

Q 3 2 0 2 2

GameFI

Research & development

Executive summary

to better understand the following pages

The current trend shows that blockchains focused on the development of GameFi enjoy over 1000% more transactions than classic blockchains. Bringing together the best out of gaming, decentralized finance and blockchain-powered features such as NFTs and cryptocurrencies, GameFi is taking gaming into a new era. Today, the industry brings over 800.000 daily players. Many of them are drawn to GameFi due to the medley of benefits it provides. However, as other themes like the Metaverse and Web3.0 continue to play out, we expect GameFi to see an ever broader adoption across audiences, platforms and use cases. Native Bitcoin has just been introduced inside a game, making it a huge step towards GameFi adoption but bigger steps must be taken in order to get mass adoption from both users and game studios.

In order to make Stacks and Bitcoin a competitive environment for GameFi, a few development steps can be achieved:

- GameFi blockchains require a high number of transactions. By using subnets in order to facilitate the high throughput required we can meet both the speed and the volume demand.
- Many games today use proprietary randomness. Fair, reliable and fully transparent randomness can be built by accessing and utilising Stacks VRF.
- By using SFTs games can store virtual assets in a decentralized way, thus enabling greater transparency and security.
- As not all processes can be performed on-chain, arbitrary message signing is needed for the authorization of off-chain operations.
- Images, audio, video and other files should be stored in a decentralized manner using tools such as Gaia and Pinata.

GameFi is a subset of the crypto industry and is affected by the ups and downs of the digital currency market. Consequently, the GameFi sector experiences a rise in activity during uptrends, but the opposite happens when there is a downtrend.

To maintain interest in GameFi platforms, developers face the uphill task of developing tools, scripts, platforms and games to help the ecosystem weather market slides.

Currently, GameFi investors are focused on improving stability and the experience overall, to build on sustainability, but the task is easier said than done.

Developers face huge challenges, but if they are successful in attracting players with features, security, ease of use and gameplay, the future of blockchain-based gaming looks bright.

Table of contents

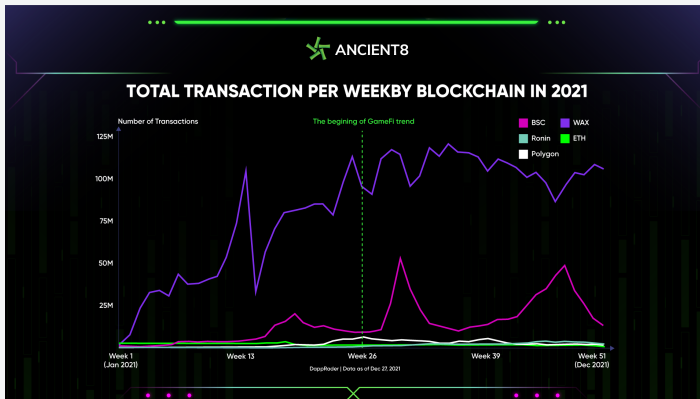
- Blockchain Comparison - pg. 3
- Blockchains in-depth - pg. 4
- Consensus Mechanisms - pg. 6
- Web3 Game Comparison - pg. 7
- STX GameFi* - pg. 8
- Tools for GameFi - pg. 10
- Game solutions - pg. 14
- GameFi requirements - pg. 15

Blockchain Comparison

Name	Mechanism	Time (s) / tx*	Fee (usd)/ tx	tx / s
BTC	POW	600	1.48	4.6
STX	POX	600	0.0015	0.1
Subnets (hyperchains)	-	60	variable	variable
BSC	POSA	3	0.23	62
ETH 1.0	POW	10-19	0.75	12-15
ETH 2.0	POS POW	12-14	-	-
Polygon	POS	2.3	0.018	10000+
WAX	DPOS	0.5	0 + stake	8000
Jumpnet (Enjin)	POA	instant	0	-
Solana	POS POH	0.8	0.0025	700
Hive	DPOS	3	0 + stake	-
EOS	DPOS	0.5	0 + stake	4000
Efinity	POS	6	-	166
Ronin	POA	3	0	-

