

Distributed ledger systems



Pavel Kravchenko

Philosophy

- Similar to the structure of existing financial system
- Based on trust to public institutions
- Sending money through chain of friends
- Distributed exchange

Similar to medieval Hawala remittance system

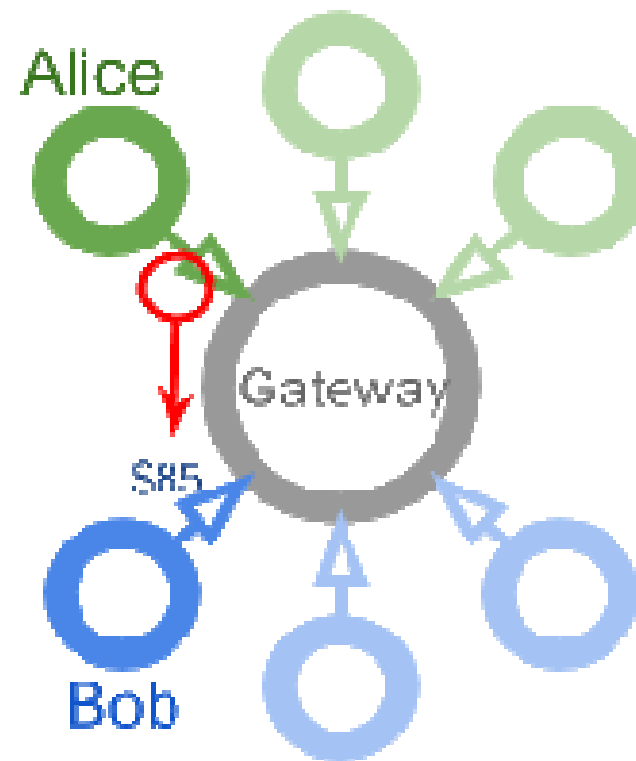
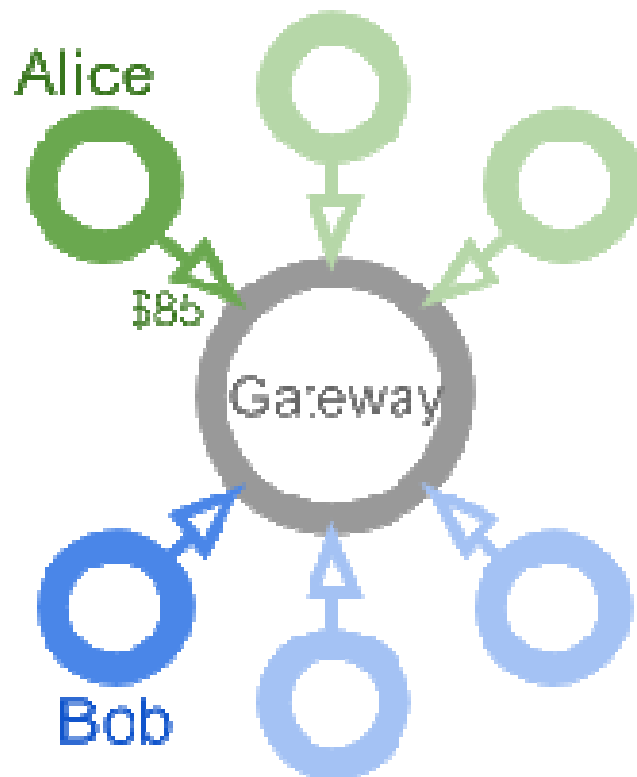
Own currencies

- Built-in in a native way
- Everybody can issue own currency
- Requires trust to the issuer



