Bitshares Poker

Online Poker- Reborn

- Centralized Online Poker Is Broken
  - **Quasi-Monopoly** – A few companies have quasi-monopolies which have a stranglehold on the industry, and do not usually have the players' best interests in mind.
    - **Higher Rake** – Limited competition results in higher rake due to free market principals.
    - **Low Standards** – Limited competition results in low standards as far as customer service and the policing of collusion and bots.
    - **The alternative** – A distributed version ran by the players for the players that have a better understanding of players' best interests.
  - **Government Interference**
    - **Oppression** – In many countries and jurisdictions worldwide (particularly in the USA, Middle East, and Asia) playing or servicing online poker to citizens is illegal, and therefore player access to online poker is limited due to government laws and regulations.
    - **"Ring fenced" gaming** – Many jurisdictions and countries have regulated online poker, but have limited the player pool to only their country or jurisdiction. This reduces the quality of the games and the number of games available for all players worldwide.
    - **Onerous taxation** – It is the players that end up paying for the taxes that governments force on legacy centralized poker networks as they will always "pass the buck" to the players.
    - **No oversight of government officials** – The sad reality of the situation is that the majority of people worldwide couldn't care less about online poker, which leaves the people who are in powerful government positions the power to do as they please in regards to the industry. They will likely remain in power no matter how bad of an online poker policy they support because the general republic (voters) don't care.
    - **Ineffective** – Even with government oversight many regulated sites have scammed players by stealing funds, cheating via the use of "superusers", or by other methods.
      - **Examples:**
        - **Curacao** – Lock poker
        - **Kahnawake Gaming Commission** – Absolute Poker, Ultimate Bet
        - **Malta Lotteries and Gaming Authority** – Everleaf Gaming, Stryyke, Eurolinx
  - **Limited or non-existent transparency**
    - **Cheating** – Centralized legacy online poker networks have been proven in the past to have cheated players via dishonest gameplay or turning a blind eye to dishonest play.
      - **Unprovable** – There is no way to prove that it is not still happening to this day (or could happen in the future.) Due to limited oversight and the fact legacy poker networks are centralized, most hand history data is kept private so there is no way for the public to prove that they are not cheating players or policing the games effectively.
      - **Prior cheating scandals** – Ultimate Bet, Absolute Poker, PitBull Poker, and all of the poker networks that turn a blind eye towards bots.
    - **Accounting** – With no transparency it is easy for centralized legacy poker networks to misappropriate players' funds with Quasi-Ponzi schemes.
      - **Prior cases** – Full Tilt Poker, BetOnSports, Etc. *(also likely many of the sites that "take the money and ran" – see below)*

        - **Players' best interest** – It is unknown how good a job legacy centralized poker networks do in combating collusion, multi-accounting, and bots as those data and statistics are kept to themselves.
            - **Prior cases** – Pokertropolis, Darren Woods, Brian Hastings, Etc., Etc. (too many cheating scandals to list that were player-discovered)
    - **Shady offshore companies** – Legacy centralized poker networks that service jurisdictions where online poker is illegal (or "grey markets") utilize off shore jurisdictions that will mostly turn a blind eye if they go bankrupt and stiff players. Therefore, shady offshore companies cannot be held accountable for their actions and there are no means of restitution for cheated players.
        - **Take the money and ran** – Many poker sites have run away with player funds in the past with little or (in most cases) no recourse.
            - **Prior cases** – Lock Poker, Absolute Poker, Ultimate Bet, Everleaf Gaming, Jet Set Poker, Stryyke, PitBull Poker, Pokerspot, Tusk Investments, and Eurolinx