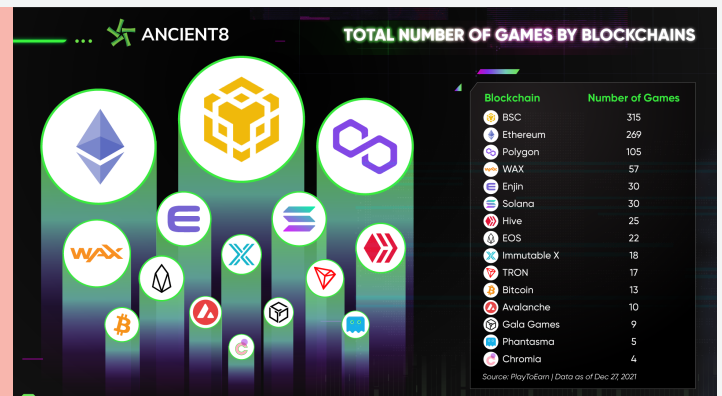
In-depth about Blockchains

let's jump in depth and analyze why different blockchains gather better traction embracing GameFi



It can be observed that blockchains that developed the GameFi sector more enjoy a higher number of transactions

The top spots for gaming blockchains are occupied by BSC, Ethereum and Polygon which combined have over 650 games.



"Gaming Blockchains" make a friendly ecosystem for the development of crypto gaming

Hive

- Created as a public fork of the centralized Steem blockchain acquired by TRON in march 2020, Hive developed a unique, future-minded decentralized blockchain and ecosystem designed to scale with universal adoption of the cryptocurrencies and platforms in mind.
- Very similar to WAX and EOS, Hive is using DPOS which is a popular evolution of the POS concept
- The mobile wallet suffers from having a bad user interface and usage inside the mobile browser is forced to desktop mode, making it hard to use

JumpNet

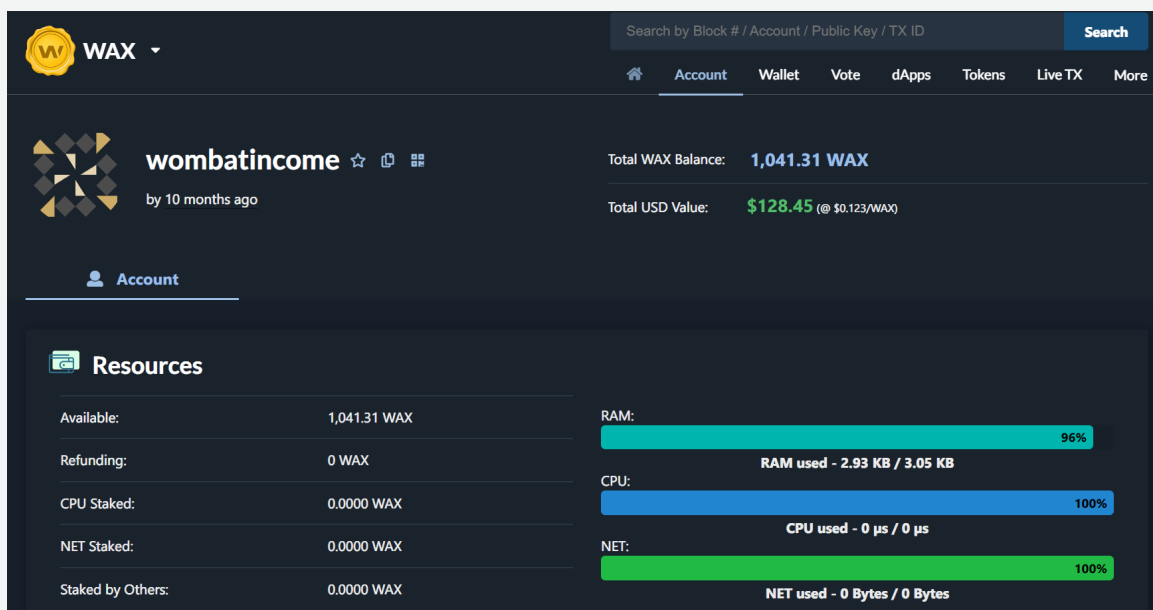
- Enjin's solution to mint NFTs for free
- JumpNet is a high-speed Proof-of-Authority (POA) method of consensus blockchain that offers the user instant, and gasless on-chain transactions.
- Migrate ENJ token from the Ethereum network to the JumpNet network for a 1 : 1 ratio ENJ : JENJ

