A Plural Voting Design for Cardano's Delegated Representativesusing Hyper-Plutocratic Depositsfor Sybil Resistance

Analysis of a DReps votes as a function of Delegation, Deposit, and Wallets

by Kenric Nelson

July 4, 2023

revision 07/05/2023: made deposit multiplier equal to (minDelegate)$^{0.25}$

This is a draft document that has not been reviewed. It is being release to allow the Cardano community to examine the proposed design prior to the Voltaire Workshop on July 11, 2023.

CIP - 1694 proposes one coin one vote (1c1v) as the process for Delegated Representative (DRep) voting for Cardano governance. Unfortunately, 1c1v cannot support the claim that Cardano is building a decentralized governance, since power-law distributions of wealth and nonlinear increases in influence with votes result in centralized concentration of voting power. In fact, corporate governance research, which uses one share one vote (1s1v), indicates that only 10%-20% of widely held shares are necessary to control the decision-making; hence, the democratic requirement for disclosure of owners with greater than 10% of shares.

Glenn Weyl invented an alternative voting method known as Plural or Quadratic Voting. It has has been implemented in both democratic (one person one vote 1 p1v) and corporate (one share one vote 1 s1v) settings. Plural Voting offsets the nonlinear increases in voting power by weighting votes by the square-root of the resource, in Cardano's case ADA coins. The full implementation of Plural Voting involves additional procedures, but a preliminary implementation for Cardano's Voltaire governance would simply apply the square-root of the ADA delegated to a DRep.

Plural Voting requires control against splitting voting weight across multiple wallets. This is usually accomplished through identity validation; however, use of self-sovereign identity is not being considered for the Cardano Minimal Viable Governance (MVG). Therefore, there is a need to design a method of Sybil resistance that does not require identity. There is in fact research deweighting wallets that have a high degree of correlation; and measures of community contribution by wallet are possible. These methods have merit but would require lengthy analysis to properly implement.

Defined and analyzed here is a method of Sybil resistance using a DReps deposit to control against the benefit of wallet splitting. By limiting a DReps votes based on the square of their deposit, the deposit weight acts in a hyper-plutocratic manner. The DRep votes is the minimum of the Plural votes from the delegates and the hyper-plutocratic votes of their deposit. This creates a competitive situation in which delegates seek to spread their delegation across many wallets, while DReps seek to concentrate the delegation into one wallet.

Aligning these two factors requires a normalization of the deposit function. Thus votesDeposit = ((minimum Delegate)$^{0.25}$ (deposit per wallet)/(minimum Deposit))^2. In the examples below minDeposit = 500 ADA, like the current Catalyst program. The minDelegate = 100,000 ADA, which is part of the Sybil attack protection. There's no minimum on delegating to a pool but the pool must have a minum of 100,000 ADA. The minimum deposit and minimum delegate enables the DRep to have ~316 votes. Each increment of 10 ADA deposit adds another 100 votes which must be matched by an additional 10,000 ADA in delegation.

The analysis examines the effect of using multiple wallets. For modest deposits (~5000 ADA) and large delegates (~ 10^8) splitting the wallet reduces the number of votes. For smaller delegates (~ 10^6) there is some benefit to wallet splitting but only over a limited number of wallets after which there are diminishing votes. A solo Rep with assets of two billion who splits 10 million for deposits across ten thousand wallets and the rest into the delegate pools would achieve ~5×10^6 rather than the one wallet plural votes of ~ 40,000 votes. However, the initial implementation of Voltaire governance, as specified in Cardano Improvement Proposal (CIP) 1694, will restrict the selection of DReps to the 10,000 with the most delegates. Thus, the wealthy solo DRep trying to exploit the system with just 200 000 delegates per wallet would have additional restrictions on their participation.

DefinitionofVotingWeightFunction

In the defining functions, the delegate and deposit variables represent the totals across all the wallets used. minDelegate and minDeposit are the minimums for a wallet. For the examples shown, the minimums are set to 10 ADA and 500 ADA respectively. The delegatePower sets the type of voting process for the delegates; 0 is a democracy (1 wallet 1 vote), 1/2 is a Pluralism, and 1 is a plutocracy (1c1v). The default used in this analysis is Pluralism (1/2). The deposit power is powerDeposit/powerDelegate. The purpose of using the two variables is to allow powerDeposit =1 be the default, while providing the option to explore other possibilities. With powerDeposit = 1, the deposit is raised to the inverse power of the delegates. For the examples examined here this is 2; i.e. a hyper-plutocratic process.