- Decentralized Poker Is Hard (Impossible?)
    - **Efficiency of cryptographic computations** – Most mental poker protocols require many resource-intensive cryptographic operations. Which in turn slows down gameplay to a point that would be unacceptable, compared to the fluid gameplay that online poker players are accustomed to from legacy centralized poker networks. The only resource efficient mental poker algorithm that is capable of fast gameplay is the one I propose we use for Bitshares Poker, but it requires some trust in third parties and is not completely decentralized. Elected transparent witnesses will take the place of trusted third parties (centralized poker networks.)
    - **Drop out tolerance** – A majority of the mental poker protocols that have been designed break if a player disconnects from the game. The protocols that do not suffer from drop out tolerance still suffer as far as efficiency is concerned.
    - **Collusion and bots** – All cryptocurrencies that currently exist are irreversible, so you cannot build a decentralized cryptocurrency to build a decentralized poker network on top of. That would not allow for the means of restitution to players in more than two player games that were wronged from bots, collusion, and multi-accounting. A cryptocurrency needs to be tailor-made for this application to allow for the freezing and reversibility that is necessary to combat collusion. The only alternative the author can think of would be to pay players that were wronged out of rake and fees earned from the poker network, but after careful consideration this amounts to a quasi-Ponzi scheme (I say quasi because legitimate profit is still being made by main chain stakeholders.)
    - **Multi-Accounting** – There is no protection from Sybil attacks in a completely decentralized network as decentralized reputation systems are ineffective versus Sybil attacks. Centralized certificate authorities will need to partner with the decentralized poker networks to effectively combat multi-accounting.
    - **Compromise** – A compromise should be struck in between decentralization and centralization, to make a decentralized version of online poker that is transparent, secure, and efficient.
- Why Bitshares?
    - **Smart assets** – Stable in-game currency is a necessity to win over non-crypto currency users and to offer a stable gaming environment. Those that do not want to be exposed to the huge swings in cryptocurrency value should not have to be.
    - **Witnesses** – Elected witnesses (previously delegates) allow the decentralized poker network to hire employees to do a vast array of tasks for the poker network.
        - **Checks and Balances** – If witnesses are doing a poor job or are found to be dishonest, then they can be replaced by someone else that would be happy to step in and take their job and the profit from being an employee.
    - **Efficiency** – Bitshares utilizes the most efficient consensus algorithm in existence, Delegated Proof of Stake, which is important with a fast pace game such as poker that will require many transactions per second depending on the final design and volume of the poker network.

- **Referral Program** – A referral program is already built in to Bitshares 2.0 which will be essential to growing the poker room.
- **Most profitable Bitshares DAC** – I speculate a poker DAC that requires many transactions for record keeping and gameplay will be the most profitable Bitshares DAC in existence due to the number of transactions and communication needed. This is purely speculation and not investment advice, and I could be way off base, this is just the author's opinion. It really depends on the success and growth of the network.

- Distribution
  - **No IPO** – IPOs are the bane of crypto currency 2.0 projects and carry a negative stigma throughout the cryptocurrency community. It is intended that this project be designed and developed by a team of volunteers such as myself that want to formulate decentralized technologies into different use cases.
  - **PoW Distribution** – There will be an initial PoW distribution, similar to Protoshares or Vericoin, which later switches to DPoS after heavily beta tested alpha and then beta releases of the distributed DPoS poker network. This is intended to widely distribute the main chain tokens to avoid cries of oligarchies, dictatorships and totalitarianisms which are often harped upon when it comes to PoS cryptocurrencies.
    - **Majority Distribution** – I propose a majority of the main chain coins should be distributed this way, as a wide distribution of the initial stake is in everyone's best interests for the future of the poker network.
    - **Utilize Multiple PoW Algorithms** – Multiple algorithms should be utilized during the initial PoW distribution, so that people with all types of mining and computer hardware can participate.
    - **Dynamic Difficulty Per Algorithm** – Each algorithm has separate difficulty so that each algorithm has an equal chance of finding the next block.
    - **Myriadcoin** - I affectionately stole the multiple algorithm and dynamic difficulty per algorithm ideas from the open source alternative crypto currency called Myriadcoin. Hence open source, this type of distribution will be easy to set up so volunteers can stay focused on designing and programming the decentralized poker network.
    - **Warning** – The date that PoW distribution is planned to begin, and a definite time that it will end, will be announced far ahead of time.
  - **Share Drop** – Several communities should be share dropped as their support to the project is vital. The percentages and communities are highly debatable at this point.
    - **Bitshares Community** – The group of people who support Bitshares the most and understand its power will be vital to the success of the project.
    - **Two Plus Two Forum Users** – The Two Plus Two poker forums are the largest community of poker players, and support from a large amount of users there will also be vital to the success of the project.
    - **Bitcointalk Forum Users** – Support from the biggest crypto currency forum would also be lucrative for the success of the poker network.
- Distributed Poker Features
  - **Profitable** – Allow main chain stakeholders to make a profit on their investment.
    - **Value** – Make a profit from the network growing and in turn the value of their main chain tokens increasing.
    - **Rake** – Make a profit from raking the poker games and charging tournament entry fees.
    - **Fees** – Make a profit from transaction fees on the network from transactions and trades in the decentralized market and ledger.
    - **Destruction** – Fees that are not needed to pay for the necessary services and employees should be destroyed, increasing the equity of main chain stakeholders' stake as fees are destroyed.
  - **Transparent** – A distributed poker network is substantially more transparent than legacy centralized poker networks.