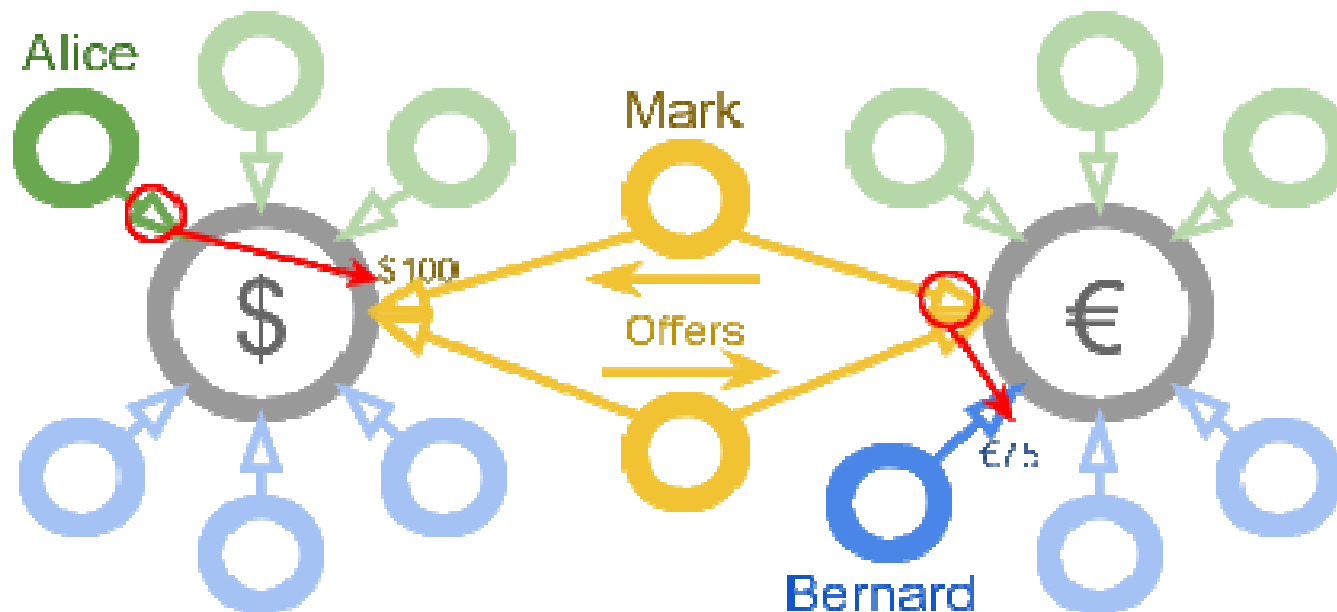
Trust level

- Adjustable trust to money issuers
- Trust lines



Payment path

- Builds chain of people who trust their peers and “ripples” money through it
- Based on offers and can be calculated automatically
- Distributed exchange effect is the result of ledger offers



