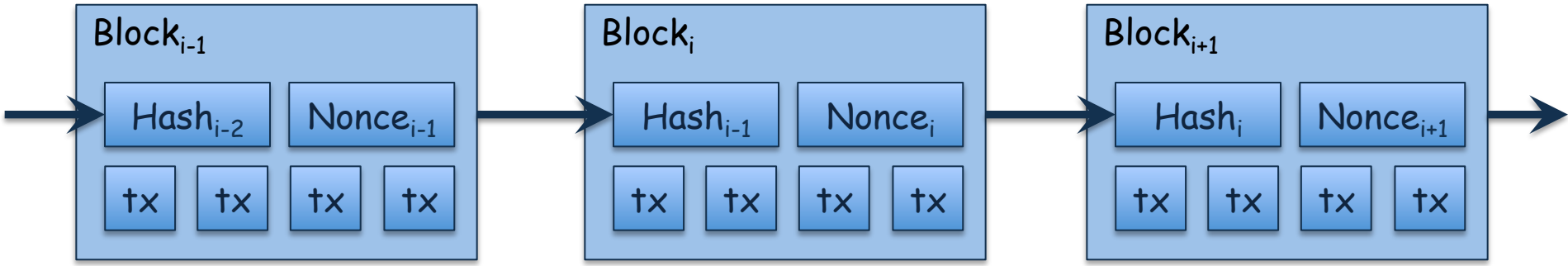
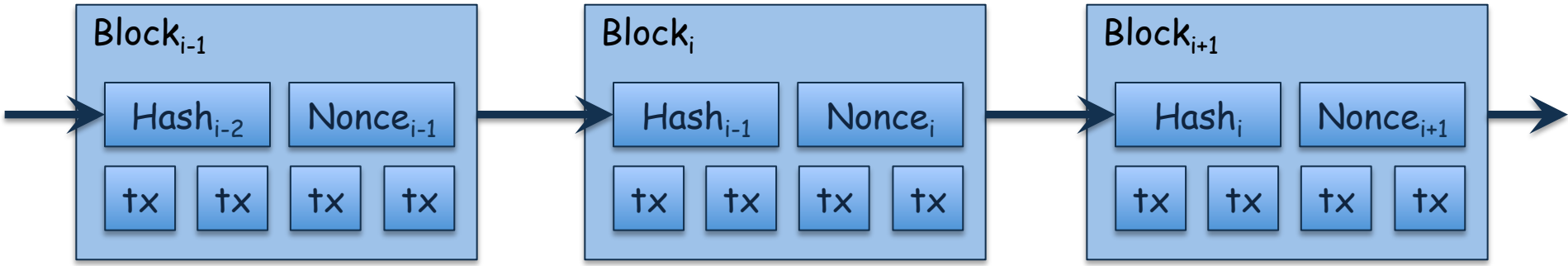
DPOS