        - **Provably Fair** – Leverage Mental Poker algorithms with the cryptographic proof that proves the gameplay is fair which are stored on a permanent and an immutable blockchain.
        - **Public record** – Fair game play, accounting and the policing of collusion, multi-accounting and bots are public record on the blockchain for anyone to scrutinize.
        - **Less Trust Required** – Leverage smart contracts to maximize the amount of processes of the poker network that are automated, so that less trust is required by players to partake.
    - **Referral Program** – Provide incentives for the poker network to grow via the network effect of affiliate marketing.
        - **Inclusive** – Allow for all participants to be an affiliate, unlike some centralized legacy poker networks that have strict policies as to who can become an affiliate.
        - **Bitshares 2.0** – A working referral program already exists in Bitshares 2.0, and a similar system could be closely modeled off of that.
        - **Optional Features** – A multi-level referral system may be better than a single level referral system.
            - **Multi-Level Referrals** – This is debatable, but I am of the opinion we should allow affiliates to earn income from user's who they've recruited who then go on to recruit other players several levels down.
                - **Magnified Network Affect** – Recruiting users that will then mainly attempt to recruit other users magnifies the network effect of an affiliate system.
                - **Levels/Structure** – To be decided… how many levels deep should it go and what should the structure be as far as percentages? I need to do more research as to MLM best practices and norms.
    - **No "Ringed Fences"** – Players worldwide in all jurisdictions would be able to play together without government interference.
    - **Bonuses** – This is optional, yet a good idea because online poker players are used to receiving them, but we could provide deposit bonuses similar to legacy poker networks that is paid for by rake or tournament fees charged for games played on the network. Bonuses cannot be paid out of transaction fees as that would qualify as a quasi-Ponzi scheme.
    - **Low Rake and Fees** – Several factors go into allowing distributed poker networks to have lower rake and fees than legacy centralized poker networks.
        - **Automation** – Leverage smart contracts to automate as many processes as possible to allow the network to have less expenses than centralized poker networks.
        - **Non-Taxable** – The profit of a distributed poker network would not be taxable by any government authority, therefore government taxes charged to the poker network itself would not be passed down to the poker players.
        - **Low Server Costs** – Due to the poker networks' decentralized properties, the network pays the bare minimum hosting costs.
        - **Better ROI** – With cheaper rake in effect, some losers will become winners and some break even players will become winners.
    - **Hirable Employees** – Allow for the decentralized network to hire employees for necessary functions by electing witnesses for specific purposes via witnesses in the DPoS consensus algorithm.
        - **Customer Support** – Pay users for providing customer support via elected witnesses.
        - **Development** – Pay developers to improve the network backend or interface via elected witnesses.
        - **Certificate Authorities** – Pay certificate authorities to police multi-accounting by player-funded certificate issuance and revocation and/or via elected witnesses.
        - **Security Analysts** – Pay users to police the games for collusion, bots, and chip dumping via elected witnesses or bounties. Speculators (see below under Poker Chips) double as Security Analysts.