The DRep Vote function is:

Votes = Min[DelegatedWeight, DepositWeight]

The delegate vote function is:

DelegateWeight =

$$\begin{cases} \left(\frac{\text{delegate}}{\text{wallets}}\right)^{\text{powerDelegate}} & \frac{\text{delegate}}{\text{wallets}} \geq \text{minDelegate} \\ 0 & \frac{\text{delegate}}{\text{wallets}} < \text{minDelegate} \end{cases}$$

The deposit vote function is:

DepositWeight =

$$\begin{cases} \left(\frac{10\ \text{deposit}}{\text{wallets}}\right)^{\frac{\text{powerDeposit}}{\text{powerDelegate}}} & \frac{\text{deposit}}{\text{wallets}} \geq \text{minDelegate} \\ 0 & \frac{\text{deposit}}{\text{wallets}} < \text{minDelegate} \end{cases}$$

The factor 10 is a constant rather than a variable because strictly speaking its not required; however, it seems more pragmatic for the minimum deposit to enable 100 votes rather than 1 vote. This could be examined in the future and removed as long as the DRep community understands that more than the minimum will be required to enable voting.

In[17]:=

```
Votes[delegate_, deposit_, minDelegate_,
   minDeposit_, wallets_, powerDelegate_ : 0.5, powerDeposit_ : 1] :=
  Min[DelegateWeight[delegate, minDelegate, wallets, powerDelegate],
   DepositWeight[deposit, minDelegate, minDeposit, wallets, powerDeposit]];
DelegateWeight[delegate_, minDelegate_, wallets_, powerDelegate_ : 0.5] :=
  wallets If[(delegate / wallets) ≥ minDelegate,
    (delegate / wallets)^powerDelegate, 0];
DepositWeight[deposit_, minDelegate_,
   minDeposit_, wallets_, powerDelegate_ : 0.5, powerDeposit_ : 2] :=
  wallets If[(deposit / wallets) ≥ minDeposit,
    ((minDelegate)^0.25 deposit / minDeposit / wallets)^(powerDeposit/powerDelegate), 0];
```

Analysis of Delegate & Deposit Weight

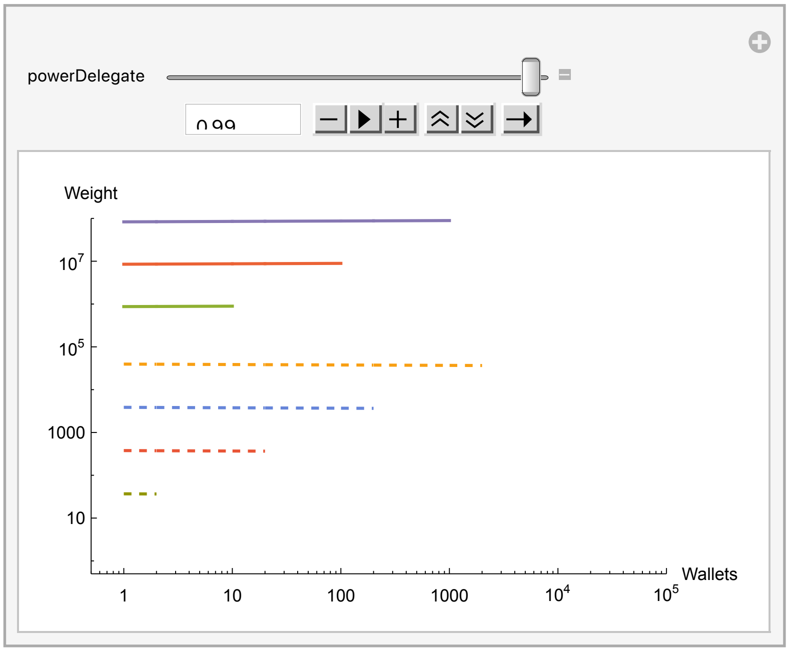
This log-log plot shows how the voting weight for the delegate and the deposit have opposite slopes as the number of wallets is increased. The intersection of a delegate and deposit line represents the maximum number of votes achievable by splitting delegate and deposit into multiple wallets.

The solid lines are the votes based on the delegate ADA. For 0 < powerDelegate < 1 these lines slope upward as the number wallets increases. The dashed lines are the votes based on the deposit ADA. For 0 < powerDelegate < 1 and powerDeposit = 1, these lines slope downward as the number of wallets increases.

