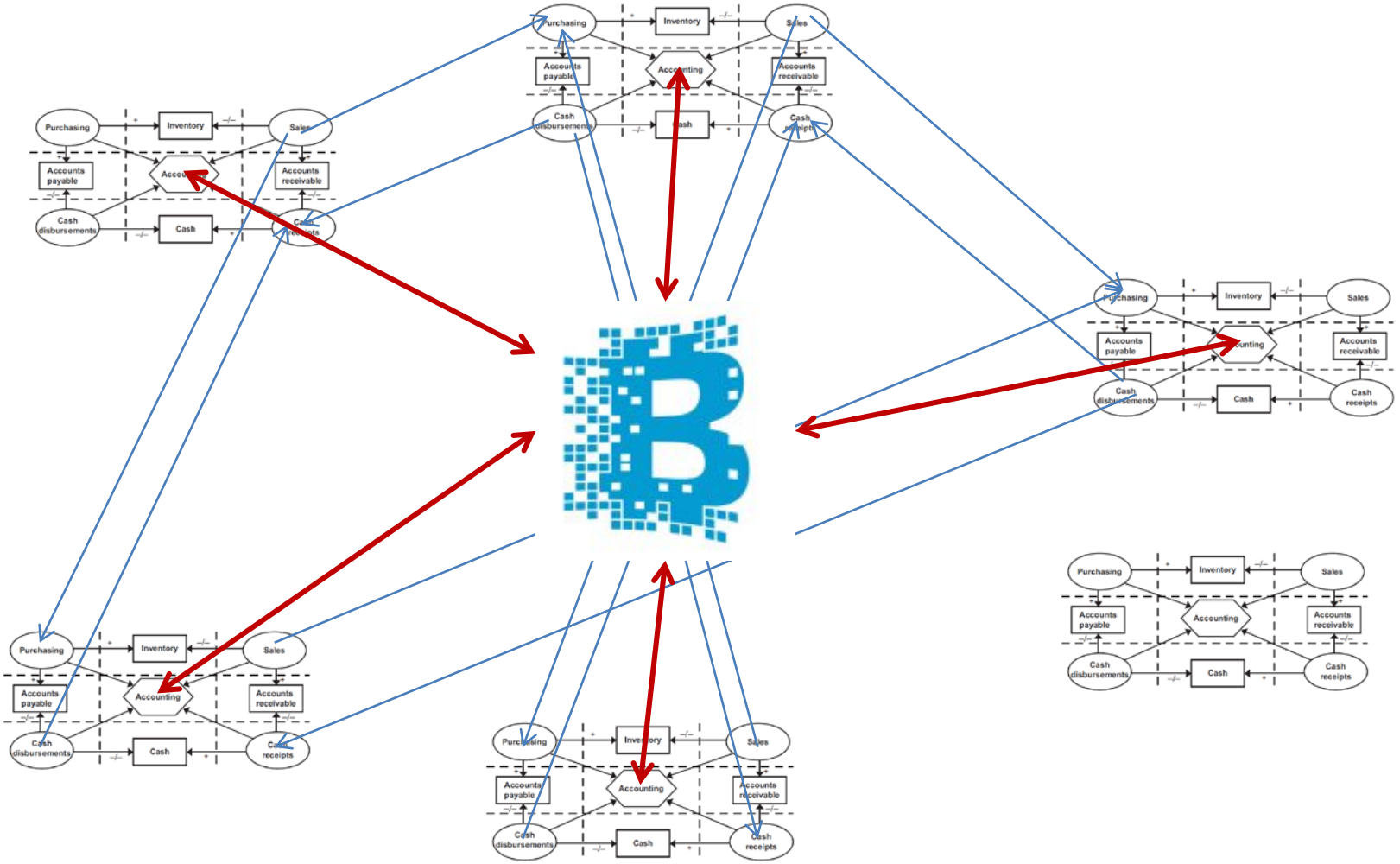
Value cycles are linked



Triple-entry accounting



Triple-entry accounting with blockchain



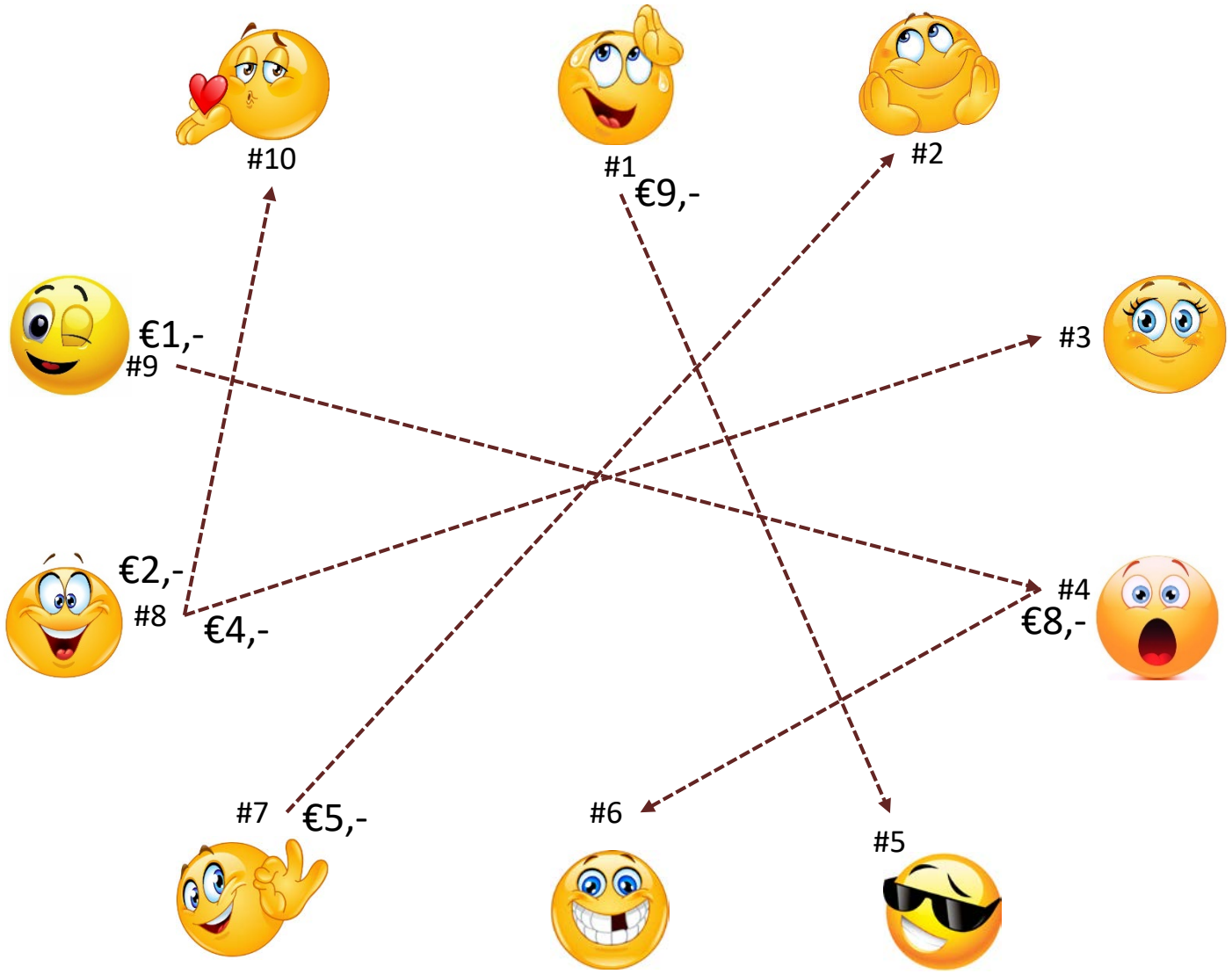
Blockchain

- A blockchain is a distributed database that contains sequentially interlinked ('chained') clusters of transactions ('blocks') with tokens that follow the rules of a specific trust protocol
- A token is a chain of digital signatures (for example an electronic coin)
- A transaction can only be recorded in the blockchain if it has been validated by a majority of the nodes that participate in the network of that blockchain
- Once a transaction is recorded in the blockchain it cannot be removed or altered
- Blockchain technology is the technology underlying the Bitcoin, Ether, Bitcoin Cash, and other (over 3000) cryptocurrencies
- A blockchain is not a substitute for information systems such as ERP, CRM, SCM, or BI; it complements information systems:
  - to enhance reliability
  - to safeguard assets
  - to enforce compliance with applicable laws and regulations
  - to make interactions between members of ecosystems more efficient and effective

Conditions for blockchain

- Shared database
- Multiple parties who write data to the shared database
- Those parties are members of different legal or economical entities
- No or limited trust between these parties
- No trusted third party possible or desired

So, how does a blockchain work?