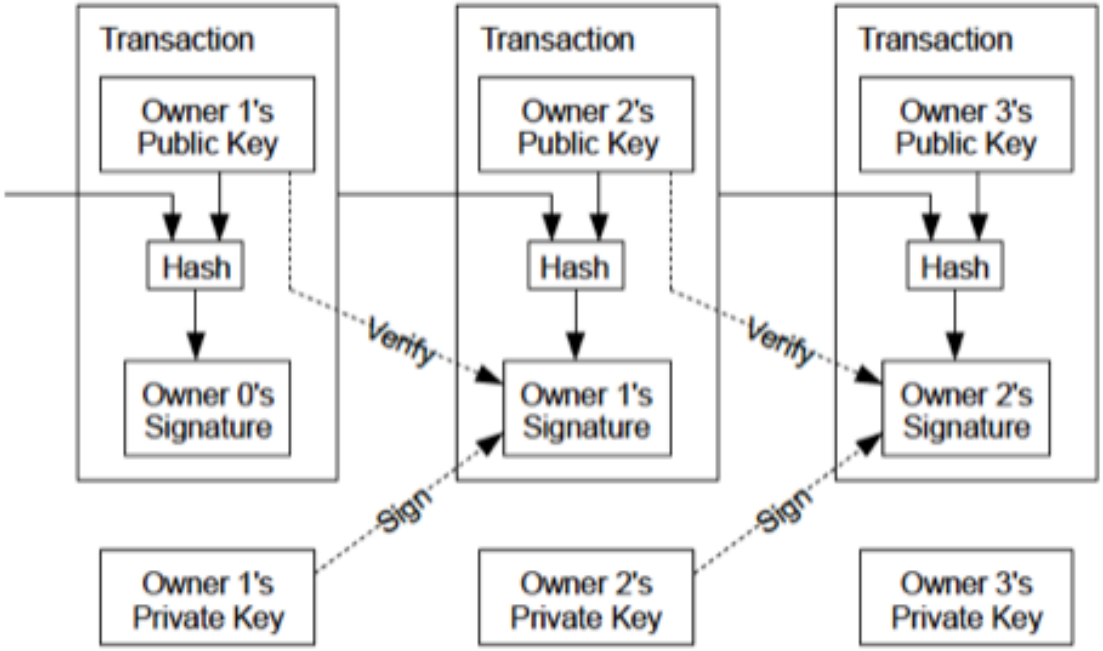
Murat Osmanoglu

Bitcoin


Block$_{i-1}$
Hash$_{i-2}$
Nonce$_{i-1}$
tx
tx
tx
tx
Block$_{i}$
Hash$_{i-1}$
Nonce$_{i}$
tx
tx
tx
tx
Block$_{i+1}$
Hash$_{i}$
Nonce$_{i+1}$
tx
tx
tx
tx

Bitcoin


Block$_{i-1}$
Hash$_{i-2}$
Nonce$_{i-1}$
tx tx tx tx
Block$_i$
Hash$_{i-1}$
Nonce$_i$
tx tx tx tx
Block$_{i+1}$
Hash$_i$
Nonce$_{i+1}$
tx tx tx tx


Transaction
Owner 1's Public Key
Hash
Owner 0's Signature
Transaction
Owner 2's Public Key
Hash
Owner 1's Signature
Transaction
Owner 3's Public Key
Hash
Owner 2's Signature
Verify
Verify
Sign
Sign
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

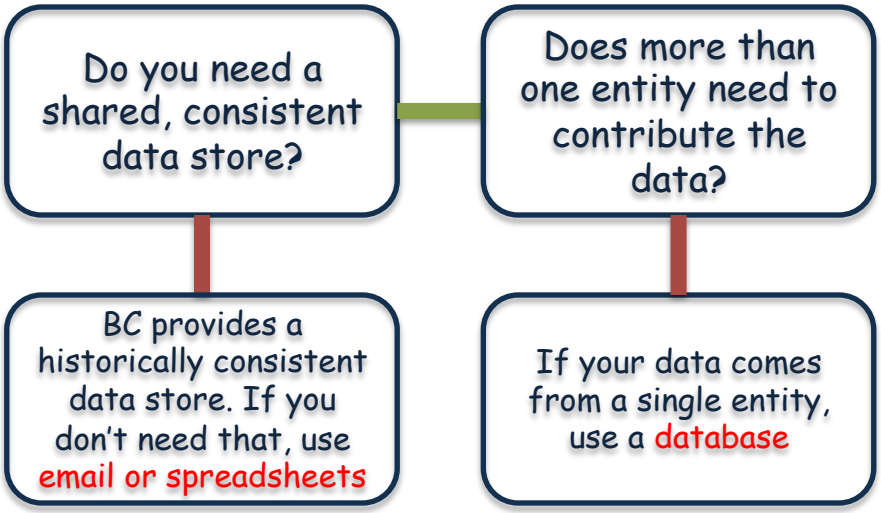
Do you really need a Blockchain?

Do you really need a Blockchain?

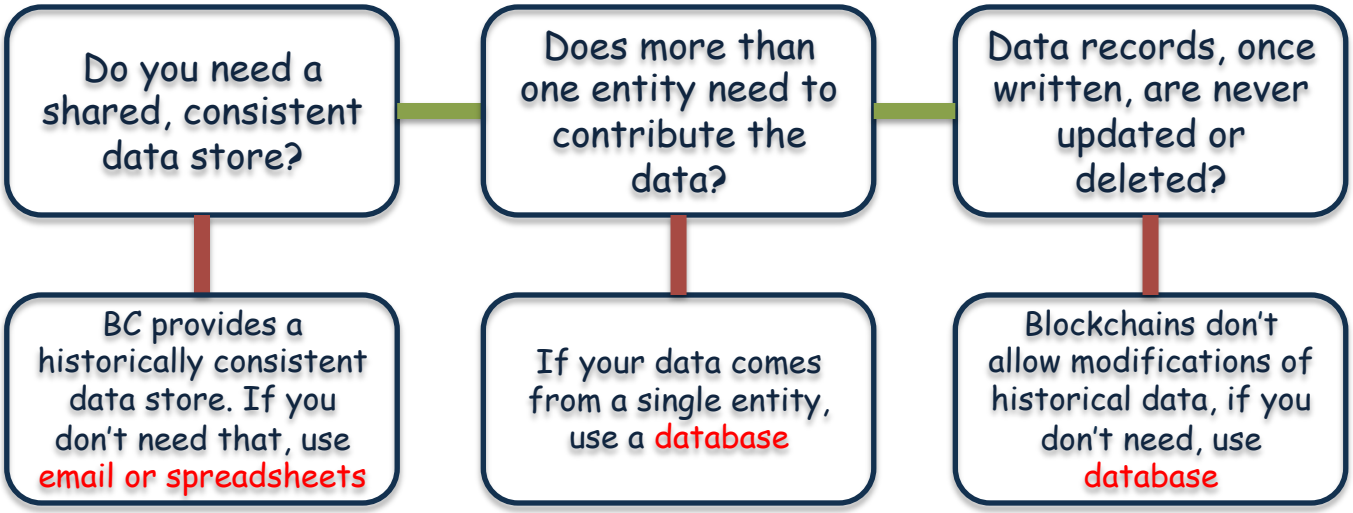
Do you need a shared, consistent data store?

