مباحث پیشرفته در فناوری اطلاعات
جلسه پنجم - بلاکچین

مرتضی سرگلزایی جوان
مرکز تحقیقات رایانش

سرفصل مطالب

- بخش اول: مقدمه و تاریخچه
- بخش دوم: کاربردهای بلاکچین
- بخش سوم: معماری و فناوری های مورد استفاده
- بخش چهارم: مبانی رمزنگاری
- بخش پنجم: الگوریتم های اجماع
- بخش ششم: قراردادهای هوشمند
- بخش هفتم: محدودیت ها


$2
BANK
$$$
$100
$98
Chandler
Trusted Third Party
Joey

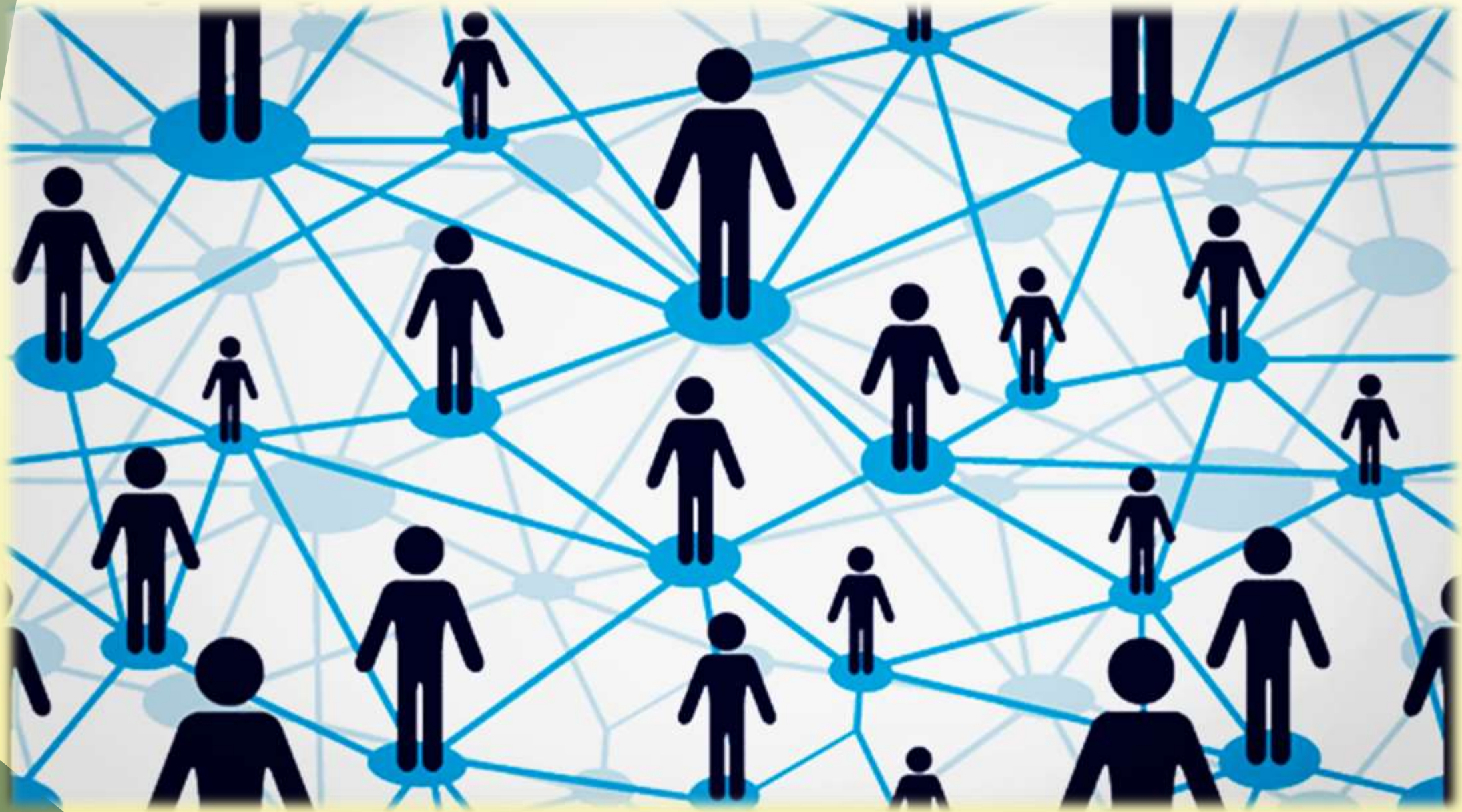
https://en.wikipedia.org/wiki/Financial_crisis_of_2007–2008

https://en.wikipedia.org/wiki/Global_financial_crisis_in_2009

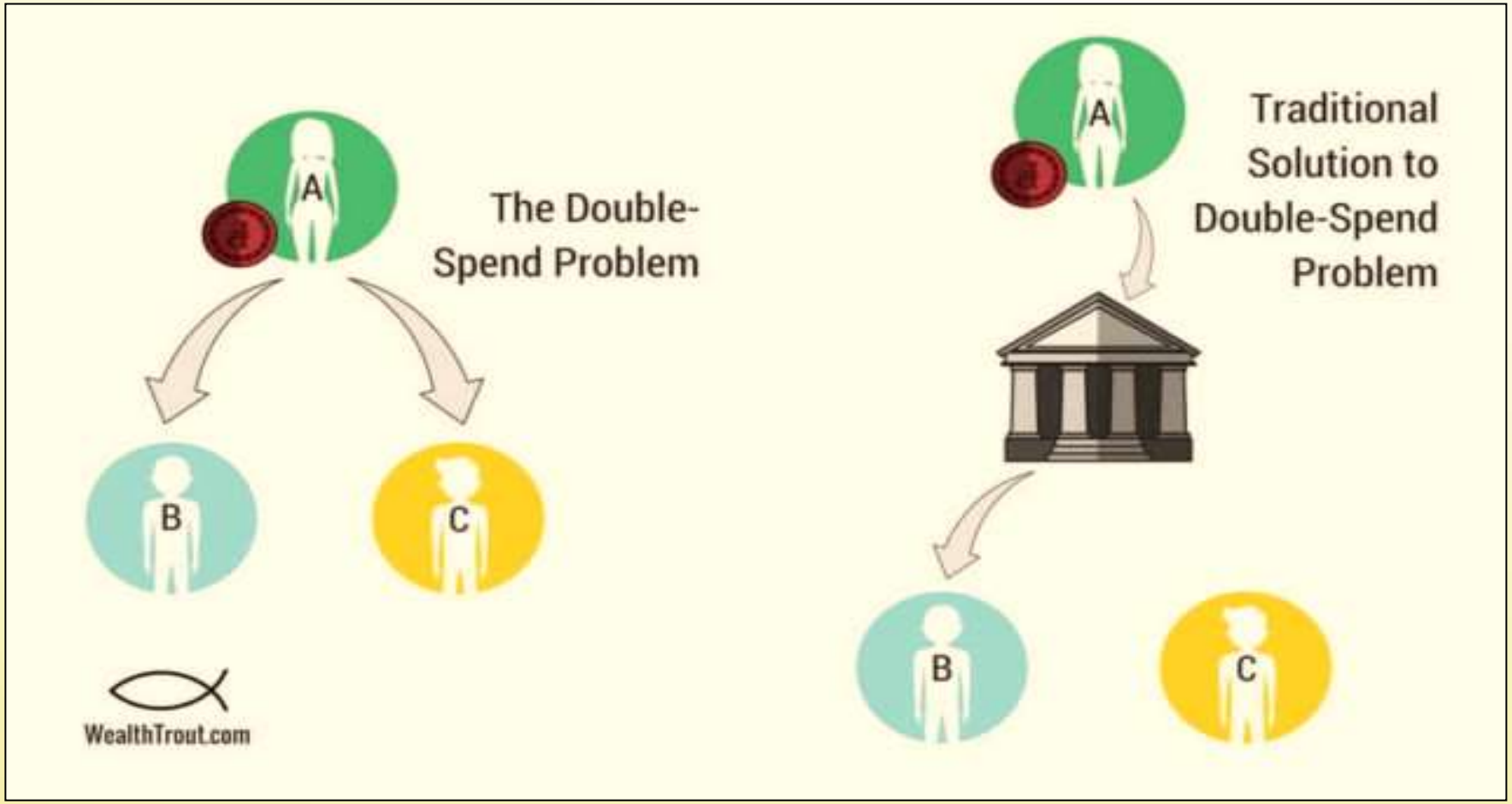
RAW HEX VERSION

BITCOIN GENESIS BLOCK

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?Lï8Ä
00000100  F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
00000110  8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```



Double-Spend Problem !?



صورت مسئله

آیا از نظر فنی

انجام معامله بدون حضور شخص سوم

امکان پذیر است؟

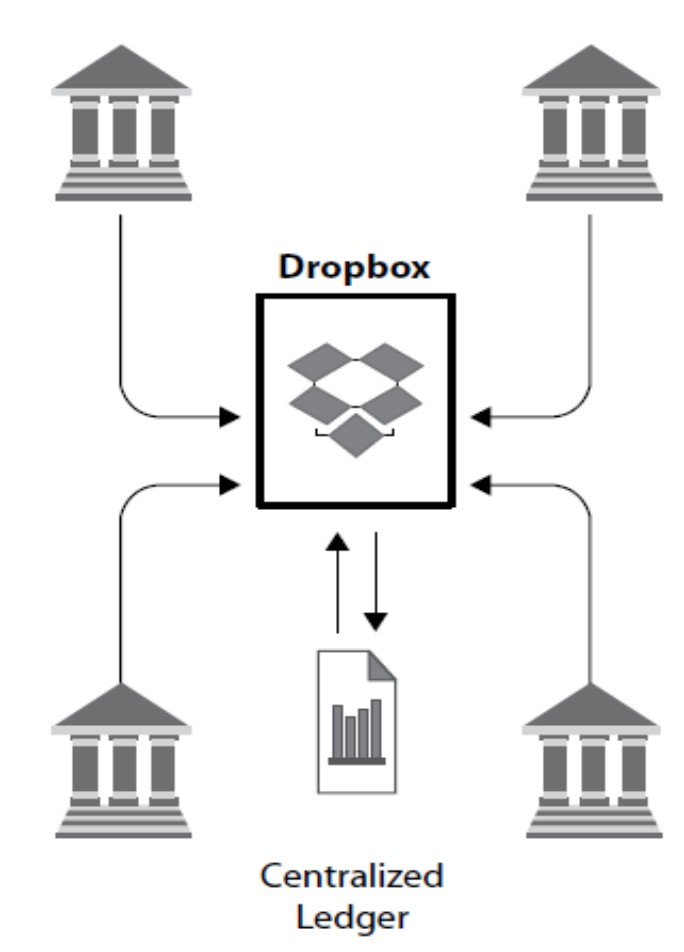
چگونه؟

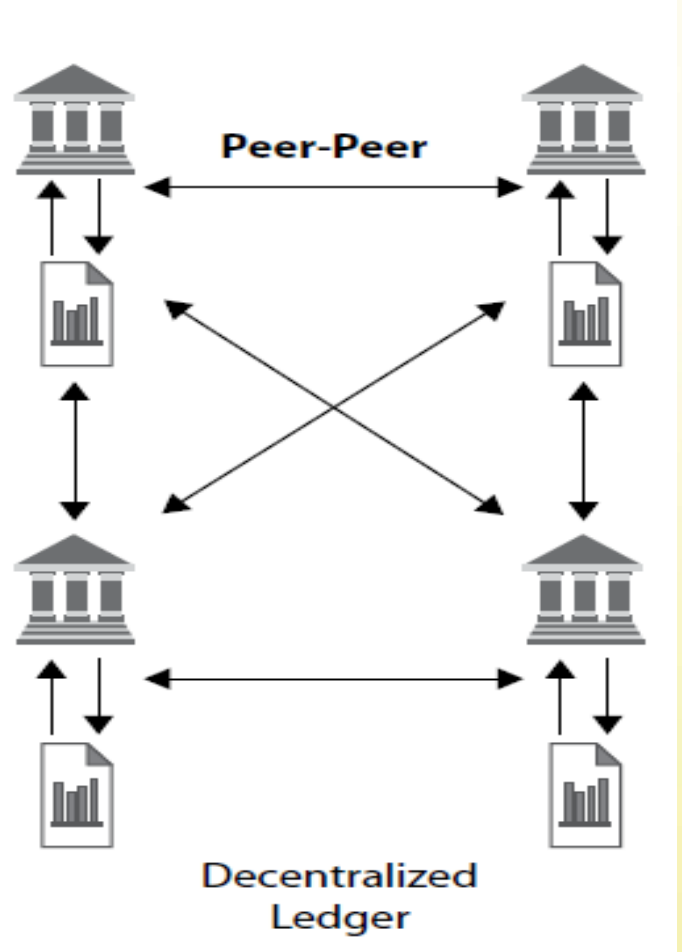
ایجاد یک پایگاه داده (دفتر کل)