#10
#1
€9,-
#2
€1,-
#9
#3
€2,-
#8
€4,-
#4
€8,-
#7
€5,-
#6
#5

Transactions in block 1

Tx	From	Amount (€)	To
1	#9	1,-	#4
2	#8	2,-	#10
3	#1	9,-	#5
4	#7	5,-	#2
5	#8	4,-	#3
6	#4	8,-	#6

Communicating the transaction is the transaction

Block 1 to be written to the ledger

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	10	10	10	10	10	10	10	10	10	10
1.1				+1					-1	
1.2								-2		+2
1.3	-9				+9					
1.4		+5					-5			
1.5			+4					-4		
1.6				-8		+8				
Eb	1	15	14	3	19	18	5	4	9	12

Mining of blocks

- By mining a block of transactions we make sure that the block, after it has been written to the blockchain, cannot be changed anymore
- Mining uses hashing
- Hashing is a one-way function: a certain input leads to a certain output, but it is impossible to calculate the input from the output

Mining serves to make a block immutable by cryptographically sealing it

Block 1 to be written to the ledger

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	10	10	10	10	10	10	10	10	10	10
1.1				+1					-1	
1.2								-2		+2
1.3	-9				+9					
1.4		+5					-5			
1.5			+4					-4		
1.6				-8		+8				
Eb	1	15	14	3	19	18	5	4	9	12

b39667cf64cd5bc6cd7adbfc711cd8446036f9144c1cceb604897b0e824a027d

Hash1 = f(T1.1-T1.6, nonce) = 7dc0b

hash of all the transactions in this block

number used once

Block 2 to be written to the ledger

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	1	15	14	3	19	18	5	4	9	12
2.1	+7		-7							
2.2					+16	-16				
2.3								+2	-2	
2.4	+3			-3						
Eb	11	15	7	0	35	2	5	6	7	12

Hash2 = f(T2.1-T2.4, hash1, nonce) = f3e44
Hash2 = f(19efe, 7dc0b, 35ea2) = f3e44

Block 3 to be written to the ledger

Tx	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Bb	11	15	7	0	35	2	5	6	7	12
3.1	+2					-2				
3.2				+8						-8
Eb	13	15	7	8	35	0	5	4	9	4

Hash3 = f(T3.1-T3.2, hash2, nonce) = abdf7
Hash3 = f(abdf7, f3e44, 41e69) = abdf7

Finding the nonce is the essence of mining

Proof-of-work

- Writing a block of valid transactions to the blockchain is only allowed after proof-of-work allows a node to do so
- The incentive to provide proof-of-work is a prize of, say, €60.000,- + some transaction fees
- The prize goes to the node that finds such a nonce that combined with the hash of the previous block, the timestamp of the current block, and the hash of all the transactions in the current block gives a hash that is smaller than the (system provided) target hash

Finding the nonce that gives a hash smaller than the target hash can only be done through trial and error (billions of trials)

Checking if a certain number indeed gives a hash smaller than the target hash is a simple calculation

The nonce is used to mine the block

- Changing a transaction in a mined block requires redoing the proof-of-work
- The more blocks are mined after the block that contains the transaction a fraudster wants to change the more difficult it is to redo the proof-of-work
- After 6 blocks it is not just difficult, it is impossible to change a transaction in a mined block
- That is why a blockchain is immutable and as a result leads to highly reliable information

Tokens live on a blockchain

- Tokens are the cryptographic representation of (digital or physical) assets
- When in the real world an asset moves from A to B, in the blockchain the token also moves from A to B
- Provenance and ownership can always be determined
- That is why a blockchain can help safeguarding assets