BC provides a historically consistent data store. If you don't need that, use email or spreadsheets

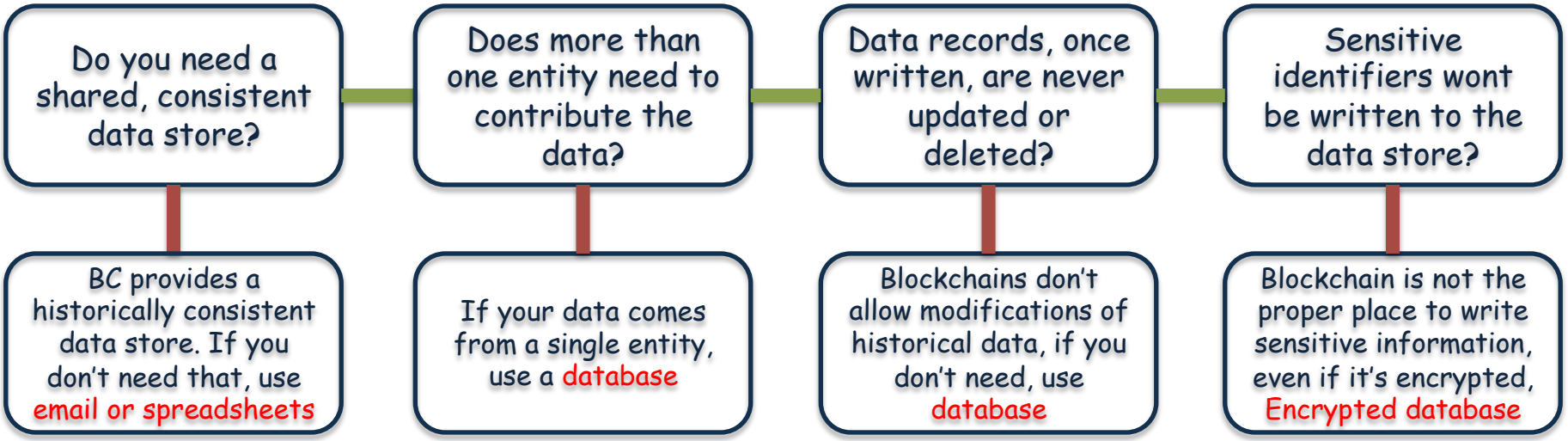
Do you really need a Blockchain?



