ASIAN BANKERS ASSOCIATION

35th ABA General Meeting and Conference
Banking in Asia
The next Frontier
Kurumba Maldives, 15 -16 November 2018

Cryptocurrencies and Risk

Reza Mostafid

Bank Pasargad

The Millenium Bank

BANK OF MALDIVES

BANK PASARGAD

Presenter's name: Reza Mostafid

On behalf of: Bank Pasargad

- major Iranian private bank offering
  - retail
  - commercial
  - investment

  banking **services**

- established in 2005

BANK PASARGAD

What are cryptocurrencies?

- Cryptocurrencies aspire to be a new form of electronic money
- They guarantee their integrity and stability through
  - the use of digital technology
  - strong cryptography

BANK PASARGAD

- Cryptocurrencies **deliberately** aim at eliminating central institutions
  - Central banks & mints
  - Financial institutions
  - Regulators
  - Established transaction networks such as **SWIFT** & **NACHA**
  - Existing payment platforms such as **VISA**, **Master Card**, **PayPal**, **Amex** etc

BANK PASARGAD

- Some call the cryptocurrency phenomenon the `**Democratisation of money**`

BANK PASARGAD

- Cryptocurrencies consist of three elements:
  - **First**, a set of rules or the "**protocol**"
    - This is essentially computer code (C++, Go, Python, Java,…) specifying how the cryptocurrency participants should transact amongst one an other
    - Strong cryptography is deployed to prevent counterfeiting and fraud.

```
extern int dword_12688; // weak
extern int dword_1268C; // weak

{
   if ( (_BYTE) extern int dword_12690; // weak
   LOBYTE(Length) = v3;
   ZwClose(Handle);
   return IoStatuk;
}

if ( (_BYTE) LOBYTE(Length) = v3;
   ZwClose(Handle);
}
return IoStatusBlock;
```

BANK PASARGAD

- **Second**, a ledger storing the history of transactions between the users

- **Third**, a decentralised computer network (supported by the internet) through which participants
  - update
  - store
  - read the ledger of transactions

BANK PASARGAD

An example: Bitcoin

- Bitcoin currency is transferred between users simply by making changes to the ledger mentioned earlier

- This ledger exists in digital form on the computer disks of every computer of the Bitcoin network

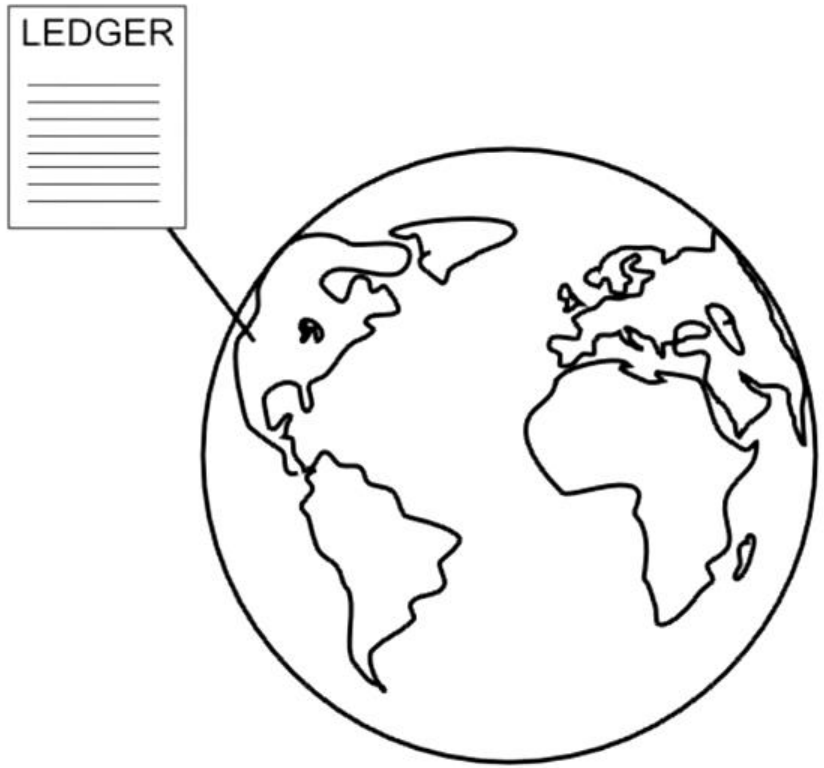
BANK PASARGAD

Ledger

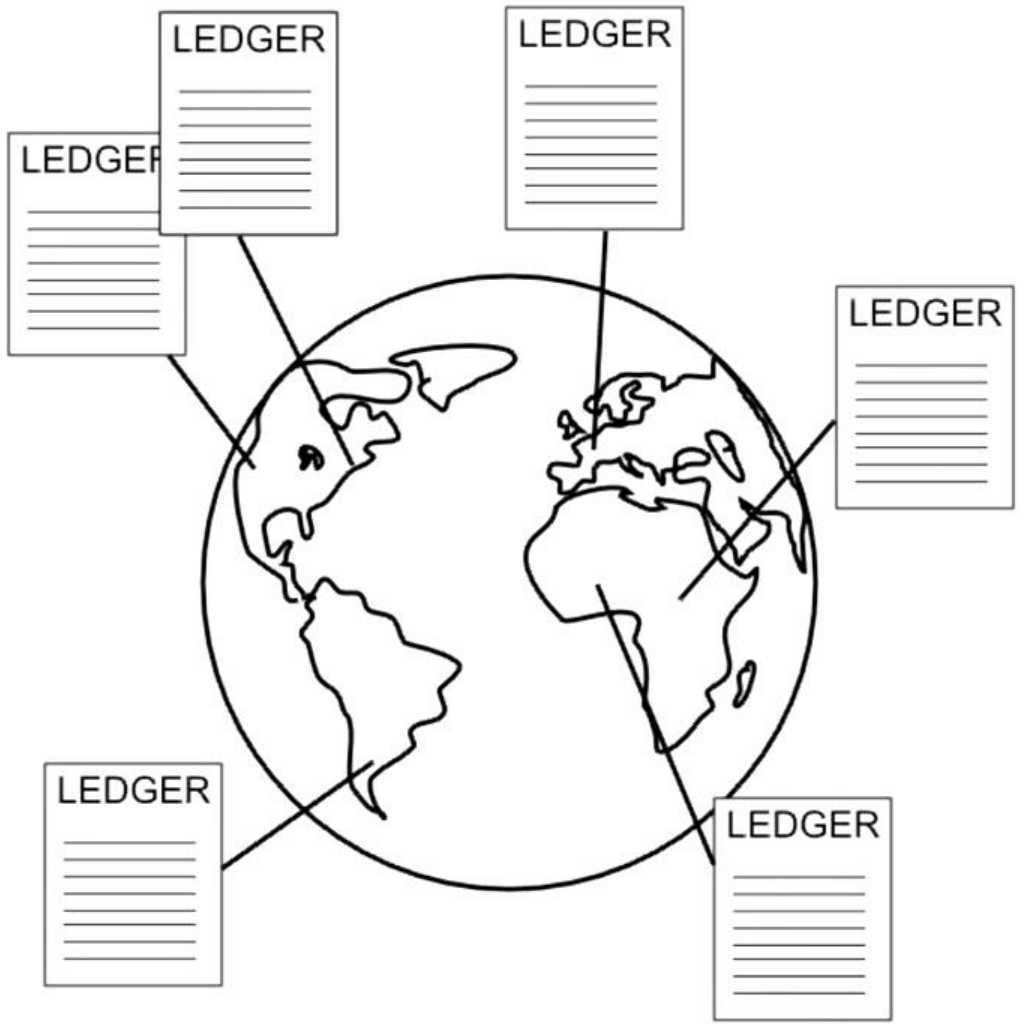
Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

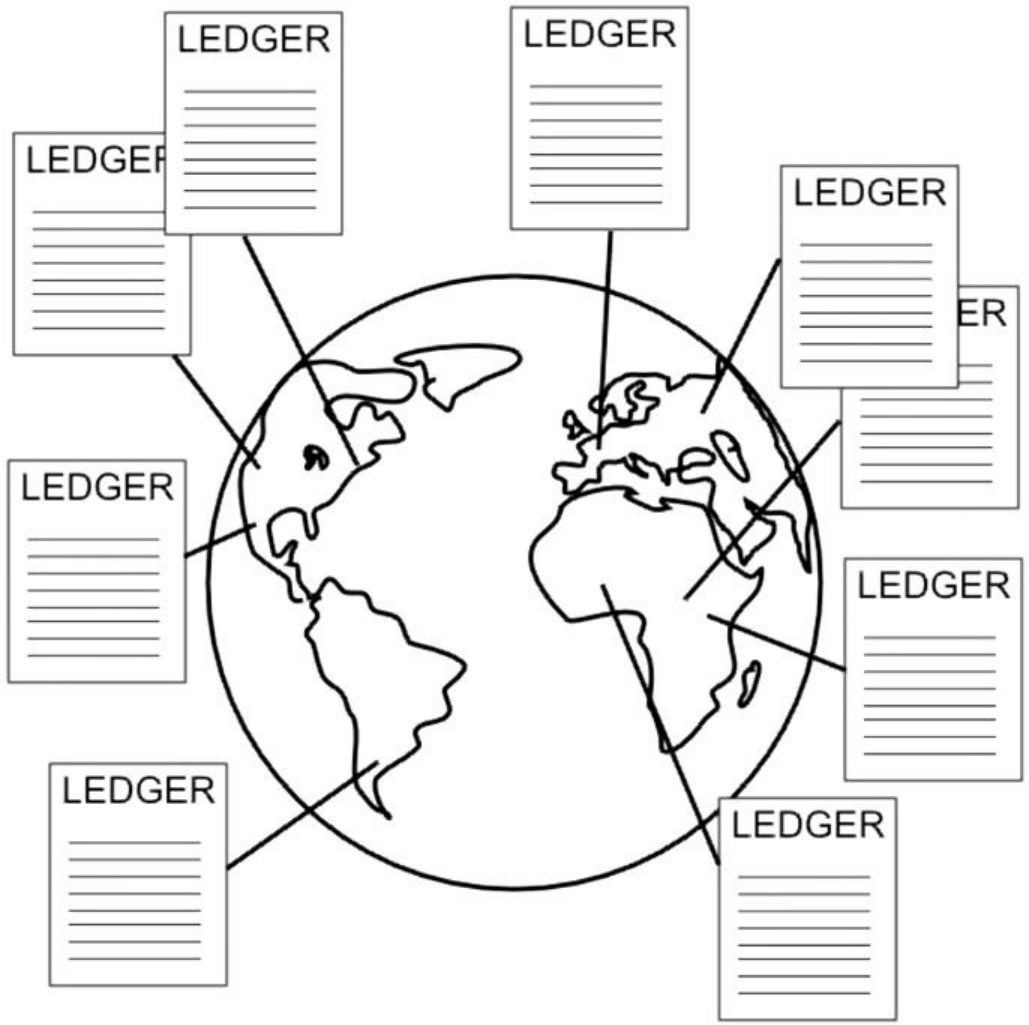
...

BANK PASARGAD

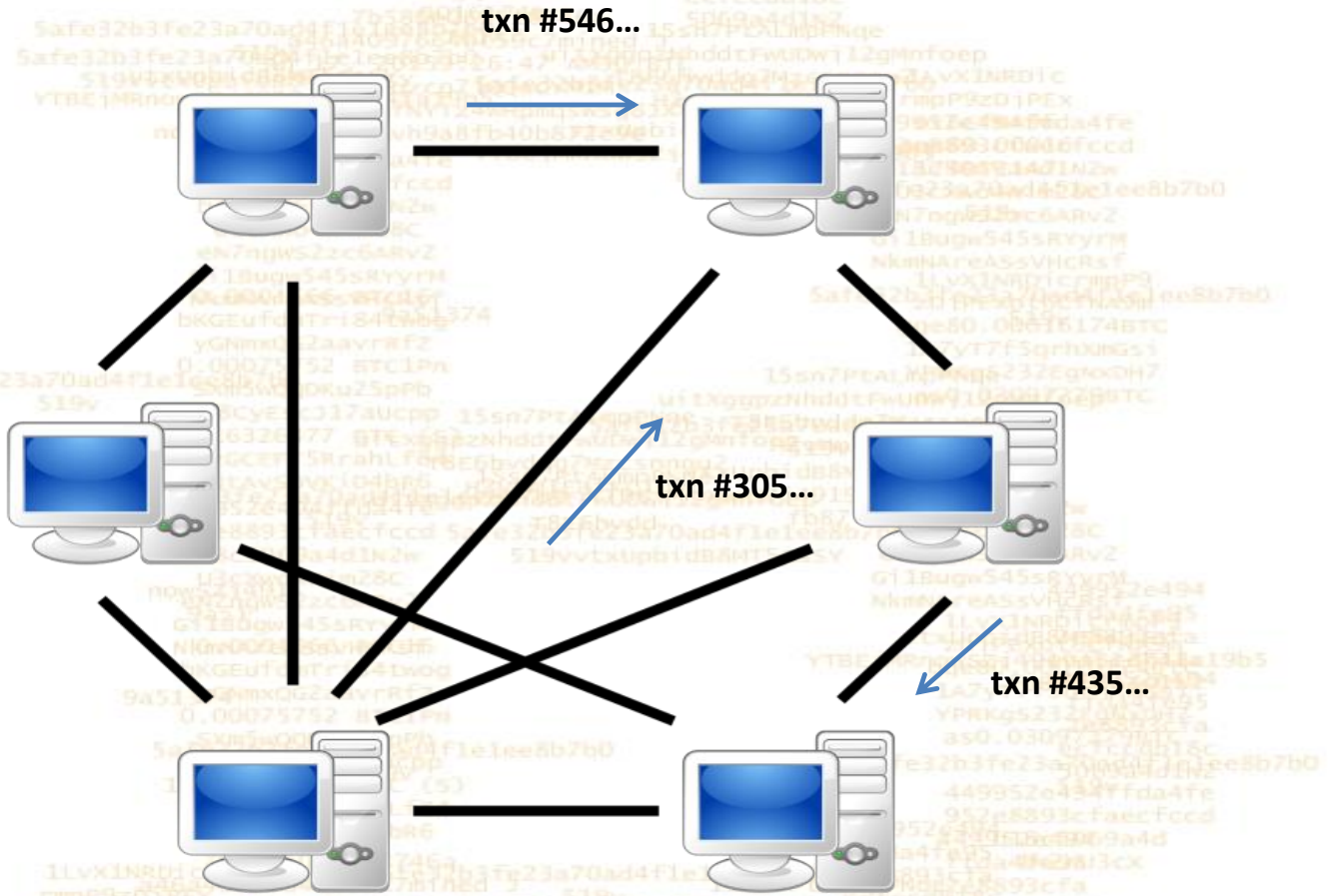


BANK PASARGAD


LEDGER
LEDGER
LEDGER
LEDGER
LEDGER
LEDGER



BANK PASARGAD



BANK PASARGAD

- Note that there are NO accounts or account balances in the ledger
  - No customer names
  - No customer details
  - No residential address
  - No telephone numbers
  - No customer account numbers

essentially a KYC nightmare!!