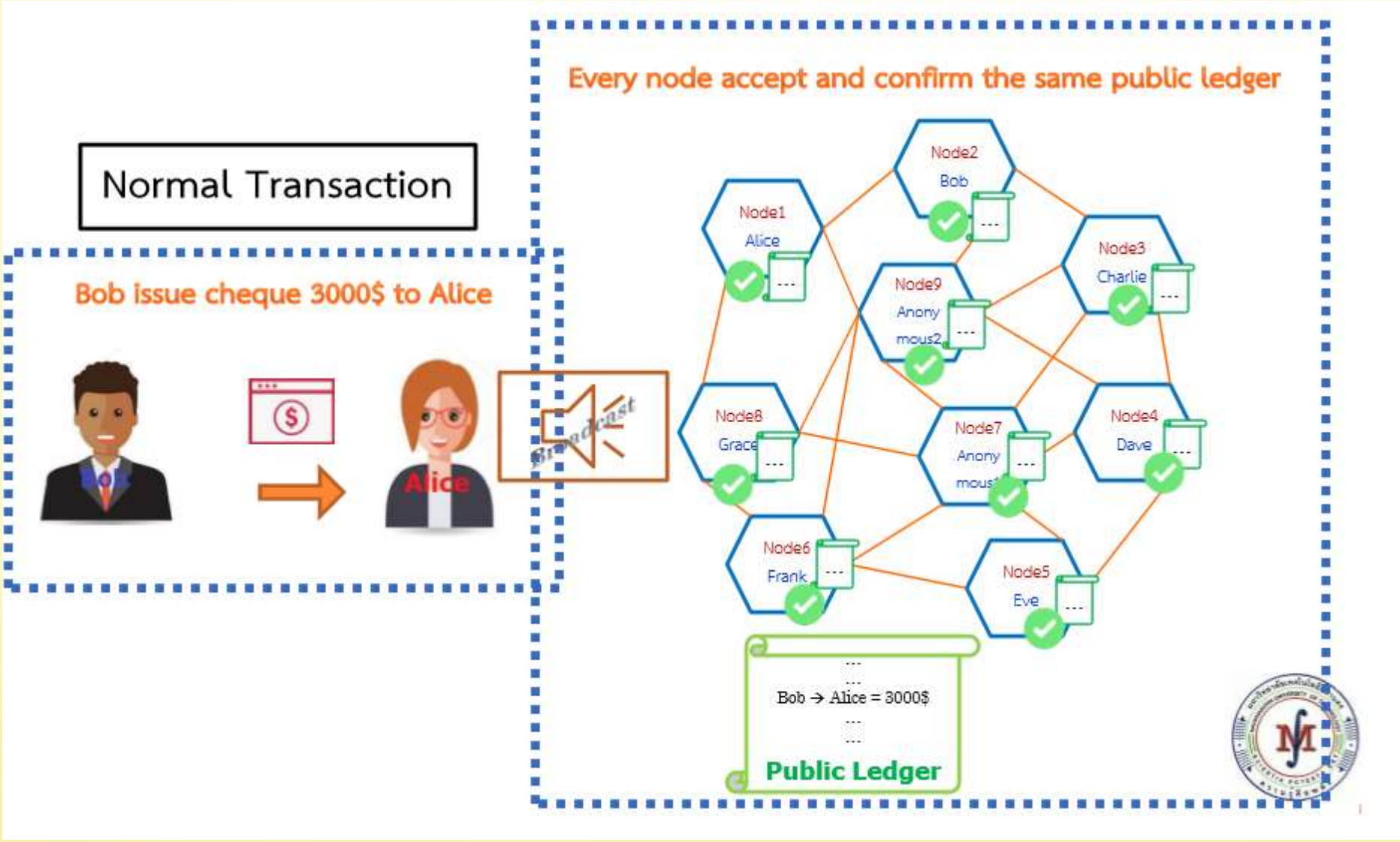
توزیع شده و غیر متمرکز

و ثبت رکورد معامله در آن

تفاوت دفتر کل متمرکز با غیر متمرکز



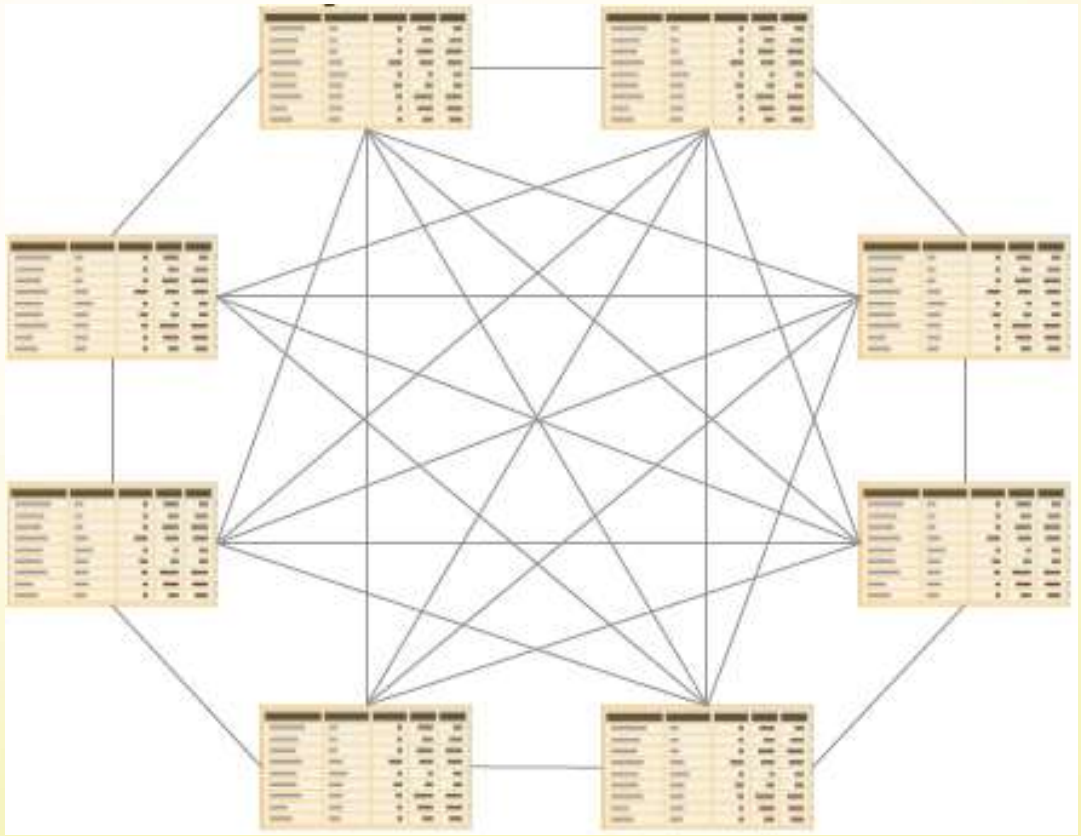



Normal Transaction
Bob issue cheque 3000$ to Alice
Alice
Broadcast
Every node accept and confirm the same public ledger
Node1
Alice
Node2
Bob
Node3
Charlie
Node9
Anony
mous2
Node8
Grace
Node7
Anony
Node4
Dave
Node6
Frank
Node5
Eve
Bob → Alice = 3000$
Public Ledger

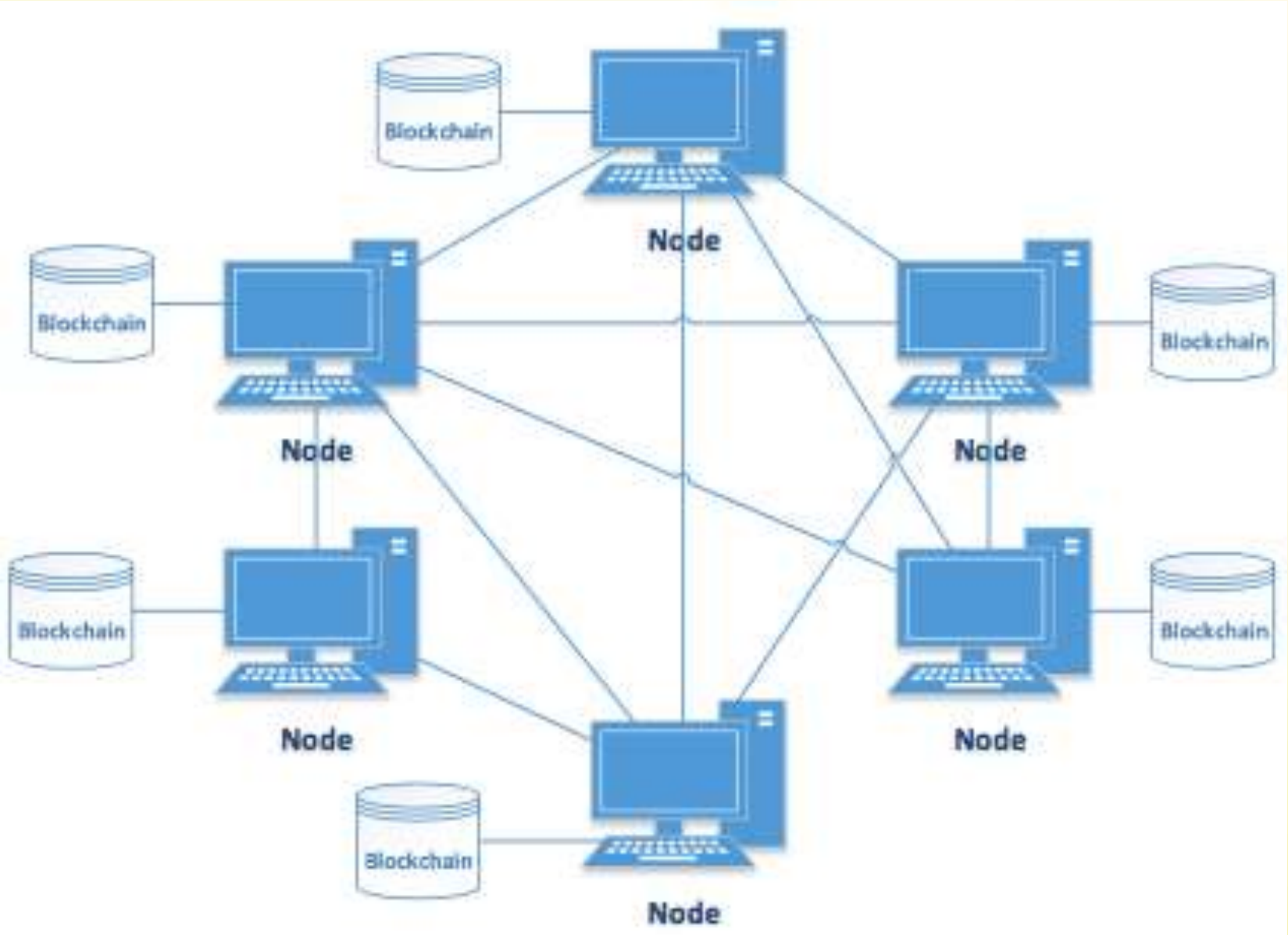
توزیع دفتر کل بین همه نودها

FROM	TO	PROPERTY	VALUE
Alex	Katie	Payment	$500
Jim	Sally	Payment	$300
Alex	Garth	Asset	Car
Katie	Tony	Payment	$100
Molly	Paula	Message	I love you

نمونه یک دفتر کل



همه شبکه یک نسخه از دفتر کل را دارند


Blockchain
Node
Blockchain
Node
Blockchain
Node
Blockchain
Node
Blockchain
Node
Blockchain
Node

دیوان سالاری

کاربردها

- در ساده ترین حالت، امکان ثبت تراکنش ها بین گروهی از افراد را فراهم میکند، به گونه ای که پس از ثبت قابل تغییر نخواهند بود. (مشابه بیت کوین)

- این فناوری برای کاربردهای دیگر نیز قابل استفاده است، زیرا کسب و کارها میتوانند بدون نیاز به اعتماد به افراد ناشناس با آنها کار کنند.

بخش دوم:
کاربردهای فناوری بلاکچین

مرتضی سرگلزایی جوان
مرکز تحقیقات رایانش ابری

روند توسعه فناوری های مرتبط

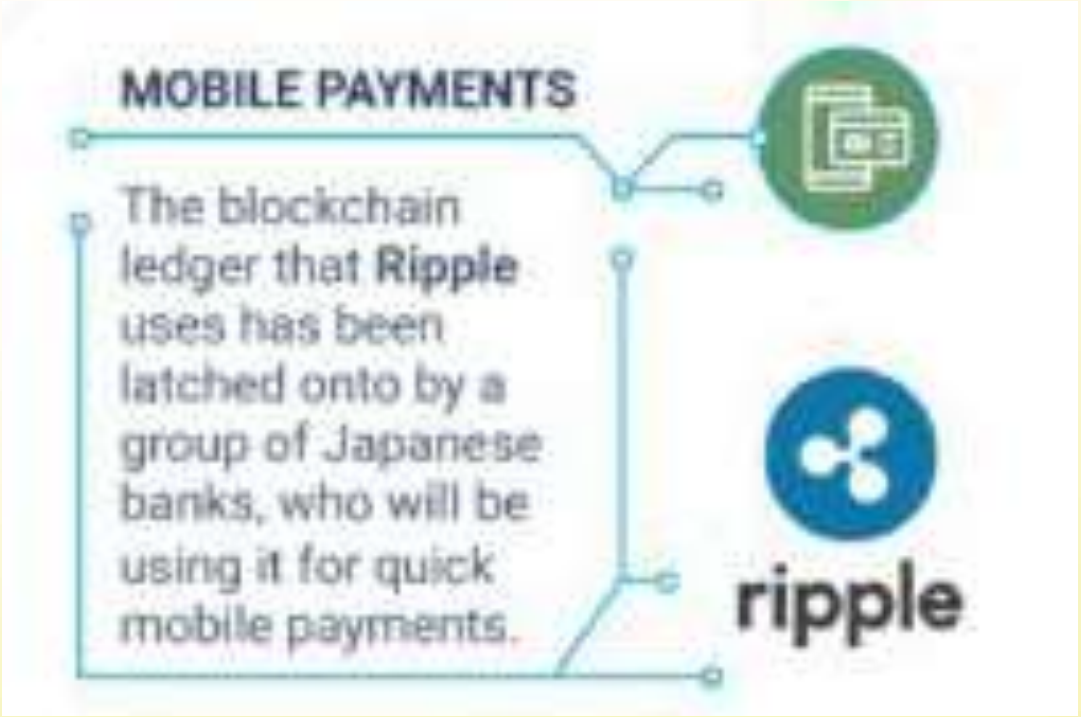
1. Bitcoin (Currency)
2. Blockchain (Interorganizational cooperation)
3. Smart Contract & DApps (Blockchain 2.0: Ethereum)
4. DAO & Consensus : Proof-of-work -> Proof-of-stake
5. Blockchain Scaling (for the Internet of Things)

کاربردهای مختلف

- مالی و پرداخت
- بیمه
- رسانه
- فناوری اطلاعات و ارتباطات
- سلامت
- دارایی ها
- دولت
- هویت
- اینترنت اشیا
- زنجیره تامین
- حمل و نقل

کاربردها در حوزه مالی

- Ripple



کاربردها در حوزه زنجیره تامین

- Provenance

آثار هنری

- Fresco

فناوری اطلاعات و ارتباطات

- Micronizationof work (pay for
- algorithms, tweets, ad clicks, etc.)
- Expanse of marketplace
- Disbursement of work
- Direct to developer payments
- API platform plays
- Notarization & certification
- P2P storage & compute sharing
- DNS

کاربردها در حوزه رسانه و سرگرمی

- Digital rights mgmt
- Game monetization
- Art authentication
- Purchase & usage monitoring
- Ticket purchases
- Fan tracking
- Ad click fraud reduction
- Resell of authentic assets
- Real time auction & ad placements

+ steem

کاربردها در حوزه احراز هویت

- Personal
- Objects
- Families of objects
- Digital assets
- Multifactor Auth
- Refugee tracking
- Education & badgingPurchase & review tracking
- Employer & Employee reviews

اینترنت اشیا

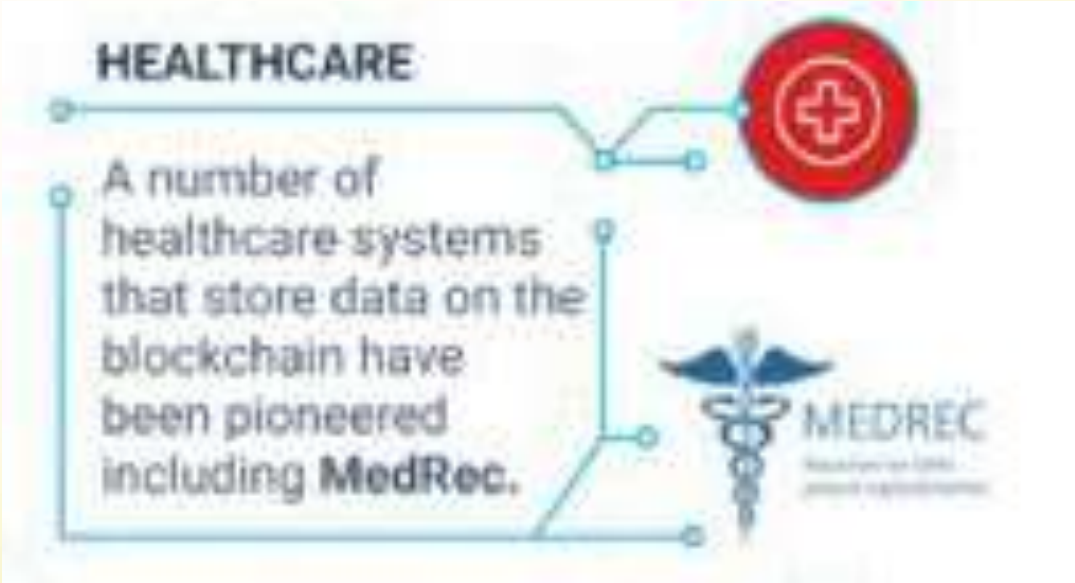
- Device to Device payments & **Interactions**
- Device directories
- Operations (e.g. water flow)
- Grid monitoring
- Smart home & office management
- Cross-company maintenance markets

بیمه

- Claim filings
- MBS/Property payments
- Claims processing & admin
- Fraud detection/prediction
- Telematics & ratings
- Digital authentication
- Asset management
- Automated underwriting
- Self-administered insurance

سلامت

- Records sharing
- Prescription sharing
- Compliance
- Personalized medicine
- DNA sequencing

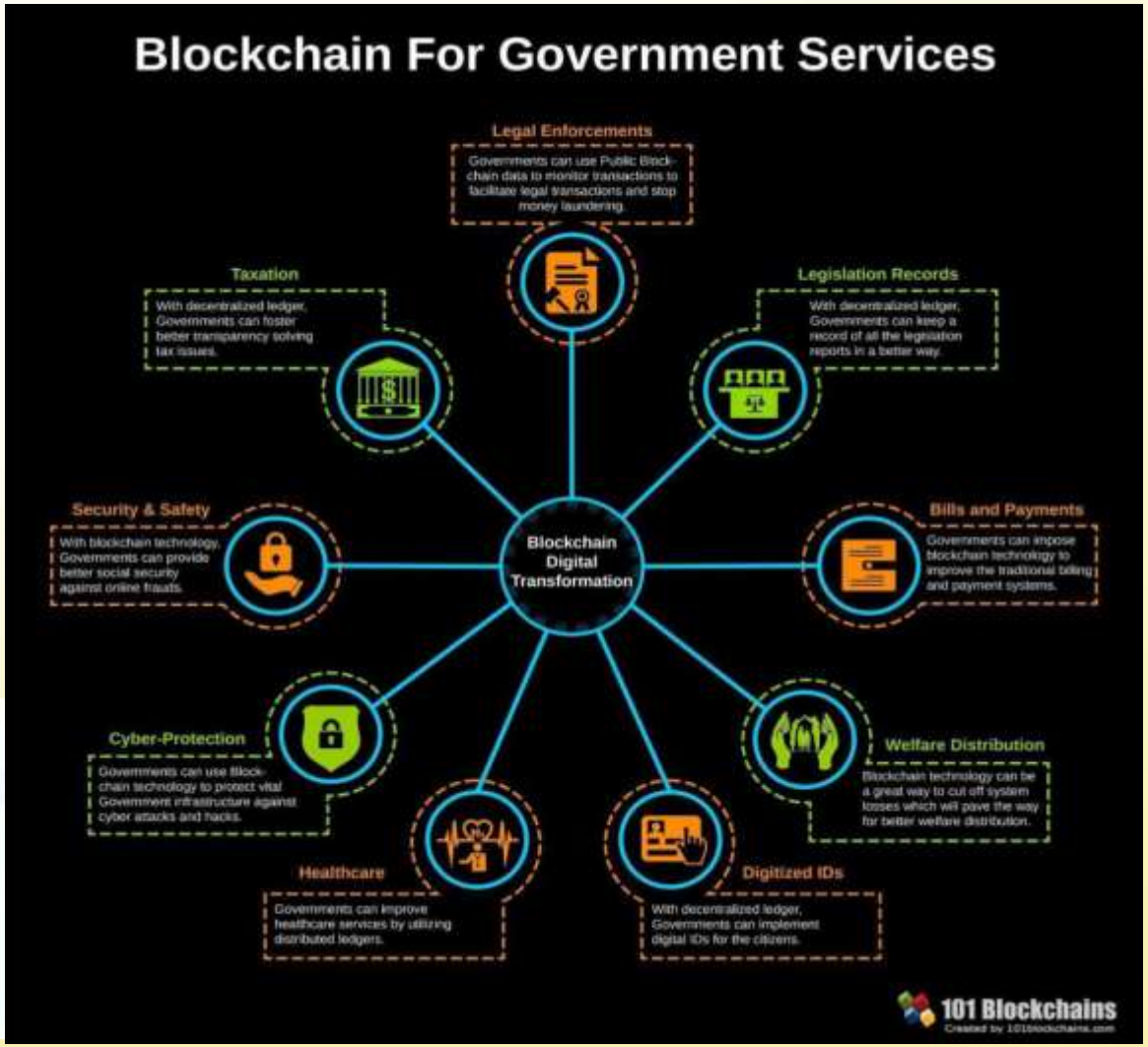


دارایی ها

- Asset Titles
- Diamonds
- Designer brands
- Car leasing & sales
- Home Mortgages & payments
- Land title ownership
- Digital asset records