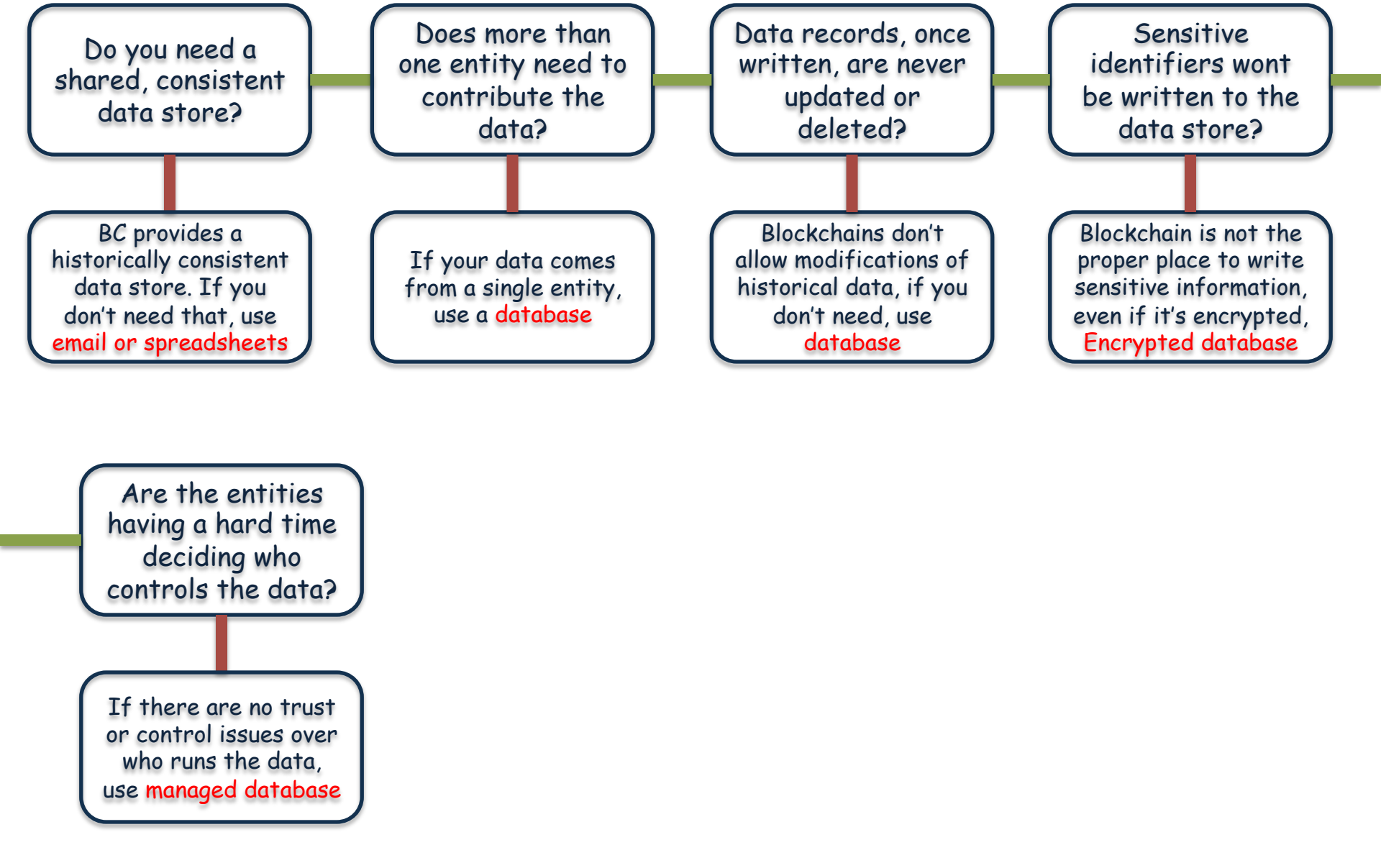
Do you really need a Blockchain?