        - **Advertising** – Pay advertisers or sponsor well-known poker players to promote the poker network.
    - **Built-In HUDs** – Utilizing a built in HUD (heads up display) puts weaker players and solid players on a more level playing field.
        - **Banning HUDs Is Impossible** – Banning HUDs is impossible and puts honest players at a disadvantage to dishonest players, in turn it is better to make such software standard for everyone to use at no added costs.
        - **Stop whining** – Providing HUDs for free will likely stop most players from complaining about their use.
        - **Increase Profits** – Some speculate if weaker players see that their stats are much looser or tighter than others than they will adjust which will make the games tougher. This is an argument against built-in HUDs being programmed into the poker network software. This is obviously bad for profitable players, but will at the same time produce more rake and transaction fees (profit) for main chain token holders because weaker players will lose slower.
        - **Remain Profitable** – In the author's opinion, although weaker players will lose slower, the games will still be profitable as weaker players will always exist. People will always exist that don't put in enough time away from the table to improve their games, like to gamble, or simply don't care and like to set money on fire to watch it burn.
- Shuffling, Dealing, and Gameplay
    - **The Deal** – The deal must be truly and completely random.
        - **52 Factorial** – It must allow for all possible permutations.
        - **Arbitrary**- Any one permutation must not be any more likely than another.
    - **Golle's Algorithm** – This is debatable, but the author suggests the use of Golle's algorithm which is one of the most efficient mental poker protocols. With one caveat… that it requires the use of multiple trusted third parties whom audit each other automatically and retrospectively via smart contracts in a transparent manner.
        - https://crypto.stanford.edu/~pgolle/papers/poker.pdf
        - **Checks and Balances** – Utilize an arbitrary number of random delegates per game to limit the amount of trust needed and run an efficient enough game.
            - **Compromise** – Find a good compromise as to integrity of the shuffle and deal versus efficiency to create an ideal playing experience for players. This should be heavily alpha and beta tested with players attempting to cheat the system to tweak the compromise.
            - **Split Keys** – The delegates that are not involved in the shuffling and dealing of each game should be shared the keys used to unlock the cards and deck in a redundant way to prevent collusion, cheating, or disconnections. These keys will then be revealed by the delegates after each game to ensure it was fair.
            - **Incentive** – Inherent incentive exists for main chain token holders to combat corruption, because their tokens will quickly become valueless if collusion is an accepted practice.
        - **Change Needed** – "I won't spend much time on how this works, except to point out that Golle's paper *may* have a small bug (though one that's easily fixed). To make a long story short, when a collision occurs in the first round of dealing -- *i.e.,* a card is dealt that already exists in a player's hand -- Golle will actually 'throwback' *both* the new card, and the card that was already in the player's hand." – Matthew Green (a respected cryptographer… you may recognize his name from the Zerocoin or Zerocash projects)
            - **Easily fixable** – As Matthew concluded, the problem is easily fixable by tweaking the algorithm. Matthew also seems to hold the algorithm in high regard as far as efficiency goes, stating "it cooks."
    - **Drop Out Tolerance** – The mental poker protocol must allow for drop out tolerance of both witnesses and players.

        - **Shamir's Secure Secret Sharing Algorithm** – Each players' or witnesses' keys to unlock each deal or hole cards should be split and shared to an arbitrary number of random witnesses before each hand. The witnesses then would have the power to combine these keys in a transparent way if requested by other players or witnesses, on the occasion that players or witnesses disconnect, refuse to cooperate, or are dishonest.