BANK PASARGAD

- Instead, each account is represented by a unique 48 digit number which is selected randomly
- something like

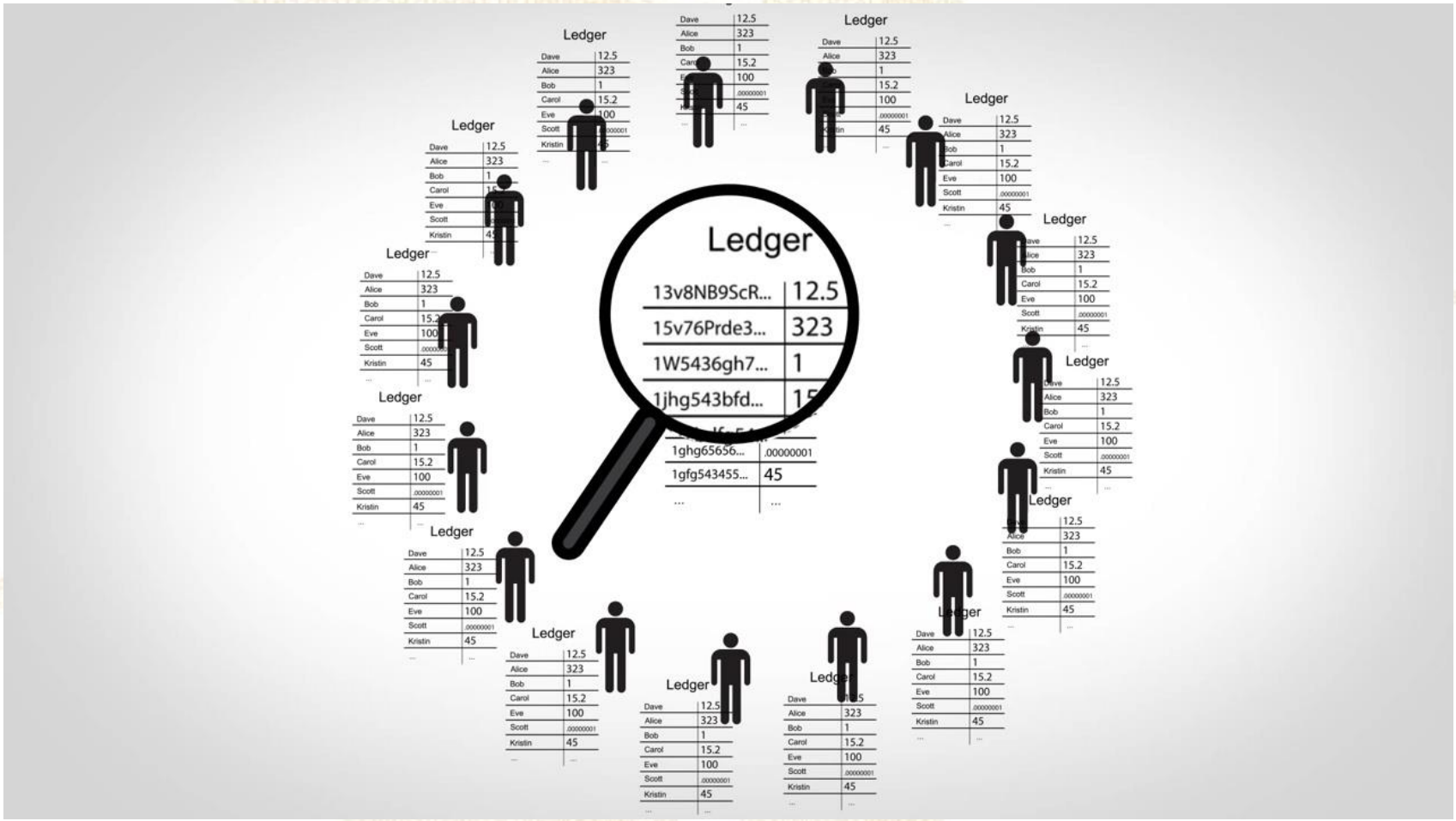
461501637330902918203684832716283019655932542976

- the 48 digit number is further encoded alphanumerically to make it more readable and manageable

36t9N7f3UqNxAS5RJDKSFeVLQcMbgarX8u

BANK PASARGAD

- This functions as an anonymous account code



BANK PASARGAD

- These codes can be advertised to the public and in Bitcoin they are referred to as an ‘**address**’

16mPSOOLgpuo15gofSmPUgJKWEzQv7dQE

1M3U1DvM6Q4ov1Qb5CazePW8pJTUA9NWoX

137zbuy3X4uV1x3jHY9rcQ3JaMEopKuBQH

equivalent to 48 decimal digits

1DMXuu34YNHdDPqrgkP2ZrpK25dLJXiE

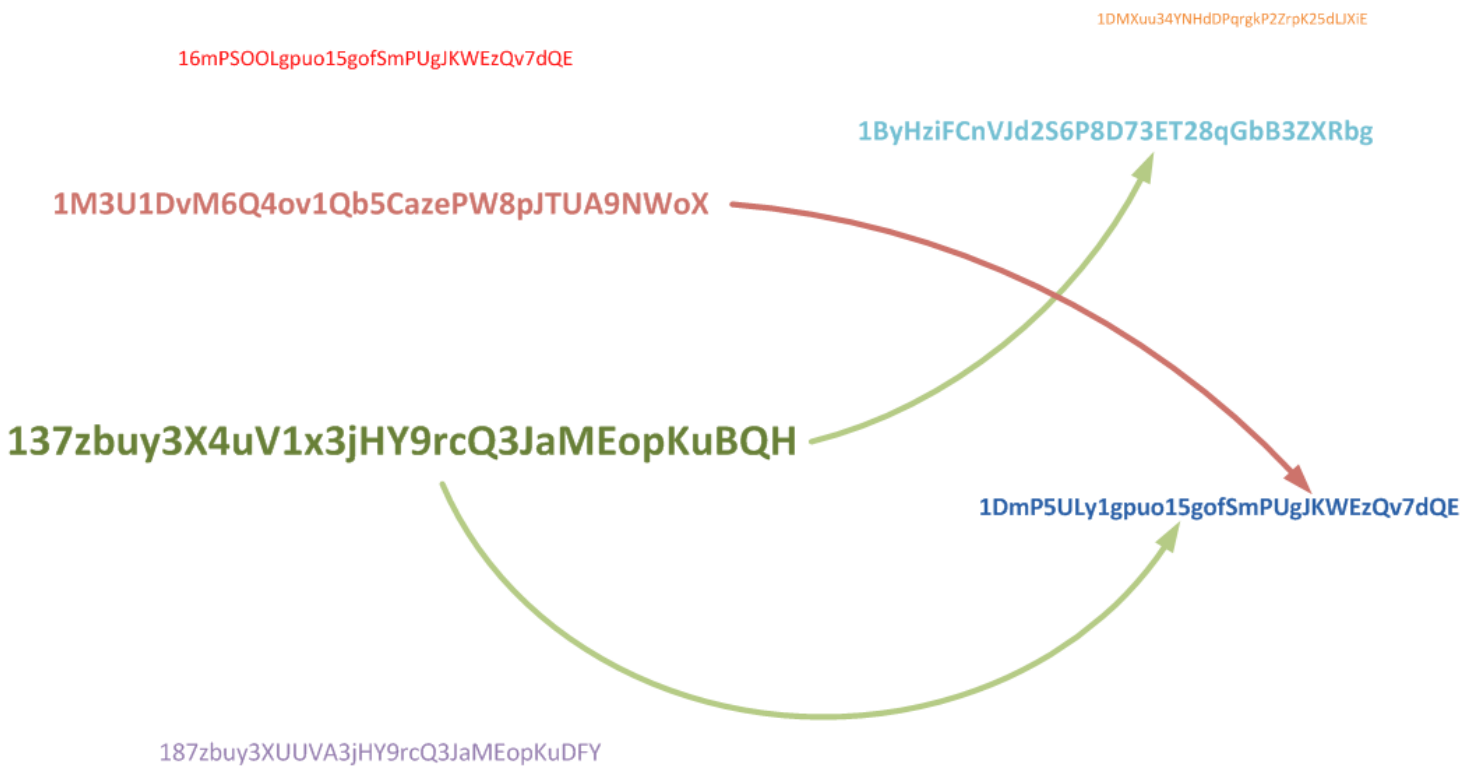
1ByHziFCnVJd2S6P8D73ET28qGbB3ZXRbg

1DmP5ULy1gpuo15gofSmPUgJKWEzQv7dQE

187zbuy3XUUVA3jHY9rcQ3JaMEopKuDFY

BANK PASARGAD

- The Bitcoin ledger only records transactions involving the transfer of bitcoins from one such address to another



- The ledger is thus simply a chronological record of Bitcoin transactions between addresses

BANK PASARGAD

- If everyone has a copy of the ledger, can everyone then see everyone else's transaction details???….
  - ….while it is possible for everyone to follow transactions to and from a particular address….
  - ….it is NOT (easily) possible to ascertain who the address belongs to
- With certain precautions, such as
  - use of proxies and anonymisers such as TOR
  - avoiding re-use of addresses

Bitcoin users addresses can maintain their **anonymity**

BANK PASARGAD

- Users ≠ Bitcoin addresses
- Users can own/control several addresses
  - as alluded to previously one can use new addresses for every transaction
- Special `wallet` SW
  - manages these addresses
  - browses the blockchain for them
  - collects all the Bitcoin transactions that have as their destination a particular address (or group of addresses)

  calculates a Bitcoin balance for that user address

- Users of bitcoin trust the Bitcoin currency system because they trust
  - The protocol
  - The science of cryptography used to enforce the protocol

- That is why bitcoin users are willing to transfer ownership of a good or provide a service in return for a higher value of bitcoins against their account within the above mentioned ledger

BANK PASARGAD

Ledger

Dave	12.5
Alice	323
Bob	1
Carol	15.2
Eve	100
Scott	.00000001
Kristin	45
...	...

Bob

Carol

Ledger

Dave	12.5
Alice	323
Bob	1
Carol	15.2
Eve	100
Scott	.00000001
Kristin	45
...	...

Bob

Carol

Ledger

Dave	12.5
Alice	323
Bob	1
Carol	15.2
Eve	100
Scott	.00000001
Kristin	45
...	...

Bob

Carol

Ledger

Dave	12.5
Alice	323
Bob	1
Carol	15.2
Eve	100
Scott	.00000001
Kristin	45
...	...

Ledger

Dave	12.5
Alice	323
Bob	1
Carol	15.2
Eve	100
Scott	.00000001
Kristin	45
...	...

Bob

Carol

Ledger

Dave	12.5
Alice	323
Bob	1
Carol	15.2
Eve	100
Scott	.00000001
Kristin	45
...	...

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	1	+5.2
Carol	15.2	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	3	+5.2
Carol	15.0	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	4	+5.2
Carol	13.0	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	4.5	+5.2
Carol	12.5	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	4.8	+5.2
Carol	12.0	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	5.0	+5.2
Carol	11.1	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

Dave	12.5
Alice	323
Bob	6.2
Carol	10
Eve	100
Scott	.00000001
Kristin	45
...	...

+5.2

-5.2

Bob

Carol

Ledger

Dave	12.5	
Alice	323	
Bob	6.2	+5.2
Carol	10	-5.2
Eve	100	
Scott	.00000001	
Kristin	45	
...	...	

Bob

Carol

Ledger

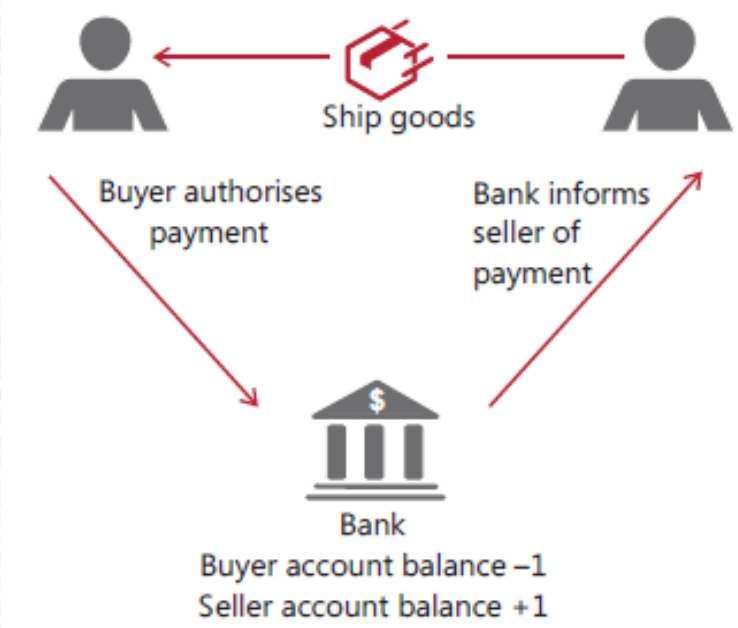
Dave	12.5
Alice	323
Bob	6.2
Carol	10
Eve	100
Scott	.00000001
Kristin	45
...	...

Bob

Carol

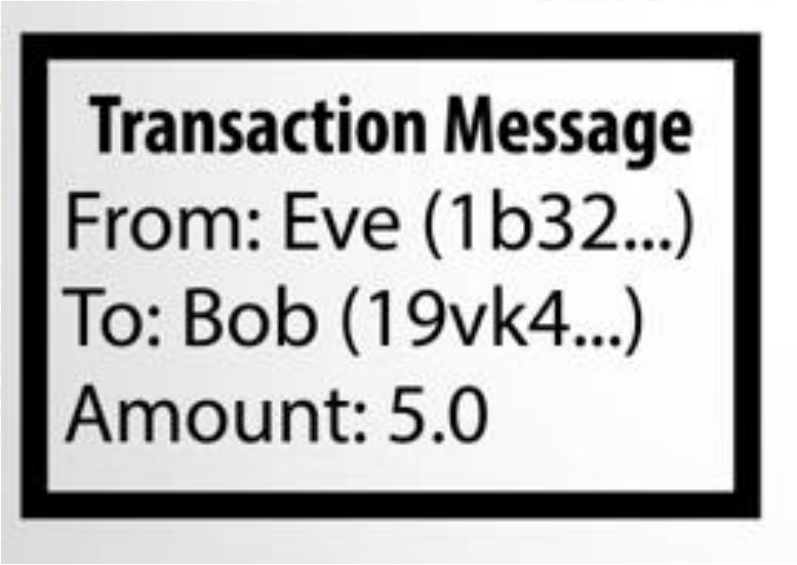
Traditional payments versus Bitcoin payments:

- In traditional payment systems a buyer authorizes a central authority (a bank) to debit his account and credit the account of the seller



- Once the seller is able to ascertain that the credit has been made to her account, she is expected to ship the goods

- In Bitcoin payments work as follows:
  - A transaction record is created which encodes instructions that a certain amount of **Bitcoins** are to be transferred from a sending address to a receiving address

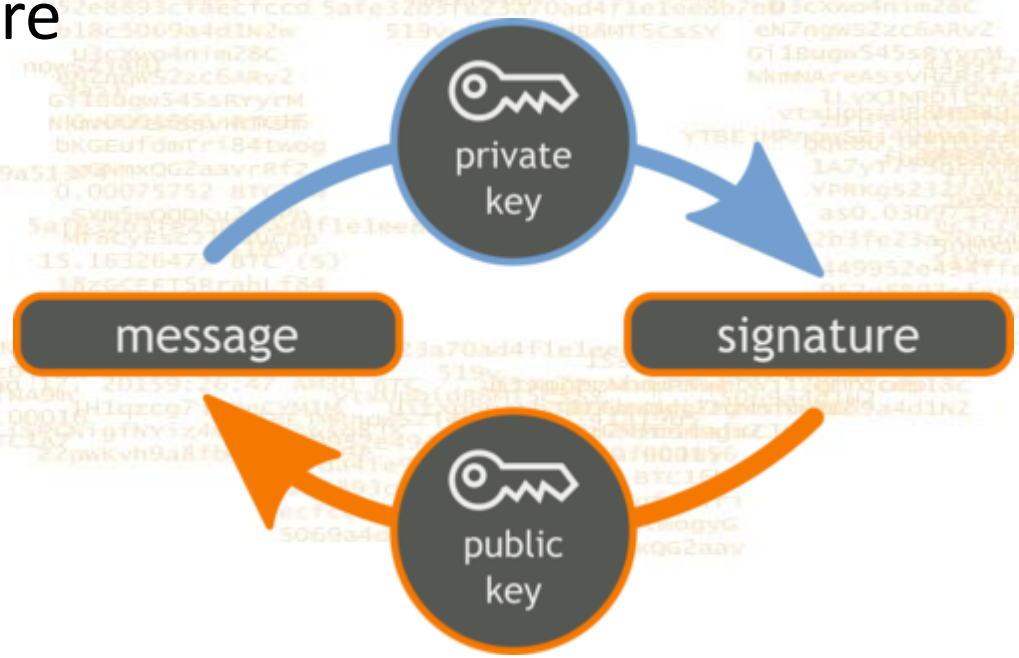


BANK PASARGAD

- A Bitcoin transaction is thus similar to a **cheque** from the traditional banking system:

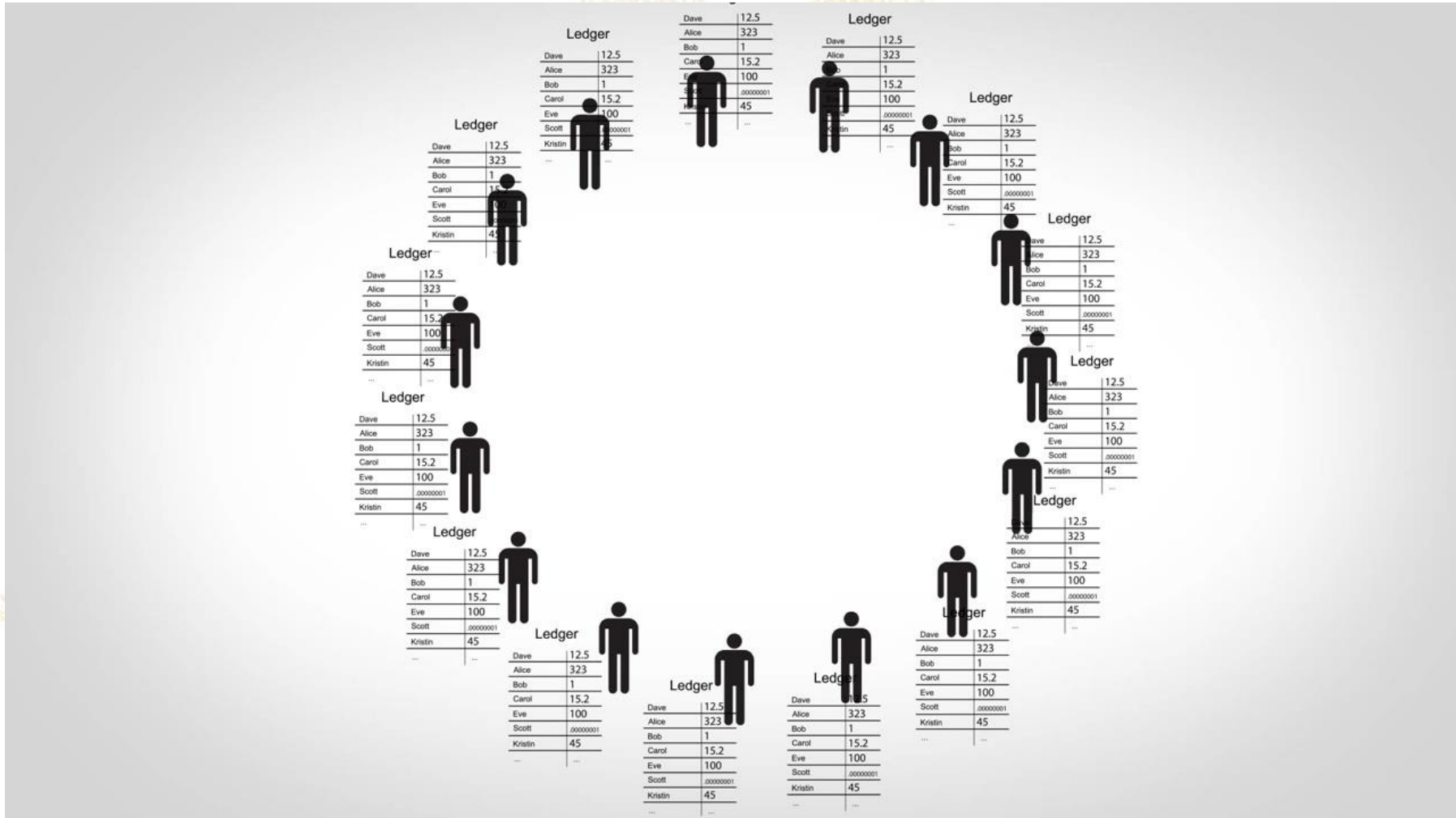
- Similar to a cheque a transaction must be signed to authorize payment