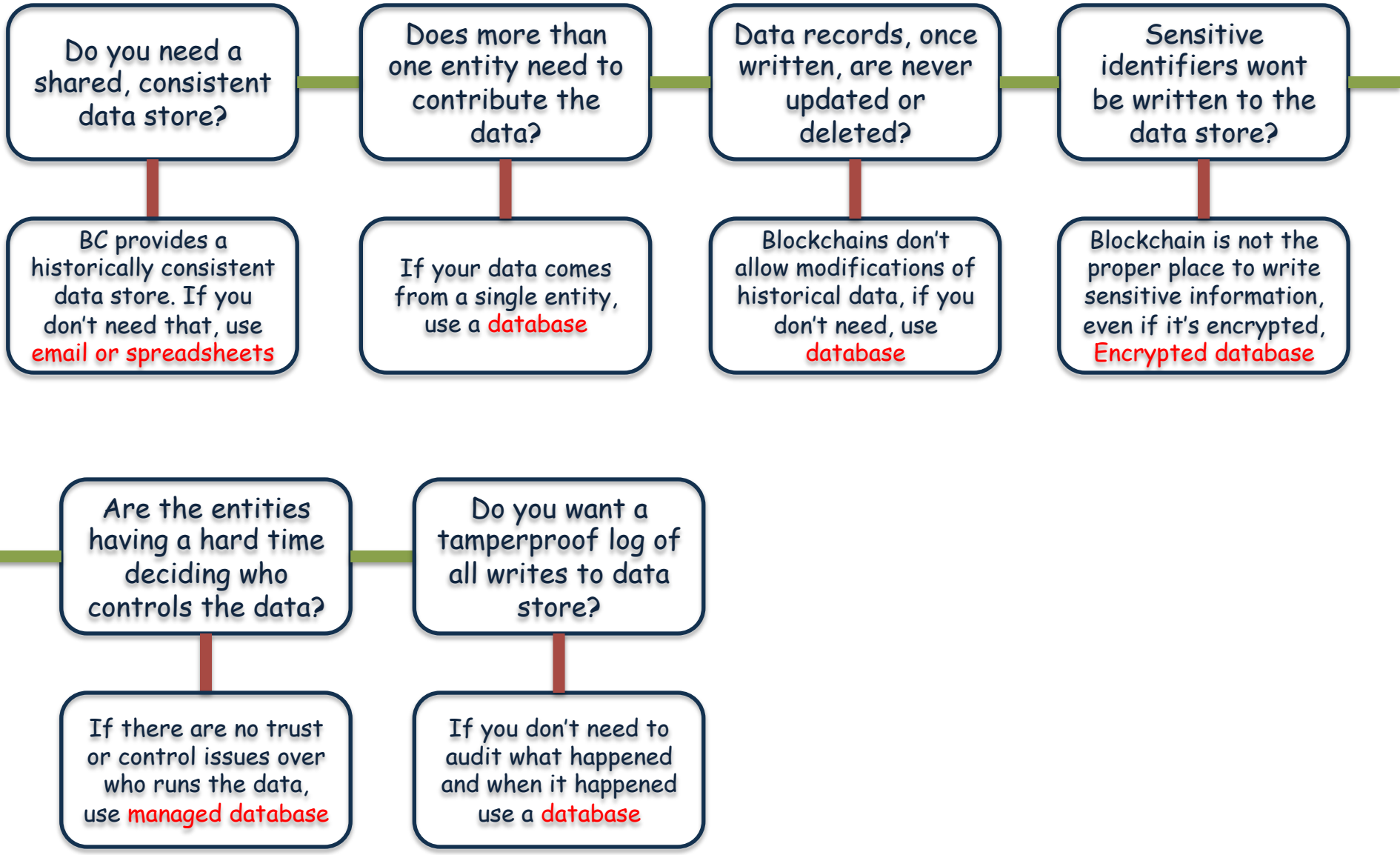
Do you really need a Blockchain?



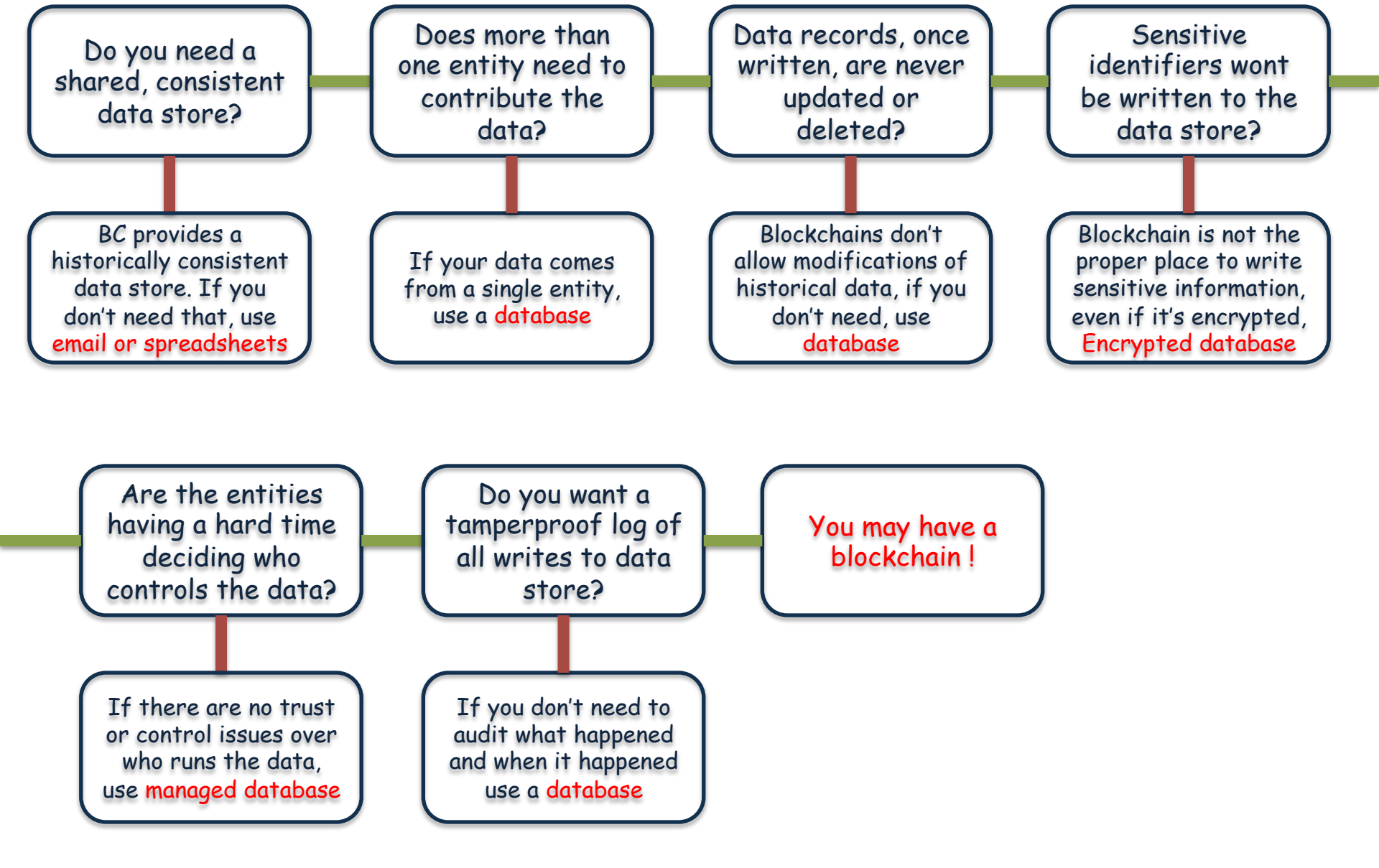
Do you really need a Blockchain?