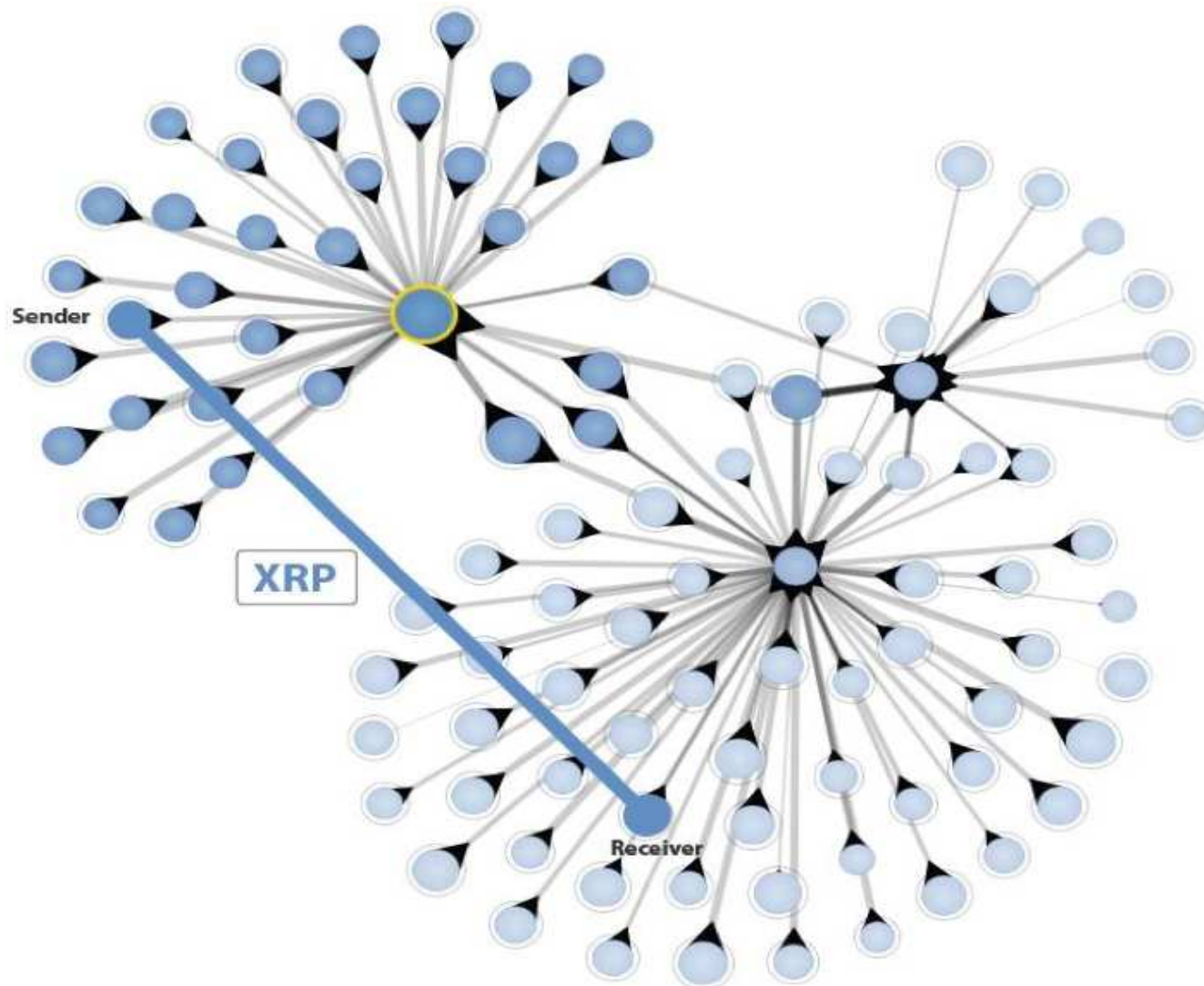
Ledger

“Extended” blockchain

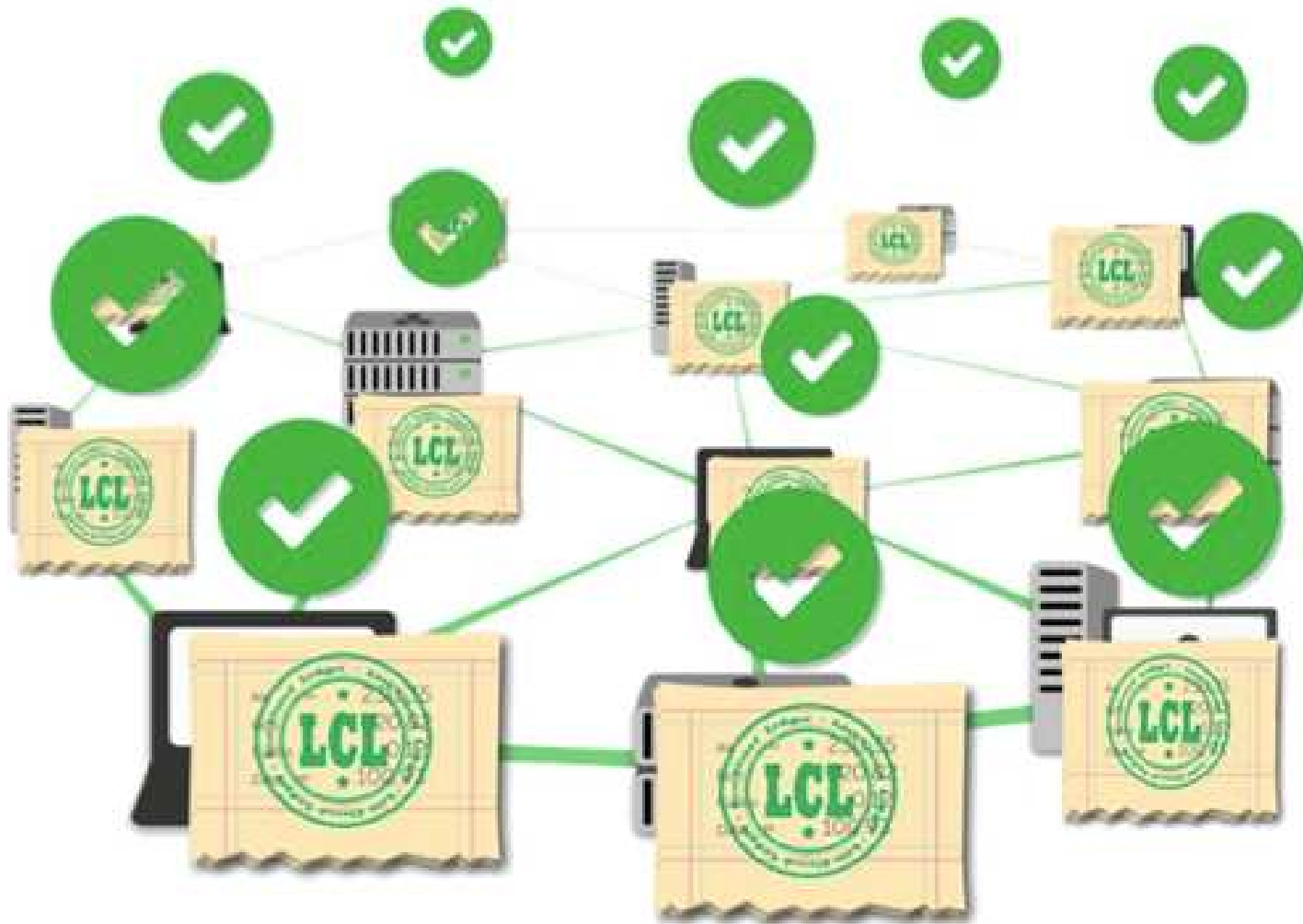
- Transactions
- Accounts
- Offers
- Trust lines