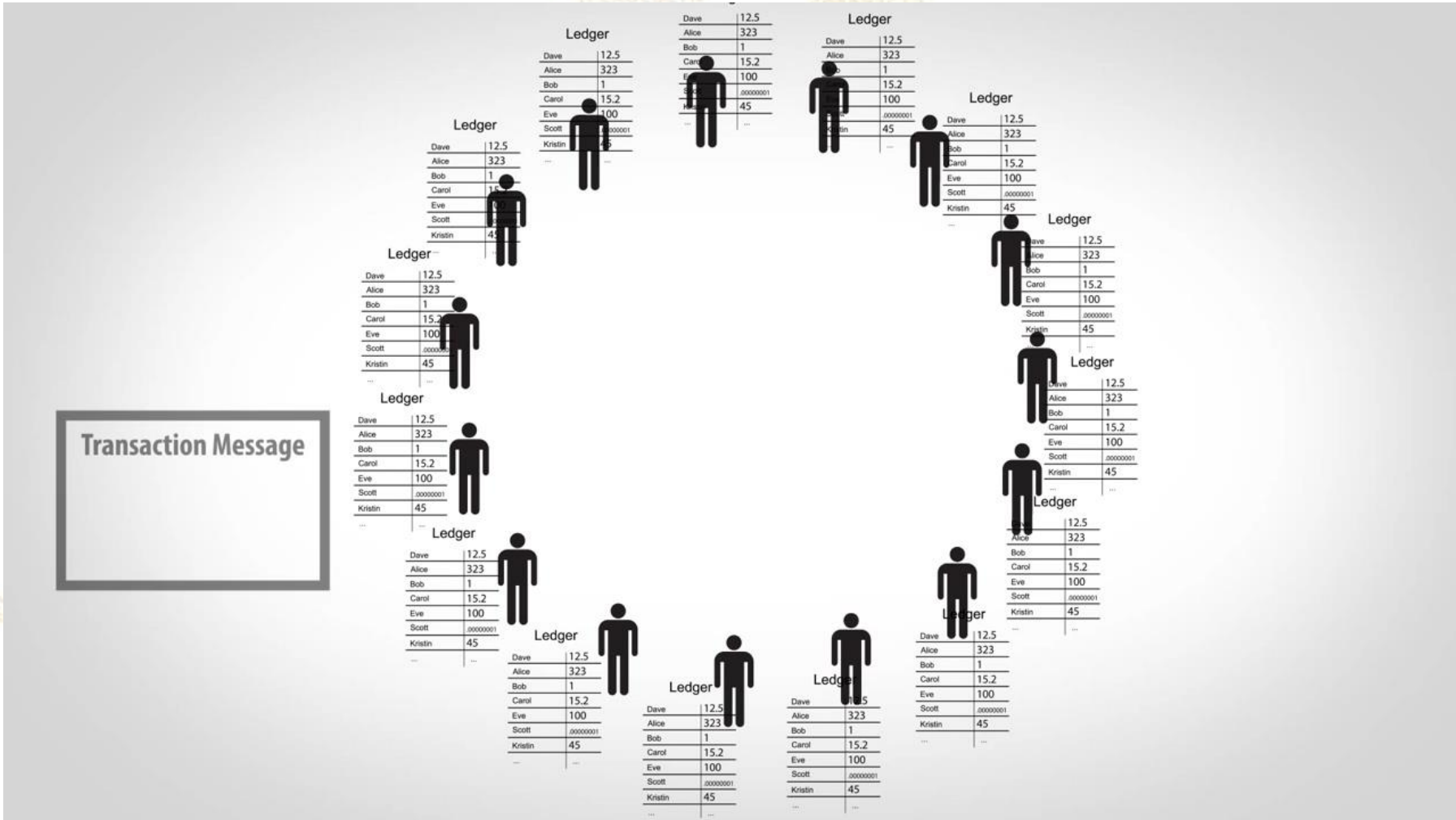
- However a transaction signature in Bitcoin is
  - made digitally using Elliptic Curve cryptography
  - orders of magnitude more secure than a physical signature



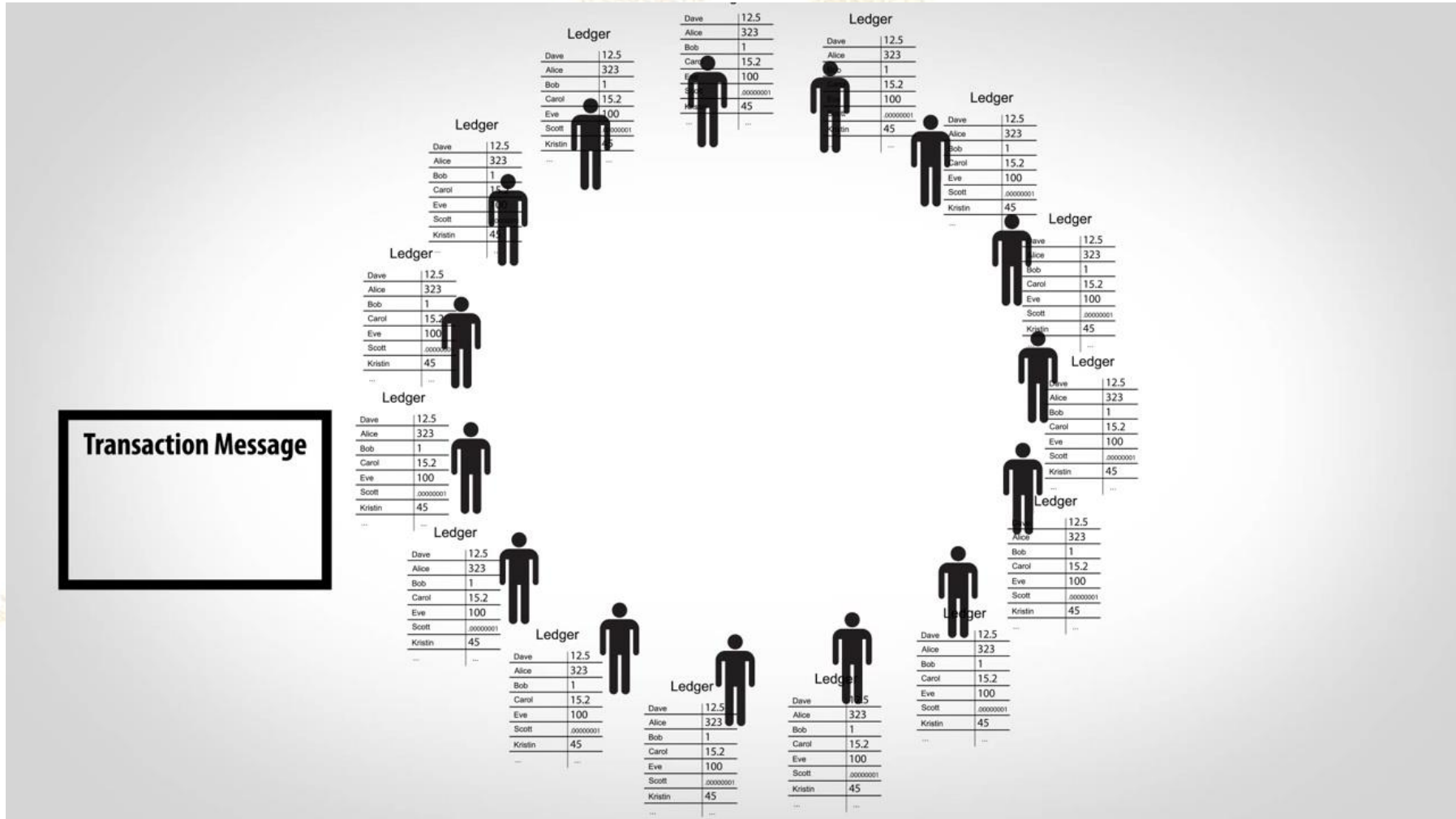
BANK PASARGAD

- The transaction is then announced by broadcasting it to other Bitcoin users across the Internet

