newmoneyhub

Business requirements for smart contract platforms

presented at
Blockchain Conference Kiev
on 20 May 2016

Alex Kampa
ak@newmoneyhub.com

newmoneyhub

“To a man with a hammer, everything looks like a nail”

- Mark Twain (apocryphal)

- *Outlandish claims by blockchain evangelists*
- *Many applications do not require blockchains*
- *Current technology is still in its infancy*

newmoneyhub

newmoneyhub

A compelling use case: SWIFT

- A “SWIFT payment” is actually not a payment, it is just a message
- The actual payment occurs independently of SWIFT
- Each bank has to maintain its own redundant IT systems and reconcile payments with all its correspondents
- Bottom line: expensive and error prone
- Setting up a world-wide central clearinghouse for banks is not a realistic solution (mainly for political reasons)

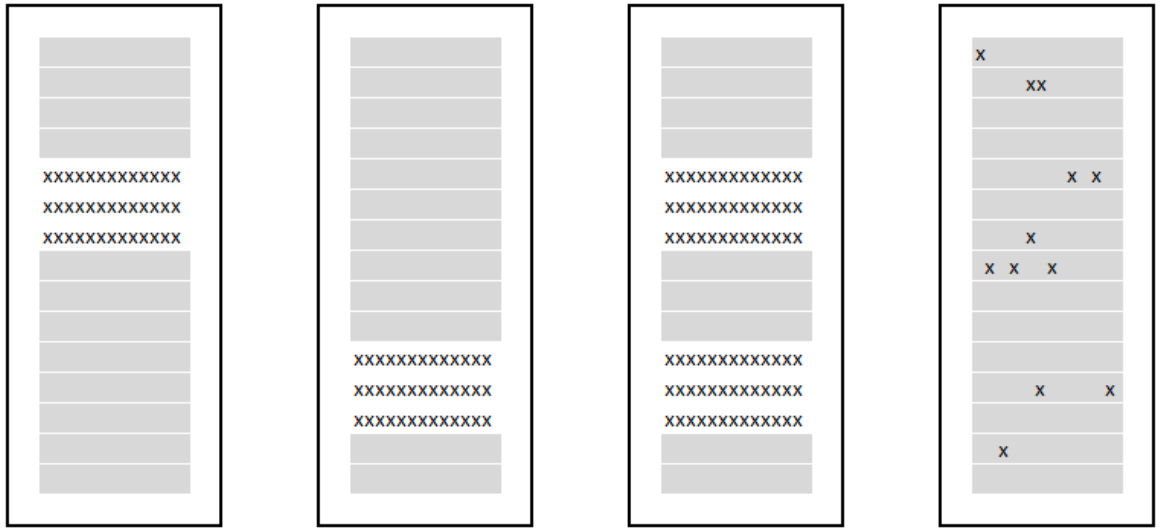
newmoneyhub

A possible future for SWIFT

- Running on a distributed ledger
- “the message is the payment” : when consensus is reached over a transaction, the payment is completed
- Resilient system: system keeps running even if some nodes are down
- Significant cost efficiency: less IT infrastructure, less manpower needed to track payment errors

newmoneyhub

But complex data confidentiality rules needed: different “views” of a distributed ledger



=> Now used for payments within a banking group, rather than between banks, because data confidentiality issues are not solved

newmoneyhub

The new/money/hub project

- A platform to run monetary systems based on credit conversion
- Goal: decentralised, self-organising and self-stabilising (graceful default handling)
- Participants issue debt and accept each other's credit according to rules they set themselves
- Participant create credit conversion links with others to "upgrade" / "modify" their credit when necessary. Fees are set by mutual agreement.
- Concept of "cheapest to deliver" – when making a payment, finding the optimal (least expensive) path

newmoneyhub

Requirement #1 : Trust

- We want to run the Dapp on trusted nodes only
- Some data may need to be on a subset of “super-trusted” nodes (e.g. customer details)
- Need fine-grained control over what information is exposed to the entire system