In[29]:=

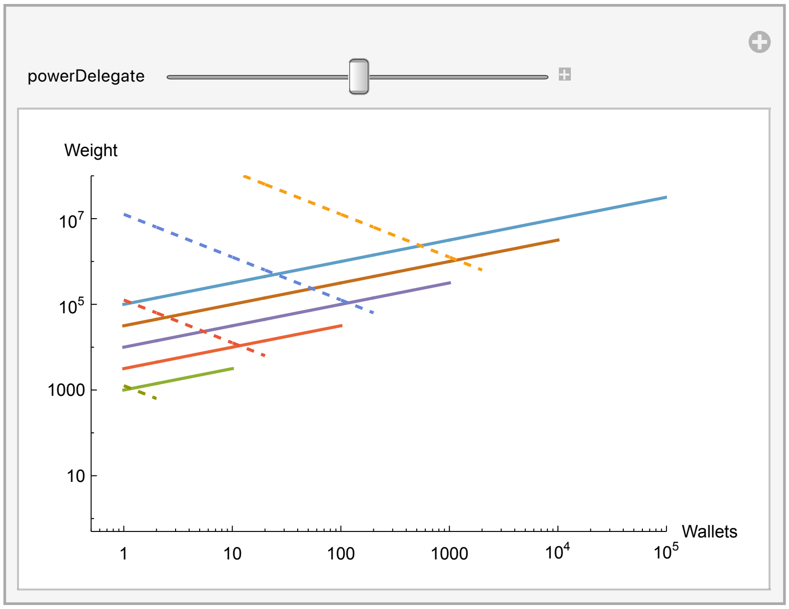
```
Manipulate[LogLogPlot[
  Evaluate[{
    Tooltip[DelegateWeight[#, 100 000, wallets, powerDelegate], #] & /@
     {10^4, 10^5, 10^6, 10^7, 10^8, 10^9, 10^10},
    Tooltip[DepositWeight[#, 100 000, 500 (*minDeposit*), wallets, powerDelegate,
        1 (*powerDeposit*)], #] & /@ {10, 10^2, 10^3, 10^4, 10^5, 10^6}}],
  {wallets, 1, 100 000},
  AxesLabel → {"Wallets", "Weight"},
  (*PlotLegends→SwatchLegend[{10^1,10^2,10^3,10^4,10^5},LegendLabel→"Deposited"],*)
  PlotRange → {{5 × 10^-1, 10^5}, {5 × 10^-1, 10^8}},
  PlotStyle → Flatten[{Table[Line, 7], Table[Dashed, 6]}]],
 {{powerDelegate, 0.5}, 0.01, .99}]
```

Out[29]=



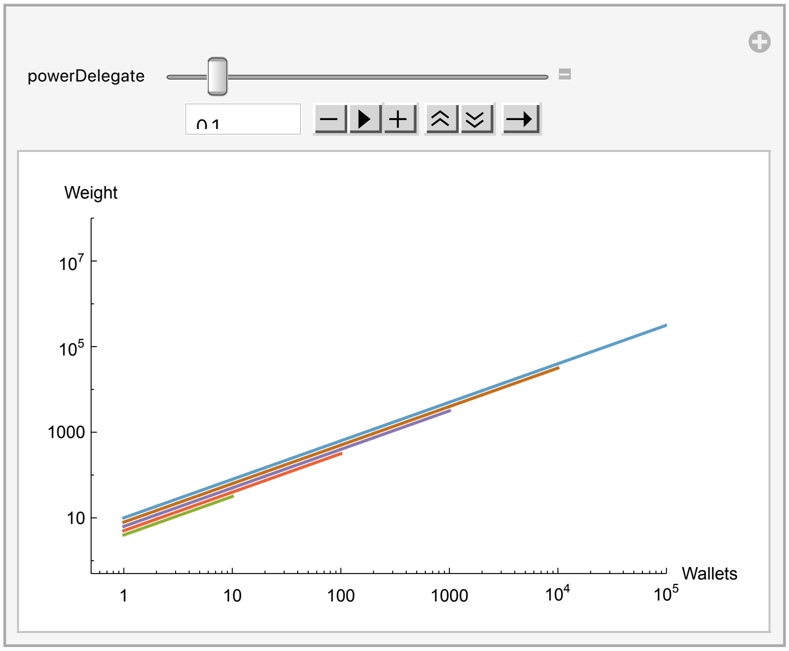
The default settings have overlap between the delegate and deposit weight, facilitating Sybil resistance in the range of 100 to 10^5 votes. The delegate lines (solid) shown range from 10^3 to 10^{10} by powers of 10. The deposit lines (dashed) range from 10^3 to 10^6 by powers of 10.