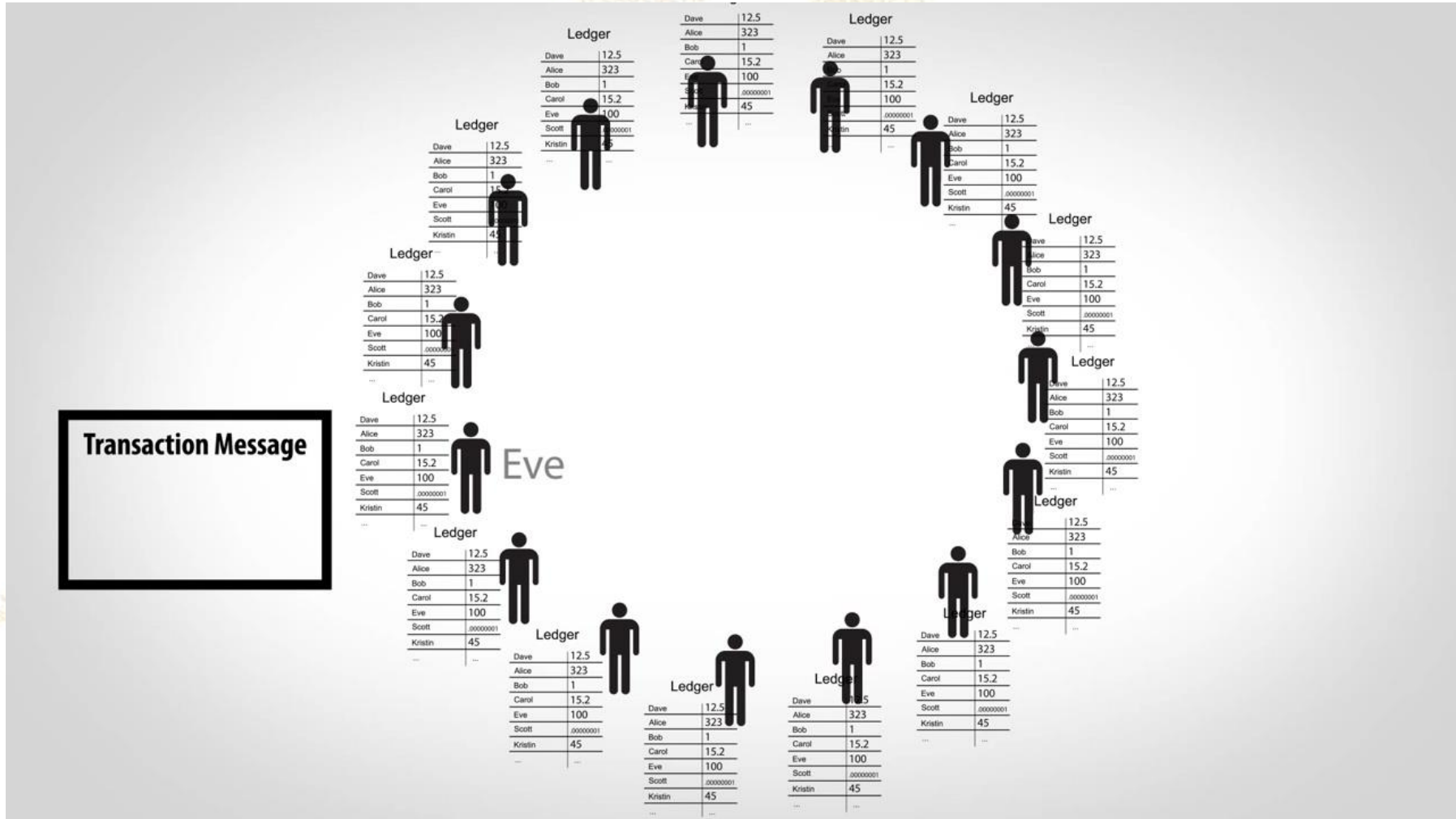




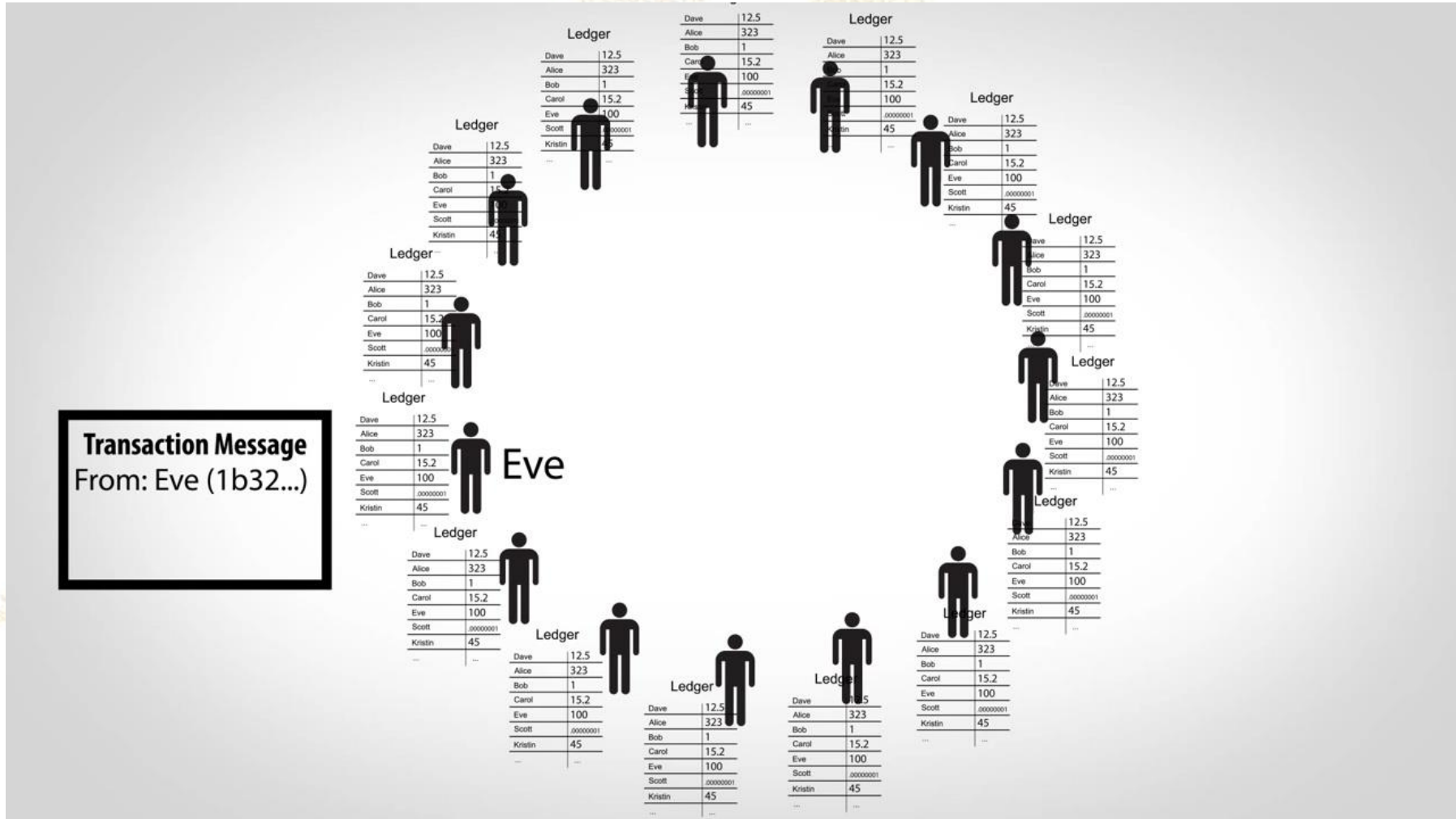
BANK PASARGAD

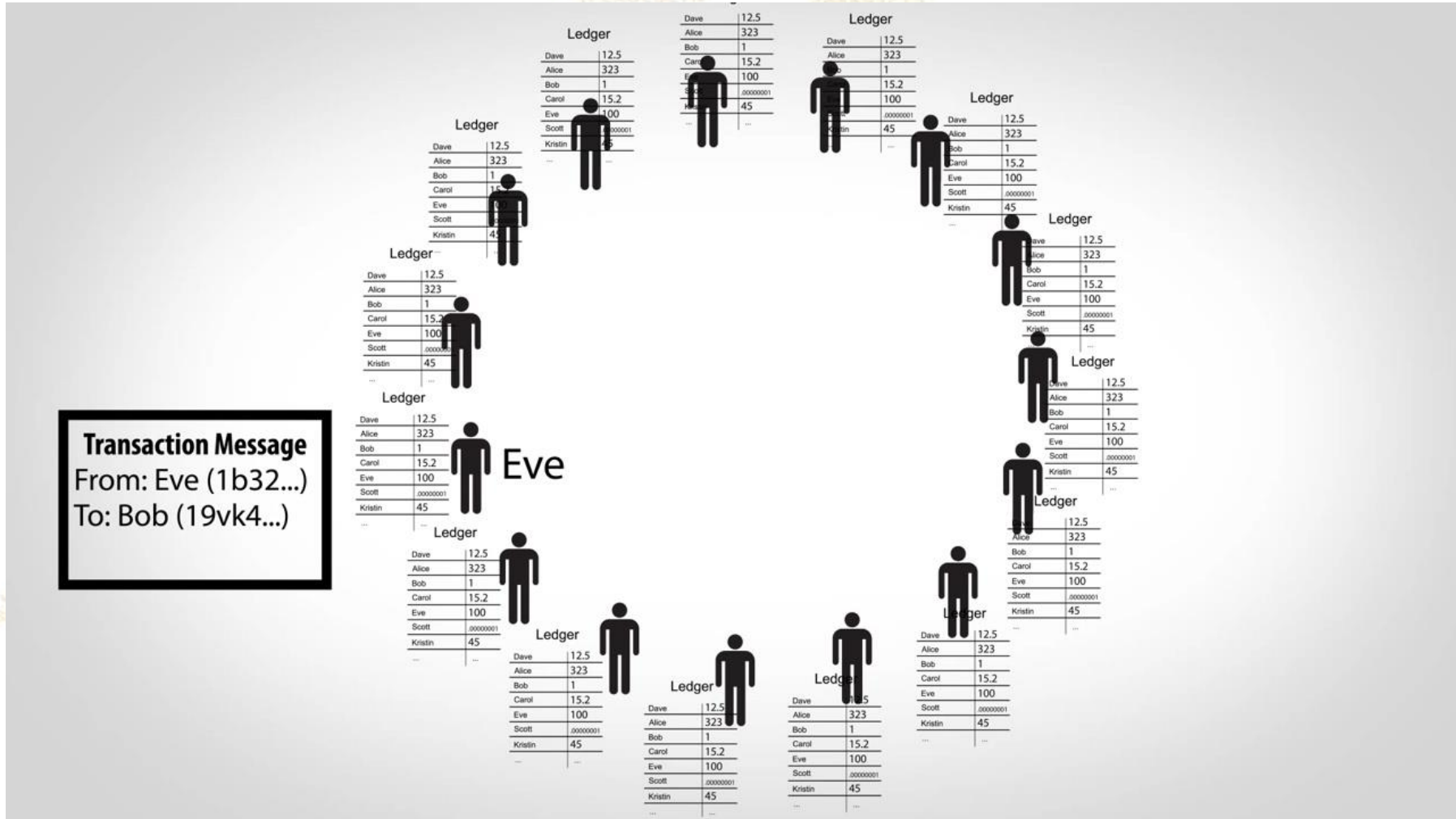


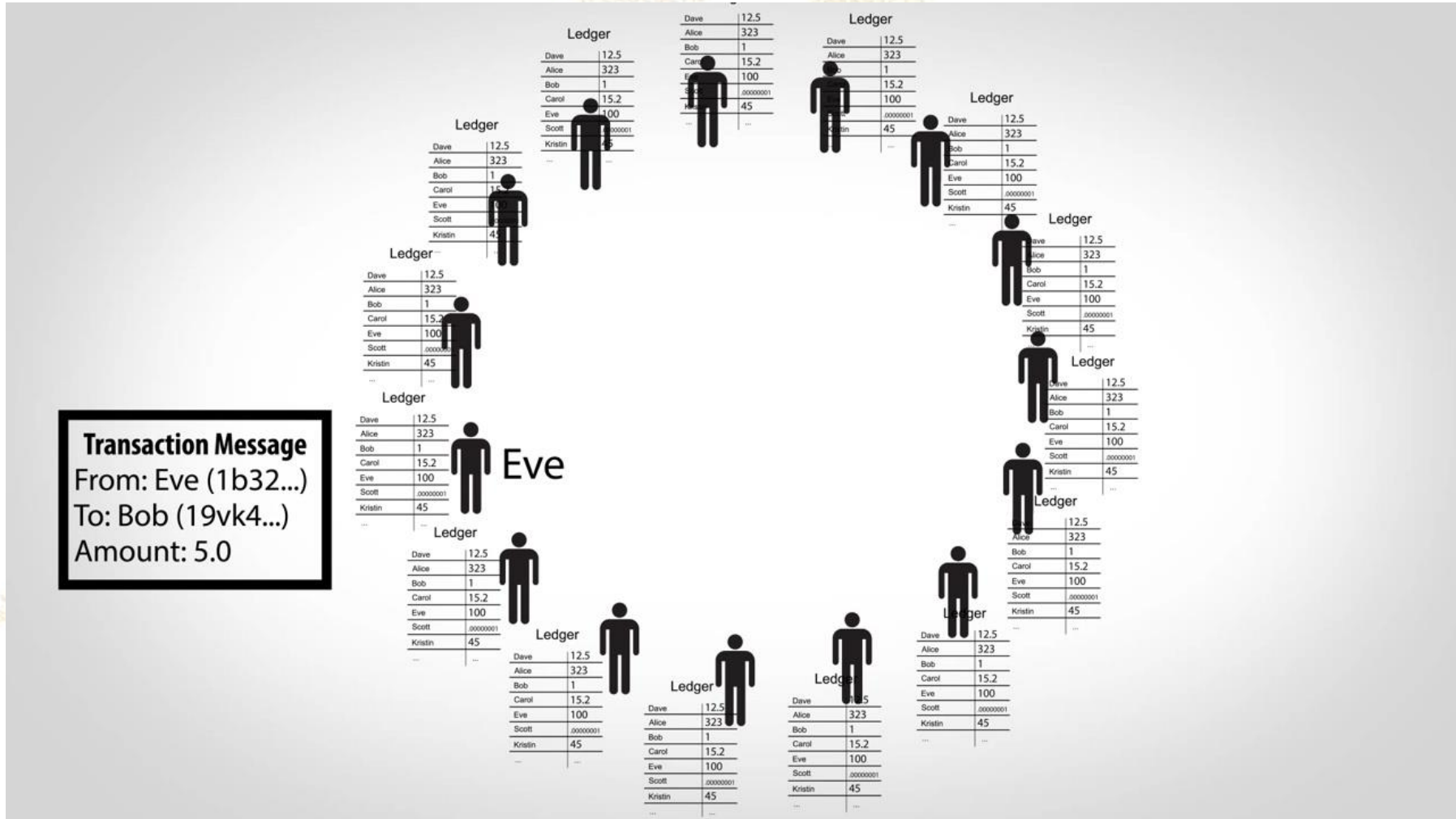
BANK PASARGAD

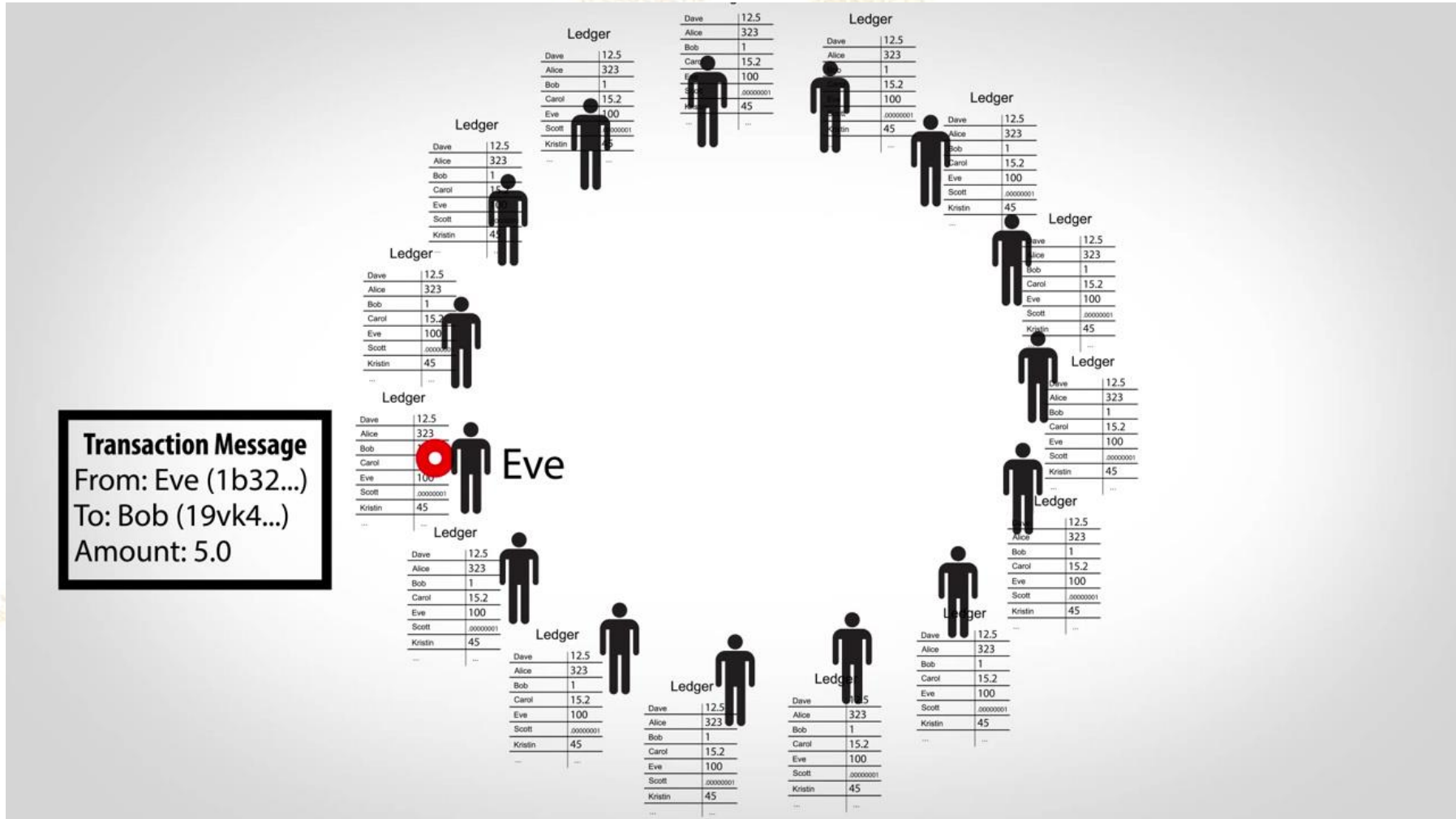


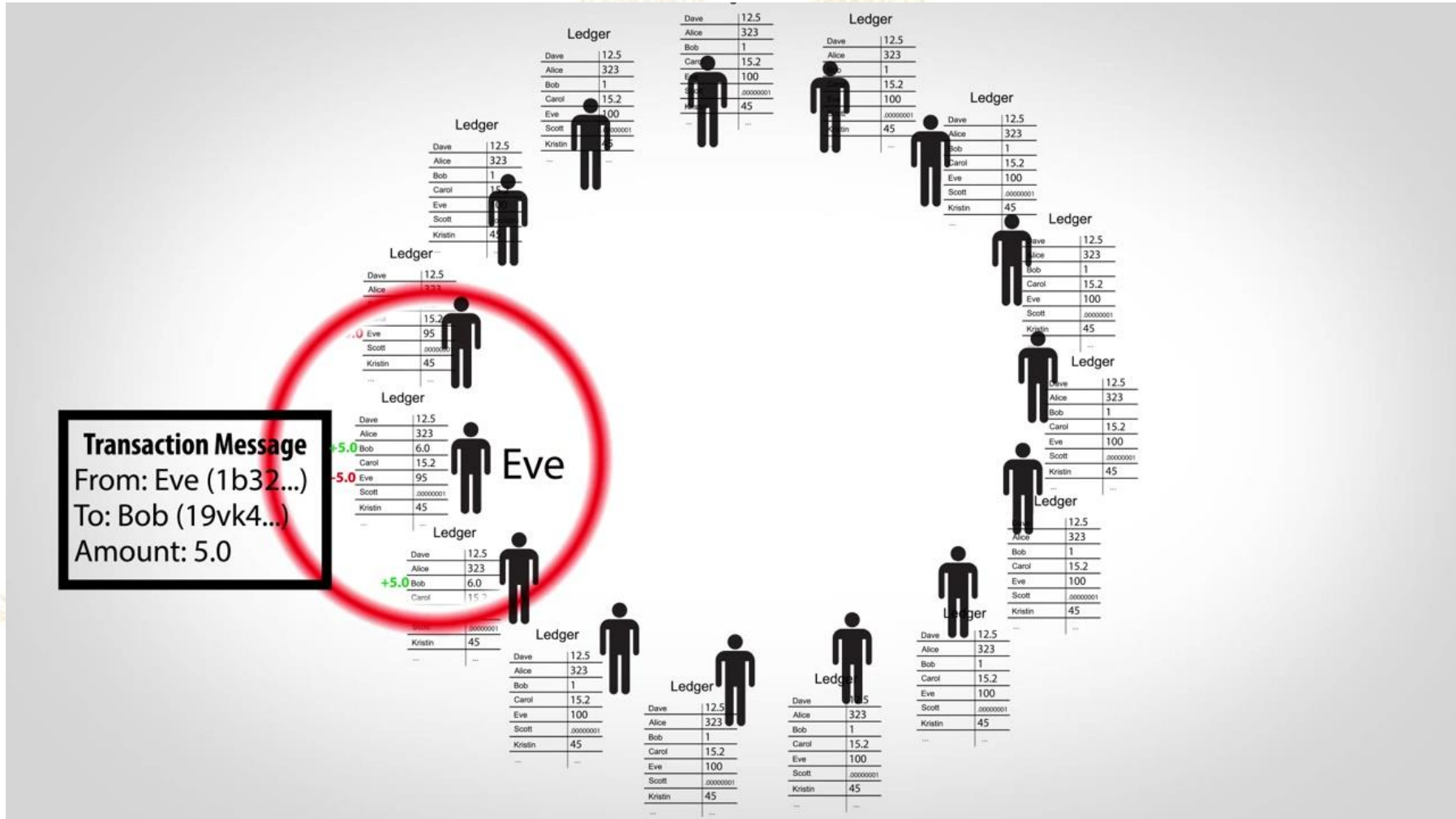
BANK PASARGAD

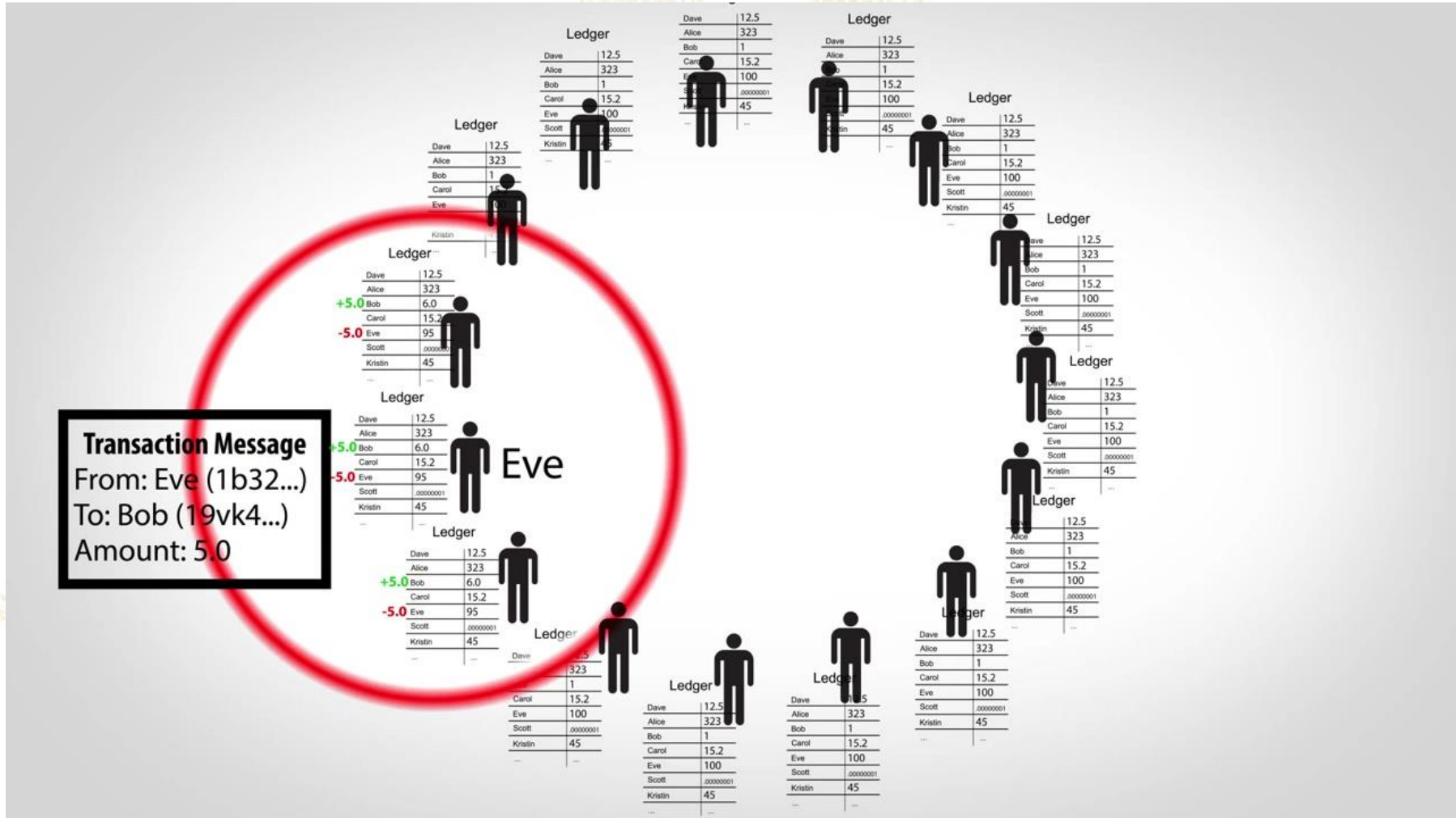

Transaction Message
From: Eve (1b32...)
Eve
Ledger
Dave 12.5
Alice 323
Bob 1
Carol 15.2
Eve 100
Scott .00000001
Kristin 45