Ronin

- is an Ethereum sidechain that was created with Axie Infinity's community in mind. Sky Mavis, the team behind Axie Infinity, needed a fast and cheap network that could cater to the demands of the game. They needed a scaling solution that put gaming first, was built to withstand the test of time and the ever-increasing demands of a fast growing game. Ronin was their answer.
- Sidechain are Ethereum compatible, independent blockchains that have their own consensus model and block parameters and run parallel to the Ethereum mainnet. They are one of the main Layer-2 scaling solutions on Ethereum that allow for more efficient processing of transactions - Polygon network is another example of a sidechain. Other popular Layer-2 scaling solutions include Optimistic Rollups such as Arbitrum.
- Ronin currently adopts a Proof-of-Authority (POA) consensus model, a reputation-based system that allows for fast transactions due to its limited number of validators and relatively centralized nature. Validators are handpicked by the team based on their credibility and unlike Proof-of-Stake blockchains, validators are "staking" their reputation instead of tokens. Validators risk losing their reputation if they become bad actors or negatively affect the network. Some examples of validators for the Ronin network include Binance, Ubisoft and Animoca Brands.

WAX

- Very similar to EOS and TELOS and based on the EOSIO technology, while being a sidechain of EOS
- It gets the computing power based on the amount of tokens staked
- Build with the focus on NFTs and integration for a video gaming platform
- Login system is focused on the current generation of consumers (centralized google / facebook / twitter login, instead of third party decentralized wallet) and may facilitate the adoption of dApps* by web2 users but at the same time it doesn't stand as a long-term solution.
- Wombat - wax gaming wallet - play featured games to earn (affiliate marketing through their register links)
- Marketed through NFT collections partnered with Sony Electronics, Atari and Street Fighter (mentioned collections are NFTs not integrated into any game)



Consensus Mechanisms

what are Consensus Mechanisms, how do they work, which are the best...

POW

- It is one of the most secure consensus mechanisms. Cryptos based on POW has more mining power and are more secure. Mining earns rewards in a typical POW model. Proof of Work is random yet fair.

POS

- Proof of Stake is faster, lower cost, and more energy-efficient than the more popular Proof of Work method. Proof of Stake has a security risk when a small number of owners control a large portion of the network's currency value, unlikely to occur with large, widely held currencies but still possible.

DPOS

- Delegated Proof of Stake (DPOS) is a popular evolution of the POS concept, whereby users of the network vote and elect delegates to validate the next block.
- Delegates are also called witnesses or block producers.
- Delegate Cartels: By putting validation into a small number of hands, Delegates can form cartels making the blockchain less decentralized and less resilient to attacks.
- If coin holders are not engaged in the voting process, the system cannot function as a proper democracy – you'll have a few people making decisions for the many.

POA

- Because the validators have to be identified, trusted, and selected by the network, the validating group is often relatively small. This offers the benefit of very high throughput, but it also means that POA networks tend to be more heavily centralized.
- Another limitation is that the requirement for network participants to be identifiable introduces the risk of corruption and manipulation. It also makes the group of potential validators necessarily quite small.

