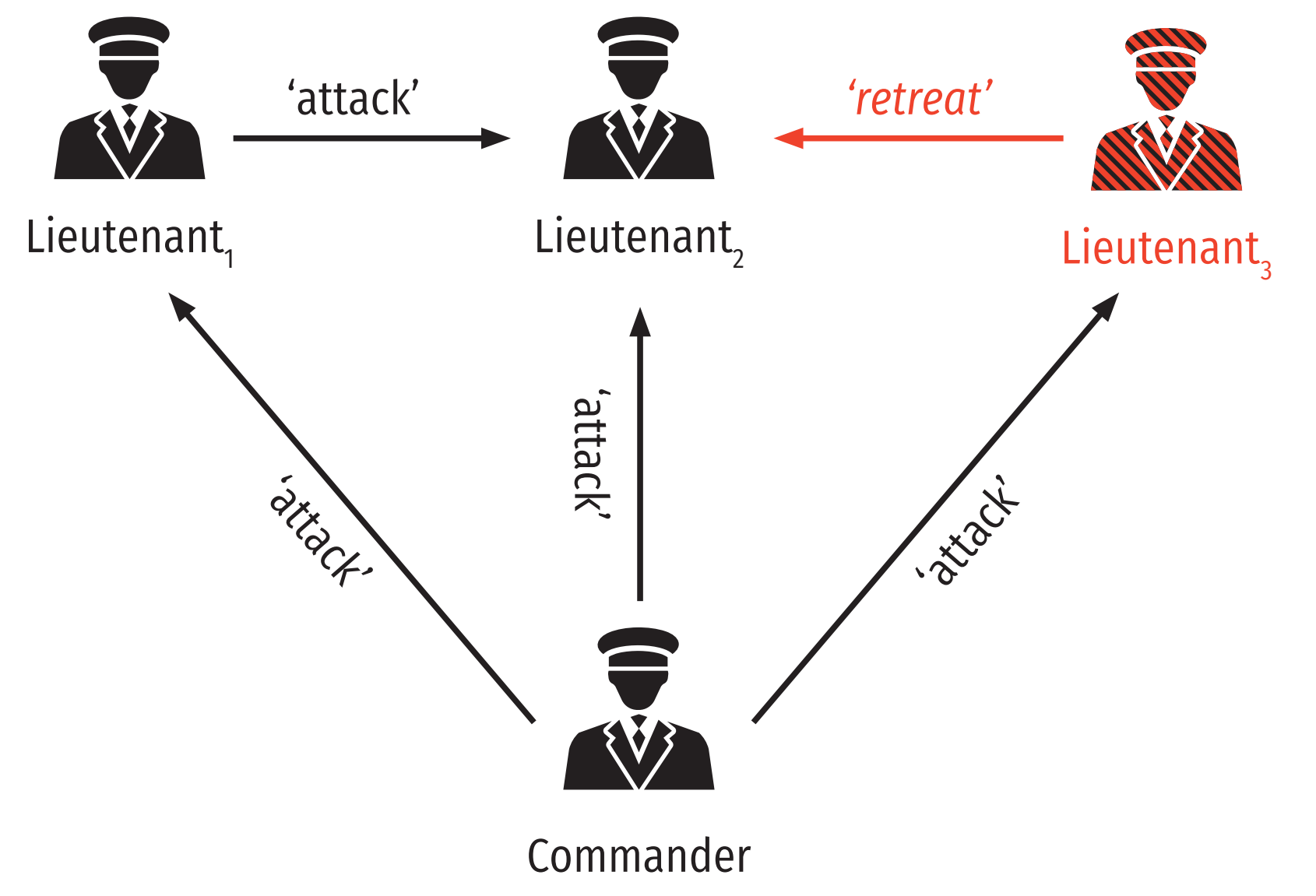
Democratic Blockchain Consensus with Evolving Constituencies

Blockchain and Distributed Ledger Technology at their core solve the problem of distributed data replication in a distrusted environment with multiple writers and readers.
As such, the well-researched challenges of distributed systems, particularly the incompatibility of consistency, availability and partition tolerance [Gilbert2002] apply.

