Scaling Blockchain Applications

Artit ‘Art’ Wangperawong

artitw@gmail.com

https://artitw.github.io
Asymmetric Cryptography

- Public key – your email address
- Private key – your password to read and send emails

Double Spending:
Can send money, but no verification of available funds
Centralized, Non-distributed Banking

Bob

cheque

Alice

Bob’s bank

Alice’s bank
Decentralized, Distributed Blockchain

P2P transaction verification

Faster, cheaper, worldwide, unstoppable

Bob

Alice

5/21/18

Artit Wangperawong
Smart contracts

Bob sends
5 BTC
to Alice

really just +/-

if Bob sends
5 ETH to Alice,
transfer Alice’s
deed to Bob

programmatic logic
Bitcoin protocol

Records are
• Validated
• Immutable
• Chronological
• Distributed
Bitcoin protocol

Fork in the blockchain: Two miners validate and broadcast blocks simultaneously
Bitcoin protocol

Miners abandon shorter fork

Miners pick up on longer fork
Proof-of-work (POW) protocol results in about 10 minutes per block, so it takes 1-2 hours for a full payment confirmation.
Blockchain – Transaction Highway
Congestion
CryptoKitties

Completely on Ethereum blockchain

$100k for a digital cat Crippled Ethereum
Transaction Volume and Fees (BTC)
Transaction Volume and Fees (ETH)

https://bitinfocharts.com/comparison/ethereum-transactions.html
Why can't I see my transaction in the blockchain?

• You can view most digital currency transactions on the network's respective [blockchain](https://support.coinbase.com/customer/portal/articles/1392055-why-can-t-i-see-my-transaction-in-the-blockchain), which records and verifies the legitimacy of transactions. However, when transferring from a Coinbase account to another Coinbase account, the transactions occur off the blockchain. This makes confirmation instantaneous, causes transactions to be fee-less, and allows for micro-transactions as small as one satoshi (0.00000001 bitcoin). For these "off-chain" transactions, you won't be able to view the bitcoin transfer in the blockchain, and there won't be an "Advanced Details" link when you click on the transaction.

https://support.coinbase.com/customer/portal/articles/1392055-why-can-t-i-see-my-transaction-in-the-blockchain
Off-chain
Off-chain

Ethereum

web3.js, web3.py, etc.

Centralized database
Side-chain - HOV
Side-chain, private/permissioned

Ethereum

Ethereum or Hyperledger
Side-chain, public/permissionless

Ethereum

Ethereum or Hyperledger

5/21/18

Artit Wangperawong
Blockchain App Scaling – Hybrid Approach

• Phase 1 – Off-chain
  • Centralized database with Ethereum integration
• Phase 2 – Private, permissioned side-chain
  • Transition to a distributed and decentralized but still controlled system
• Phase 3 – Public, permissionless side-chain
  • Transition to a fully public blockchain
Local + Highway + HOV
Lightning Network for BTC
Off-chain payment channels

Bitcoin blockchain

Payment channel between Alice and Bob using multisignature wallet

Numerous transactions occur off chain

Open channel

Close channel
Network of off-chain channels (Layer 2)