POSA

- As applied by the network, is a combination of Delegated Proof of stake (DPOS) and Proof of Authority (POA).

POC

- Proof of Capacity is used in blockchains that allows for mining devices in the network to use their available hard drive space to decide mining rights and validate transactions. This is in contrast to using the mining device's computational power (as in the proof of work algorithm) or the miner's stake in the cryptocurrencies (as in the proof of stake algorithm).

POB

- Proof of burn is one of the several consensus mechanism algorithms implemented by a blockchain network to ensure that all participating nodes come to an agreement about the true and valid state of the blockchain network. This algorithm is implemented to avoid the possibility of any cryptocurrency coin double-spending.

Web3 Games Innovations

Name	Chain	Web3 Features & Tech	Style
Splitterlands	Hive	NFTs	Card Game
Alien Worlds	WAX	message signing, mining	MMO
Pegaxy	Polygon	NFTs	auto-clicker
Crypto Kitties	ETH	NFT Breeding	-
Axie Infinity	Ronin	NFT Breeding	Card Game
Mobox	BSC	NFTs as items	auto-clicker
Tiny World	BSC	SFTs erc-1155, log in message	auto-clicker
BinaryX	BSC	-	MMO
UPLand	EOS	NFTs for property	metaverse
Decentraland	ETH	NFTs as customizables	metaverse
Prospectors.io	EOS	Signed transactions	MMO
Crypto Blades	BSC	-	MMO
Stacks Degens	STX?	Online lobbies, lootboxes	Arcade
-	-	-	-



Stacks and GameFi

The current strategy of game studios is to create a hybrid gaming experience, probably because of how unaccustomed most gamers are with Web3. One example would be WAX, which favors a fast integration of the user by creating the account using the Web2 login systems (google, facebook, twitter, reddit, etc.) and then gives an actual address.

GameFi on Stacks is currently lagging behind other chains, but Stacks possesses a number of unique technical/design features that could make it a much better and more competitive environment to develop games.

There are key factors that are being developed in this direction right now. For authenticity of ownership, message signing is available and more features for an easier integration are on the way. The integration of a game engine is also in progress and this will help any Unity game creator, indie or studios, to port their game to Stacks more easily. Another big thing especially for free-to-play games is the possibility to sponsor the transactions. This can drastically increase the adoption as it would not require a big initial investment for newcomers the way most GameFi projects require right now.

Bitcoin integration is a great feature that can increase Stacks' utility for a wider range of users, and thus, its adoption. Assets could be moved directly from a BTC wallet to a STX wallet and vice versa, and the same would apply between STX and subnets. By building in this direction, games would be playable using BTC addresses with the speeds of the subnets which are almost instantaneous.

Limitations of STX blockchain

Stacks 2.0 is made to synchronize with the Bitcoin network. This means aprox. every 10 minutes, as a new Bitcoin block is produced, a new Stacks block is also produced, which has data that relates to the new Bitcoin block. This increases the security of Stacks, but also makes it dependant on the BTC block time, making it slow compared to other blockchains.

Recent Blocks

	#76320 → #754735 Anchor block · 67 transactions	12 minutes ago 0xbd680...12962
	0x559df...8ec45 Microblock	12 minutes ago
	#76319 → #754734 Anchor block · 50 transactions	14 minutes ago 0x0d31d...78677

Another obstacle to consider is the limited number of transactions an account can have in the mempool at the same time, which is 25 transactions. New transactions made by the same wallet are declined if the previous 25 transactions are still in the mempool or the microblock, and are yet to be confirmed in the anchor block.

The libraries are mainly developed in JavaScript. For the best performance of a AAA* game, it would be required to be natively integrated with the game, meaning the libraries should be ported to those specific programming languages.

Subnets are a great solution for the time limitations of the Stacks' Mainnet when it comes to confirming a block. They are in an early stage of development, so more documentation, APIs and technical information regarding them will be available in the near future.