Byzantine Fault Tolerance

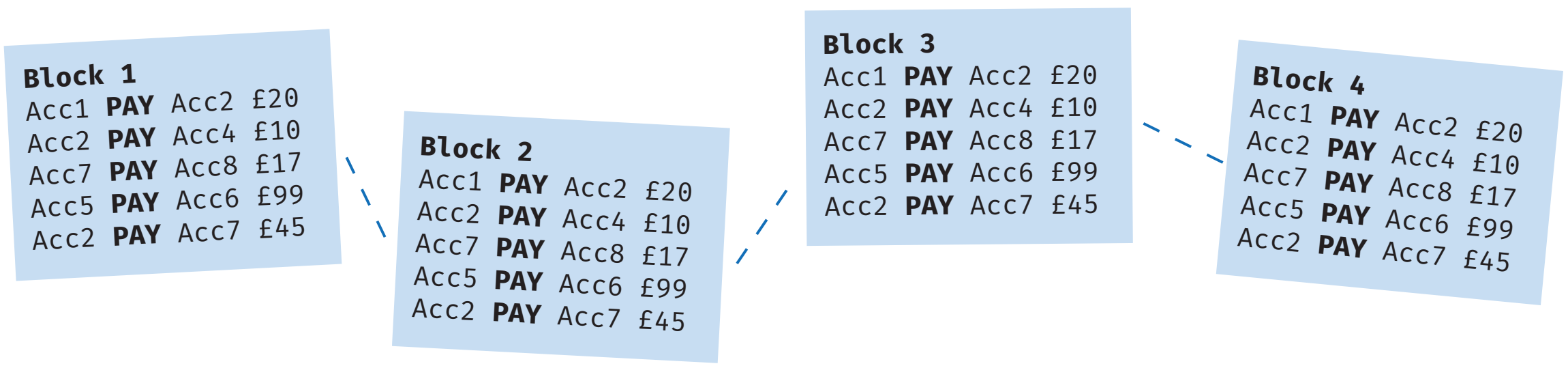
The challenges in a distributed system with potentially distrusting participants go further though. The 'Byzantine Generals Problem' [Lamport1982] describes a problem in which a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan, i.e. whether to attack or to retreat. However, one or more of the troop leaders may be traitors who will try to confuse the others.
Lamport et. al. have shown that this scenario can absorb up to ⅓ malicious actors. This threshold also applies to Blockchain/Distributed Ledger Technology, i.e. no known system will be able to manage more than ⅓ malicious writers. While this is understood to be the theoretical threshold, different mechanisms to achieve consensus are in use.



Consensus as a Key Concept to Distributed Data Replication

Data on a Blockchain is grouped in *blocks*, each of which contains multiple *transactions*. Blocks are to be replicated over a 'Byzantine' network. This means that writers can act malicious in different ways:

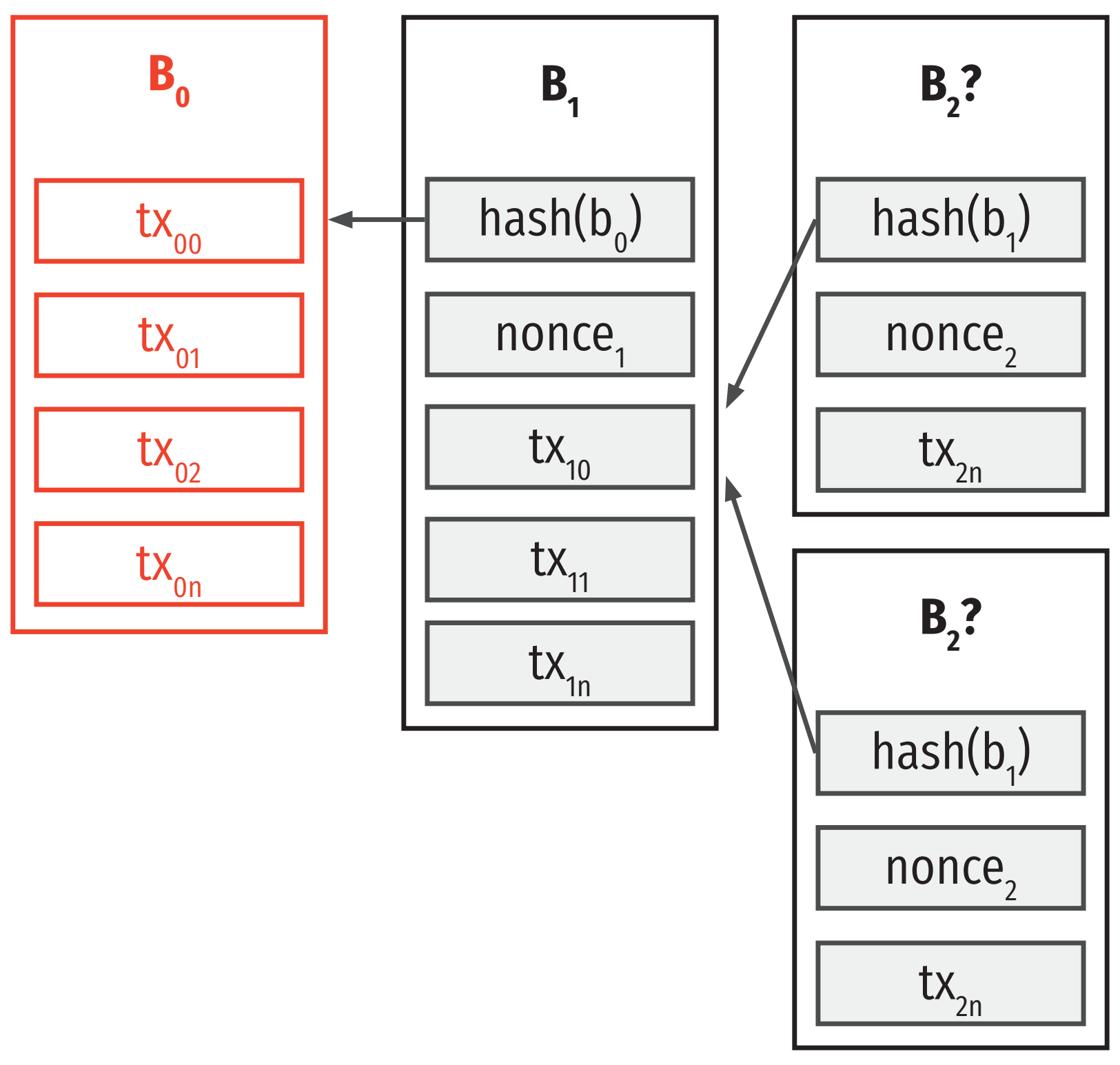
- ☐ Attempts to store incorrect/invalid transactions on the Blockchain
- ☐ Use one input state multiple times
- ☐ Censor the Blockchain by systematically withholding particular transactions



Similar to the 'Byzantine Generals Problem', participants on the network (representing the 'generals') must ensure the blocks they are presented with contain feasible information. They must also understand which block to treat as correct under uncertainty (i.e. when they are presented with alternative blocks).

Proof-of-Work

The original 'Bitcoin' electronic cash system, the first occurrence of a blockchain protocol, records transaction by 'by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work' [Nakamoto2008].
Participants have to earn the right to add a block to the existing chain of blocks by solving a computationally expensive challenge based on the content of the previous block.
There is no true finality in *Proof-of-Work*. The protocol dictates that clients accept the longest chain of blocks as the true representation of facts, but block creators can diverge at any given point by creating a 'fork' as long as they deliver proof of work. As such, finality is *probabilistic*, in that after a certain number of subsequent blocks have been created, a fork is considered to be very unlikely.