Do you really need a Blockchain?



Do you really need a Blockchain?



Democracy

Democracy

Forms of Government

- Autocracy – rule of the one
- Oligarchy – rule of the few
- Democracy – rule of the majority

Democracy

Forms of Government

- Autocracy – rule of the one

autos(self) + kratos(to rule)

- Oligarchy – rule of the few

oligos(few) + arkho(to rule)

- Democracy – rule of the majority

demos(people) + kratos(to rule)

Democracy

Democracy

- best way to ensure that an organization serves the interests of all its members fairly and equitably is to spread the ultimate power of decision and action evenly among all of its members

Democracy

- best way to ensure that an organization serves the interests of all its members fairly and equitably is to spread the ultimate power of decision and action evenly among all of its members

  but how the agreement be achieved on making rules or taking actions in the case of inevitable disagreements, conflict of interest, and varying levels of time, knowledge, and abilities among members

Democracy

- best way to ensure that an organization serves the interests of all its members fairly and equitably is to spread the ultimate power of decision and action evenly among all of its members

  but how the agreement be achieved on making rules or taking actions in the case of inevitable disagreements, conflict of interest, and varying levels of time, knowledge, and abilities among members

- voting is the key component in decision-making

Democracy

- best way to ensure that an organization serves the interests of all its members fairly and equitably is to spread the ultimate power of decision and action evenly among all of its members

  but how the agreement be achieved on making rules or taking actions in the case of inevitable disagreements, conflict of interest, and varying levels of time, knowledge, and abilities among members

- voting is the key component in decision-making

  voting used for the purpose of making decisions or electing representatives ?

Democracy

- best way to ensure that an organization serves the interests of all its members fairly and equitably is to spread the ultimate power of decision and action evenly among all of its members

  but how the agreement be achieved on making rules or taking actions in the case of inevitable disagreements, conflict of interest, and varying levels of time, knowledge, and abilities among members

- voting is the key component in decision-making

  voting used for the purpose of making decisions or electing representatives ?

  direct democracy and representative democracy

Democracy

Direct Democracy

Democracy

Direct Democracy

- to ensure maximum equality and fairness, all members for an organization should directly get involved in all important decision-making processes

Democracy

Direct Democracy

- to ensure maximum equality and fairness, all members for an organization should directly get involved in all important decision-making processes

- may not be possible for big organizations such as state or country

Democracy

Direct Democracy

- to ensure maximum equality and fairness, all members for an organization should directly get involved in all important decision-making processes
- may not be possible for big organizations such as state or country
- Even if is feasible, it may not be desirable

Democracy

Direct Democracy

- to ensure maximum equality and fairness, all members for an organization should directly get involved in all important decision-making processes
- may not be possible for big organizations such as state or country
- Even if is feasible, it may not be desirable

  there is a wide variance in knowledge, interests, and abilities among the members of an organization.
  if the influence of each member is equal, the effective wisdom of collective may not be better than the average
  even it can be worse than average if that is the aggregation of conflicting policies

Democracy

Representative Democracy

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy
  but a powerful minority may take over the power for a long period of time

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy
  but a powerful minority may take over the power for a long period of time
- it may promise proportional representation along certain lines (geographic),

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy
  but a powerful minority may take over the power for a long period of time
- it may promise proportional representation along certain lines (geographic),
  but may also incline disproportionalities along different lines (ethnic, racial, gender)