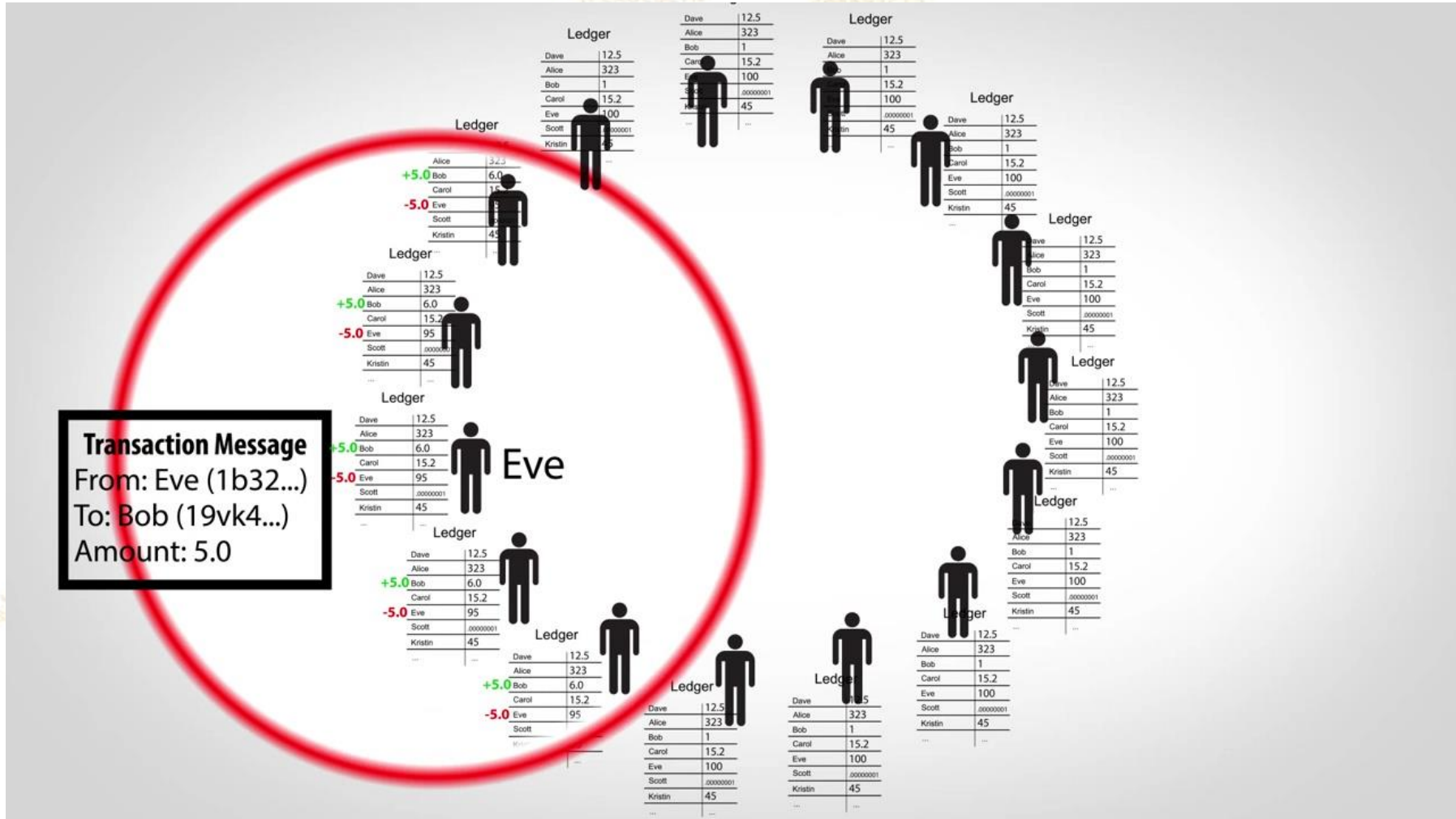




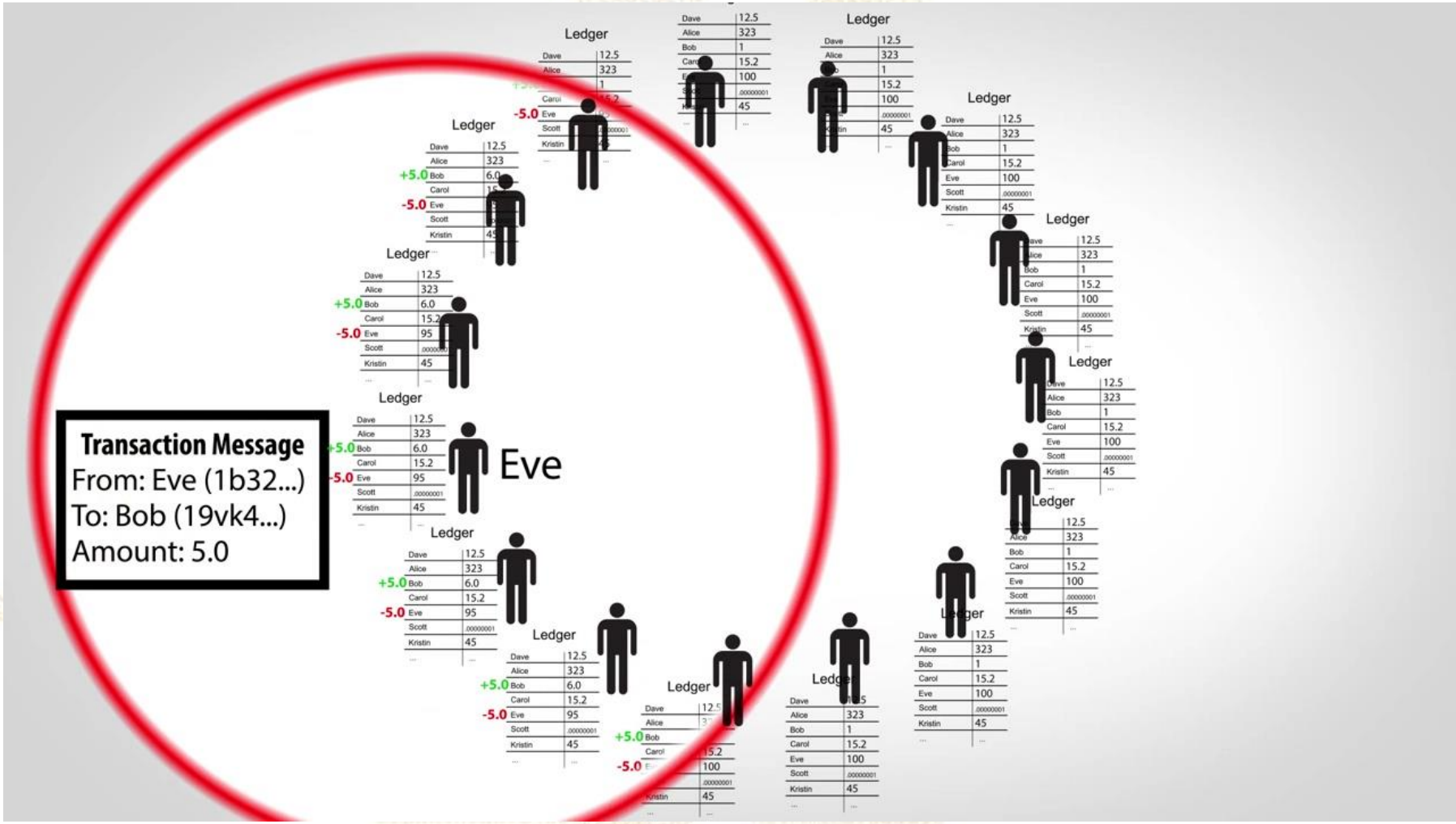


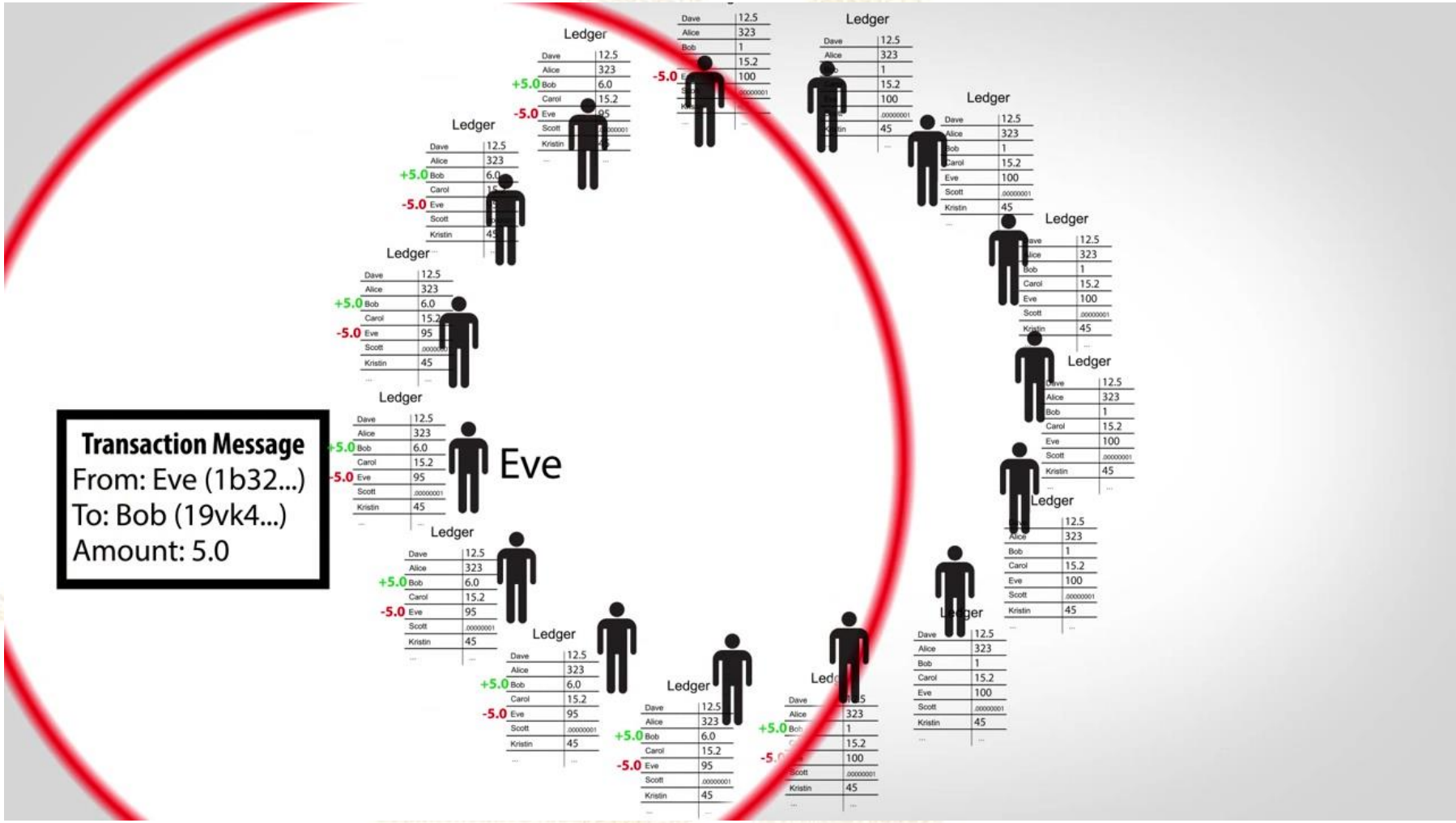




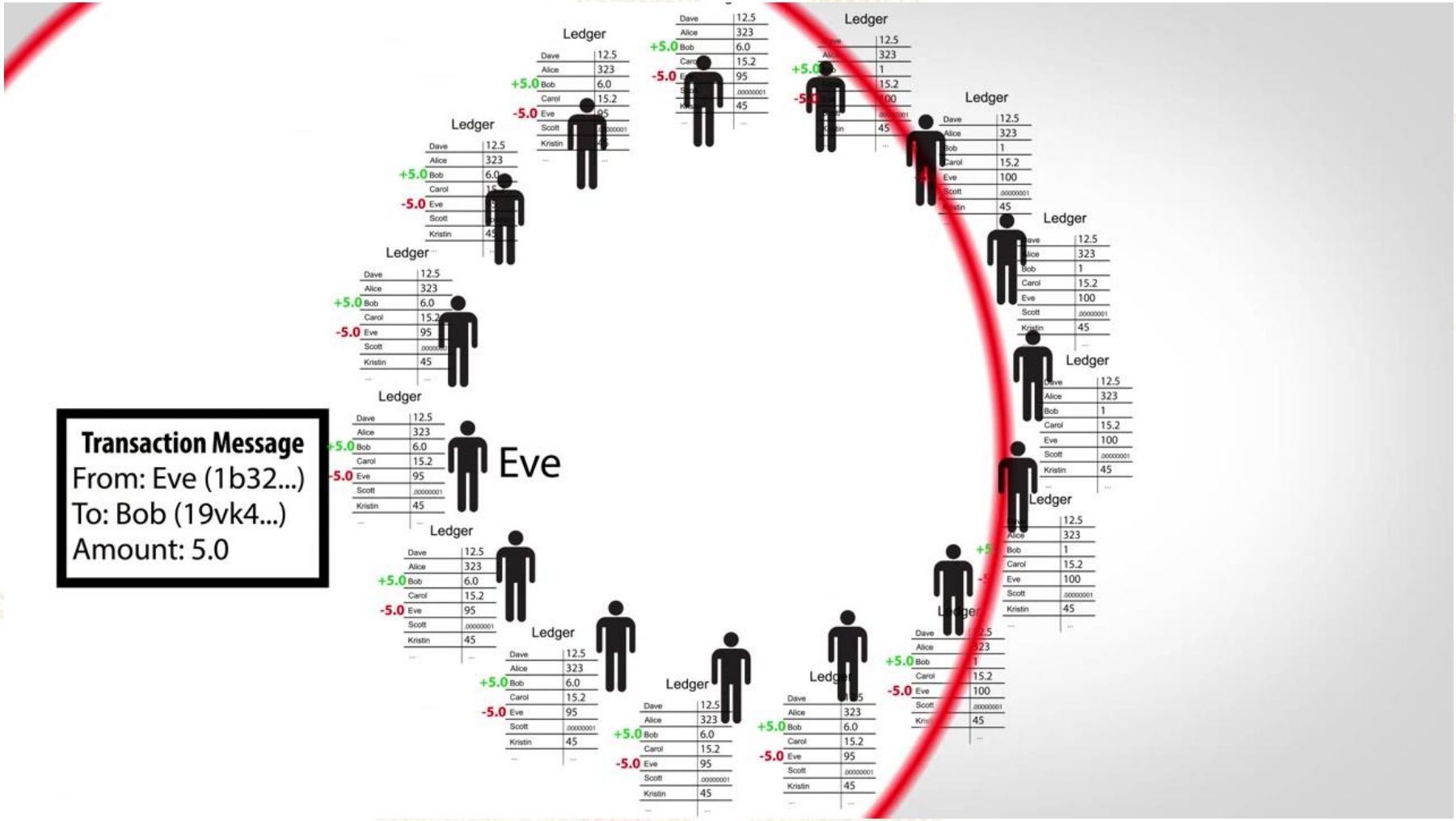


BANK PASARGAD

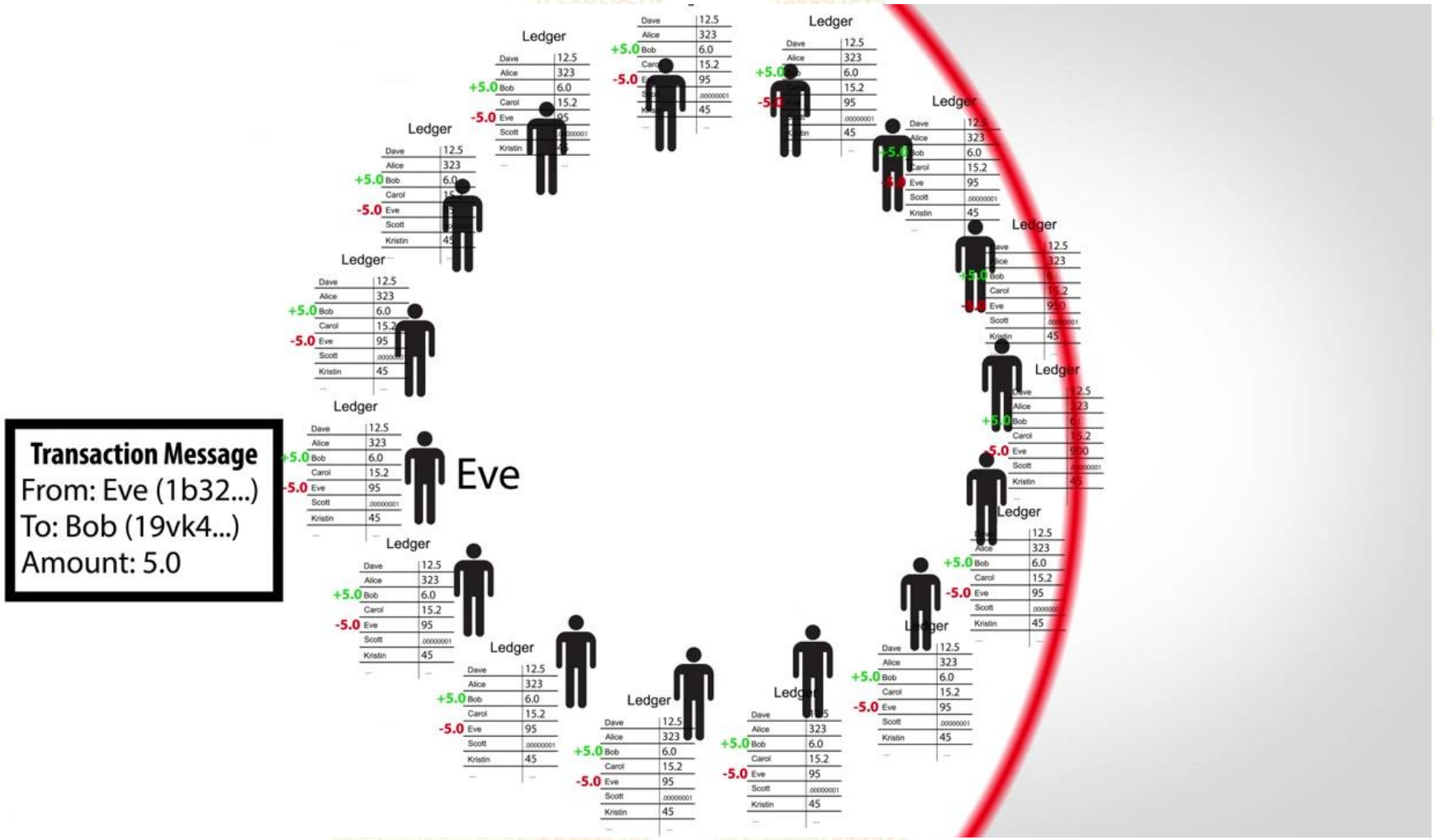

Transaction Message
From: Eve (1b32...)
To: Bob (19vk4...)
Amount: 5.0
Eve
Ledger
Dave 12.5
Alice 323
Bob 1
Carol 15.2
Eve 100
Scott .00000001
Kristin 45
+5.0 Bob 6.0
-5.0 Eve 95