BTC Gamefi is based on operations through STX

There are functionalities that are possible directly from BTC. Moving STX assets with BTC transactions can enroll new users directly by using the wallet they already have, the BTC wallet. **EVERY STACKS ADDRESS HAS AN EQUIVALENT BTC ADDRESS.** This enables possibilities like:

- Verify that a BTC address has a certain NFT (in the STX address)
- Trigger actions such as mint NFTs (in the equivalent STX address)
- Moving an asset out of the wallet probably will need a confirmation from the STX wallet

GameFi on Stacks can be expanded by creating usage of the bitcoin address directly in the game by decoding it to the STX address and querying it to fetch the tokens owned. That gives the ability to select and play with the given NFTs. This can also be extended with SFTs. Examples on how the STX-BTC flow can work:

- Paying 'x' amount on BTC to trigger smart contracts calls on STX
- RPC (remote procedure call) endpoint from BTC chain to Stacks chain
- Chainhooks - observe and perform actions based on BTC/STX events

Tools to boost GameFi

which tools can come to use, how?... and where do we find them?

A faster on-chain solution for games

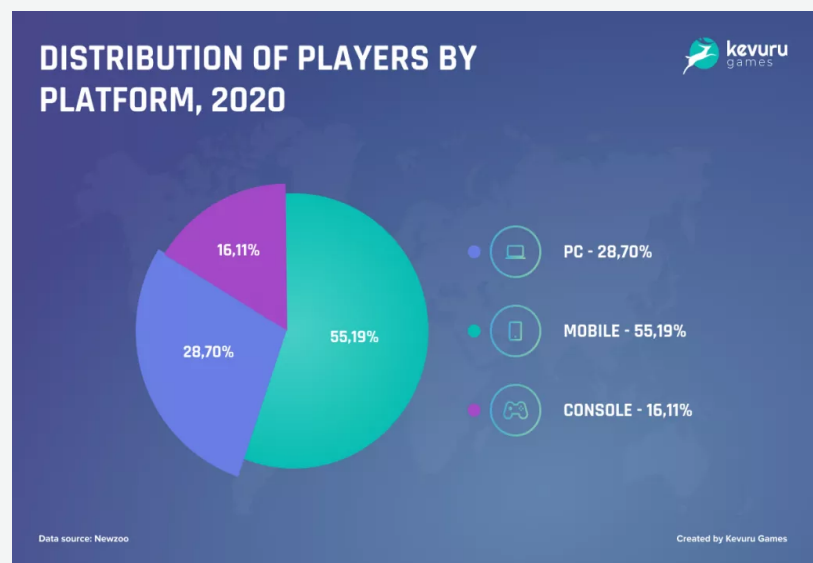
Games need fast processing speeds as gamer's attention span is focused on short periods of time. On-chain operations that take 10 minutes or more would be a big disadvantage compared with other blockchains. Subnets* offer the solution for this problem. For example: since microblocks in subnets offer finality, subnets can be useful for any type of game. Picture a game where you evolve your city, gather resources and interact with other cities and players. With subnets, those operations would be happening close to real time, so you can have the game flow getting confirmed with finality at a low latency. A general subnet where early GameFi projects can test their games accelerates their integration into the ecosystem. As games perform many operations, the optimal solution is to not block the subnet with excess throughput when the game has many players and operations ongoing, but instead, move to a custom solution configured for that game.

- a general subnet for early GameFi projects can facilitate integration
- easy subnet configuration for GameFi projects with a high number of players/transactions must be accesible by game studios

Mobile integratiton

Mobile gamers are a major part of today's gaming community. If games interact with the blockchain and can be played directly on smartphones, they would have a great growth chance because of this high percentage of mobile gamers. The mobile tool can read data from the blockchain, creates and submits transactions on-chain, and is already in development in C# for direct integration with Unity.