- Poker Chips
    - **SmartCoins** – Poker Chips will work similar to that of SmartCoins in Bitshares.
    - **Decentralized Exchange** – Exchangeable on a decentralized exchange with no trusted third parties needed.
    - **Restitution** – Collusion and bots cannot be policed real-time as evidenced by logical reasoning and many research papers in academia. Therefore, a retroactive means of restitution has to be made available to players.
    - **Collateral** – Poker Chips backed by irreversible main chain tokens similar to the way Bitshares' SmartCoins work.
        - **Transparent** – No fractional reserve banking or Ponzi schemes.
    - **Stable** – Must not be subject to volatility like other cryptocurrencies.
    - **Reversible SmartCoins** – To pay back those wronged by collusion.
        - **Consensus** – SmartCoins should only be reversible by a large consensus of main chain token stakeholders.
            - **Large consensus** – The percentage of consensus is debatable, but a large consensus should be had to reverse coins away from those who cheat. I propose a large percentage above 51%, more like 75%+
            - **Voting pools** – Utilize voting pools to combat voter apathy, accounts can choose to vote with accounts that they trust to do what's best for main chain stakeholders.
        - **No Alternative** – The only alternative to this is irreversible SmartCoins which would allow colluders to literally "free roll" the poker network. In this alternative scenario, the poker network would save a percentage of rake and/or network fees to pay back those wronged by collusion.
            - **The alternative is a Ponzi scheme** – If victims can only be paid back by a percentage of the rake, then it creates a Ponzi-like structure in that if the games dry up then victims could never be paid back. The ability to pay players back then relies on the success of the network. Reversible SmartCoins is the lesser of two evils.
            - **The alternative can be further gamed** – If victims can only be paid back by a percentage of the rake and colluders are allowed to keep their ill-gotten gains, then colluders could form a coalition by getting several accounts on the same table. One account (or more) in the coalition that is wronged by the collusion and the others that do the colluding. If there was no way to reverse the coins stolen from colluding accounts, then the colluding group could keep the funds gained by colluding and also get the coins paid back to the user of the collusion group that was "wronged" by collusion, which in turn increases their take from the scheme.
    - **Freezable SmartCoins** – Freeze players' buy ins for a set amount of time, so that no one can bypass the SmartCoin's reversibility function, by utilizing smart contracts and awarding them with one "Risky Chip" for each "Poker Chip" frozen after using a Poker Chip to play in a game or receiving it as winnings from a game. The amount of time they should be locked is arbitrary and debatable, and will require extensive beta testing.
        - **Unavoidable** – If Poker Chip winnings were not frozen for X amount of time after playing, then it would allow cheaters to bypass the reversibility of Poker Chips. In turn, this would effectively allow them to "free roll" the poker network, and immediately exchange poker chips with irreversible main chain tokens.

- **Risky Chips** – For sake of discussion in this paper, the proposed name of the SmartCoins that are frozen from the decentralized exchange is “Risky Chips”.
    - **Locked** – 1 Poker Chip will be locked onto the blockchain for each Risky Chip in circulation by utilizing smart contracts.
    - **Not Accepted for Gameplay** – Risky chips will not be accepted for gameplay and one must convert their Risky Chips into Poker Chips in order to play a game (if they do not want to wait until the stale date of the Risky Chips on which date they will convert back to Poker Chips.)
    - **Tradeable** – Risky Chips are tradeable for Poker Chips on a ledger instead of a decentralized exchange to allow for people to cash out their Risky Chips immediately if they like.
        - **No Decentralized Exchange** – There will be no decentralized exchange for Risky Chips, but instead there will be a decentralized ledger that closely resembles Localbitcoins. This allows people to pick and choose who they wish to trade with and analyze the amount of risk they are taking by scrutinizing the reputations of each user.
        - **Escrow** – Escrow agents which are governed by a reputation system can be utilized to police the trades.
        - **Speculators** – Buyers of risky chips would be speculating on the fact that the Risky Chips may be confiscated by the network due to collusion, and will charge a premium for taking that risk.
            - **Profit or Loss** – Speculators can make a profit by buying discounted Risky Chips that later turn into Poker Chips after a set amount of time. They also risk the confiscation of the Risky Chips they buy and therefore risk losing money on the transactions. A comprehensive and well thought out reputation system is necessary to make this system work.
            - **Businesses** – Securities could be issuable by main chain token holders for main chain stakeholders to pool resources and create for-profit speculation businesses. This will spread the risk among Speculators and provide greater liquidity on the Risky Chip market.
            - **Improve Game Integrity** – Savvy speculators would analyze a players’ recent games for collusion, multi-accounting or botting before trading, which in turn improves the integrity of the games (along with analyzing their reputation.)
            - **Premium** – The premium charged by each speculator can and should be on a case by case scenario.
                - **Reputation** – Users with good trust ratings via a reputation system will get closer to face value (one Poker Chip) for each Risky Chips. Users with little or no reputation will inherently get worse deals on Risky Chip trades.
                - **Amount of time left frozen** – Risky chips that have 1 day left frozen would likely be worth more than Risky Chips that will be frozen for 30 days, as by that time it is less likely that they will be reversed to cheating.
                - **Free market** – The amount of premium charged by speculators will be lowered to the bare minimum by speculators competing in a free market environment, which allows players to receive the most value from their Risky Chips that is feasible

when taking into account the risk taken by speculators.