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy
  but a powerful minority may take over the power for a long period of time
- it may promise proportional representation along certain lines (geographic),
  but may also incline disproportionalities along different lines (ethnic, racial, gender)
- full-time positions for the representatives (nothing for the losers),

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy
  but a powerful minority may take over the power for a long period of time
- it may promise proportional representation along certain lines (geographic),
  but may also incline disproportionalities along different lines (ethnic, racial, gender)
- full-time positions for the representatives (nothing for the losers),
  smaller body is less costly to maintain, and more efficient to act

Democracy

Representative Democracy

- relatively small number of people are elected by the members to make decisions on their behalf
- it creates stability or cohesiveness of policy
  but a powerful minority may take over the power for a long period of time
- it may promise proportional representation along certain lines (geographic),
  but may also incline disproportionalities along different lines (ethnic, racial, gender)
- full-time positions for the representatives (nothing for the losers),
  smaller body is less costly to maintain, and more efficient to act

  larger body is better to establish close relationship between the members and the representatives, and better in terms of reflecting the overall decision

Democracy

Delegative Democracy (or Liquid Democracy)

Democracy

Delegative Democracy (or Liquid Democracy)

- The members of the organization should have the widest possible direct choice of representatives

Democracy

Delegative Democracy (or Liquid Democracy)

- The members of the organization should have the widest possible direct choice of representatives
- They may build close relationships with their representatives

Democracy

Delegative Democracy (or Liquid Democracy)

- The members of the organization should have the widest possible direct choice of representatives
- They may build close relationships with their representatives
- No specific limit on the number of representatives

Democracy

Delegative Democracy (or Liquid Democracy)

- The members of the organization should have the widest possible direct choice of representatives
- They may build close relationships with their representatives
- No specific limit on the number of representatives
- Delegates don't have to compete with each other as in representative democracy
  They may compete to get votes from the members, but they don't win or loose seats

Democracy

Delegative Democracy (or Liquid Democracy)

- The members of the organization should have the widest possible direct choice of representatives
- They may build close relationships with their representatives
- No specific limit on the number of representatives
- Delegates don't have to compete with each other as in representative democracy
  They may compete to get votes from the members, but they don't win or loose seats
- As a member, there is no need to study candidates or party programs,
  just delegating your vote to someone you trust

Democracy

Delegative Democracy (or Liquid Democracy)

Democracy

Delegative Democracy (or Liquid Democracy)

- is there any upper bound for the number of members a delegate can represent ?

Democracy

Delegative Democracy (or Liquid Democracy)

- is there any upper bound for the number of members a delegate can represent ?

- How do we maintain such body?(the cost of the maintenance?)

Democracy

Delegative Democracy (or Liquid Democracy)

- is there any upper bound for the number of members a delegate can represent ?
- How do we maintain such body?(the cost of the maintenance?)
- How do we implement the voting process ?

Democracy

Delegative Democracy (or Liquid Democracy)

- is there any upper bound for the number of members a delegate can represent ?
- How do we maintain such body?(the cost of the maintenance?)
- How do we implement the voting process ?
- How do we implement the decision-making process among the delegates ?

Delegated Proof of Stake

(Ouroboros)

Delegated Proof of Stake
(Ouroboros)

- to be able to create blocks, stakeholders must be online, but this is not attractive for the one having small stake

Delegated Proof of Stake
(Ouroboros)

- to be able to create blocks, stakeholders must be online, but this is not attractive for the one having small stake
- to be able generate fresh randomness for the leader election, majority of the elected stakeholders should participate in MPC protocol, that creates a strain on the network

Delegated Proof of Stake
(Ouroboros)

- to be able to create blocks, stakeholders must be online, but this is not attractive for the one having small stake
- to be able generate fresh randomness for the leader election, majority of the elected stakeholders should participate in MPC protocol, that creates a strain on the network
- stakeholders will authorize other stakeholders to create blocks on their behalf and to represent them in leader election

Delegated Proof of Stake
(Ouroboros)

- to be able to create blocks, stakeholders must be online, but this is not attractive for the one having small stake
- to be able generate fresh randomness for the leader election, majority of the elected stakeholders should participate in MPC protocol, that creates a strain on the network
- stakeholders will authorize other stakeholders to create blocks on their behalf and to represent them in leader election
- a delegate may join in the protocol only if he represents a number of stakeholders whose stake exceeds a given threshold

Delegated Proof of Stake
(Ouroboros)