- The vast majority of gamers are mobile based
- Development of easy & straight ftorward mobile authentication for Dapps is required for traction of new users inside the crypto and GameFi spaces



Storing on-chain data that used to be off-chain in Web2

There are multiple game styles and they have different flows, capabilities and necessities. For a better on-boarding process, smart contracts have to be developed for these actions. For loot boxes, card packs, or any gambling feature, the mechanism can be developed using the Stacks VRF* (true randomness via blockchain).

Most games nowadays rely on a system based on items and resources. Items have different stats based on the item itself, an iron sword is better than a wooden one, and based on their level, a level 5 sword is better than a level 2. These stats are stored directly on-chain using SFTs which permits having all this info stored directly on a smart contract or dynamically in multiple smart contracts. Resources are stored in the same format and interact with the items (using them in exchange or for upgrading the items).

Besides these, it is common for games to offer different customizations: for your avatar, for your car, for your forged weapon. As avatars are unique and they are represented by all the characteristics they present, it is representative to have them on-chain through customizable NFTs. If a characteristic is changed, the old one is taken down and the new one appears on the traits of the NFT. Same way, if all the characteristics are separate, they can be assembled together to create the whole avatar, and if an avatar is no more in use but his characteristics would continue to be used for others, it can be disassembled into parts.

The ability to play against others in small groups is present in many competitive games. Such games are League of Legends, Call of Duty and Forza Horizon. By playing in the equivalent lobbies on-chain you have all the information in a fully transparent manner directly on the blockchain. The rewards are given from a smart contract pool and the mechanism emphasize on winning while also rewarding the others using a formula with a custom distribution. The formula is also fully customizable so it can reward more the winning players or distribute the rewards across all players.

- Smart contracts for multi-purpose applicabilities
 - VRF enables true randomness
 - Gambling
 - Loot Boxes
 - SFTs for upgrading the web2 mechanics of different kinds of games to truly decentralized Web3 games
 - MMORPG - World of Warcraft, Runescape
 - RTS - Clash of Clans
- Node setup + APIs config specific for the publisher's chosen game
- Smart contracts with specific applications.
 - Customizing NFTs
 - On-chain lobbies

Verification of authenticity

While pushing the boundaries of GameFi, DeFi, DAOs and other decentralized applications, developers need a way for their users to authorize both on and off-chain activities with their wallet beyond transaction signing and broadcasting for asset transfers, contract executions and contract deployments.

That's where arbitrary message signing is useful. It refers to using digital signatures to enable users to do two things:

- A. Prove they have control over a wallet address
- B. Sign the content of any type of message that they authorize for usage elsewhere in the same application or in the later downstream of on-chain effects.

This new functionality enables a range of new use cases for developers building applications on Stacks. With this feature, an application can prompt a user to submit a signature to prove it controls an address or to authorize an action. A great implementation for developers is a client-server application which confirms the authenticity of users after the prompts confirm they signed. That can be used in a multitude of GameFi flows. A few examples are :

- In a MMO* RPG users change an equipped SFT sword
- In a MMO RTS while collecting resources (iron, gold, etc.) from a mine and attacking other player's islands or villages
- In a MMO Racing to confirm the authenticity after finishing the race in 1st place, or when swapping any car parts
- Customizing NFTs
- On-chain lobbies



Decentralized storage solutions

Decentralization is important in Web3. The best way to provide it for the stored assets such as images, text info, audio etc. is through a decentralized solution like Gaia or Pinata. They have different formats for keeping the data stored. Gaia is the Stacks solution for hosting, an easy way for developers to store assets and user-created content. This can be done through a series of scripts and examples based on what type of content games would generally store.