Out[•]=



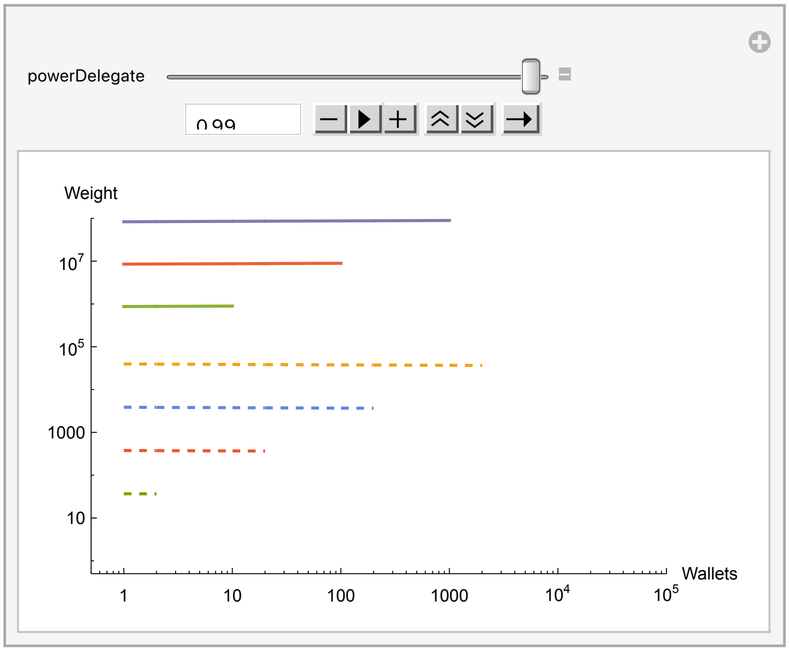
With powerDelegate = 0.1 the delegate voting is close to democratic (1w1v). The delegate line has a steeper slope and they are more closely spaced. The deposit lines are not visible in this plot but will have a close to vertical downward slope.

Out[•]=


powerDelegate 0.1

A powerDelegate = 0.99 is similar to 1c1v. In this design, the both the delegate deposit weight are plutocratic. Thus, the deposit is required to match the delegate. While this example isn't practical, the powerDeposit parameter could be used to modify the properties.

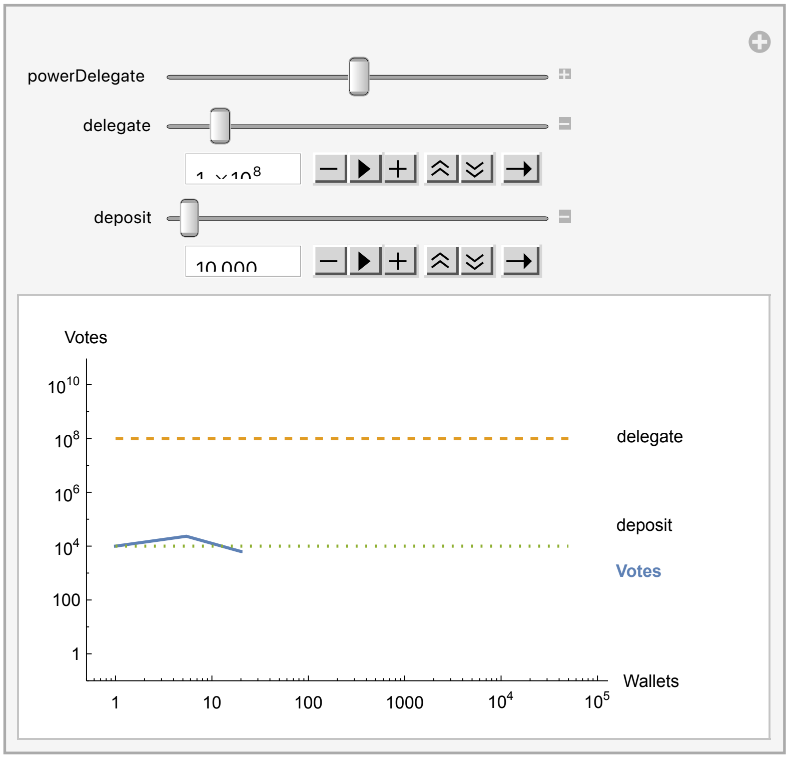
Out[ ]=



Analysis of DRep Votes using multiple wallets

```
In[23]:= minDelegateforPlot = 100 000;
         minDepositforPlot = 500;
         Manipulate[LogLogPlot[
            {Labeled[
              Votes[delegate, deposit, minDelegateforPlot,
               minDepositforPlot, wallets, powerDelegate, 1],
              Text[Style["Votes", {ColorData[97, 1], Bold}]]],
             Labeled[delegate, "delegate"],
             Labeled[deposit, "deposit"]},
            {wallets, 1, 50 000},
            AxesLabel → {"Wallets", "Votes"},
            (*PlotLegends→SwatchLegend[{10^1,10^2,10^3,10^4,10^5},LegendLabel→"Deposited"],*)
            PlotRange → {{5 × 10^-1, 10^5}, {10^-1, 10^10}},
            PlotStyle → {Line, Dashed, Dotted}],
          {{powerDelegate, 0.5}, 0.01, .99},
          {{delegate, 10^7}, 10^4, 10^9},
          {{deposit, 5 × 10^3}, minDepositforPlot, 10^6}]
```