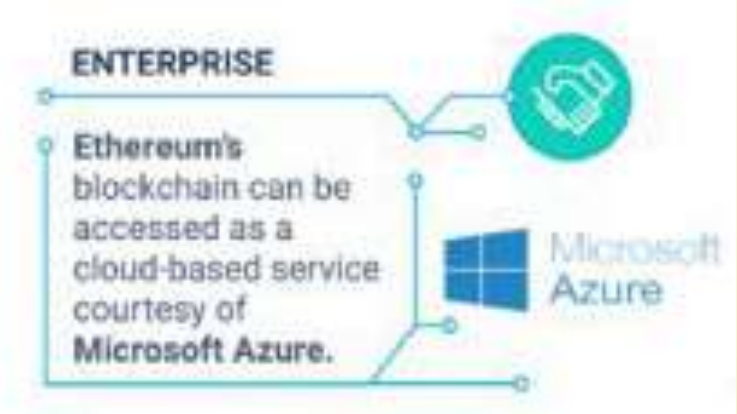
دولت

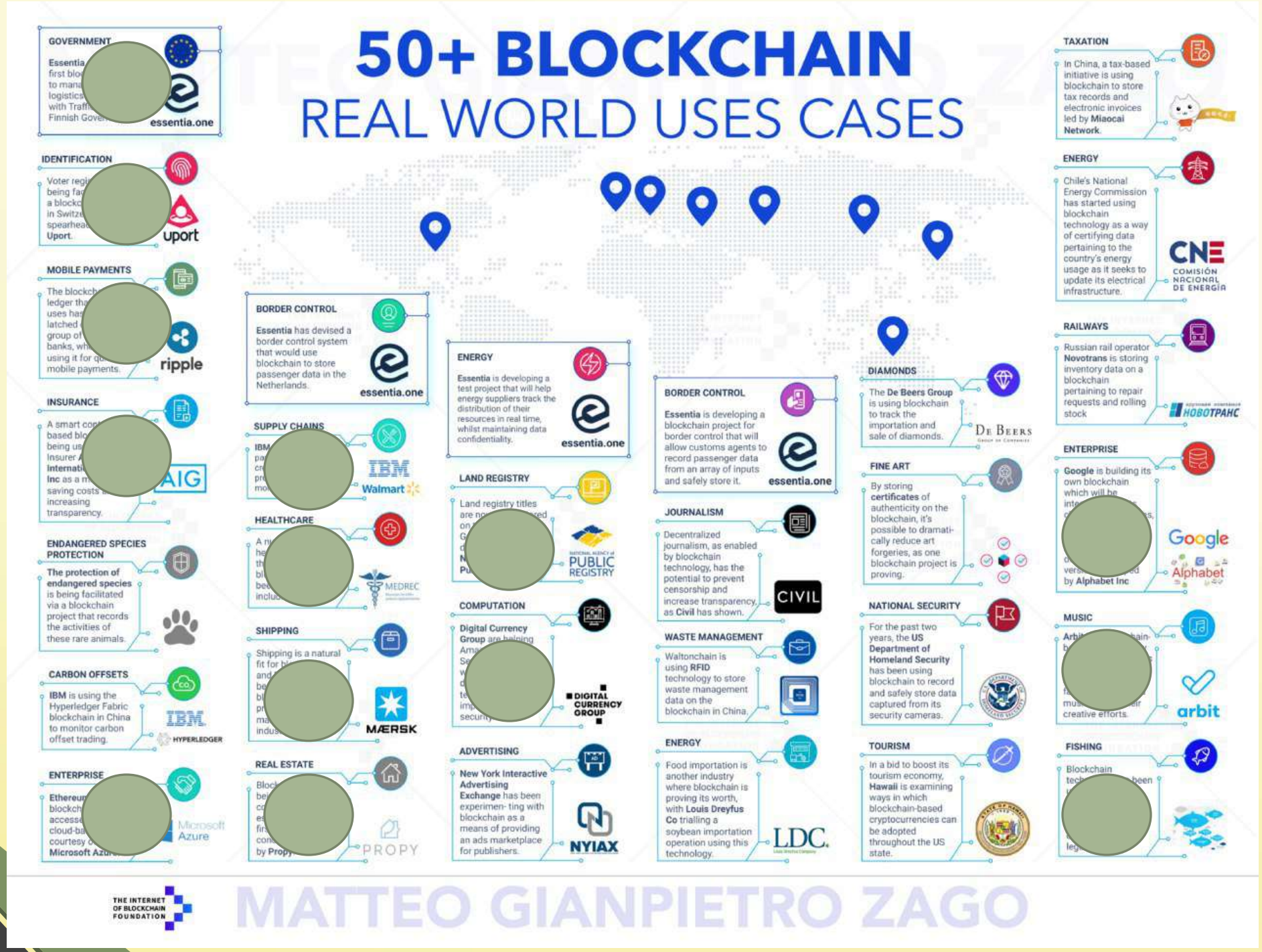
- Voting
- Vehicle registration
- WIC, Vet, SS, benefits, distribution
- Licensing & identification
- Copyrights

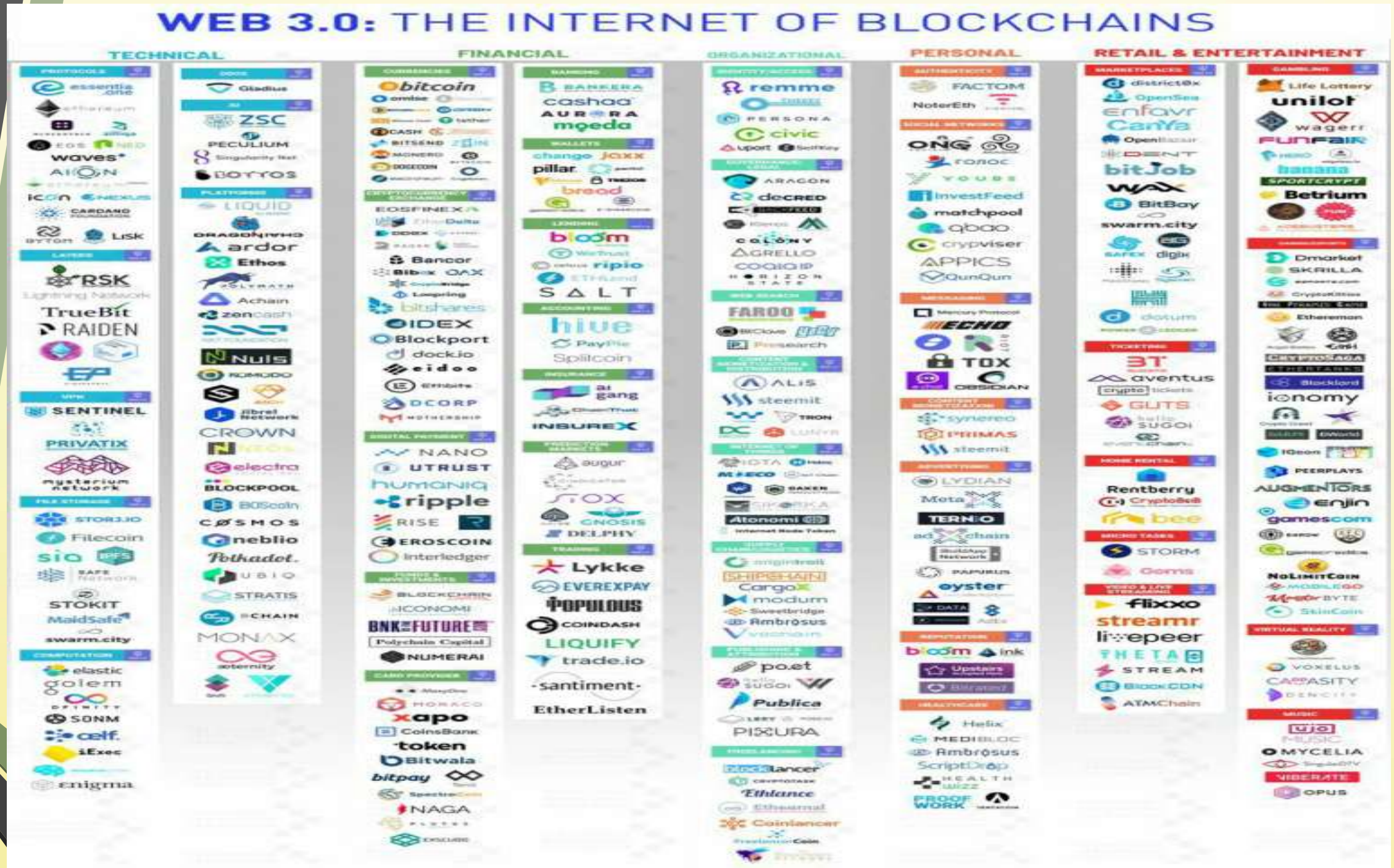


کاربردهای سازمانی

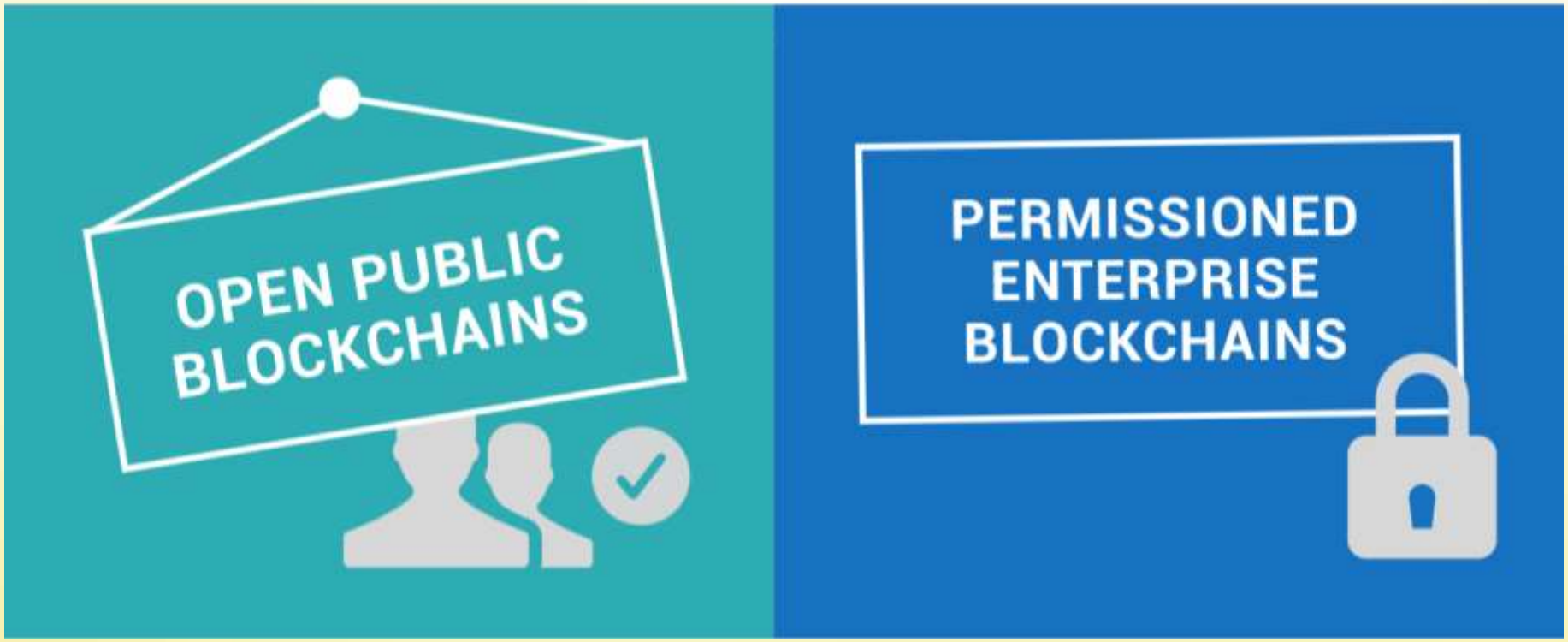
- B2B Integration
- Inter Department
- Data Sharing




50+ BLOCKCHAIN
REAL WORLD USES CASES
GOVERNMENT
essentia.one
IDENTIFICATION
uport
MOBILE PAYMENTS
ripple
INSURANCE
AIG
ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.
CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.
IBM
HYPERLEDGER
ENTERPRISE
Microsoft Azure
BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.
essentia.one
SUPPLY CHAINS
IBM
Walmart
HEALTHCARE
MEDREC
SHIPPING
Shipping is a natural fit for
MÆRSK
REAL ESTATE
PROPY
ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.
essentia.one
LAND REGISTRY
Land registry titles are no
PUBLIC REGISTRY
COMPUTATION
Digital Currency Group are helping
DIGITAL CURRENCY GROUP
ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.
NYIAX
BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.
essentia.one
JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as Civil has shown.
CIVIL
WASTE MANAGEMENT
Waltonchain is using RFID technology to store waste management data on the blockchain in China.
ENERGY
Food importation is another industry where blockchain is proving its worth, with Louis Dreyfus Co trialling a soybean importation operation using this technology.
LDC
DIAMONDS
The De Beers Group is using blockchain to track the importation and sale of diamonds.
DE BEERS
FINE ART
By storing certificates of authenticity on the blockchain, it's possible to dramati- cally reduce art forgeries, as one blockchain project is proving.
NATIONAL SECURITY
For the past two years, the US Department of Homeland Security has been using blockchain to record and safely store data captured from its security cameras.
TOURISM
In a bid to boost its tourism economy, Hawaii is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.
TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by Miaocai Network.
ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.
CNE
COMISIÓN NACIONAL DE ENERGÍA
RAILWAYS
Russian rail operator Novotrans is storing inventory data on a blockchain pertaining to repair requests and rolling stock
НОВОТРАНС
ENTERPRISE
Google is building its own blockchain which will be
by Alphabet Inc
Google
Alphabet
MUSIC
arbit
FISHING
Blockchain
been
THE INTERNET OF BLOCKCHAIN FOUNDATION
MATTEO GIANPIETRO ZAGO



انواع بلاکچین



بخش سوم:
معماری و فناوریهای مورد استفاده

مرتضی سرگلزایی جوان
مرکز تحقیقات رایانش ابری

اجزای تشکیل دهنده بیت کوین

- **Bitcoin: A Peer to Peer Electronic Cash System, 2008 [3]**
  - **Distributed Public Ledger**
    1. Basic Blockchain Technology (secure timestamping of docs), 1991 ~ 1993 [2]
       - A signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed.
    2. Broadcast Transactions (b-money), 1998
    3. Proof-of-Work (hashcash), 2002

