Feasibility of Cryptocurrencies on Mobile devices

Anas Younis & Sander Lentink
University of Amsterdam
MSc System and Network Engineering

RP1

06-02-2018

Disclaimer

Assumed knowledge;

- Cryptocurrencies
- The principle of Distributed Ledger (Bitcoin)

Which aspects are required to make cryptocurrency feasible on mobile devices?

- *Which consensus methods?*
- *Which techniques to keep in sync?*

Scoped vs. Out of scope

Trust[less|ed]		
Transaction speed		
Scalability		
		Traceability/privacy
		Security
	Transaction fees	
	Image	

Trusted vs. trustless

The *Why?* of cryptocurrencies;

Early adopters of Bitcoin (cryptocurrency) desired an open trustless system.

Permissioned vs. permissionless

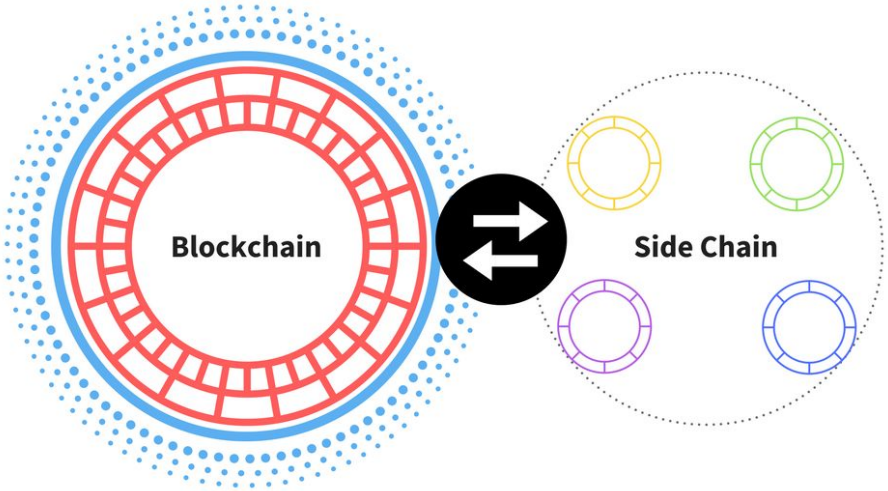
Private	Public
Trusted	**Trustless**
Faster consensus	Slower
Managed	Public ownership
Private membership	**Open** access
Controlled access to ledger	**Transparent**

Ripple

Bitcoin / Ethereum

DL (Distributed Ledger) consensus

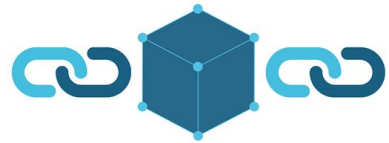
Sidechains*



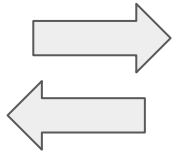
- Use asset of X on Y
- No exchange/conversion
- Enables innovation with conservative coins
- Assets migrated through locking, not destroying

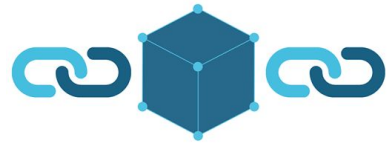
* requires soft fork

Sidechain example: wholesale payment network



Public
Permissionless
Slow consensus





Private
Permissioned
Instant payments

SPV (Simple Payment Verification)

1. Client requests headers since last know state
2. Client sends request for the addresses corresponding to the wallet

- More secure than web wallets
- Useful when combined with fast blockchain

Stellar Consensus Protocol

- Consensus method
  - Traditional Byzantine agreement
  - Membership through central authority (bitcoin has no central authority) ⟶ **centralised (permissioned)**
  - Make it **permissionless (decentralised)** ⟶ **Federated Byzantine Agreement**
  - Distributed network security problem

Stellar Consensus Protocol

- Quorum
  - Set of nodes required to reach agreement across the whole system
  - Problem: malicious nodes can join in and outnumber
- Quorum slices
  - Each node votes with quorum slices whom to trust