Out[25]=



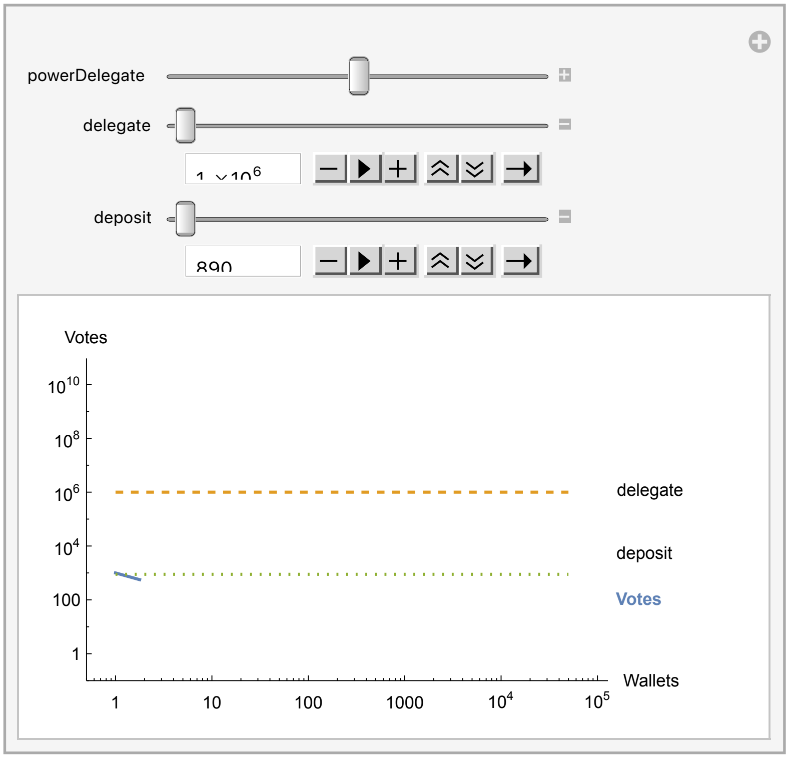
powerDelegate

delegate 1 × 10^8

deposit 10 000

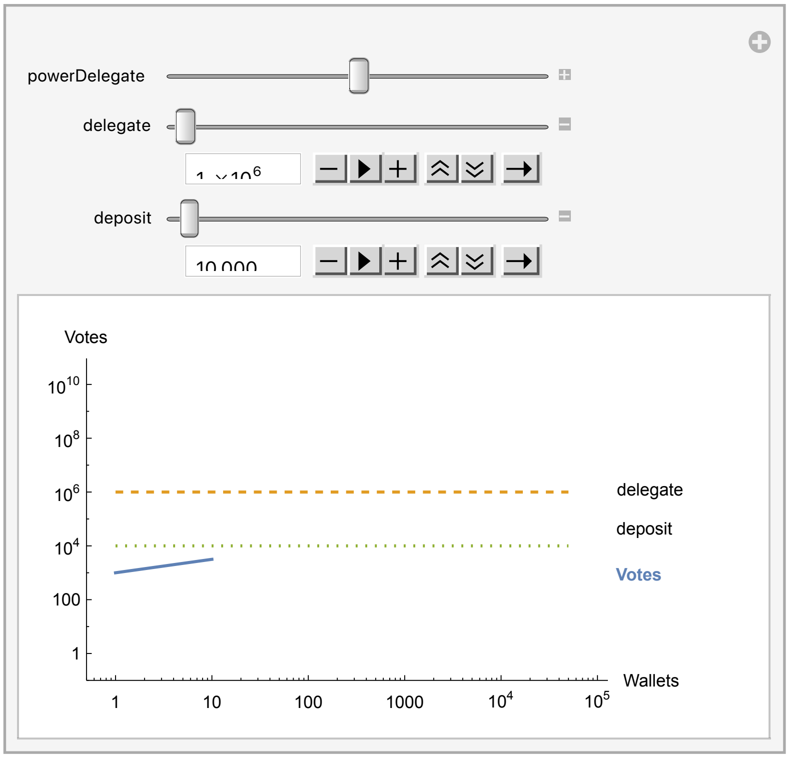
A DRep that can attract a modestly large delegation (10^6 ADA) and uses the minimum required deposit to support this delegation (890 ADA) has 1000 votes with one wallet. They would not have sufficient deposit to split to two wallets.