فناوری های مورد استفاده

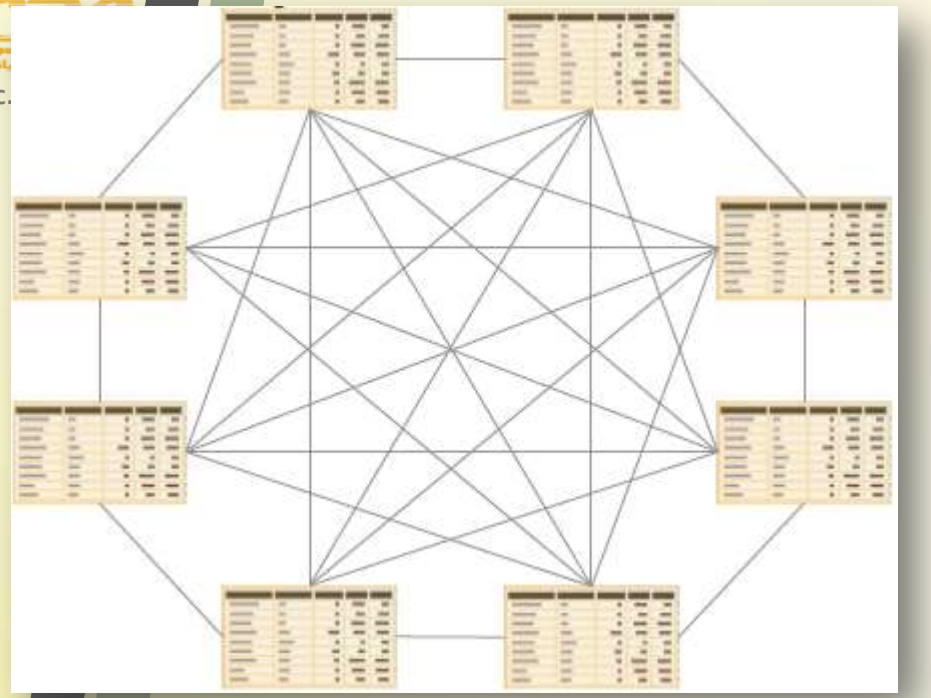
- علوم رایانه (Linked Lists و شبکه های توزیع شده)
- اصول رمزنگاری (تابع هش، امضای دیجیتال، رمزنگاری نامتقارن)
- مفاهیم اقتصادی (دفترکل)

تعریف

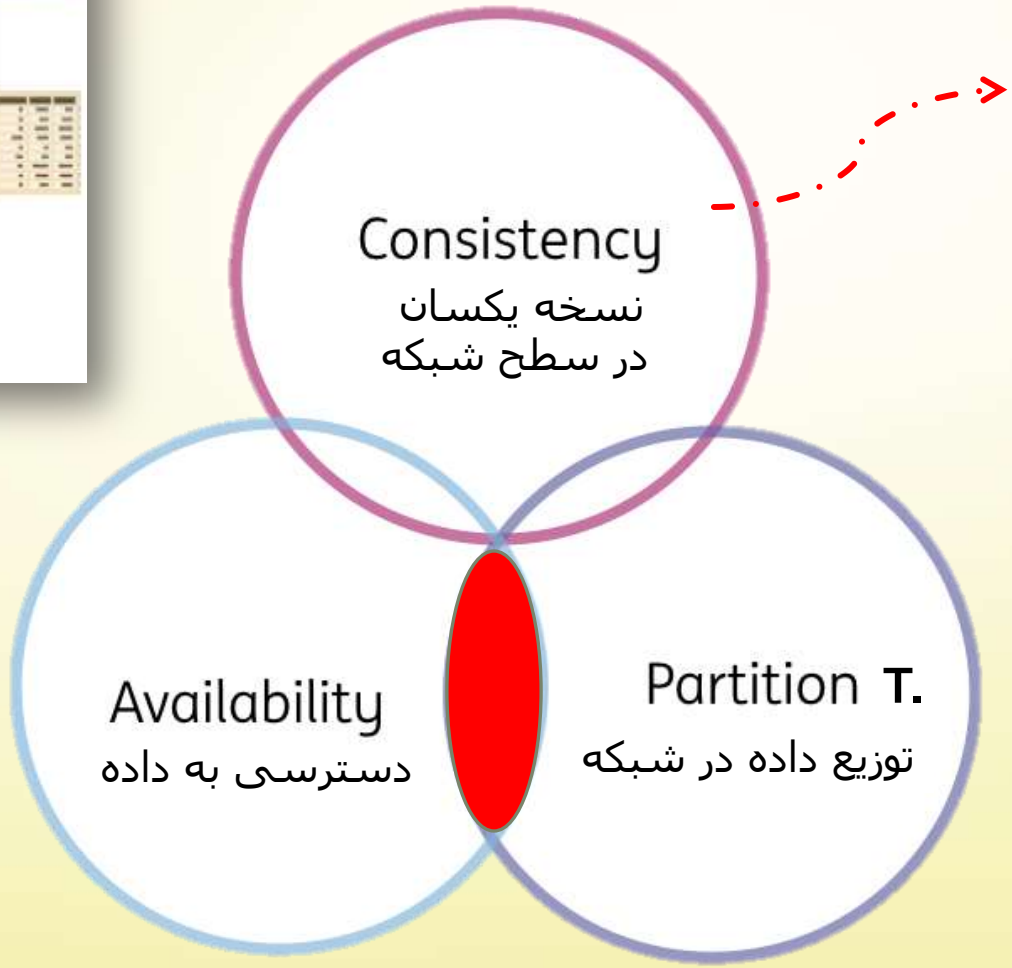
Blockchain is a secured, shared, distributed, immutable database

تعریف از استاندارد NIST 8202

- Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision.
- As new blocks are added, older blocks become more difficult to modify (theoretically immutable). New blocks are replicated across all copies of the ledger within the network, and any conflicts are resolved automatically using established rules.



تئوری CAP



Eventually Consistent

معماری منطقی

Applications (Crypto Currency, DApp, DAO, GUI, TA,...)

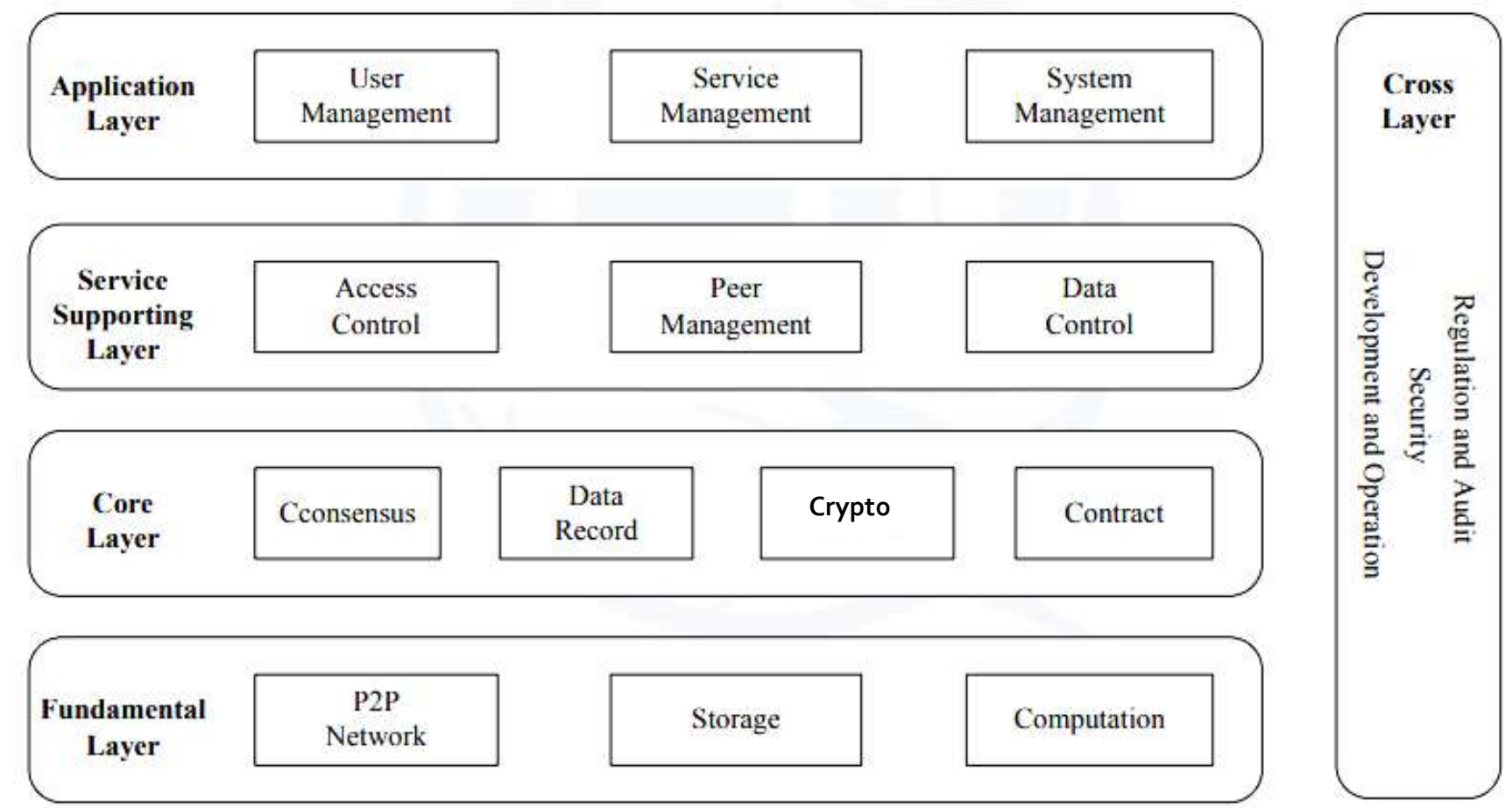
Runtime (Script, SmartContract, ...)

Consensus (PoW, PoS, BFT, ...)

Data (Blockchain,...)

Network (P2P,...)

معماری مرجع (کارکردی)

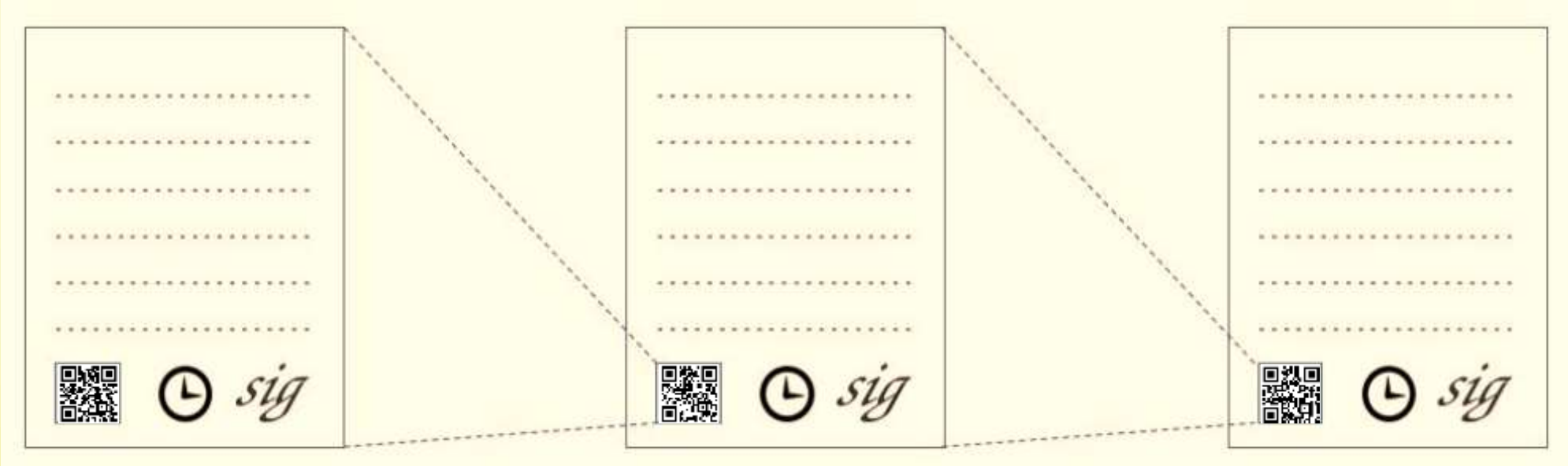


بخش چهارم:
مبانی رمزنگاری

مرتضی سرگلزایی جوان

مرکز تحقیقات رایانش ابری

برچسب زمانی امن



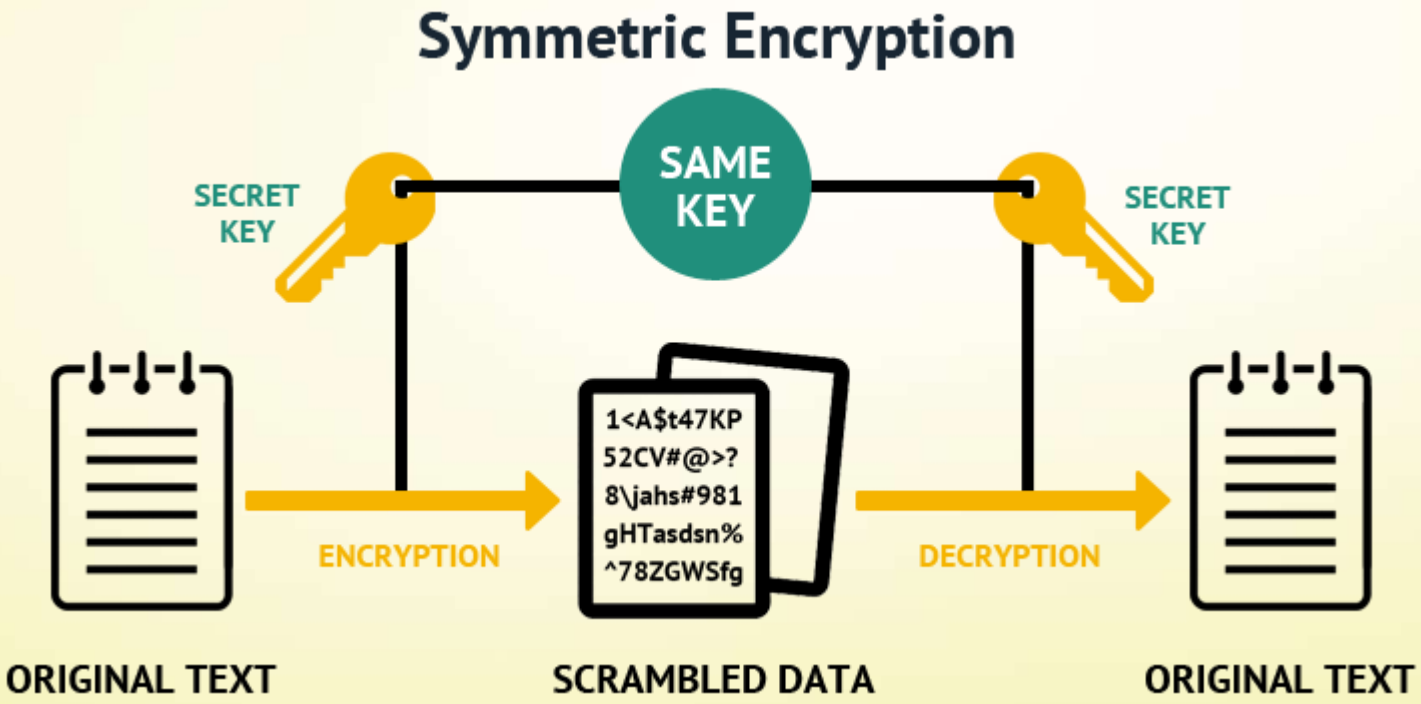
تابع درهم سازی (هش)

Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

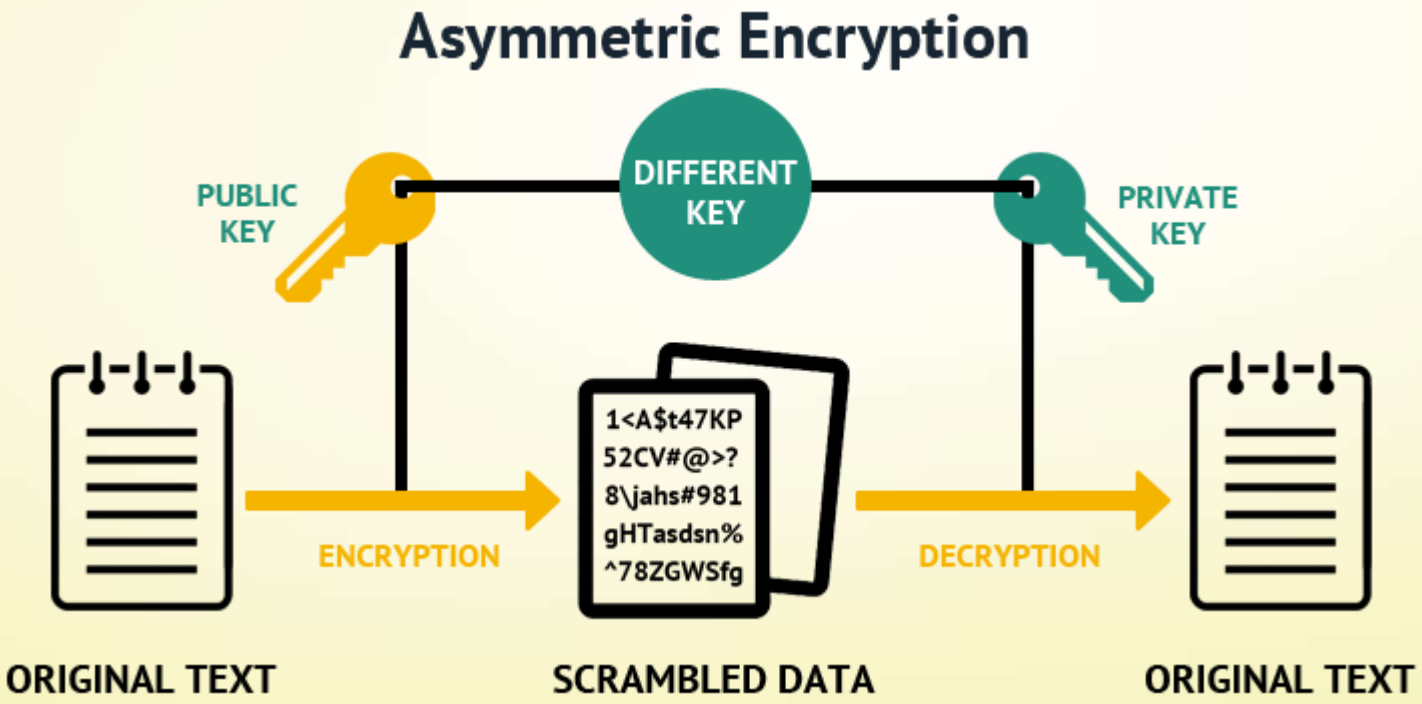
تراکنش

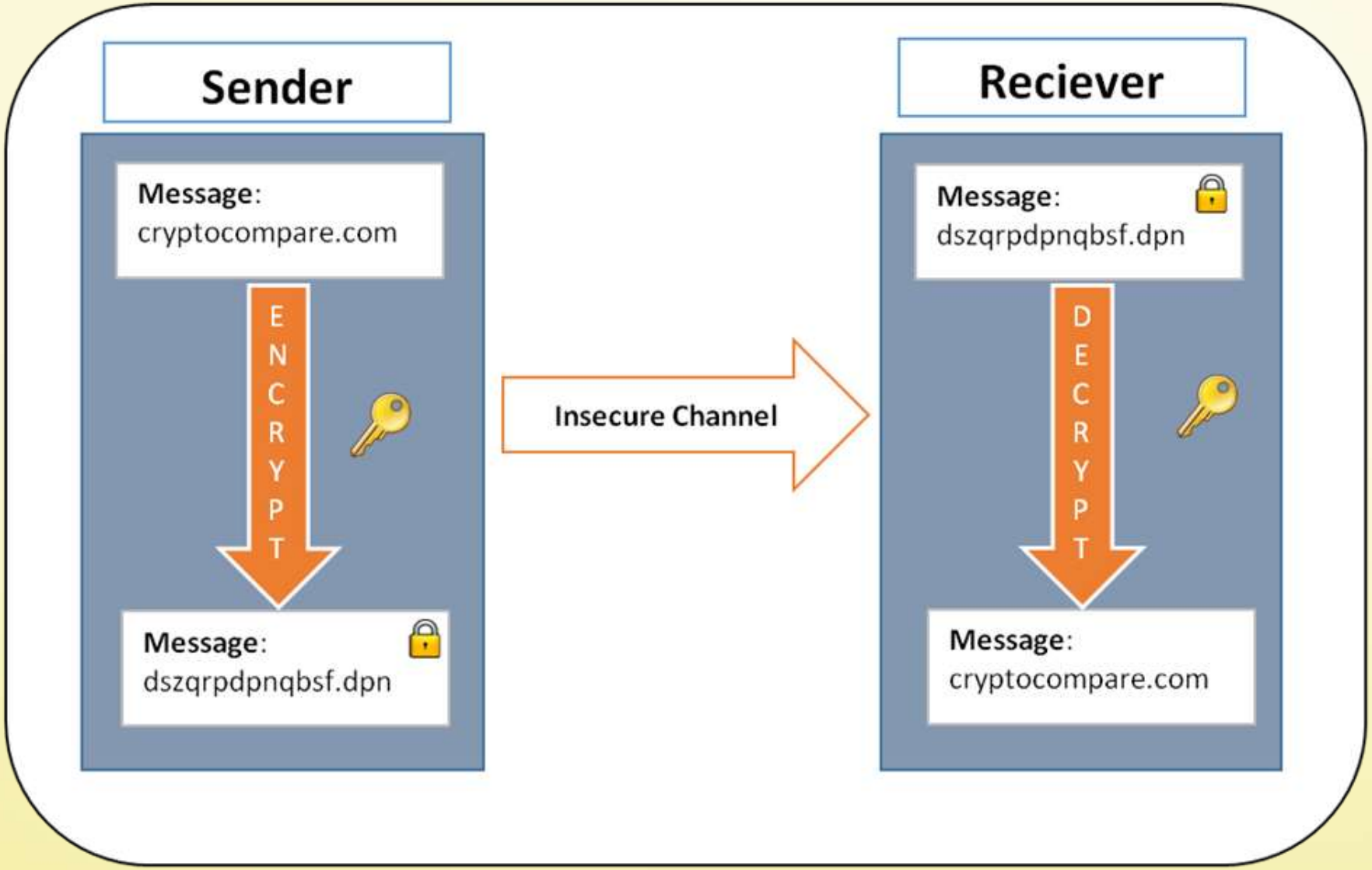
	Input	Output	Amount	Total
Transaction ID: 0xa1b2c3	Account A	Account B	0.0321	
		Account C	2.5000	
				2.5321

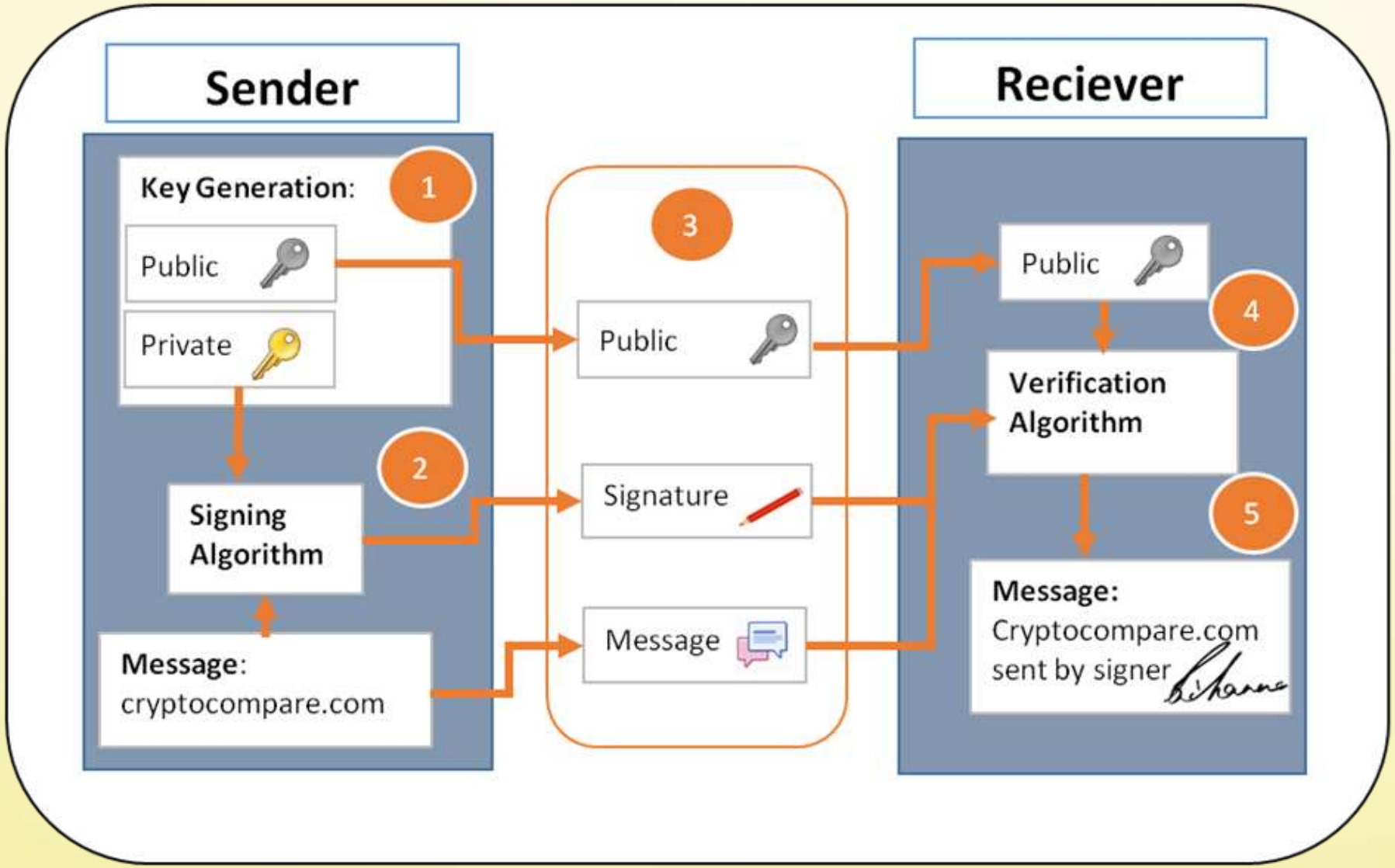
رمز نگاری متقارن



رمز نگاری نامتقارن




Sender
Message:
cryptocompare.com
ENCRYPT
Message:
dszqrpdpnqbsf.dpn
Insecure Channel
Reciever
Message:
dszqrpdpnqbsf.dpn
DECRYPT
Message:
cryptocompare.com

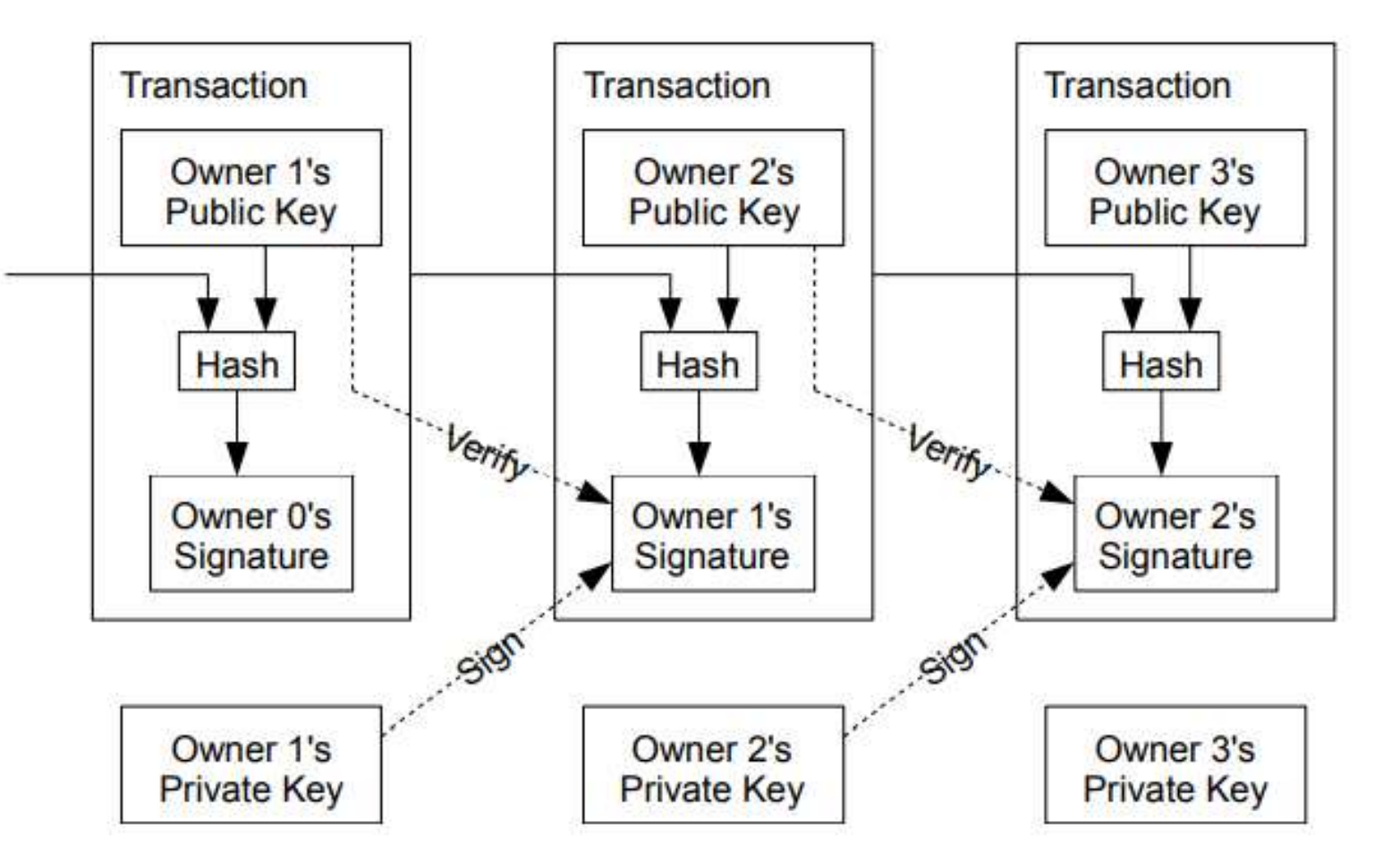

Sender
Reciever
Key Generation:
1
Public
Private
2
Signing Algorithm
Message:
cryptocompare.com
3
Public
Signature
Message
Public
4
Verification Algorithm
5
Message:
Cryptocompare.com
sent by signer

امضای تراکنش (۱)

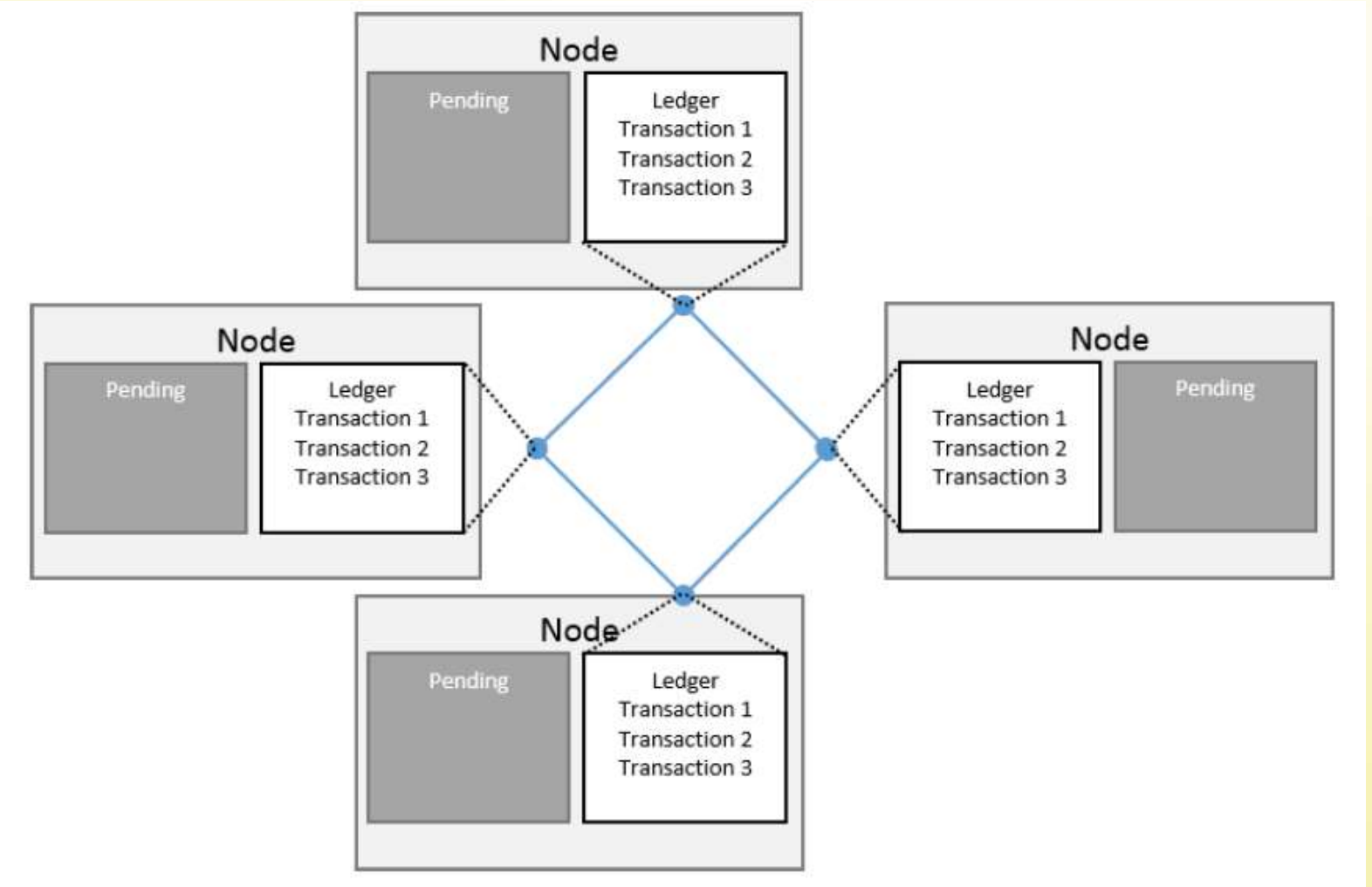
	Input	Output	Amount	Total
Transaction ID: 0xa1b2c3	Account A	Account B	0.0321	
		Account C	2.5000	
				2.5321