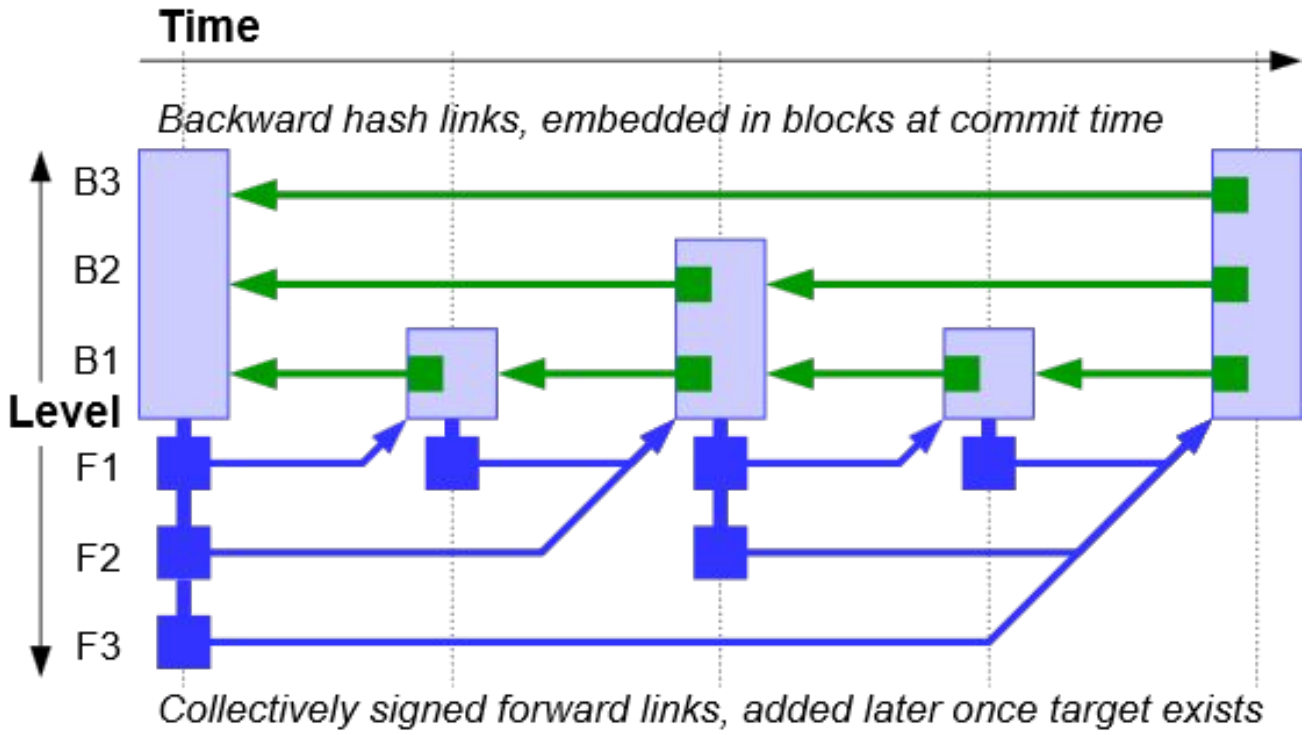
Stellar Consensus Protocol

- Current usage
  - MobileCoin and Stellar
- Nodes
  - Intel Software Guard Extensions (SGX) nodes
  - set aside private regions of code and data
- Fast transaction confirmation time
- Transaction fees Stellar
  - Less than $0.01
  - Motivation: elimination of gaps between closed systems

Skipchains

- Based on blockchain
- Permissioned ⟶ Permissionless (decentralised)
- Consensus method:
  - BFT-Collective Signatures (CoSi)

Skipchains


Time
Backward hash links, embedded in blocks at commit time
B3
B2
B1
Level
F1
F2
F3
Collectively signed forward links, added later once target exists

