參與式亂數生成機制是一種利用多個參與者的輸入來產生不可預測的亂數的方法，這樣做的好處是每位參與者只需要提供部分亂數，不需要知道其他參與者的亂數，從而保護了亂數的安全性。

實際應用場景包含區塊鏈。區塊鏈是一種分散式的資料庫，它需要多個節點之間達成一致，才能確認交易的有效性。為了避免惡意的節點攻擊或操縱系統，區塊鏈需要一種公平且不可預測的方式來選擇下一個區塊的產生者。

儘管有諸多好處，但參與式亂數生成機制需要多個參與者之間的協調和通訊，這可能增加了系統的複雜度和開銷。然而參與式亂數生成機制仍是一種提供更安全和可靠的重要技術。