Signed With Private Key

امضای تراکنش (۲)



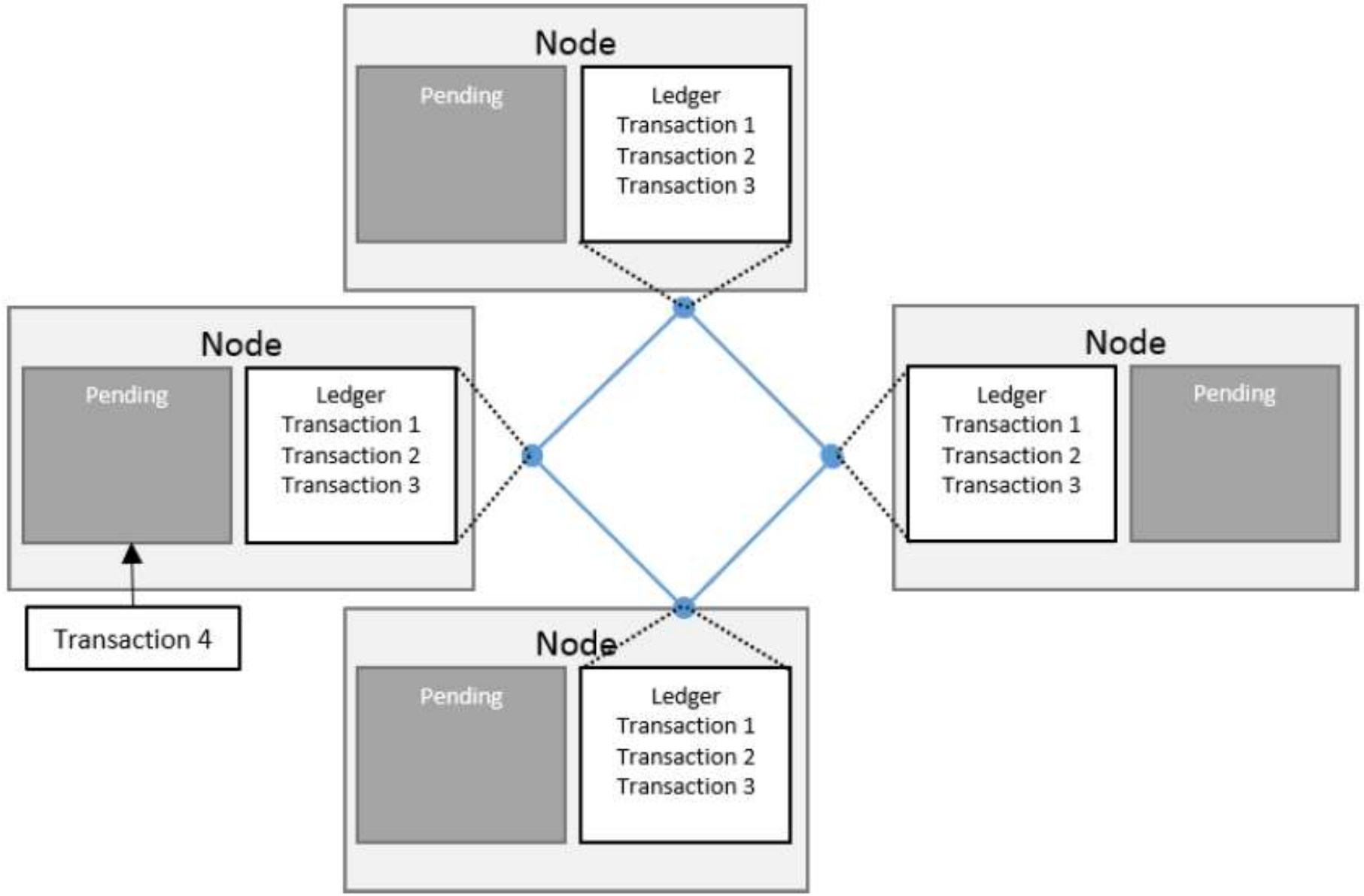
ثبت تراکنش در دفتر کل

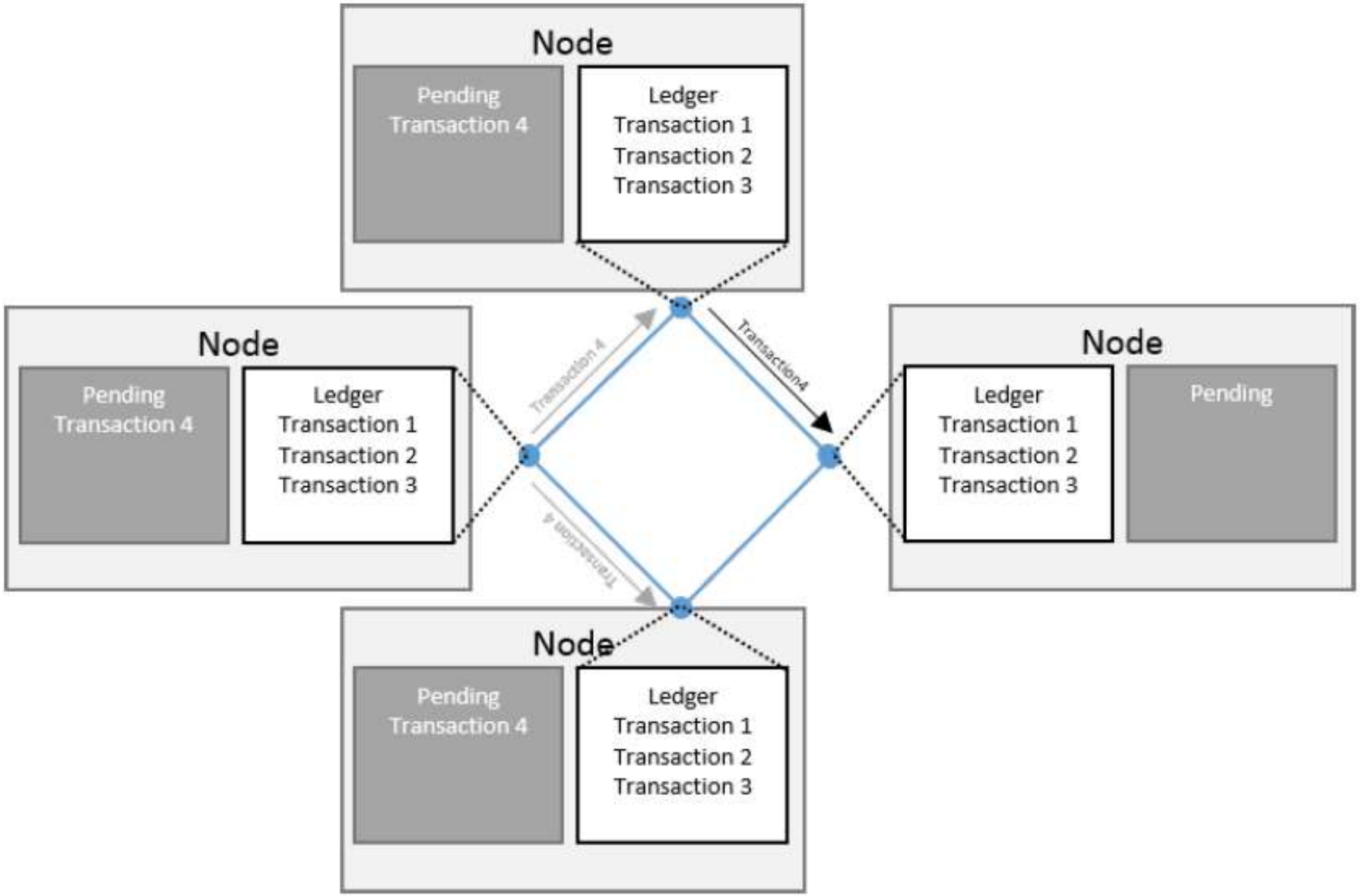


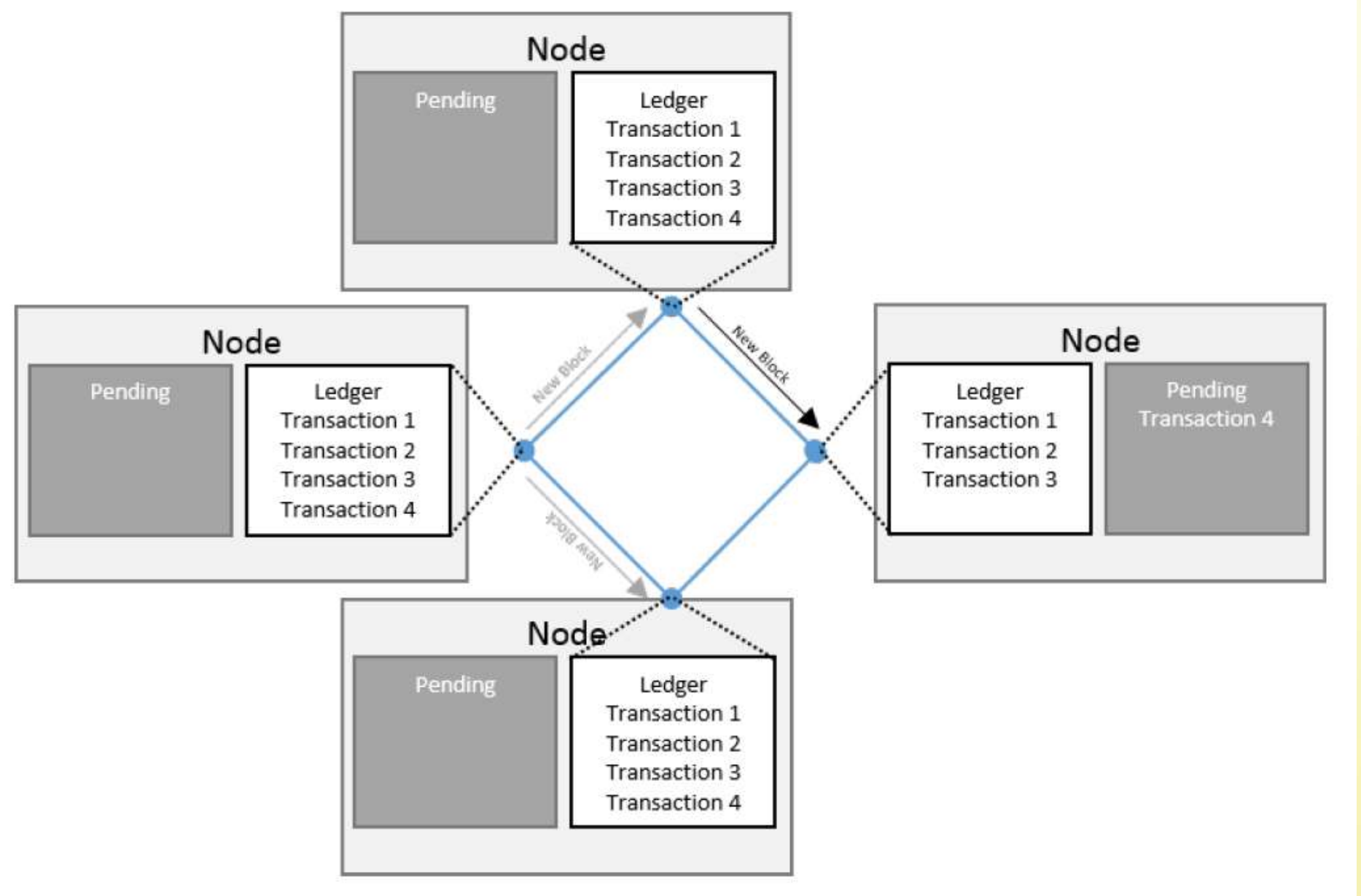
بخش پنجم:
الگوریتم های اجماع

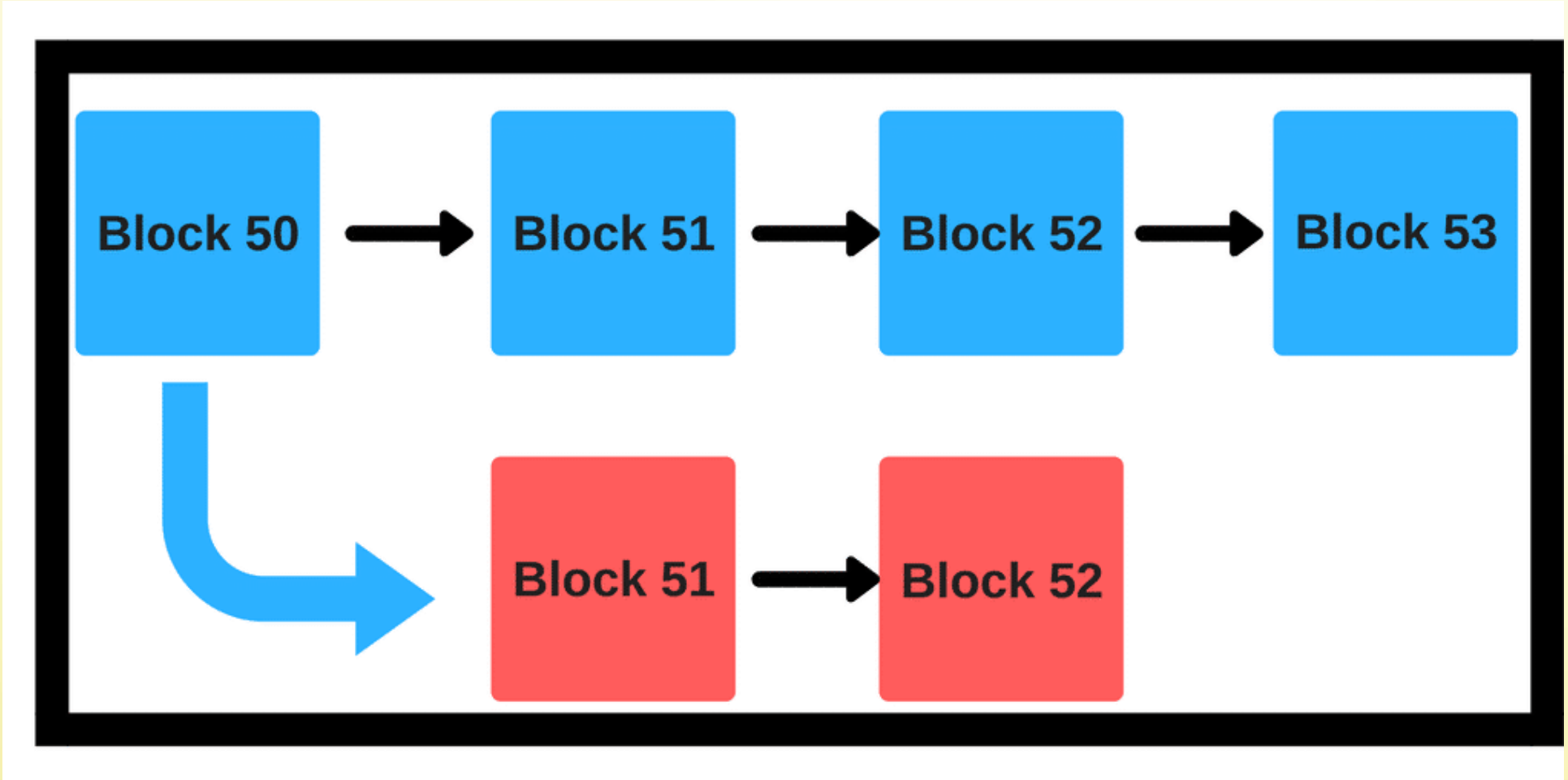
مرتضی سرگلزایی جوان

مرکز تحقیقات رایانش ابری

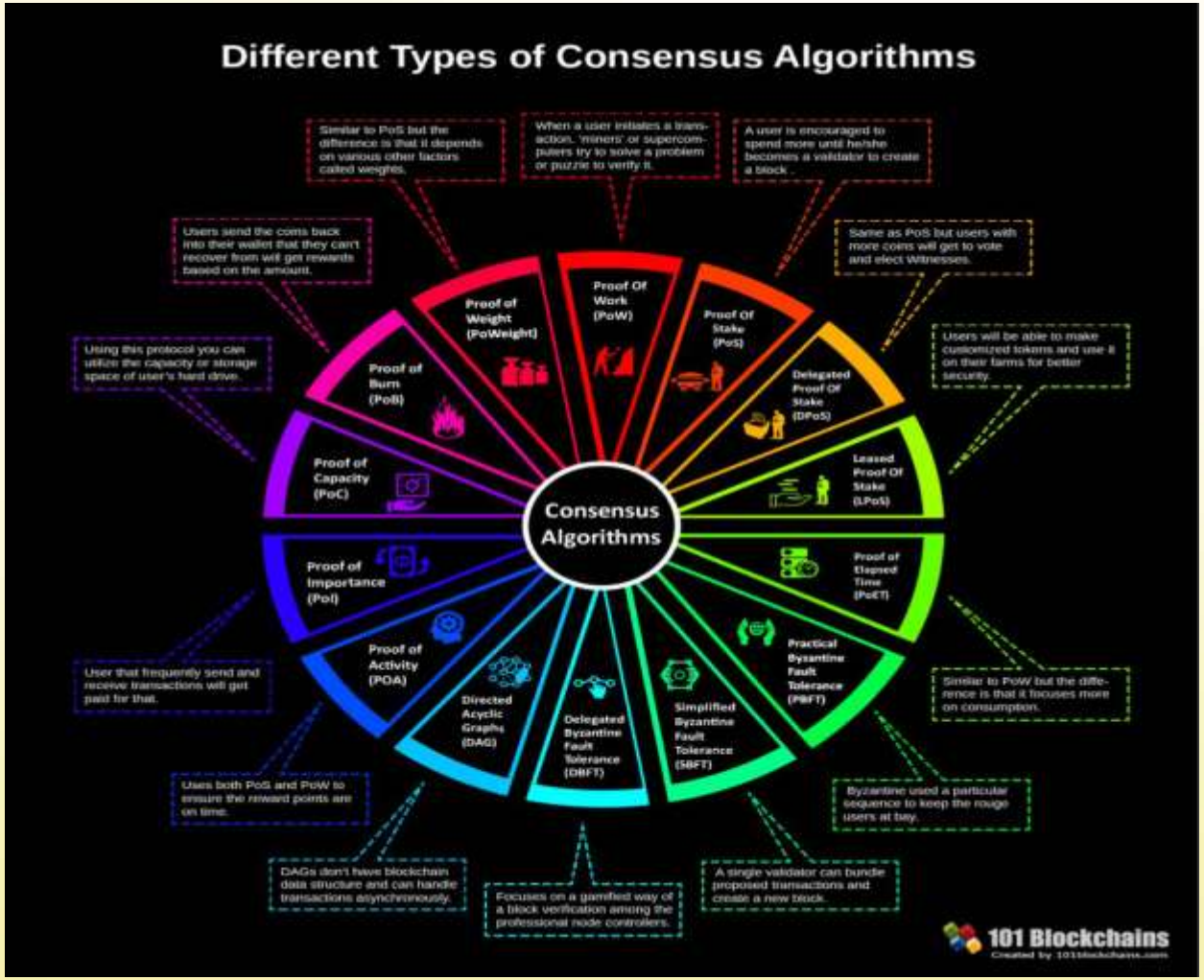

Node
Pending
Ledger
Transaction 1
Transaction 2
Transaction 3
Node
Pending
Ledger
Transaction 1
Transaction 2
Transaction 3
Node
Ledger
Transaction 1
Transaction 2
Transaction 3
Pending
Transaction 4
Node
Pending
Ledger
Transaction 1
Transaction 2
Transaction 3


Node
Pending
Transaction 4
Ledger
Transaction 1
Transaction 2
Transaction 3
Node
Pending
Transaction 4
Ledger
Transaction 1
Transaction 2
Transaction 3
Transaction 4
Transaction4