Skipchains - ByzCoin

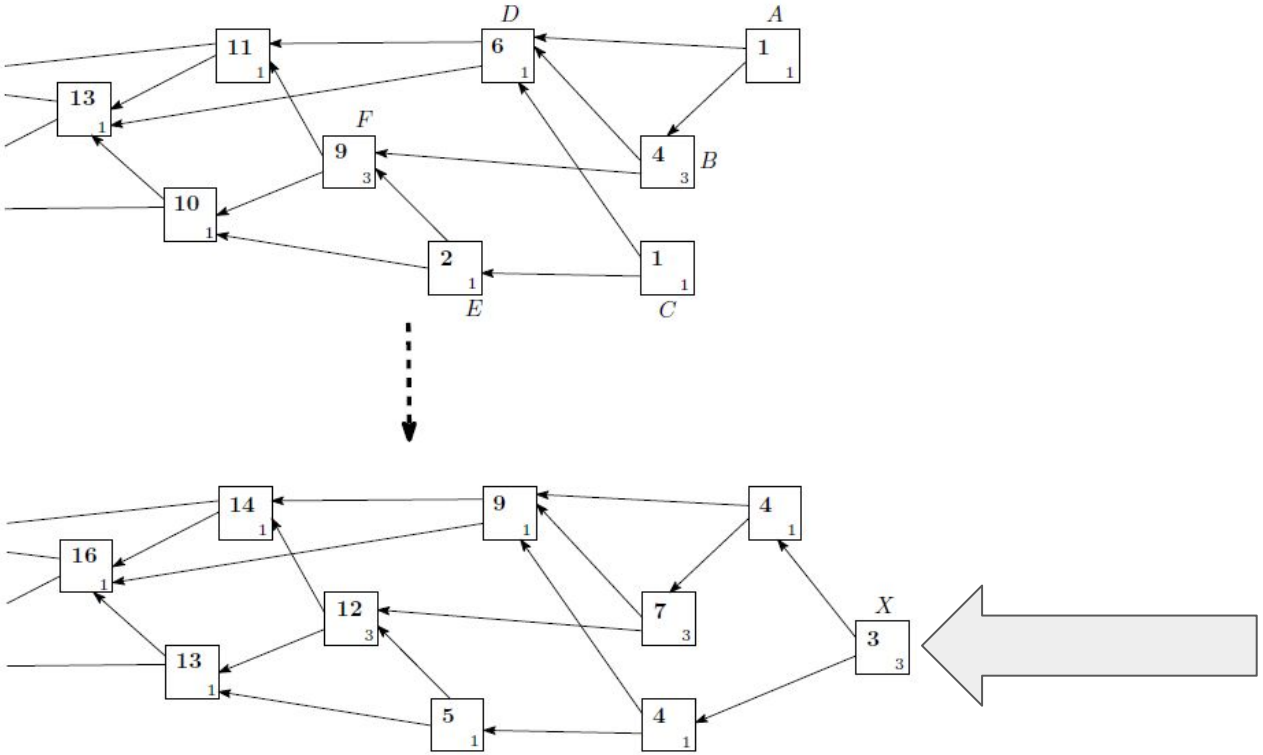
- Current usage
  - ByzCoin
- Fast transaction confirmation time
- Transaction fees
  - Splitting fee with miners and group members
  - Miner gets the most because of the hash power
  - Consensus group members remain live and participate for rewards

Blockchain vs. DAG (Directed Acyclic Graph)

Tangle

- Directed Acyclic Graph (DAG)
  - Directed: one-path
  - Acyclic: same transaction cannot be encountered more than once
- Directly and indirectly validate transactions
- Weight and cumulative weight
  - Weight by the work the node has done
  - Cumulative weight: helps with conflicting transactions