Popular games on Web2 development to STX

Use the popular games - what would mean to have the infrastructure for the Web2 game to be completely ported on Web3t

- Integration as modular as possible for any legacy game that is ported to Web3

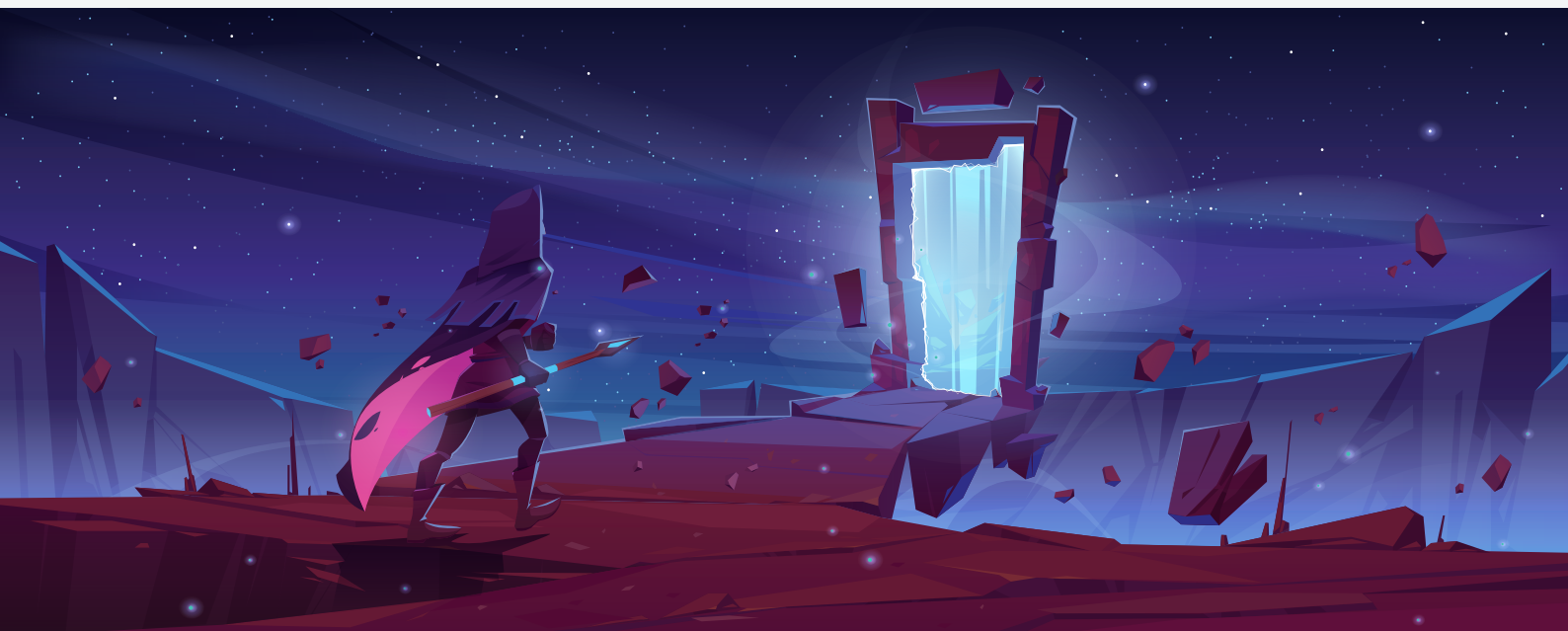
Take into consideration multiple games will be on Stacks blockchain in the same time so the infrastructure should sustain them all:

- Subnet for startup games or games in early versions
- Each game with a considerate amount of players/ transactions should have its own subnet.

Example of transitions in existing games:

- Roblox to Decentraland sandbox*
- Hearthstone to Splitterlands
- Bitefight to BinaryX
- Clash of Clans to Prospectors.io

* These are close examples from the current development. The Web3 version can have more on-chain operations and be more decentralized.