Out[ ]=



Even with an investment of 10,000 for the deposits, the maximum votes is limited to 10 wallets because of the minimum delegate requirement of 100,000.

Out[•]=



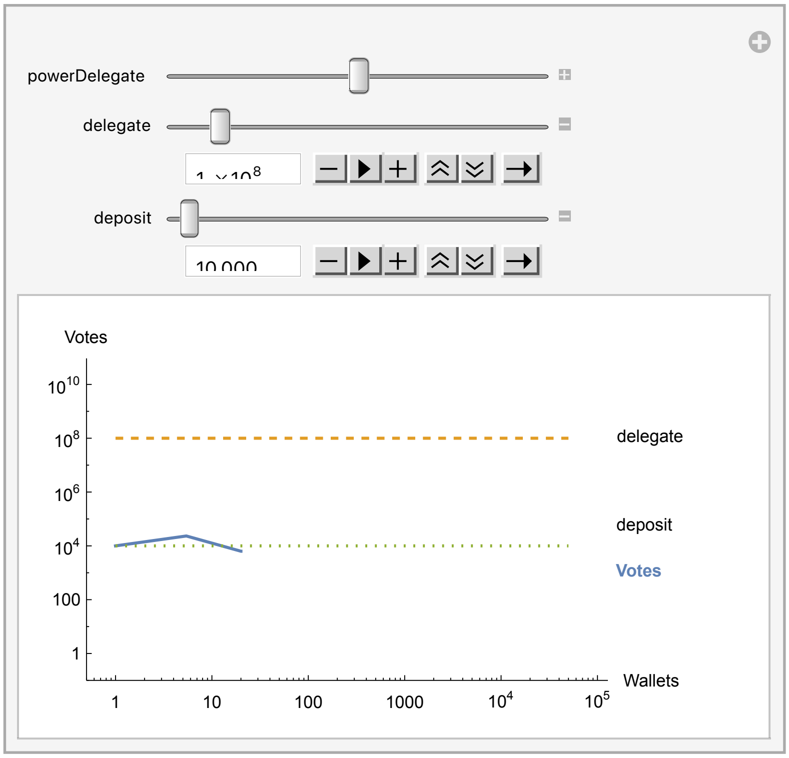
powerDelegate

delegate 1×10^6

deposit 10 000

Furthermore, if this DRep investing 10,000 ADA in deposits could increase their delegate to 100 million ADA, they would have to reduce the number of wallets used to improve their votes.