Tangle



Sub-tangle DAG

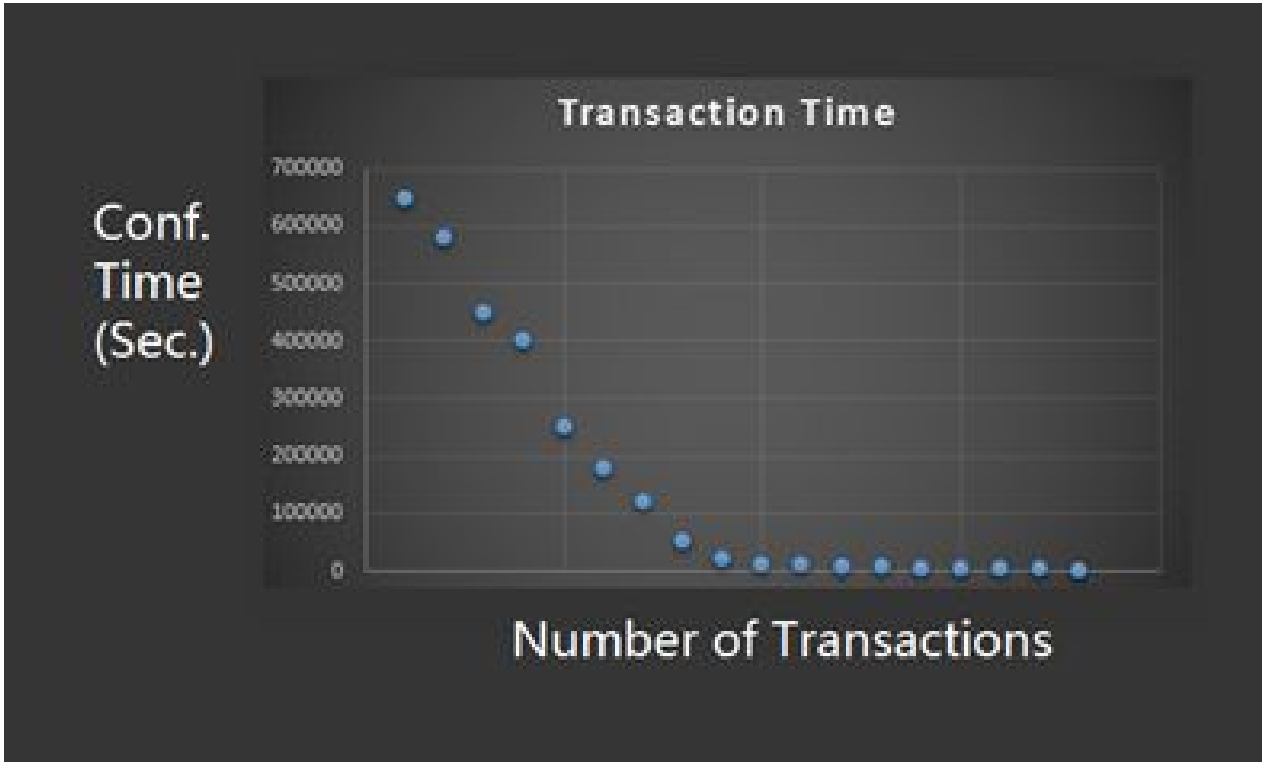
Tangle - IOTA

- Current usage
  - IOTA
- Decentralisation
  - Currently not completely decentralised
  - Coordinators
    - Nodes placed in secret location
  - Will gradually become centralised as the network grows

Tangle - IOTA

- Fast transaction confirmation time
  - Validate two transactions for each transaction a user does
    - More nodes, faster network

Tangle - IOTA


Transaction Time
Conf. Time (Sec.)
7000000
6000000
5000000
4000000
3000000
2000000
1000000
0
Number of Transactions

Tangle - IOTA

- Transaction fees
  - No transaction fees
    - No miners with monetary rewards
    - Entire network of participants is directly involved in the approval of transactions
    - Transact sub-cent values
      - Bitcoin can have situations where paying a fee is larger than the amount of value being transferred

Conclusion

	Tangle	SCP	BFT	BFT-CoSi	PoW	PoS
permissionless	X	X		X	X	X
tx time < 10s	X	X	X	X		X
miners		X	X	X	X	X
incremental throughput	X					

- Efficiency (offloading)
- Trustless as foundation
- Speed of transaction dictated by consensus mechanism
- Currency X used with consensus Y through chain linking
- Blockchain not the only solution

Research question

- *Which consensus methods?*
  - *Transaction speed*
- *Which techniques to keep in sync?*
  - *SPV (Simple Payment Verification)*
  - *Tangle*
  - *Skipchains*

Future work

- Traceability/privacy
- Image of coin
- Address management (needed for recurring payments)
- Secure storage and backup of private keys
- Fungibility of coins
- Education
- Cloud wallet

References of images

- http://study-aids.co.uk/dissertation-blog/wp-content/uploads/2016/05/2008-Financial-Crisis.jpg
- https://perfectial.com/wp-content/uploads/2017/09/PoWPoS-img.jpg
- http://trackenergy.com.au/wp-content/uploads/2013/05/Coal-vs-Renewable.jpg
- https://cdn-images-1.medium.com/max/1600/0*gHDyU65BfvNG-VHn.png
- https://images-na.ssl-images-amazon.com/images/G/01/gc/designs/livepreview/a_generic_white_10_us_noto_email_v2016_us-main._CB277146614_.png
- https://bitcoin.org/img/icons/opengraph.png
- https://coinsutra.com/wp-content/uploads/2017/06/What-is-Blockchain.gif
- http://bford.github.io/2017/08/01/skipchain
- https://iota.org/IOTA_Whitepaper.pdf
- http://www.dimitri.co.uk/business/business-images/pile-currency-coins-silver-gold-question.jpg
- https://sirinlabs.com/
- https://jumbotron-production-f.squarecdn.com/assets/221582607f1d70fcf52d.jpg
- https://upload.wikimedia.org/wikipedia/commons/thumb/3/31/KPMG.svg/1200px-KPMG.svg.png