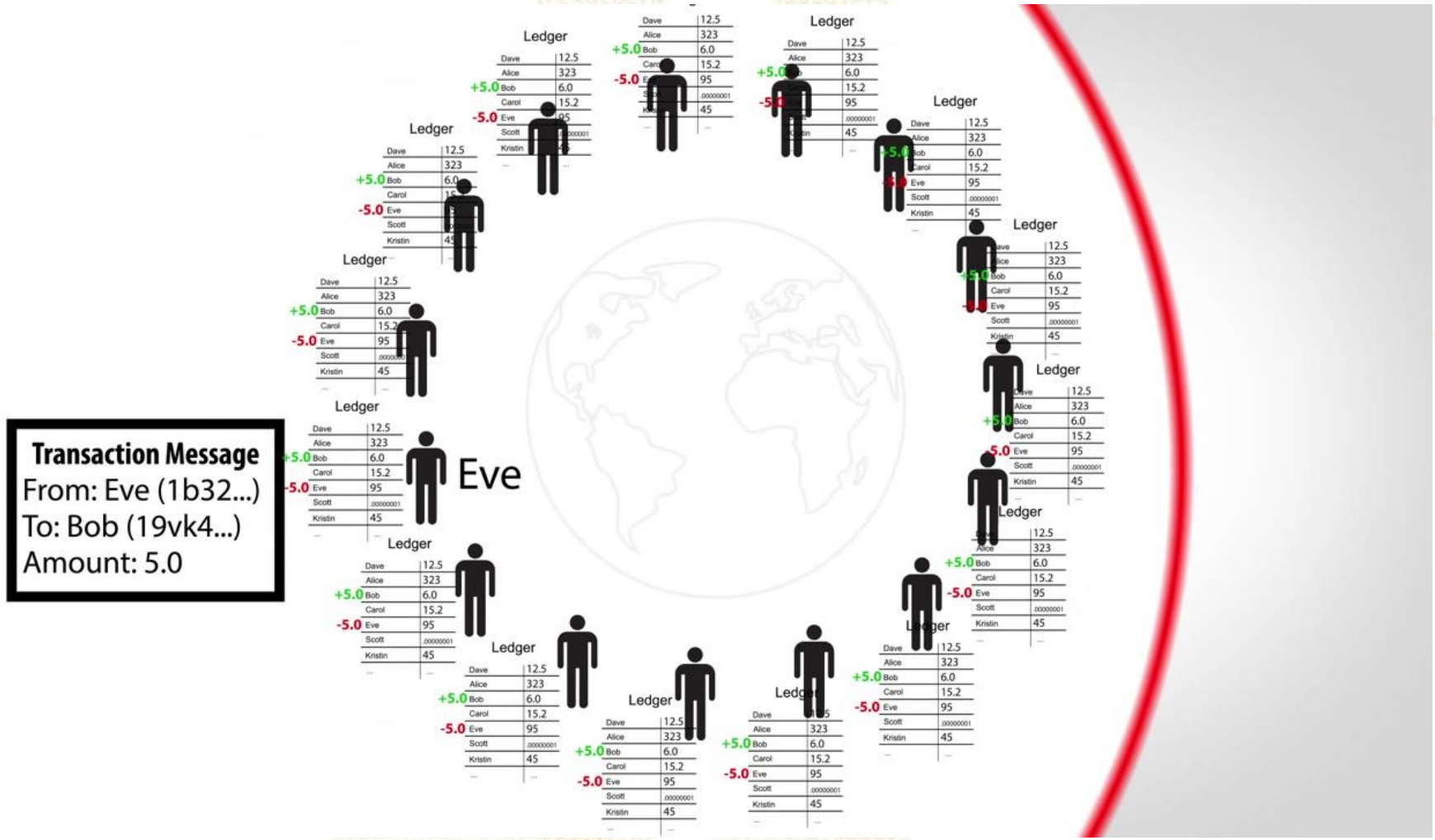
BANK PASARGAD



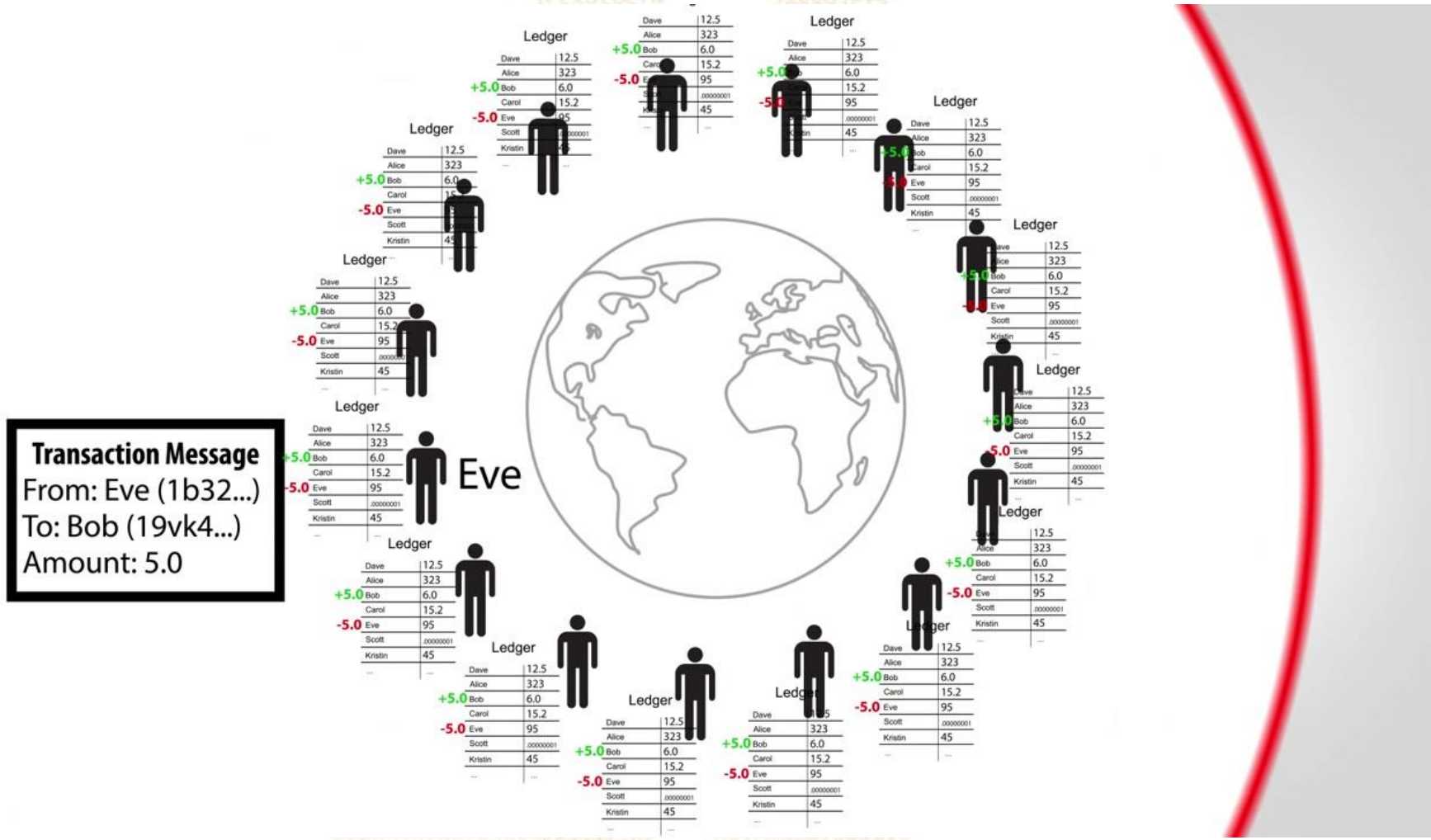
BANK PASARGAD



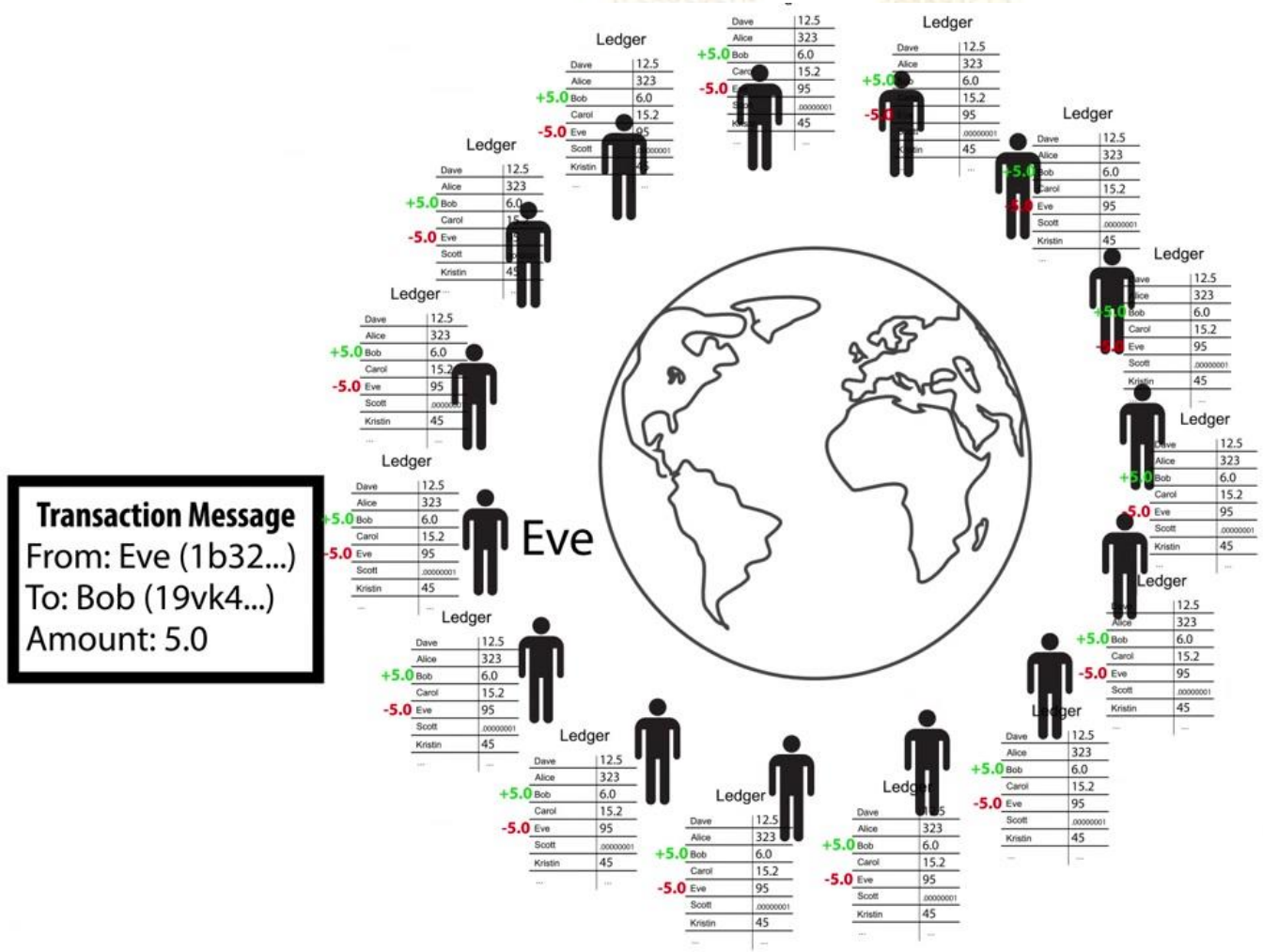
BANK PASARGAD



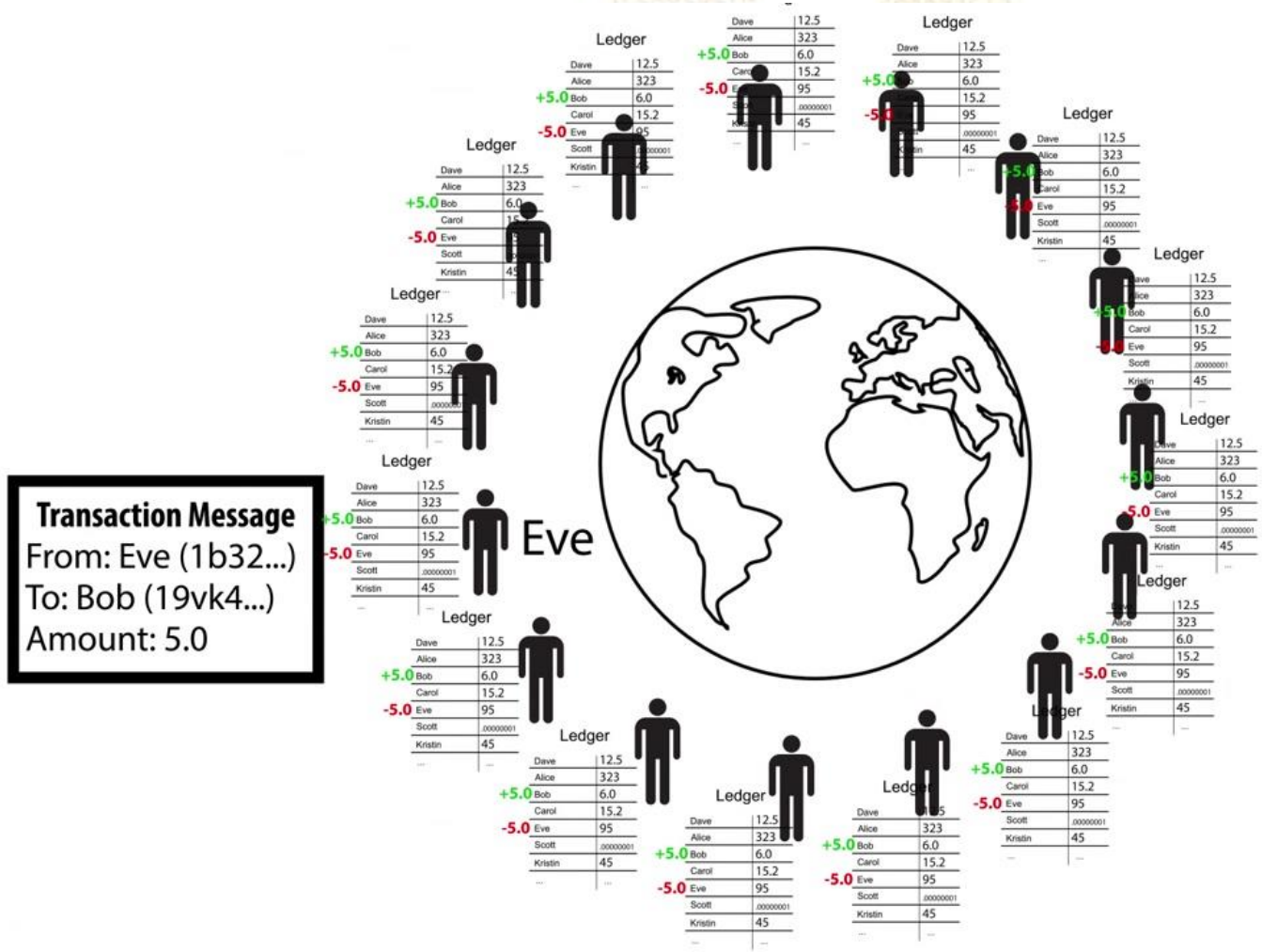
BANK PASARGAD



BANK PASARGAD



BANK PASARGAD

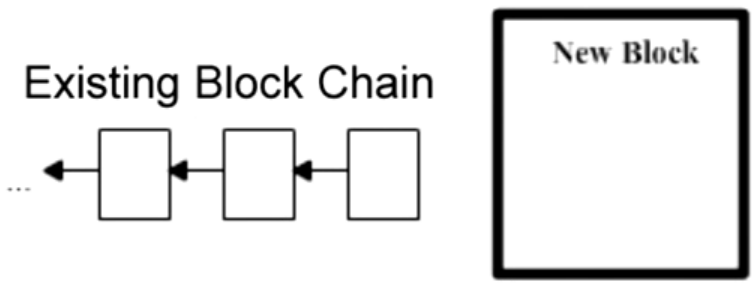


BANK PASARGAD

- In Bitcoin some users volunteer resources to help in
  - validating and processing the broadcast transactions
  - adding the transactions into the ledger