- Collusion, Bot, and Multi-Accounting Detection
    - **Profitable** – Economic incentives to make collusion detection profitable.
        - **Employees** – Fight collusion similar to how centralized poker networks do, by paying people to police the games via elected witnesses.
        - **Incentive** – Inherent incentive exists for main chain token holders to combat collusion, because their tokens will quickly become valueless if collusion is an accepted practice.
        - **Speculators** – Savvy speculators from the Risky Chip market will also perform due diligence on sellers by checking for collusion and bots for a profit by gaining Risky Chips at a discount to the value of Poker Chips.
    - **Reportable** – Provide the ability for players to report collusion.
        - **False accusations** – Refundable fees should be charged to players to combat the system against spam attacks and deter false accusations.
        - **Reduced costs** – Players will only report collusion when they are certain that it happened as otherwise it would cost them money, which in turn reduces the amount of rake that needs to be charged to address such accusations. I estimate centralized poker networks spend a ton of time investigating false accusations, or simply do not investigate them at all in most cases (which is not good either.)
    - **Reputation** – Allow players to police the games themselves via a reputation system which is also used in the Risky Chip market.
        - **Increasingly strict by stake** – Require increasingly strict reputation requirements to play in higher stake games where cheating is more lucrative.
        - **Build reputation over time** – Reward honest players with good reputations built over time via honest gameplay.
        - **Collateral –** For those who do not wish to take the time to build good reputations, allow players to buy one by locking tokens into the blockchain as collateral.
        - **Social Identity** – Leverage social network identity for people to establish identity and improve their reputation scores (similar to OneName.)
        - **Ratings** – Allow players to rate players they know in real life that are trustworthy, or players they have successfully bought Risky Chips from without them being reversed.
    - **Collusion and Bot Algorithm** – Algorithmic stats should be published publicly on the blockchain for everyone to analyze to identify collusion and bots.
        - **Hole Cards** – Hole cards are revealed at the end of each tournament or session, or every 24 hours… whichever comes first. This allows for the aggregation of all statistics legacy centralized poker networks use to combat collusion and bots. Player strategies are protected by utilizing a random name for each game which is later tied to a main account when the whole cards are revealed.
        - **Data points** – Collect as many data points as possible from gameplay and store them on the blockchain.
        - **Multiple reports** – There does not exist one report that can detect all types of collusion or all poker bots.
            - **Provide necessary tools** – Allow players to analyze a combination of all data points in a vast array of default and customizable formats. This could be a separate program, or ideally part of the client, which queries the blockchain for historical player statistics.
    - **Blacklist** – Permanently ban people who collude, run bots, or scam in the decentralized ledger market for Risky Chips.
        - **Identity** – Blacklists require identity verification procedures be in place via certificate authorities or biometrics.
        - **Problem Gamblers** – Provide for a system to where problem gamblers can exclude themselves.

        - **Minors** – Provide for a system that can exclude minors from participating.
    - **Restitution Fund** – Leverage smart contracts which save a percentage of rake as a "restitution fund" which can be utilized to pay back those wronged by collusion, bots, or multi-accounting. This should only be used as a last resort to pay back those wronged by collusion that was not caught during the timeframe that their game-used Poker Chips are locked up as Risky Chips.
        - **Consensus** – Funds can be paid out of the restitution fund by requiring a large percentage of consensus from stakeholders.