Out[∘]=



powerDelegate

delegate

1×10^8

deposit

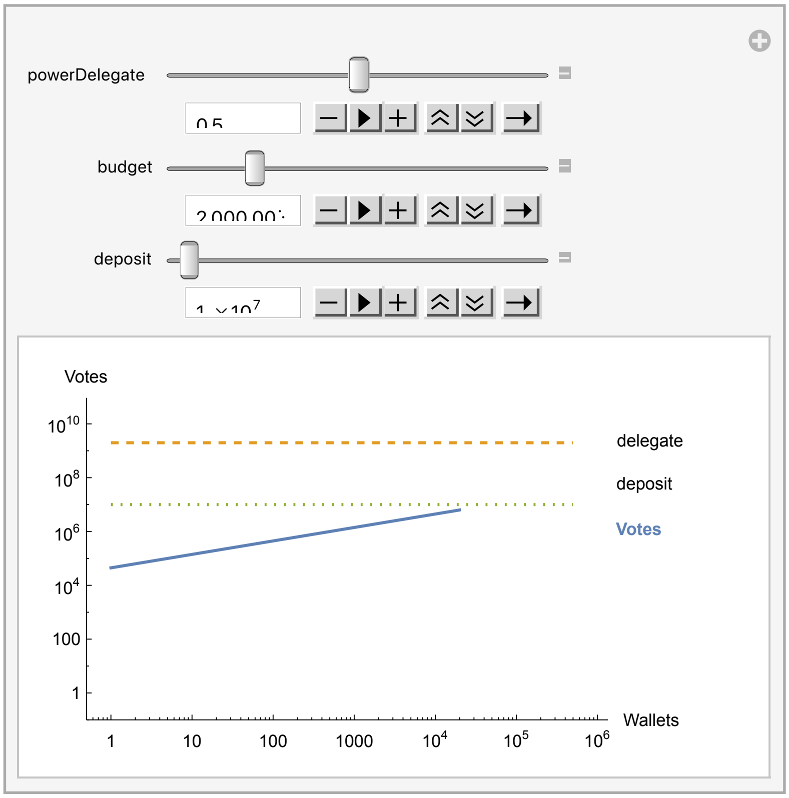
10 000

Analysis of solo DRep

Analysis of solo DRep

```
In[26]:= minDelegateforPlot = 100 000;
         minDepositforPlot = 500;
         Manipulate[
          delegate = budget - deposit;
          LogLogPlot[
            {Labeled[
               Votes[delegate, deposit, minDelegateforPlot,
                minDepositforPlot, wallets, powerDelegate, 1],
               Text[Style["Votes", {ColorData[97, 1], Bold}]]],
             Labeled[delegate, "delegate"],
             Labeled[deposit, "deposit"]},
            {wallets, 1, 500 000},
            AxesLabel → {"Wallets", "Votes"},
            (*PlotLegends→SwatchLegend[{10^1,10^2,10^3,10^4,10^5},LegendLabel→"Deposited"],*)
            PlotRange → {{5 × 10^-1, 10^6}, {10^-1, 10^10}},
            PlotStyle → {Line, Dashed, Dotted}],
          {{powerDelegate, 0.5}, 0.01, .99},
          {{budget, 10^6}, 10^6, 10^10},
          {{deposit, 1 × 10^3}, minDepositforPlot, 10^9}
         ]
```