Node
Ledger
Transaction 1
Transaction 2
Transaction 3
Pending
Transaction 4
Node
Pending
Transaction 4
Ledger
Transaction 1
Transaction 2
Transaction 3

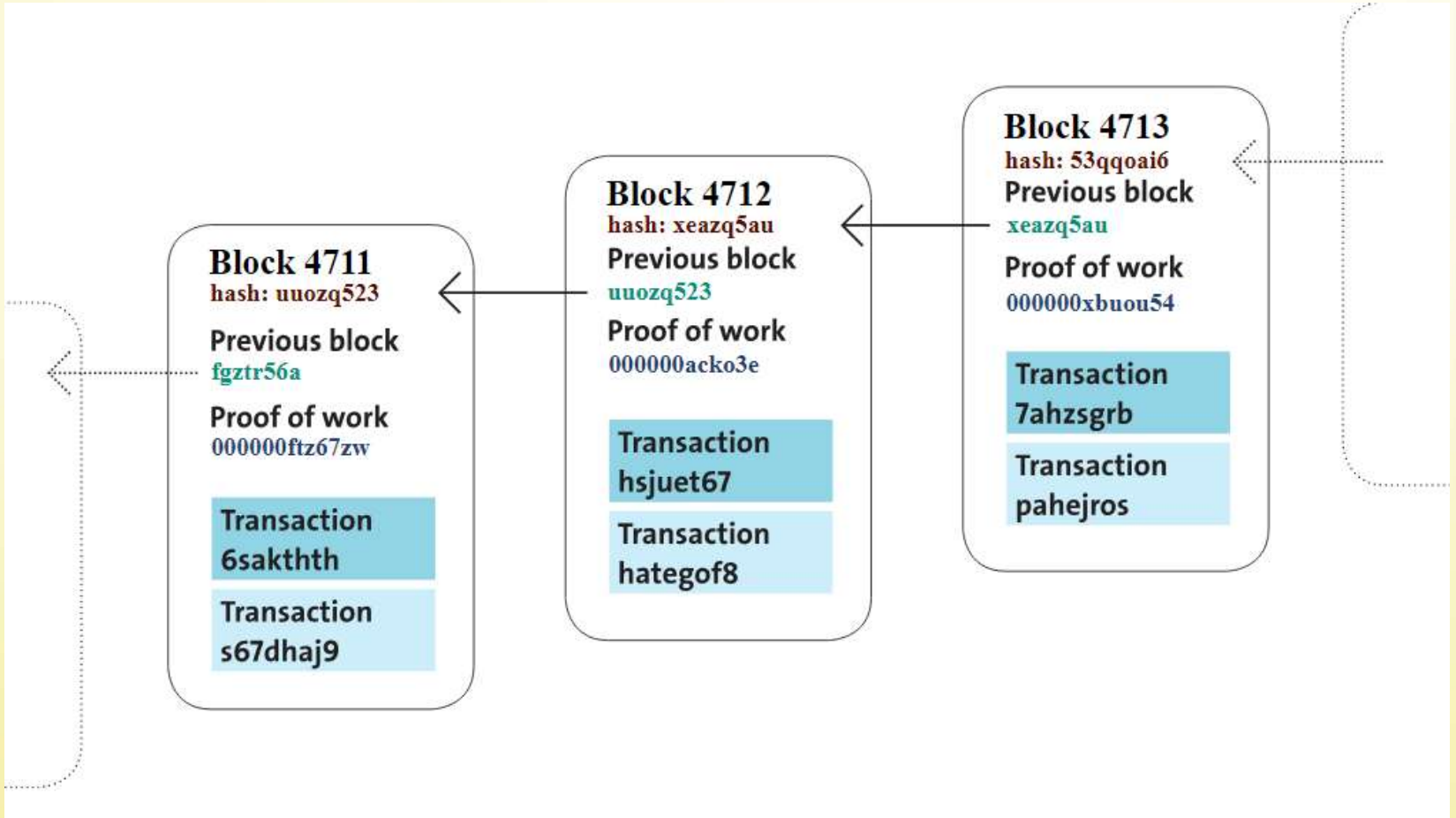

Node
Pending
Ledger
Transaction 1
Transaction 2
Transaction 3
Transaction 4
Node
Pending
Ledger
Transaction 1
Transaction 2
Transaction 3
Transaction 4
New Block
New Block
New Block
Node
Ledger
Transaction 1
Transaction 2
Transaction 3
Pending
Transaction 4
Node
Pending
Ledger
Transaction 1
Transaction 2
Transaction 3
Transaction 4


Block 50
Block 51
Block 52
Block 53
Block 51
Block 52

الگوریتم اجماع



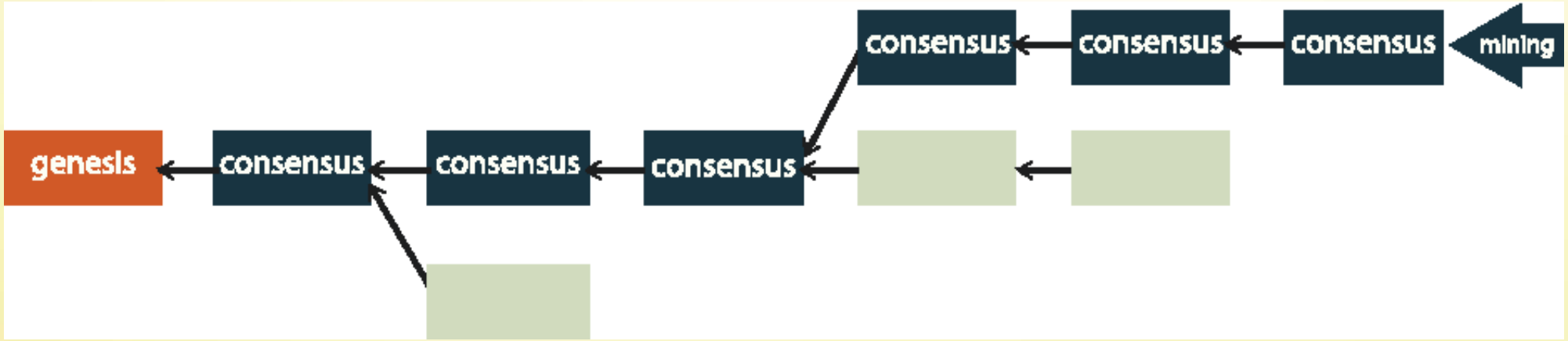
اجماع به روش Proof-of-Work (PoW)



عملیات ماینینگ (استخراج)

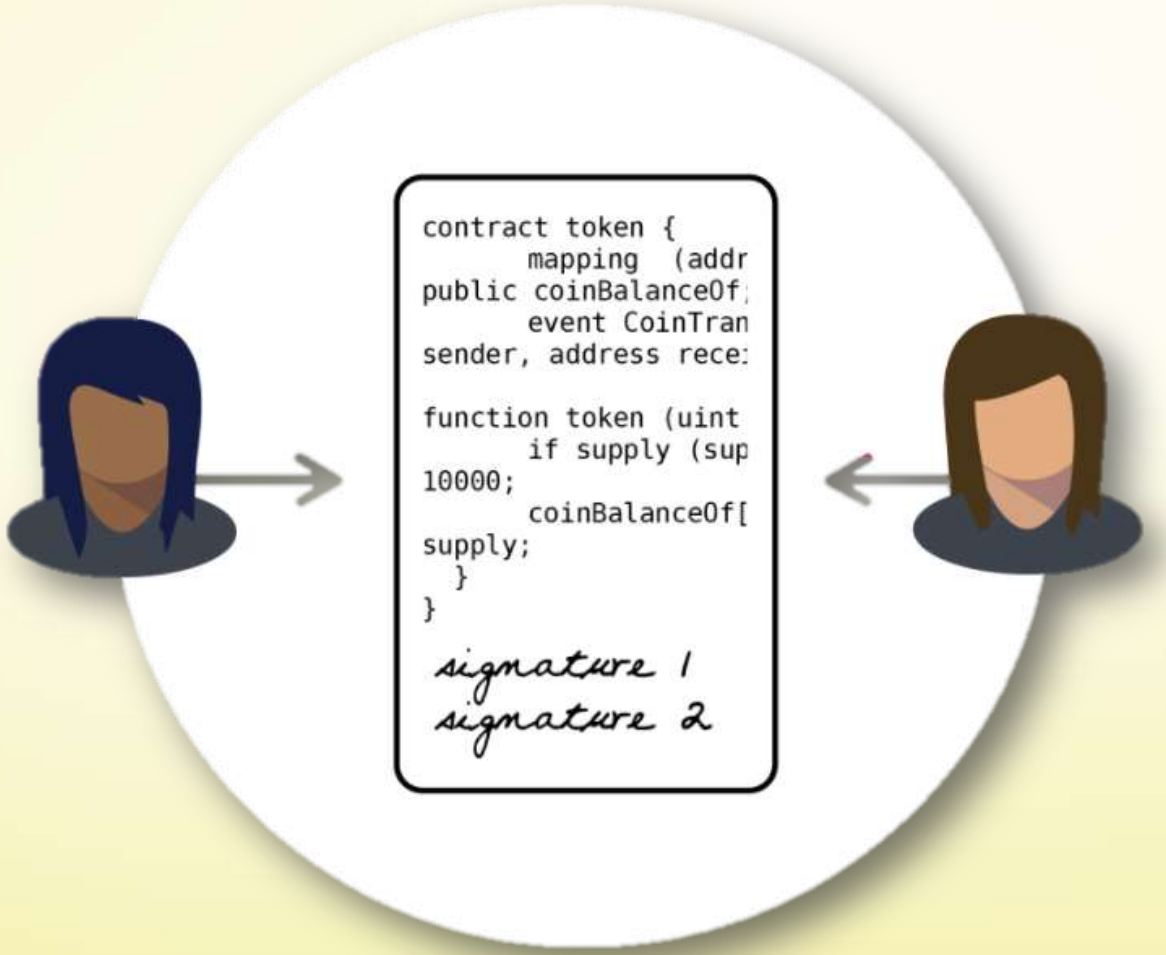
در اجماع به روش Proof-of-Work (PoW)