Two level architecture



Consensus based not on speed



Consensus. Process

1. All nodes collect transactions
2. At a particular time they start distribute their proposals about which transactions should be included in the next block
3. Nodes acquire missing transactions from their peers
4. They (probably) change their proposals
5. Nodes “vote” for the transaction including it into the next proposal set
6. Consensus is reached when 80% of nodes have the same vision

Stellar transaction example

```
{
  "result": {
    "engine_result": "tecNO_DST",
    "engine_result_code": 124,
    "engine_result_message": "Destination does not exist. Send STR to create it.",
    "status": "success",
    "tx_blob":
      "120000228000000024000002AC61D4871AFD498D000000000000000000000000055534400000000078064F19696F4ADD2438
      E27070E5EA51B4DD233668400000000000000A7320053DC64AE87B36159EA11EC9C387699E71596A4FE1FBD32EDE814D789E3
      F5221744007A7EB6CE0DD8A77C86B4A14590859A92F87E3F94C6B9FF64DDABDE61B689EEBAA9BECC5B3C5BBF74F8971EF4
      3E8E71D1EC40236A4C5CFAEE56957033CCFCF008114DF8286CDBB009AA5C29F526B5C3B4C480B44EABE8314ED6EC1D865C
      C2D4720B6CED71C42B4BA0E4E4B93",
    "tx_json": {
      "Account": "gM4Fpv2QuHY4knJsQyYGKEHFGw3eMBwc1U",
      "Amount": {
        "currency": "USD",
        "issuer": "gBAde4mkDijZatAdNhBzCsuC7GP4MzhA3B",
        "value": "2"
      },
      "Destination": "g4eRqgZfzfj3132y17iaf2fp6HQj1gofjt",
      "Fee": "10",
      "Flags": 2147483648,
      "Sequence": 684,
      "SigningPubKey": "053DC64AE87B36159EA11EC9C387699E71596A4FE1FBD32EDE814D789E3F5221",
      "TransactionType": "Payment",
      "TxnSignature":
        "07A7EB6CE0DD8A77C86B4A14590859A92F87E3F94C6B9FF64DDABDE61B689EEBAA9BECC5B3C5BBF74F8971EF43E8E71D1
        EC40236A4C5CFAEE56957033CCFCF00",
      "hash": "61464CE357C1D0F7D8ECD5A13D8FF74C0197A0BD8B24C9D01BAC4C087B39CAC3"
    }
  }
}
```

Fee policy

- Processing servers don't take fees
- Each currency issuer sets own fee for operation with it