Smart contracts

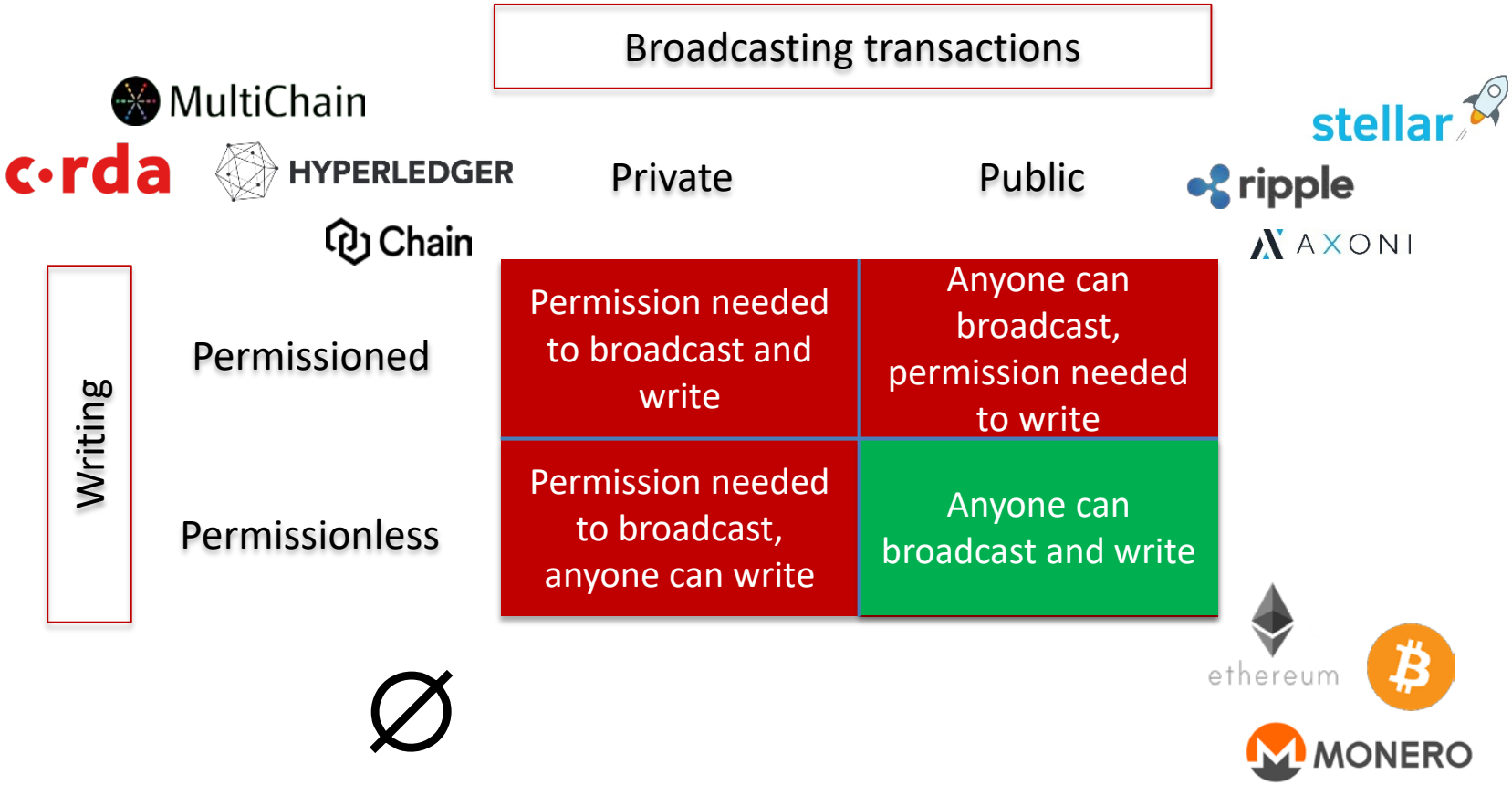
- Merely pieces of software that execute pre-programmed actions if certain conditions are met
- Can run on a blockchain
- Unstoppable
- Compliance by default
- That is why a blockchain can enforce compliance with applicable laws and regulations

The trust protocol

- The trust protocol replaces a trusted third party
- So, disintermediation
- No man-made delays or mistakes
- That is why a blockchain makes interactions between members of ecosystems more efficient and effective

Many so-called blockchains are merely distributed ledgers

Distributed ledgers



Use cases in control, audit and oversight

Use case	Reliability	Safeguarding	Compliance	Efficiency & effectiveness
Land registry	v	v		v
Tickets			v	v
Elections	v		v	v
Track and trace in supply chains		v		v
Electronic markets	v	v		v
Intellectual rights management	v	v	v	v
Licenses			v	v
Personal credentials for job applications	v			v
Zero knowledge range proof for privacy	v		v	v
Liquid assets swapping at banks	v	v		v
Energy exchange		v		v
Triple-entry accounting	v			v

Takeaways

- Distributed ledger technology (DLT) is the versatile variant of blockchain technology
- Through its versatility DLT has great potential in control, audit and oversight regarding the following objectives:
  - Information reliability (for example ‘triple-entry accounting’)
  - Safeguarding of assets (for example ‘supply chains’)
  - Compliance with applicable laws and regulations (for example ‘privacy’)
  - More efficient and effective interactions between members of ecosystems (for example ‘energy’)
- Each user must have a basic understanding of the language of DLT (distributed, mining, hashing, cryptography, smart contracts) to meaningfully and safely interact with the distributed ledger