Out[28]=

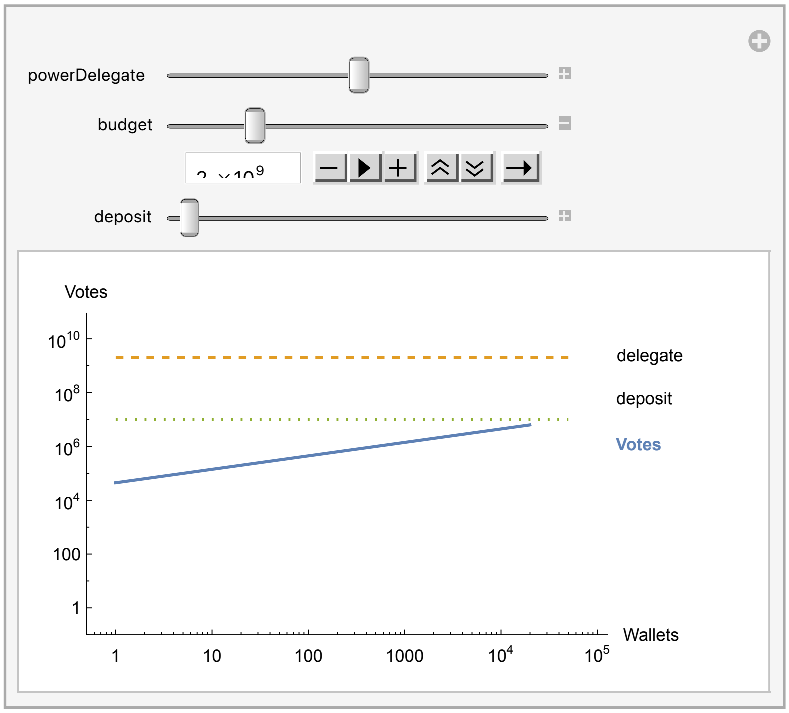


powerDelegate 0.5

budget 2,000,00

deposit 1×10^7

Out[ ]=

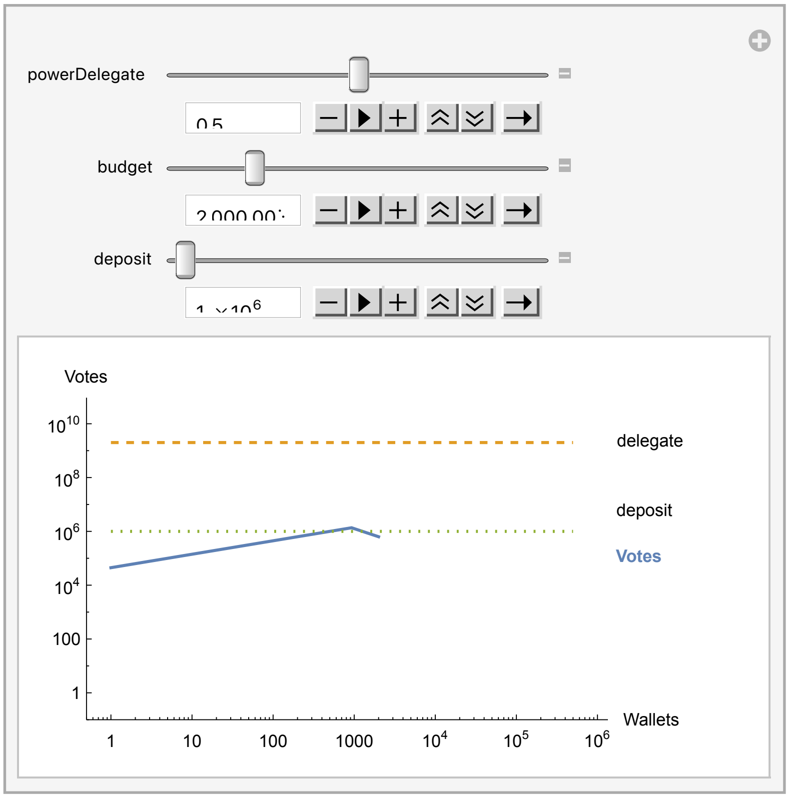


An important security question is whether a wealthy individual can run a large number of pools and thereby circumvent the Sybil resistance. The current supply of ADA is ~36 Billion. If there is 50% participation in DRep delegation and someone had 10% of the supply, that would be ~ 2 Billion ADA.

So let's examine an individual or institution with 2 billion ADA to place on the delegate pools and deposits across an unlimited number of DRep wallets.

If 1 million of the budget is applied to the deposits, the votes peaks at approximately 1000 wallets. The one wallet votes of 10^5increases to approximately 10^6. So there is only a factor of 10 increase despite the use of 1000 wallets. Each pool has approximately 5 million delegate ADA.

Out[•]=



powerDelegate 0.5

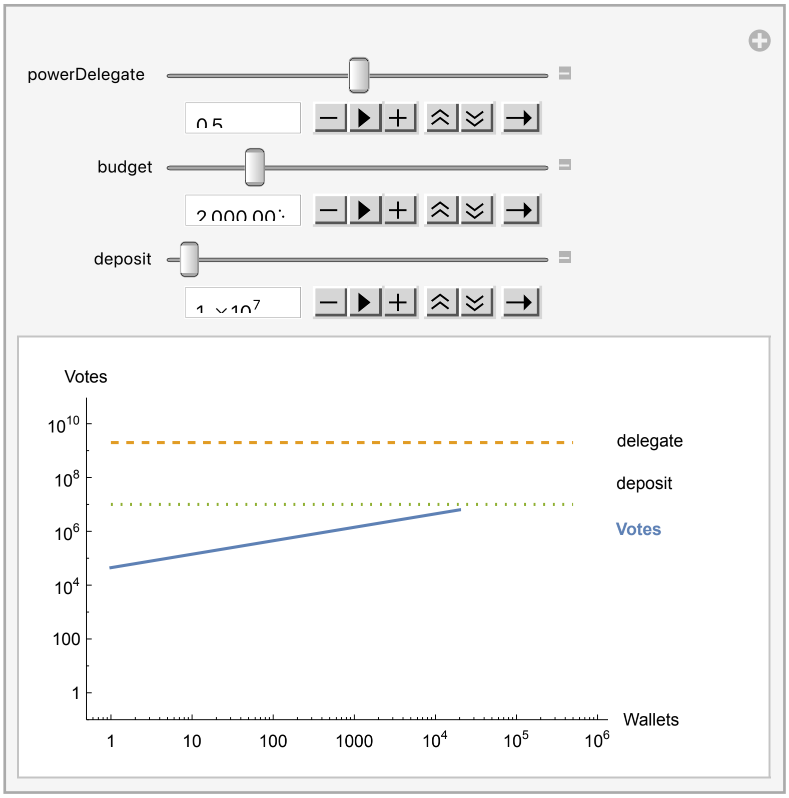
budget 2 000 00

deposit 1×10^6

If the investment in the deposit is increased to 10 million (and the delegate is therefore 2 billion - 10 million), the votes peak at approximately 20,000 wallets after which the votes go to zero because the minimum delegate per pool hasn't been met. The votes are 10^7 million, a factor of 100 over the single wallet votes and a factor of 200 less than the 1c1v solution. Across 20,000 wallets the delegation per wallet has dropped to 100,000.

If increased Sybil resistance is desired, this is easily achieved by increasing the minimum deposits.

Out[∘]=



powerDelegate 0.5

budget 2 000 00

deposit 1×10^7