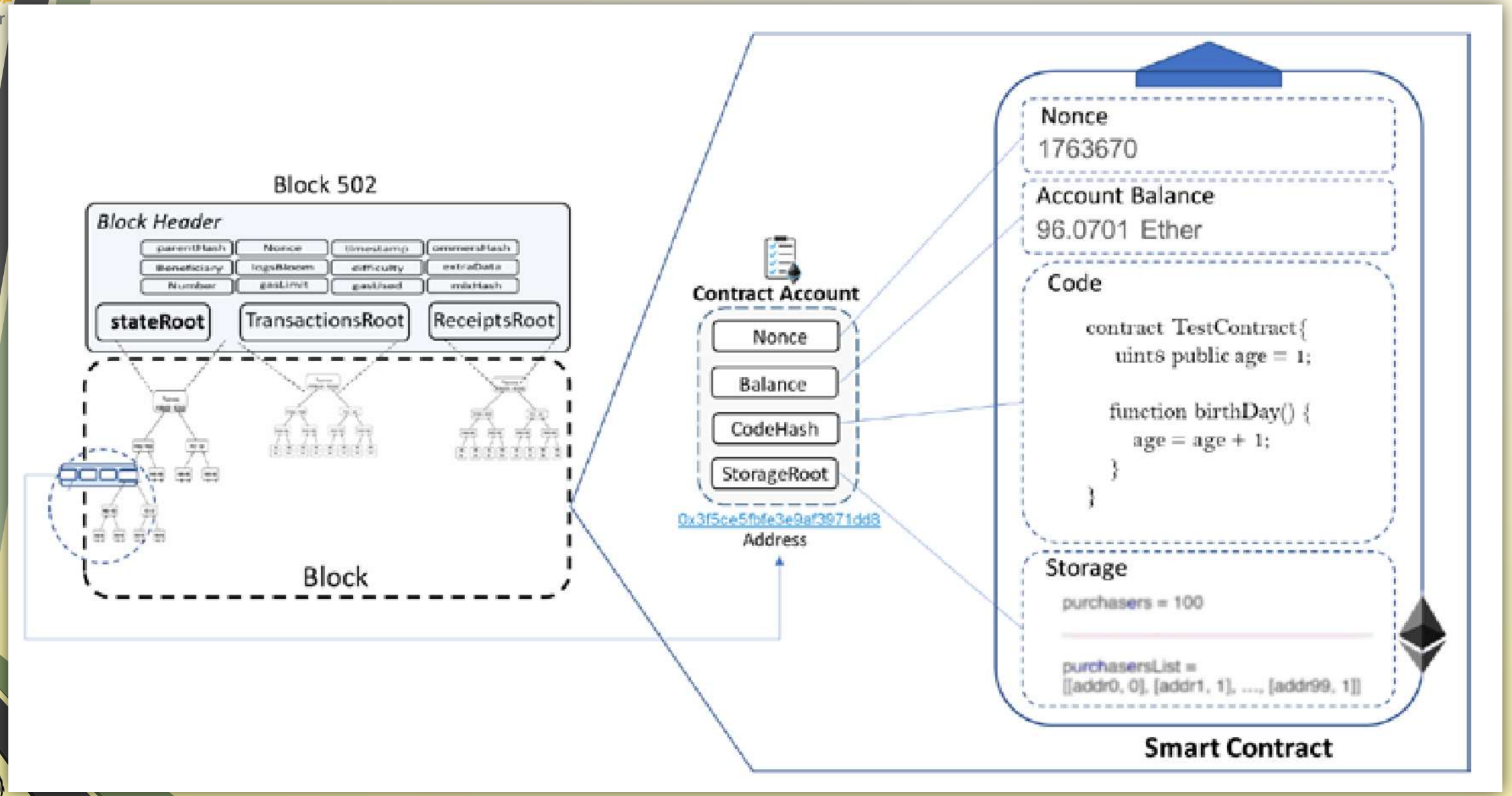
Working on a Computational Problem

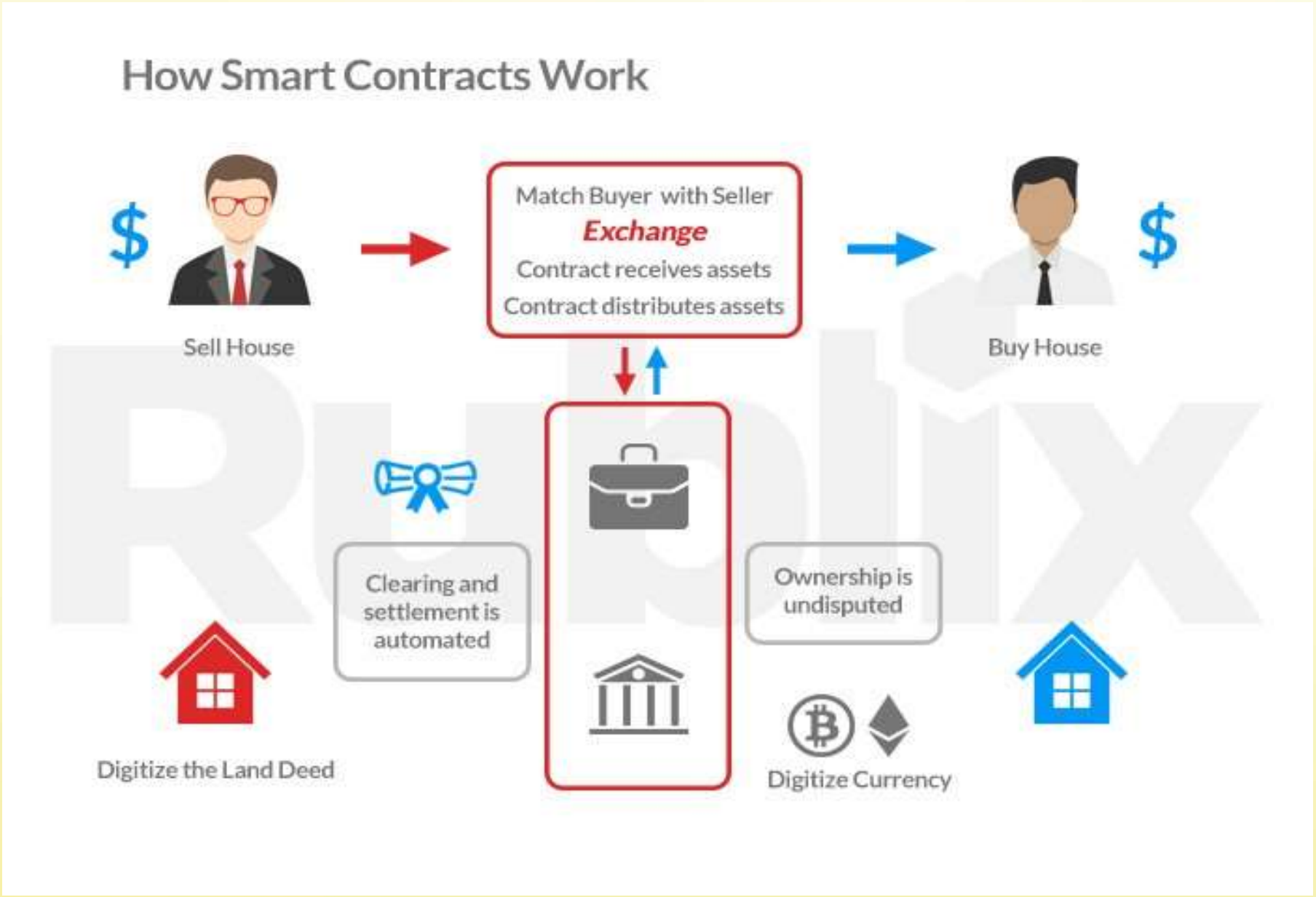


بخش ششم:
قراردادهای هوشمند

مرتضی سرگلزایی جوان
مرکز تحقیقات رایانش ابری


contract token {
mapping (addr
public coinBalanceOf;
event CoinTran
sender, address rece:
function token (uint
if supply (sup
10000;
coinBalanceOf[
supply;
}
}
signature 1
signature 2

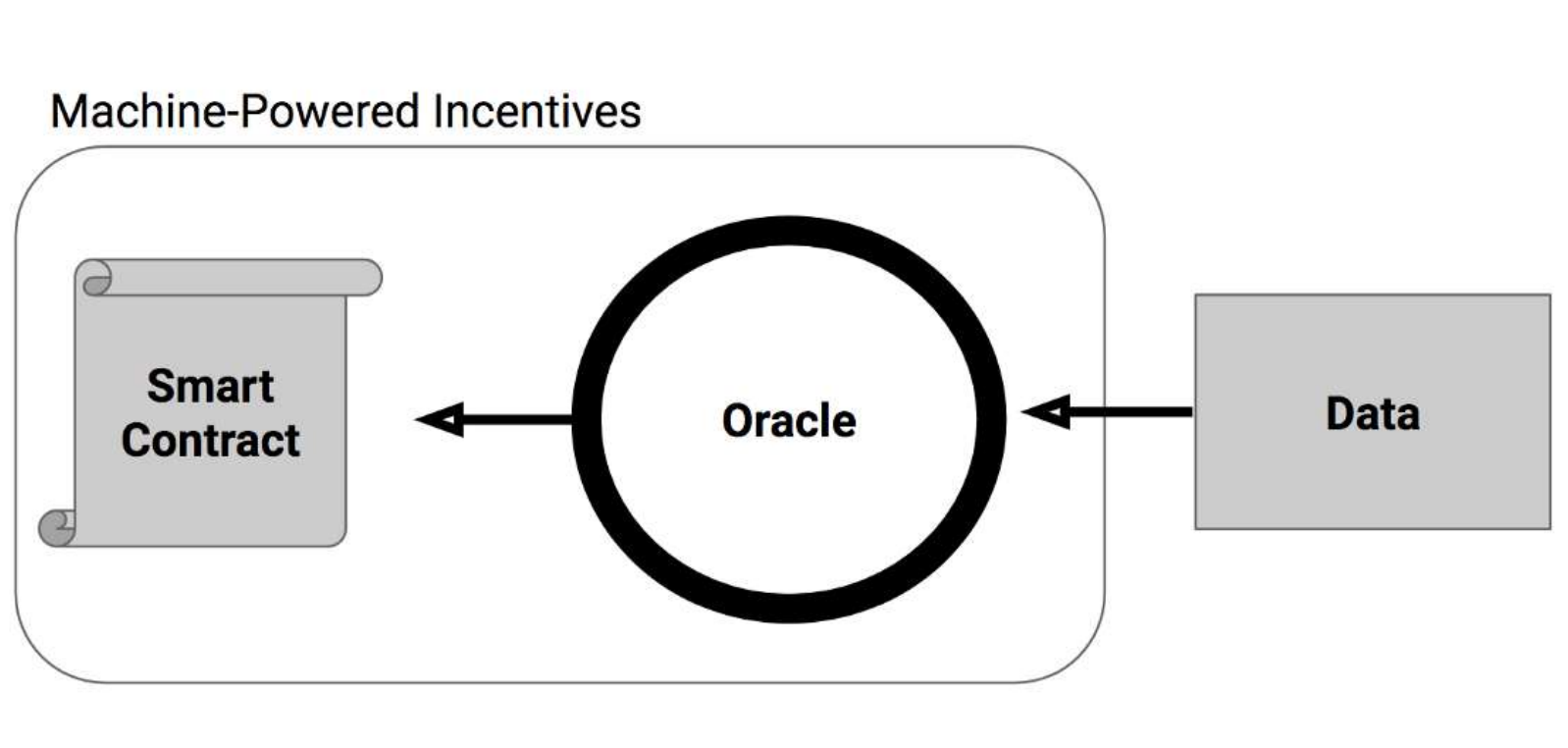

Block 502
Block Header
parentHash
Nonce
timestamp
ommersHash
Beneficiary
logsBloom
difficulty
extraData
Number
gasLimit
gasUsed
mixHash
stateRoot
TransactionsRoot
ReceiptsRoot
Block
Contract Account
Nonce
Balance
CodeHash
StorageRoot
0x3f5ce5fbfe3e9af3971dd8
Address
Nonce
1763670
Account Balance
96.0701 Ether
Code
contract TestContract{
uint8 public age = 1;
function birthDay() {
age = age + 1;
}
}
Storage
purchasers = 100
purchasersList =
[[addr0, 0], [addr1, 1], ..., [addr99, 1]]
Smart Contract


How Smart Contracts Work
$
Sell House
Match Buyer with Seller
Exchange
Contract receives assets
Contract distributes assets
Buy House
$
Clearing and settlement is automated
Ownership is undisputed
Digitize the Land Deed
Digitize Currency

ویژگی های قرارداد هوشمند

- self-executable
- self-enforceable
- self-verifiable
- self-constraint

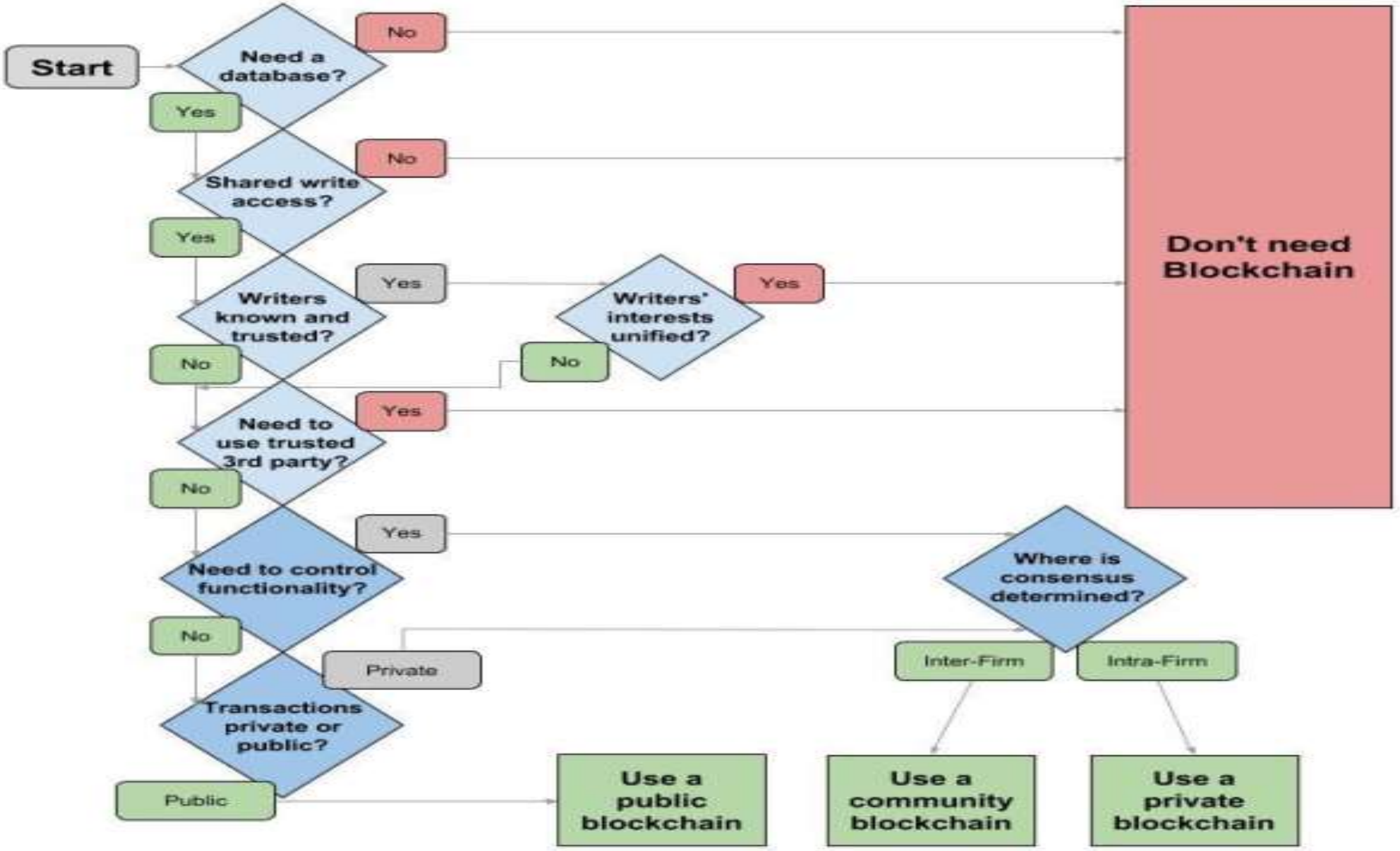
مفهوم اوراکل در قراردادهای هوشمند



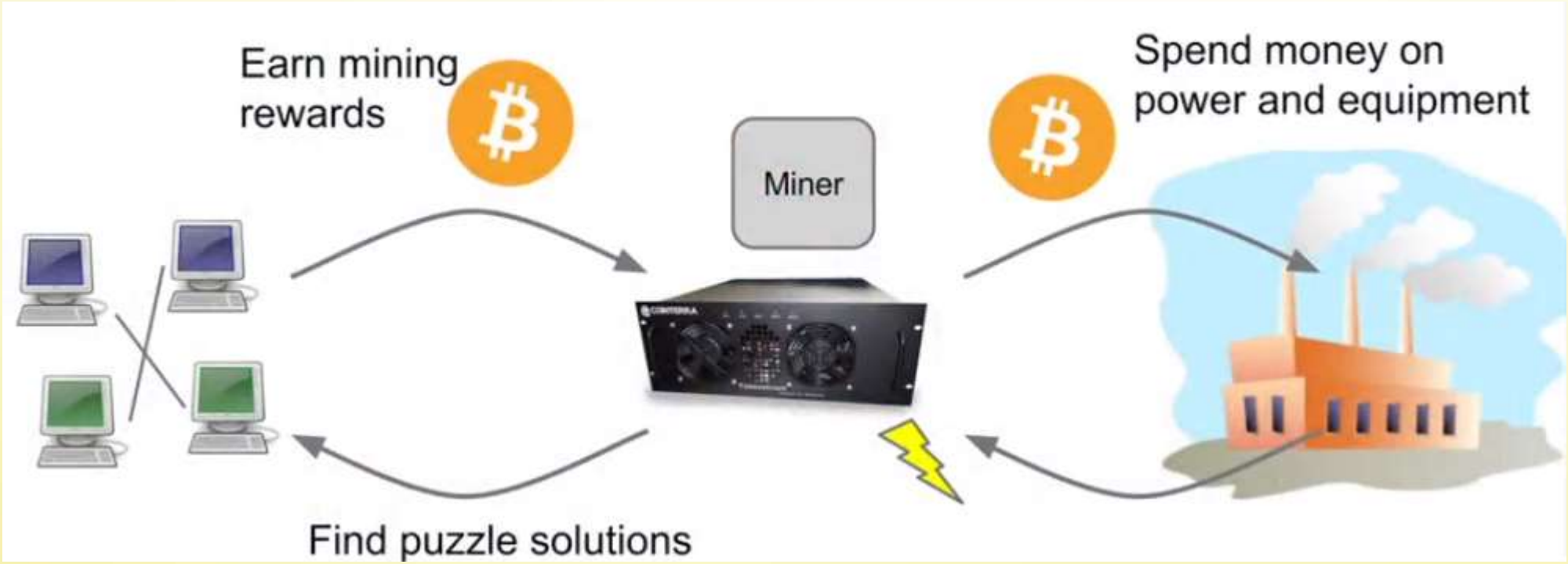
بخش هفتم:
محدودیت های بلاکچین

مرتضی سرگلزایی جوان
مرکز تحقیقات رایانش ابری

Blockchain Applicability Framework



- The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes


Earn mining rewards
Miner
Spend money on power and equipment
Find puzzle solutions

جمع بندی

- مقدمه و تاریخچه
- کاربردهای بلاکچین
- معماری و فناوری های مورد استفاده
- مبانی رمزنگاری
- الگوریتم های اجماع
- قراردادهای هوشمند
- محدودیت ها

جیبیتال: رمزارز با کاربردهای آموزشی

- http://cafebazaar.ir/app/ir.jibital.wallet
- http://jibital.ir