- to be able to create blocks, stakeholders must be online, but this is not attractive for the one having small stake
- to be able generate fresh randomness for the leader election, majority of the elected stakeholders should participate in MPC protocol, that creates a strain on the network
- stakeholders will authorize other stakeholders to create blocks on their behalf and to represent them in leader election
- a delegate may join in the protocol only if he represents a number of stakeholders whose stake exceeds a given threshold

  Setting a threshold value avoids the fragmentation attack that aims to increase the delegate population in order to damage the performance

Delegated Proof of Stake
(Ouroboros)

- any stakeholder can authorize a delegate to generate blocks on his behalf by utilizing a proxy signature scheme

Delegated Proof of Stake
(Ouroboros)

- any stakeholder can authorize a delegate to generate blocks on his behalf by utilizing a proxy signature scheme

  proxy signature enables someone (original signer) to delegate another one (proxy signer) to sign messages on his behalf, in case of temporal absence, lack of time, or computational power

Delegated Proof of Stake
(Ouroboros)

- any stakeholder can authorize a delegate to generate blocks on his behalf by utilizing a proxy signature scheme

  proxy signature enables someone (original signer) to delegate another one (proxy signer) to sign messages on his behalf, in case of temporal absence, lack of time, or computational power

- to limit the block generation power of the delegate to a certain range (slots or epoch), the stakeholder can put a limit on the message space

Delegated Proof of Stake
(Ouroboros)

- any stakeholder can authorize a delegate to generate blocks on his behalf by utilizing a proxy signature scheme

  proxy signature enables someone (original signer) to delegate another one (proxy signer) to sign messages on his behalf, in case of temporal absence, lack of time, or computational power

- to limit the block generation power of the delegate to a certain range (slots or epoch), the stakeholder can put a limit on the message space

  the proxy can only sign the message ending with a slot number sl_j

Delegated Proof of Stake

(Larimer)

Delegated Proof of Stake
(Larimer)

- every participant may delegate his voting power to a representative.

Delegated Proof of Stake
(Larimer)

- every participant may delegate his voting power to a representative.

- top 100 representatives holding the total votes take turns to generate the next 100 blocks on defined schedule

Delegated Proof of Stake
(Larimer)

- every participant may delegate his voting power to a representative.
- top 100 representatives holding the total votes take turns to generate the next 100 blocks on defined schedule
- all representatives earn equal amount of money which is 10% of the transaction fees included in the average block

Delegated Proof of Stake
(Larimer)

- every participant may delegate his voting power to a representative.
- top 100 representatives holding the total votes take turns to generate the next 100 blocks on defined schedule
- all representatives earn equal amount of money which is 10% of the transaction fees included in the average block
- if one of the representatives do not produce block, then this slot is skipped, and the protocol will continue with the next representative

Delegated Proof of Stake
(Larimer)

- every wallet has a preference window that enables users to choose one or more representatives to vote

Delegated Proof of Stake
(Larimer)

- every wallet has a preference window that enables users to choose one or more representatives to vote

- once decided, user creates a transaction to transfer votes to the representative without a fee

Delegated Proof of Stake
(Larimer)

- every wallet has a preference window that enables users to choose one or more representatives to vote
- once decided, user creates a transaction to transfer votes to the representative without a fee
- users can also monitor their representatives through their wallet, and change them according to the performance

Delegated Proof of Stake
(Larimer)

- every wallet has a preference window that enables users to choose one or more representatives to vote
- once decided, user creates a transaction to transfer votes to the representative without a fee
- users can also monitor their representatives through their wallet, and change them according to the performance
- as long as more than half of the scheduled 100 blocks are produced after a transaction is broadcasted, then this transaction assumed to be on the majority fork.

Delegated Proof of Stake
(Larimer)

- any transaction approved by even one of the representative can be included in the ledger in less than 30 min (block produced in 30 seconds)

Delegated Proof of Stake
(Larimer)

- any transaction approved by even one of the representative can be included in the ledger in less than 30 min (block produced in 30 seconds)

  so none of the representatives can benefit by excluding transactions that for the other representatives

Delegated Proof of Stake
(Larimer)

- any transaction approved by even one of the representative can be included in the ledger in less than 30 min (block produced in 30 seconds)

  so none of the representatives can benefit by excluding transactions that for the other representatives

- top 100 are given equal weight regardless of votes delegated to them.

Delegated Proof of Stake
(Larimer)

- any transaction approved by even one of the representative can be included in the ledger in less than 30 min (block produced in 30 seconds)

  so none of the representatives can benefit by excluding transactions that for the other representatives

- top 100 are given equal weight regardless of votes delegated to them.

  One representative may control multiple representatives, even more than half since the votes may not be distributed equally. it can quickly be identified, and eliminated