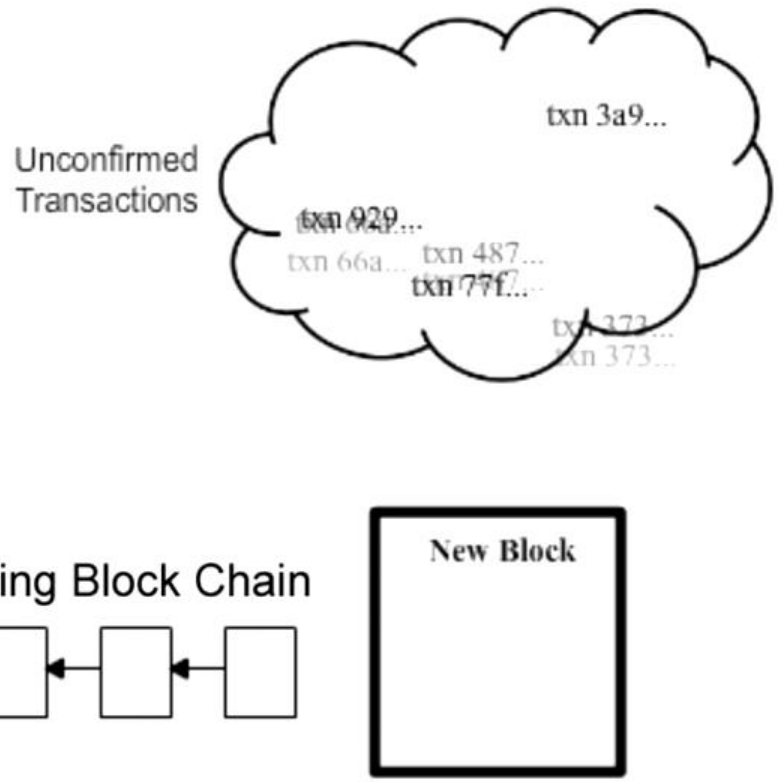
- These users group the validated transactions into **blocks of transactions**

Block Creation



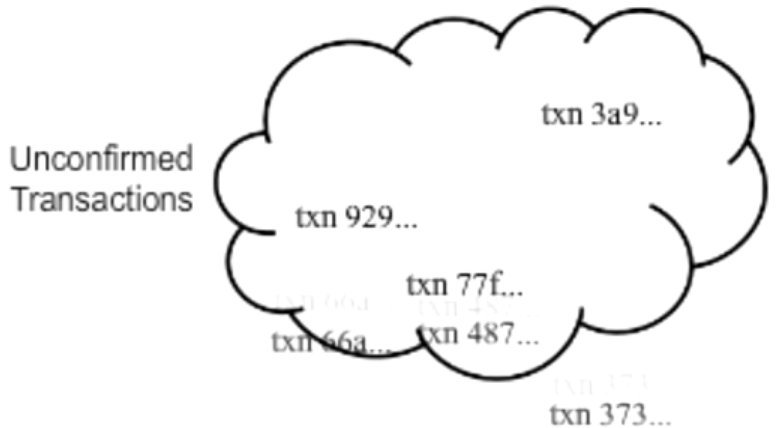
BANK PASARGAD

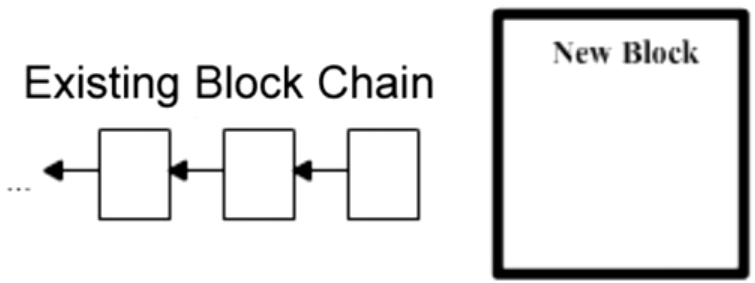
Block Creation



BANK PASARGAD

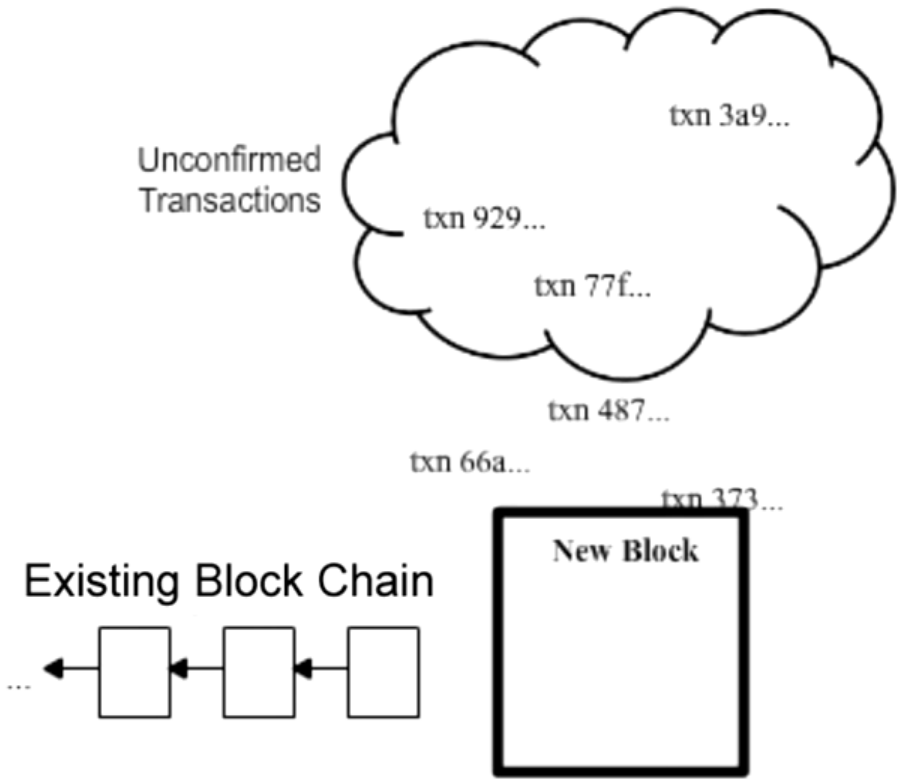
Block Creation





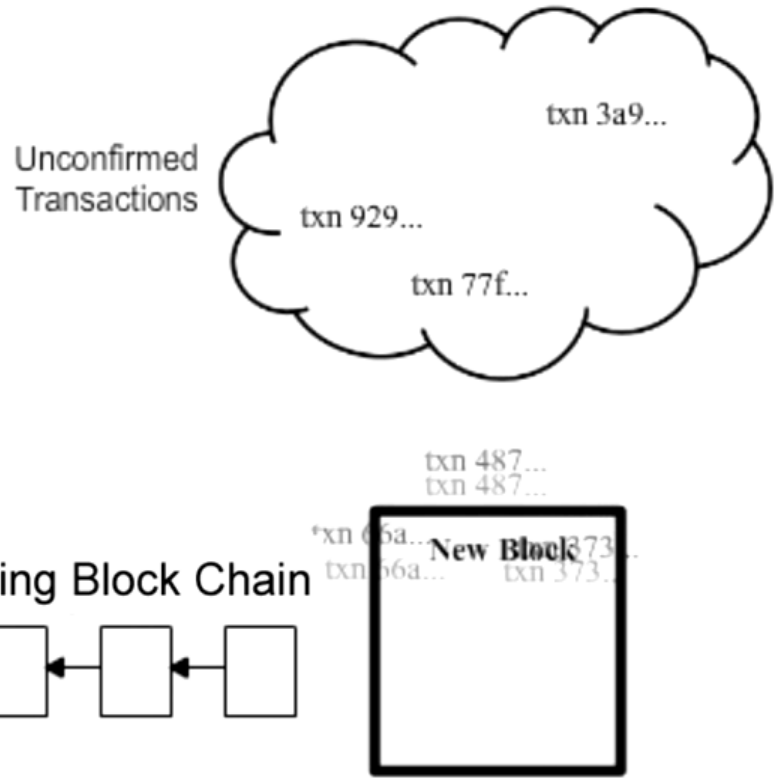
BANK PASARGAD

Block Creation



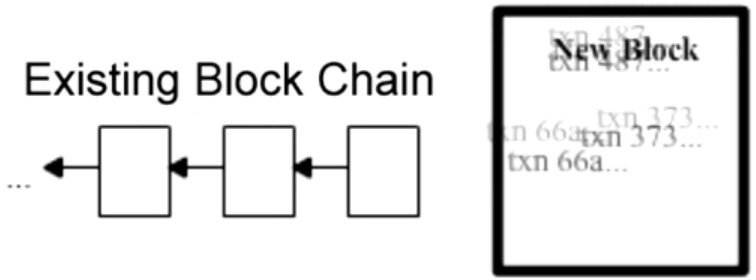
BANK PASARGAD

Block Creation



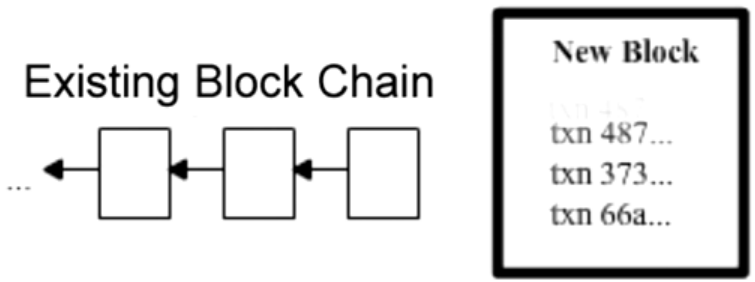
BANK PASARGAD

Block Creation



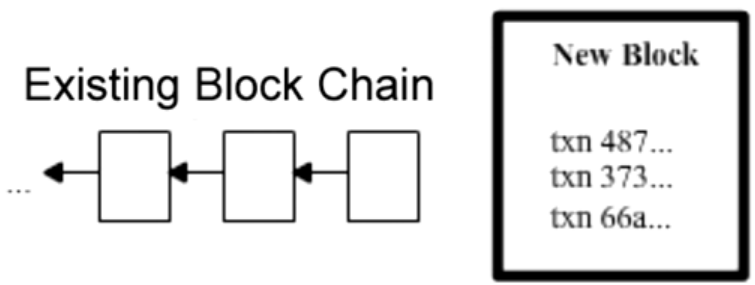
BANK PASARGAD

Block Creation



BANK PASARGAD

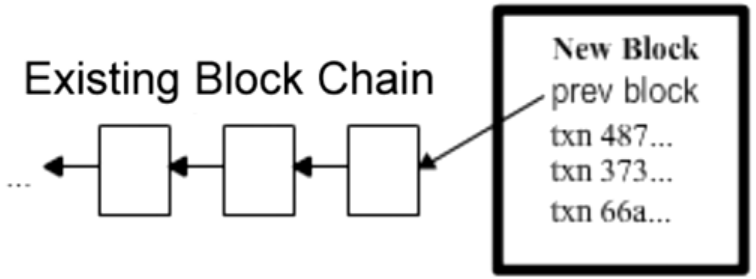
Block Creation



BANK PASARGAD

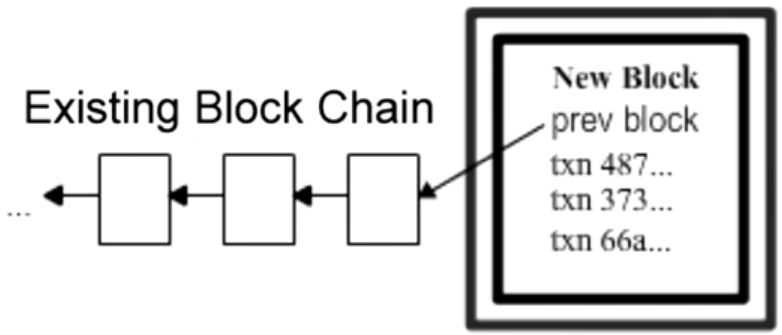
- The newly formed transaction blocks are added to previously recorded transaction blocks on the ledger by chaining them using strong cryptography

Block Creation



BANK PASARGAD

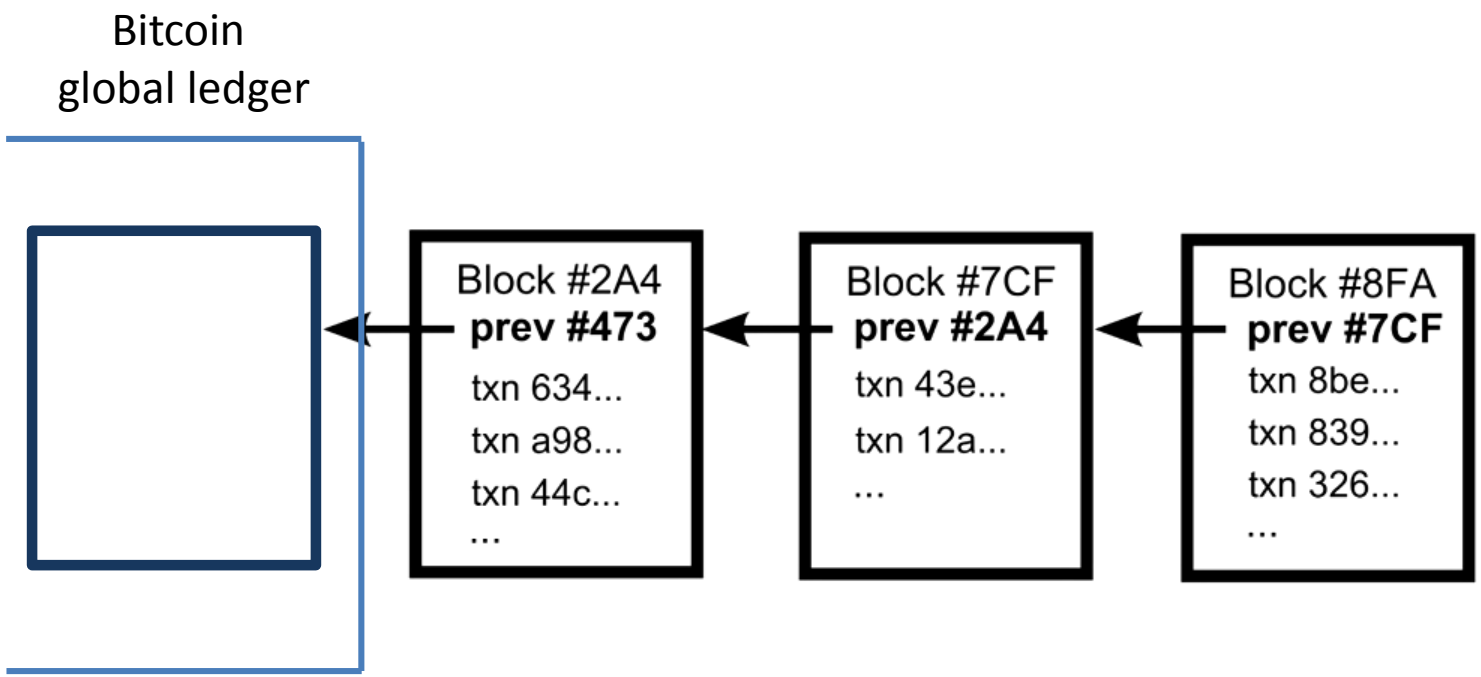
Block Creation



BANK PASARGAD

- In this way transactions are recorded as a cryptographically secured chain of transaction blocks on the ledger

Ordering Solution: The Block Chain



BANK PASARGAD

- Hence the term '**BLOCKCHAIN**'
- The Bitcoin distributed ledger is implemented as a **blockchain**

- Note that while **anyone can**
  - browse the blockchain
  - verify the transactions for themselves

  it is next to **impossible**
  - to **change** the **contents**
  - to modify the **order** of the blocks

  in the chain

- The users performing
  - the transaction validation
  - grouping
  - recording

  are called `**miners**` and receive incentives in the form of transaction fees and newly created bitcoins for each new block added to the blockchain

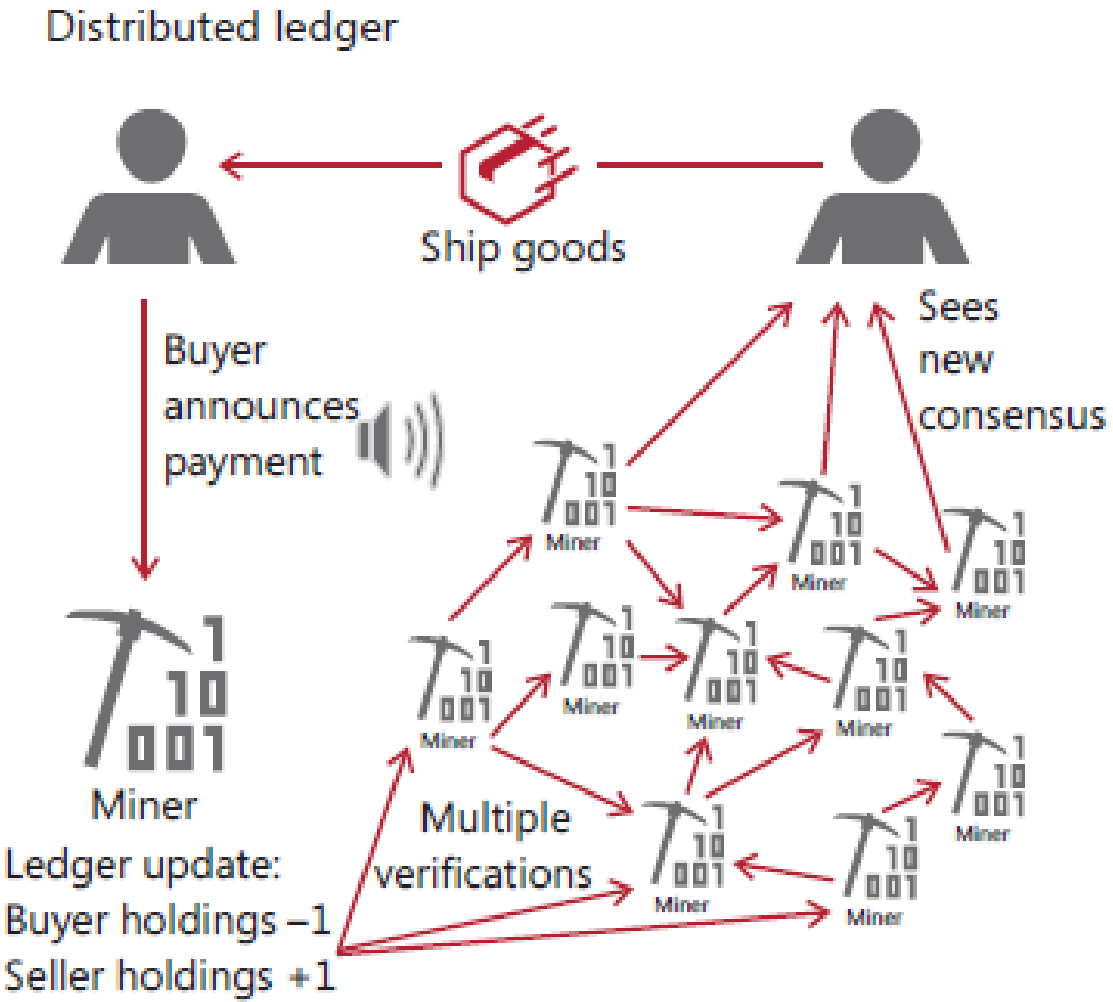
BANK PASARGAD

- Each block contains in the order of 2,500 transactions
- A new block is added approximately every 10 minutes
- This makes for an approximate transaction throughput of roughly 4.2 transactions/sec

BANK PASARGAD

- In summary, in the Bitcoin system a buyer's transaction is
  - First broadcast to the network
  - Next validated and added to a block
  - Finally that block is then added to the ledger by adding it to the chain of previous blocks on the ledger
- Once the above has occurred and the seller sees a transaction ordering payment to her address appearing on the blockchain, she can deem he payment is having been committed and can proceed with shipping her goods

BANK PASARGAD



- **NOTE:** For transactions involving larger sums, sellers usually wait until 6 more blocks have been added on top of the block containing the payment transaction of interest to them. This provides further assurances that the payment is irreversible.