newmoneyhub

Requirement #2 : Cost

- Cost must be predictable, especially if operating on small margin with a large volume of transactions
- Cost should go down as computing and storage cost goes down
- Current models of smart contract platforms are not suitable: for example, on Ethereum, users want ETH to go down, speculators want it to go up
- NB becoming a miner is not an option – it's a different business

newmoneyhub

Requirement #3 : Speed

- In the payment area, speed is critical …
- … but transaction optimisation is resource-intensive (and not deterministic)
- Running on too many nodes does not make sense, even running the same Dapp on a small number of nodes seems like a waste
- One solution: run optimisation on each node, and reach consensus based on the best solution to the optimisation problem
- Similarity to mining: finding an optimal solution is hard, checking the result is very easy

newmoneyhub

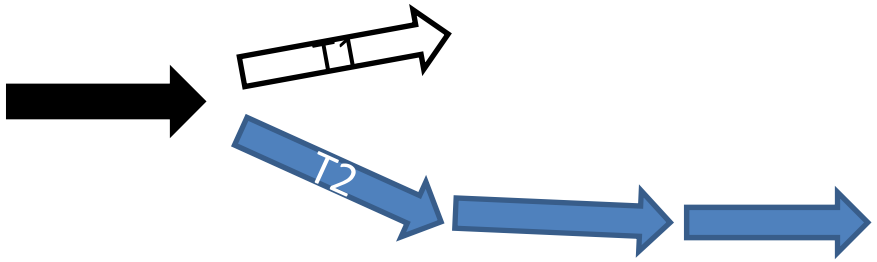
Optimisation consensus protocol

- One way to start: use a few “reasonable” deterministic algorithms that will compute quickly and yield a “baseline result”
- Every node independently tries to improve on the baseline result
- After spending a predetermined time and/or processing power, the nodes seek consensus: the optimal solution wins
- Because it is easy to verify the solution, each node can do it independently
- Open issue: each node may not have the same state!

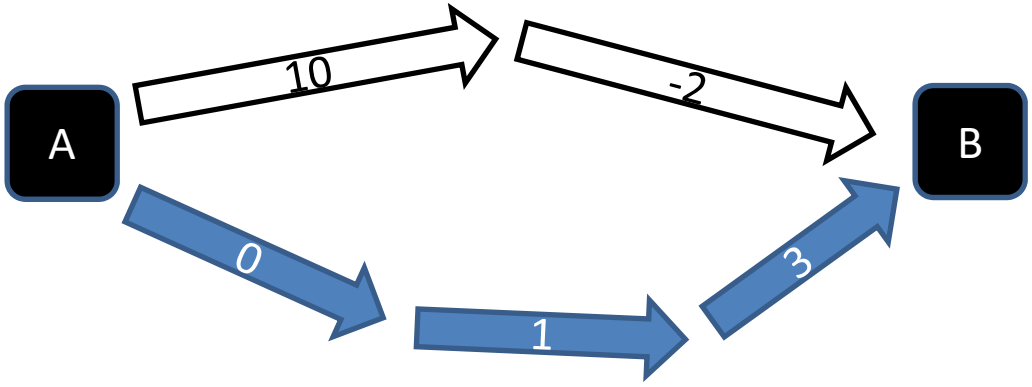
newmoneyhub

Applications

- Trade settlement / securities lending : maximise the transaction volume



- Payments / delivery : “cheapest to deliver”



newmoneyhub

Feature recap

- Trust => choice of nodes, control over information exposed to the network
- For many applications, an open network will not be acceptable (i.e.all active nodes, trusted or not, must be known)
- Cost control => exposure to crypto-currency not acceptable
- Speed => leverage distributed processing power

newmoneyhub

Thank you !

Alex Kampa
ak@newmoneyhub.com
http://www.newmoneyhub.com