Proof-of-Stake

Here, as opposed to relying on solving computationally expensive tasks, the protocol will probabilistically determine who has the right to create the next block based on their 'stake' in the network. Stake is normally quantified by the amount of cryptocurrency a participant holds.

Participant	Holdings
Owner$_1$	💰💰💰💰💰💰💰💰
Owner$_2$	💰
Owner$_3$	💰💰💰💰
Owner$_4$	💰💰

Applying a naïve protocol to the holdings shown in the table would give Owner$_1$ a ~53% chance of being given the right to create a new block, Owner$_2$ would merely have a ~6.6% chance. Ultimately, finality is probabilistic in this use case as well.

Proof-of-Authority

Using pre-approved *validator* nodes, permissioned Blockchain systems using PoA can operate quicker by letting those nodes take turns approving transactions in blocks. This approach requires a nominated and approved consortium of validators to operate. It is thus more akin to a distributed database ran by multiple trusted third parties.

Contribution: Proof-of-Identity

Neither method is democratic in nature as they depend either on ownership of assets (PoS), on access to compute resources (PoW) or on pre-approval (PoA). I propose an extension to the 'Proof-of-Personhood' protocol [Borge2017] that uses a coloured coin approach to assign identity assertion levels to participants on the network.
Consider two hypothetical entities that have knowledge of the identity details of persons:
Issuer$_A$ and **Issuer$_B$**. Consider a Blockchain system in which Issuer$_A$ is the primary identity provider. Assume Person$_1$ and Person$_2$ are recognised by Issuer$_A$. This means they each hold an identity token issued by Issuer$_A$.

Participant	Identity Assertion
Person$_1$	●
Person$_2$	●

This identity assertion values now give the same rights to participate in consensus that 'stake' does in *Proof-of-Stake*. This means that both persons would have stake value 1 and would thus each have a 50% chance to create the next block. One of the novel aspects of the protocol is, that the set of allowed identity issuers is subject to on-ledger voting. Assuming that a vote is cast to add Issuer$_B$ and that this vote is successful (i.e. both Person$_1$ and Person$_2$ voted for it), persons with identity tokens issued by Issuer$_B$ could join the system.

Participant	Identity Assertion
Person$_1$	●
Person$_2$	●
Person$_3$	●

Furthermore, Participants can express mistrust towards individual issuers. For example, in situations where they suspect the identity issuer is acting maliciously. Assuming Person$_3$ expresses mistrust towards Issuer$_A$ through on-ledger voting, this would impact the value of all tokens issued by them in the amount of the share of network participants that expressed mistrust. In the above example that means that both identity assertion values for Person$_1$ and Person$_2$ would be negatively impacted. Going forward, they would only have stake value ~0.666 at their disposition.

Participant	Identity Assertion
Person$_1$	◕
Person$_2$	◕
Person$_3$	●

This simple example shows how an identity-based protocol could combine the benefits of a fully permissioned systems with those of a Proof-of-Stake based system. Various entities could serve as identity issuers in networks ranging from small to very large.

Gilbert, S. & Lynch, N.
Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-tolerant Web Services
SIGACT News, ACM, **2002**, 33, 51-59

Lamport, L.; Shostak, R. & Pease, M.
The Byzantine Generals Problem
ACM Trans. Program. Lang. Syst., ACM, **1982**, 4, 382-401

Nakamoto, S.
Bitcoin: A peer-to-peer electronic cash system
2008

Borge, M.; Kokoris-Kogias, E.; Jovanovic, P.; Gailly, N.; Gasser, L. & Ford, B.
Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies
1st IEEE Security and Privacy On The Blockchain, **2017**

Moritz Platt, PhD Student, Department of Informatics, King's College London
moritz.platt@kcl.ac.uk