- # Identity Verification
    - **Necessary** – Identity verification is necessary to combat multi-accounting because decentralized identities are not possible at this point due to many complications.
    - **Problems with Decentralized Identities**
        - **Examples** – OpenID, OAuth, OneName, BitPassport (all not Sybil-proof)
        - **Sybil** – There is no way to establish decentralized identity that is immune to Sybil attacks, Sybil attacks can only be mitigated in a decentralized system.
        - **Privacy** – There is no way to be Sybil-proof without publishing everyone's identity publicly which is not even considerable considering privacy concerns.
        - **Biometrics** – Eventually biometrics could be utilized to create Sybil-proof and anonymous identities, but the technology isn't there yet unfortunately.
    - **Anonymous Identities** – At the start of each game or cash game session, players will generate anonymous identities in a transparent and provable way which protects the players' strategies for each session or tournament.
        - **Revealed** – The anonymous identities are revealed after each session or tournament to allow for the aggregation of data for the detection of collusion, botting and multi-accounting.
        - **Transparent** – This is more transparent than other poker networks' anonymous identities (such as Bovada) since each players' identity is revealed after each session or tournament and their lifetime statistics are stored on the blockchain.
        - **Protects Players Strategy** – Generating a random name for each tournament or session combats the massive data mining that would otherwise be possible since all actions, stats and hold cards are eventually made public record.
    - **Certificate Authorities** – Verify players' identities the way the legacy poker networks do by manually verifying an identity, then issuing a certificate of identity.
        - **Standard** – Players are as safe as they are on a legacy centralized poker network when it comes to multi-accounting as this is the same system they utilize.
        - **Profitable** – Allow certificate authorities to make a profit which provides incentive for them to be honest (and go into business as "partners") with the distributed poker network.
        - **Proof** – Store proof of the issuance of such certificates on the blockchain.
        - **Revocation** – Certificates are revocable in case someone's private key is compromised and they need to switch accounts.
        - **Expiration** – Certificates should expire every year so that the integrity of the certificate is maintained, a stale date should be publicized at the time a certificate is issued.
        - **Multiple Authorities** – Allow for multiple certificate authorities which compete, and the players can then select which certificates authorities they trust and would like to play with other players with.
            - **Cheaper** – A free market of Certificate Authorities will lower the costs of such services to the bare minimum due to free market economies.
            - **Safer** – Require certificates from multiple authorities for greater assurance of identity.
        - **Risks –** Risks involved with certificate authorities
            - **Identities revealed** – The certificate authorities could be hacked and the data dumped.

        - **Fresh start** – Allow for the ability for players to make a new account in the case of a certificate authority being compromised to retain privacy.
        - **Standards** – Create industry security standards for securing player documents sent to certificate authorities.
    - **Regulate** – The distributed poker network should have strict regulations in place, as to the security of the data certificate authorities and standards, so that certificates identities and identity documents are secure, certificates are compatible across multiple certificate authorities, and no one can create multiple identities.
    - **Limited risk to the integrity of the gameplay** – Certificate authorities could not gain an advantage in game play as anonymous identities are generated for each session or tournament, and only later revealed after the session or tournament has ended
- **Certificate Authority Best Practices**
    - All CA accounts should utilize multi-signature or account permissions to protect the integrity and validity of the certificates.
    - All CAs should make their identities public and prove they own the account they are issuing the certificates from.
    - All CAs should sign a contract stating that they will not misuse identifying documents and the identities of account holders, and follow the standards outlined by the community.
    - Files sent to each CA should be encrypted to a public key published on the blockchain so only the CA can view the files.
    - Files received by the CA should only be unencrypted on an offline computer for privacy reasons, to avoid interception of the identity files.
    - After receiving identifying documents, a one-way hash function should be used by the CA to create an identity signature according to the certificate standards set by the community.
        - Standard “Identity String” Example: “Full name, Date of Birth, Sex, Eye Color, Physical Address, Country”
        - CAs should use a standard one-way hash function, thus the input for each player’s information will result in the same output.
        - Why more than a name and birth date? Same names, generational same names, and “The Birthday Problem”
    - After creating an identity signature, the unencrypted and encrypted files used to generate the identity signature should be permanently destroyed via secure file shredding methods.
- **A means to an end** – When the technology is feasible, phase out certificate authorities with the use of biometrics and cryptographic fingerprints.
    - **Decentralization** – Eliminating certificate authorities will reduce the amount of trust and centralization required by participants.
    - **Costs** – Phasing certificate authorities out will lower the costs (effective rake) for players.