Summary and lead-in to next section

- From the example of Bitcoin, it should be clear by now that the distinguishing feature of cryptocurrencies is the absence of centrality
  - whether in an administrative sense (no central authority)
  - or in a physical sense (no central `server` node)
- Since Bitcoins are not created by any institution
  - they are no one's liability
  - they cannot be redeemed **from** a central institution
  - their value derives only from the expectation that they will be accepted by other users of the currency

BANK PASARGAD

- Crypto's anonymity renders them as an ideal instrument for
  - tax evasion
  - money laundering
  - finance of illegal activity

  even though these were **never** incorporated as an **intentional design feature** but are rather an exploitation of their design features for use in illegal activity

BANK PASARGAD

- **Visa & Mastercard** process more than **5,000** transactions per second with capacity to process volumes multiple times that number
- **Bitcoin** in contrast takes **10 minutes** to clear and settle a single transaction
- **Ethereum** does the same in **15 seconds**
- The number of merchants accepting bitcoin as payment is increasing
- But Bitcoin acceptance is still far less common than that of the major credit cards (Visa and Mastercard are accepted at more than 44 million locations across the globe).

BANK PASARGAD

- As of the time of preparing this presentation, the prices and the market capitalisations of three of the major cryptocurrencies have increased multiple folds compared to their March 2017 prices

  - Bitcoin's price is at approx. 5 x its March 2017 price
  - Ethereum's price is at approx. 12 x its March 2017 price
  - Litecoin's price is at at approx. 13 x its March 2017 price

  this despite a drop from their respective all-time peaks in January 2018

BANK PASARGAD

- The **Ripple Labs** blockchain based global RTGS, the **Ripple payment protocol** and its cryptocurrency **XRP** is finding interest with over 100 Banks, payment providers and digital asset exchanges such as
  - MUFG
  - CIBC
  - Royal Bank of Canada
  - Commonwealth Bank of Australia
  - UBS
  - Santander
  - Credit Agricole
  - ……

  just to name a few

ripple

BANK PASARGAD

- Furthermore there is intense interest in re-purpousing the blockchain technology of today's cryptocurrencies for other related uses by countless banks, companies and institutions such as
  - Bank of England
  - J.P. Morgan Chase
  - Royal Bank of Scotland
  - BAE Systems
  - …..

just to name a few

BANK PASARGAD

- Fair to assert that cryptocurrencies are going to impact the future of payments technology and money
- It is also fair to assert that cryptocurrencies should not be ignored by financial institutions
- The previously cited involvement of banks in cryptocurrencies has so far mostly been with their underlying blockchain technologies rather than exposure to any of the major cryptocurrencies themselves

BANK PASARGAD

- What shape might the banking industry's involvement with cryptocurrencies take?
  - Deposits and loans?
  - Derivatives?
  - Investments in cryptocurrencies as digital assets?
  - Crypto-2-fiat exchanges?

- There has been **very little precedent** from financial institutions which have exposed themselves to cryptocurrencies directly

- It is not clear what risk functions would be affected

- What follows in the remainder of this discussion should be interpreted as guesses and glimpses into the future rather than hard and fast rules

BANK PASARGAD

Risk functions possibly affected by cryptocurrencies

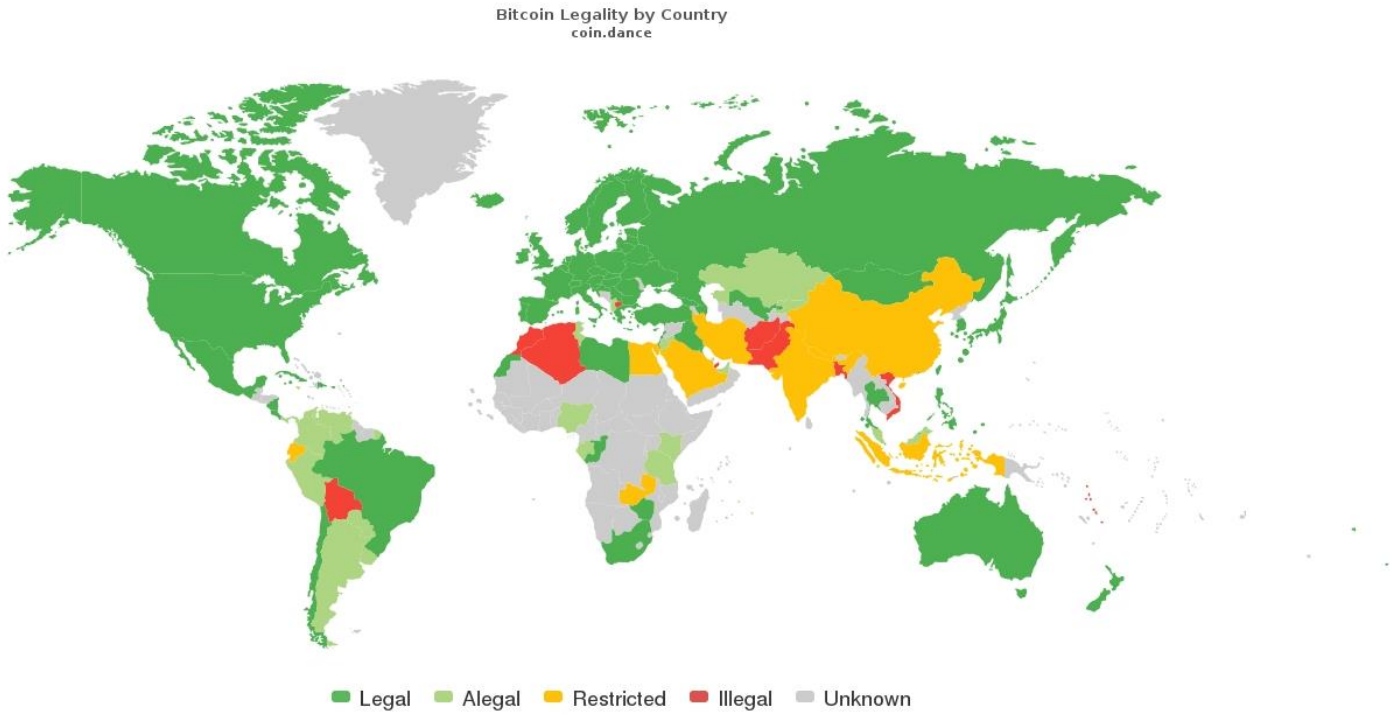
Regulatory Risk

- The regulatory landscape concerning cryptocurrencies is still in its infancy and in a great **state of flux**

- In many jurisdictions
  - authorities have not yet come to grips on what to make of the phenomenon of cryptocurrencies
  - let alone pass legislation concerning its use

BANK PASARGAD

- The range of regulatory policies vis-à-vis cryptocurrencies ranges from
  - permissive with focus only on fiscal classification and integration into existing fiscal frameworks (Japan, US, Canada, most of Europe …)
  - restrictive responses resulting (in some cases) in an outright ban of cryptocurrencies (India, China, ….)



BANK PASARGAD

- A further complication is that cryptocurrencies differ from one another
  - in their protocols
  - policies
  - functions
  - Cryptographic primitives
  - Architectures

  thus potentially requiring different legislation approaches from currency to currency

- For banks directly exposing themselves to cryptocurrencies, the regulatory risks are amplified
- At least in the next few years the constantly changing regulatory requirements might render certain crypto exposures illegal even though an institution might have had done its due diligence and had acted in good faith

BANK PASARGAD

Compliance Risk

- The anonymity that most cryptocurrencies afford their users greatly amplifies this risk category for banks choosing to expose themselves directly to cryptos

- Since there is no centralised route for
  - monitoring transactions
  - screening transactions

  Customer Due Diligence (CDD) will be made complicated and more difficult than for fiat currencies and new methods will be required

- Cryptocurrencies are effectively borderless and they function without the established transaction networks like
  - SWIFT
  - NACHA

  so that monitoring, tracing and re-tracing transactions will be even more complicated and expose institutions with even greater risks of falling out of compliance

BANK PASARGAD

- The exception here may be the Ripple payments protocol which was designed with banks in mind and facilitates seamless SWIFT message integration

- Recall that:
  - Even though the distributed ledger is publicly accessible for everyone to scrutinise the participants in the transactions are semi-anonymous (or pseudonymous)
  - Additionally users can use electronic tools and anonymity networks (**TOR**) to disguise themselves even further, which can make the origins of a transaction completely untraceable

BANK PASARGAD

- Cryptocurrency exchanges
  - constitute the entry and exit points for crypto currencies into the regulated fiat money networks
  - obvious focal point for money laundering

  their monitoring is crucial

- Yet perhaps paradoxically exchange operations may provide suitable entry points for banks into the cryptocurrency space

  - they would provide a familiar operational paradigm
  - simultaneously they serve by placing a very risky aspect of cryptocurrency operations under a financial institution's own direct surveillance
  - thus provide leverage in the mitigation of compliance risks

BANK PASARGAD

Liquidity Risk

- The overwhelming majority of currently existing cryptocurrencies and certainly the ones that will remain in use after the tulip-mania has subsided, do not allow double spending

- Once a certain amount of cryptocurrency – say 10 Ether - is sent to a particular address it is either
  - `**spent**` in which case some or none of the 10 Ether may remain for referencing /use in other transactions
  - or the address is never referenced again as an input to further transactions in which case all or some of the 10 Ether can be used in subsequent transactions

BANK PASARGAD

- Fiat (Fractional reserve system):
  - customer deposits 100 Euros with a financial institution
  - the institution can create a loan of 90 Euros of backed by that deposit

- In effect money is created
  - the bank must honour its liability of 100 Euros to the depositing customer
  - while claiming the 90 Euro loan to another customer as an asset (the other customer can go ahead and spend the loan)

- Cryptocurrencies (no double spending):
  - a depositor deposits 1,000 Moneros
  - the bank loans 900 of the 1,000 Moneros to someone else
  - the depositor wants to withdraw in excess of 100 Moneros
  - the bank must transfer the amount of Moneros to be withdrawn from another address in order to honour its liability to the depositing customer

BANK PASARGAD

- The alternative would be to create traditional bank accounts with crypto deposits as digital-asset kind of liabilities, but that would be like issuing IOUs

- Whether or not cryptos render themselves to traditional banking models and operations is something for the experts to decide

- Nevertheless the point made above is worth considering due to the potential for liquidity issues

BANK PASARGAD

Operational Risk

- By far one of the risk functions affected the most would be the operational risk category
- Here we list some of these risks in terms of the corresponding **Basel categories** (only those deemed affected are reported)

BANK PASARGAD

Level 1	Level 2 (sub-category)	Examples
1. Internal fraud	**1.1 Unauthorised activity** **1.2 Theft and fraud**	- misappropriation of assets - theft of private keys
2. External fraud	**2.1 Theft and fraud** **2.2 Systems abuse**	- theft of private keys - hacking damage or permanent corruption or destruction that is irreversible for portions of the currency held by customers - theft of cryptocurrency from exchanges and storage facilities by third parties

BANK PASARGAD

Level 1	Level 2 (sub-category)	Examples
4. Clients, products and business practices	**4.1 Conduct** **4.2 Advisory activities and mis-selling** **4.3 Product Flaws** **4.4 Improper Business or market practices** **4.5 Customer or client selection and exposure**	- market manipulation - improper trade - product defects (design problems with security & coin generation) - Fiduciary breaches: high reliance on high-level of technical expertise from specialists required by non-specialists who may be bank personnel and customers. - Cryptos are open to third party manipulations which may also impinge on the fiduciary expectations placed on corporate officers

BANK PASARGAD

Level 1	Level 2 (sub-category)	Examples
5. Damage to physical assets	**5.1 Disasters and other events**	- cyber terrorism and attacks on networks and storage facilities may be initiated to benefit certain members or destroy cryptocurrency account details and digital records - cyber vandalism from hackers: for example exploiting a vulnerability to mount DDOS attacks on a currency's network

BANK PASARGAD

Level 1	Level 2 (sub-category)	Examples
6. Business disruption and system failures	**6.1 Systems**	- Software failures (a badly executed fork in a cryptocurrency may result in failures in mining, transaction verification or even encryption) - Hardware failures (nodes on the mining network required to process block chains and perform network verifications may fail resulting in extensive delays in transaction processing)

BANK PASARGAD

Reputational Risk

- A lot of technical expertise is needed for cryptocurrency operations, specifically
  - Cryptographers
  - Cyber security experts
- If breeches and failures occur due to weaknesses resulting from inadequate technical staffing and in-house expertise within an institution, serious reputational damage may result for a financial institution

BANK PASARGAD

FOREX Risk

- Cryptocurrencies have so far displayed a very **high volatility** of their exchange rates to fiat currencies
- For the time being, cryptos are still limited in acceptance for trade and finance
  - exchange into conventional fiat assets will continue to be important
  - current high volatility of cryptocurrency to fiat exchange rates will certainly pose a risk (for the time being at least)

BANK PASARGAD

Strategic Risk

- Cryptocurrencies are still gaining in popularity and acceptance
- Not all of the 1700 cryptos around today will survive the next 5 years
- Only a handful may remain viable
- Despite the above prognosis cryptocurrencies will, without a doubt, have a lasting impact on
  - Payments systems
  - Financial technology
  - Monetary systems

BANK PASARGAD

- Cryptocurrencies in their current form may not yet have the traction needed to be deemed as a successful replacement for existing fiat currencies
- However their underlying technology will without a doubt develop rapidly
- New cryptocurrencies may evolve which may seriously displace current fiat monies

BANK PASARGAD

- Financial institutions are therefore facing innovation threats from cryptocurrencies and it is wishful thinking to believe that this may simply go away in the future
- Any omissions and neglects in strategy w.r.t. this new phenomenon may place a financial institution at a serious competitive disadvantage
  - …perhaps not now….
  - but likely at some point in the future

BANK PASARGAD

- The discussion of the possible risks mentioned so far and the volatile nature of the cryptocurrencies certainly demand that any steps in exposing one's institution to cryptocurrencies directly should be taken with extreme caution

- In this context on is reminded of the old adage

  "**Damned if you do, damned if you don't**"

BANK PASARGAD

References:

- **Books, media and websites:**
  - **ImponderableThings (Scott Driscoll's Blog)**
    www.imponderablethings.com
    - YouTube (recommended): How Bitcoin Works in 5 Minutes
    - YouTube (highly recommended): How Bitcoin Works Under the Hood
  - **Mastering Bitcoin, Programming the Open Blockchain (2nd Edition)**
    Superb & detailed introduction by **Andreas Antonopolous**
    Published by O'Reilly Media Inc.
    This an Open Edition book and it is available freely at
    https://github.com/bitcoinbook/bitcoinbook
  - **LEARN ME A BITCOIN (Greg's Blog)**
    learnmeabitcoin.com
    Superb, concise yet simplified explanation of Bitcoin explained using cartoons

BANK PASARGAD

- **Papers:**
  - Managing the risks of cryptocurrency, BAE Systems
  - BIS annual economic report 2018, chapter V. Cryptocurrencies: looking beyond the hype
  - Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective (Gareth W. Peters, Ariane Chapelle and Efstathios Panayi)

BANK PASARGAD