Game solutions for current resources

Given the subnets limit of approximately 60 seconds for each block the following use cases for GameFi would be a viable option:

- Clash of Clans MMO style:
 - Items, buildings and resources can be on chain using SFTs as described here
 - Players have broader markets
 - Data regarding the stats or your village are stored on-chain
 - Game mechanics use directly the attributes for the given item's level (when an attack is happening, the health, defense and other can be fetched from the blockchain directly, giving true transparency and accuracy)
 - The waiting time for block confirmation is alright for players of this genre of game as upgrading buildings and creating troops takes time in the matter of hours and days
- MMO Strategy style
 - Starting an action (fight / expedition / any action that requires the account) - message signing
 - Items as SFTs (consumables, items)
 - Skins as NFTs
 - Open market for players to trade the items
- Lobby games with real time action - League of Legends, Call of Duty, Fortnite
 - Skins as SFTs/NFTs - fetched and displayed in game
 - Open marketplace for skins*
 - Search time can be approx. the same (extra state - searching and pending transaction, joins lobby only after confirmation)
 - Game history on chain
 - Open market for trading and saving badges and achievements directly on chain.

Minimum requirements for breaking into GameFi

a level priority list for sustainable development of GameFi

- **Tooling and platforms**
- **Examples and tutorials**

LVL 3

- **SFT & NFT infrastructure**
- **APIs for BTC - SFT or NFT**

LVL 2

- **Security**
- **Speed**
- **Mobile integration**
- **Accessibility**

LVL 1

Level 1

the base upon we start to build

Security - arbitrary signing for various operations (send specific data):

- Arbitrary signing to confirm the identity of a user when doing any type of action
 - Racing game: submit score & address when finishing a race
 - MMO/ RPG*: change item equipped in inventory - weapon, shield etc
 - MMO Strategy: Perform action to attack another player's village / collect resources
 - Upgrade a building (applicable if it has some conditions needed but resources are not necessary, otherwise it's a transaction)

- Transactions with NFTs/SFTs for actions
 - Upgrade a building using NFTs & SFTs (use NFTs buildings and FTs resources that are burned/ transferred and mint the new NFT building)
 - Upgrade buildings using SFTs (use SFT resources that are burned and mint the new building)

Speed - subnets:

- Docs & examples on how to configure a subnet on devnet
- A general subnet on testnet for early GameFi projects
- Easy configuration of subnets for GameFi projects with high number of players/transactions

Mobile integration:

- Authentication in Dapps to communicate with the mobile wallet
- Transactions to communicate with the mobile wallet
- Arbitrary message signing to communicate with the mobile wallet

Level 2

getting in depth...

BTC interactions to use NFTs in game:

- Send/mint NFTs using the BTC wallet - decode address to STX & trigger certain actions

NFTs and SFTs integrations in game:

- Integration built on top of APIs to get the owned assets of a given user from the wanted Smart Contracts
- If the player uses a BTC wallet and interacts with the app to log in with that address, the address can be decoded to a STX address using the BTC wallet, then the user can play.

SFTs infrastructure:

Web3 games need to host their items, characters and all kind of assets that are owned by the players. Smart contracts for specific games as their dynamics and needs are different:

- MMO Strategy - resources (gold, silver, wood) and buildings (town hall lvl 9, tower of fire lvl 3, storage lvl 5)
- RPG - resources (gold, stamina, health) and items (wood sword lvl 2, steel armor plate lvl 4)
- Card Game - resources (gold) and cards (every single card is another type of SFT with its attack, health, mana cost and other stats)

Decentralized storage:

- Gaia integration to host the game resources in a decentralized manner (map, NPCs and other rendered resources that are not owned by players)
- Script to host the SFTs images, jsons* in a decentralized manner (Pinata or Gaia)
- Script to host the NFTs images, jsons in a decentralized manner (Pinata or Gaia)

Level 3

focus on finishing touch and ease of use

Tools SFTs/ NFTs:

- Back end scripts to confirm actions done - in a GameFi space the user burns the resources and the admin would provide new mints (upgraded buildings, items etc)
- Also applies for NFTs when customizing a specific NFT using others
- Without this system and these scripts the user would be able to mint any resource directly from the Smart Contract*.