grincon<US>(0)
19.01.28 // hero city, san mateo (CA)

How to Mine Grin

Converting Electricity to Magic...

@quentinlesceller

For more presentations like this and updates on Grin, sign up here

A LOT of questions

What is Primary/Secondary PoW?

Can I CPU mine?

What is AR/AF?

What should I mine?

What is the best CPU?

Can I mine with my Radeon HD 4850?

Which mining software should I use?

What is a Cuckaroo?

Can I adopt a Cuckatoo?

Is Grinmint really the best mining pool?

PoW

Which PoW to choose?

Software

Which software is the best?

Hardware

Which hardware is the more profitable?

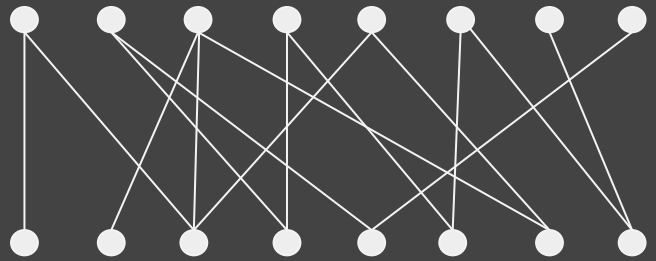
Pool

Which pool is the best for me?

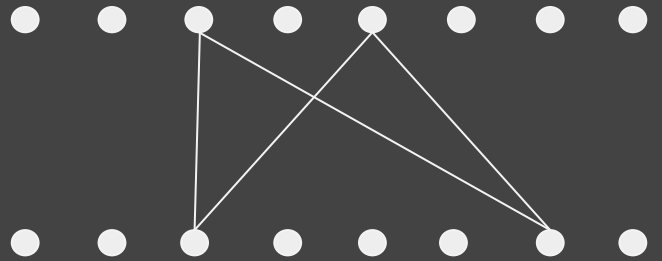
Proof-of-Work

Cuckoo Cycle Family

Finding 42-cycles in a random bipartite graphs with billions of nodes. Creator: John Tromp



Begin with a mess



End up with a cycle

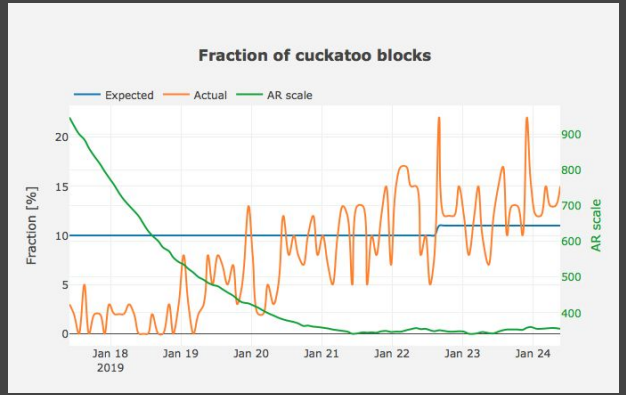
A Dual-PoWs Cryptocurrency

Grin uses 2 proof of work algorithms

- Primary Proof of Work: ASIC Friendly
- Secondary Proof of Work: ASIC Resistant, GPU Friendly

Why?

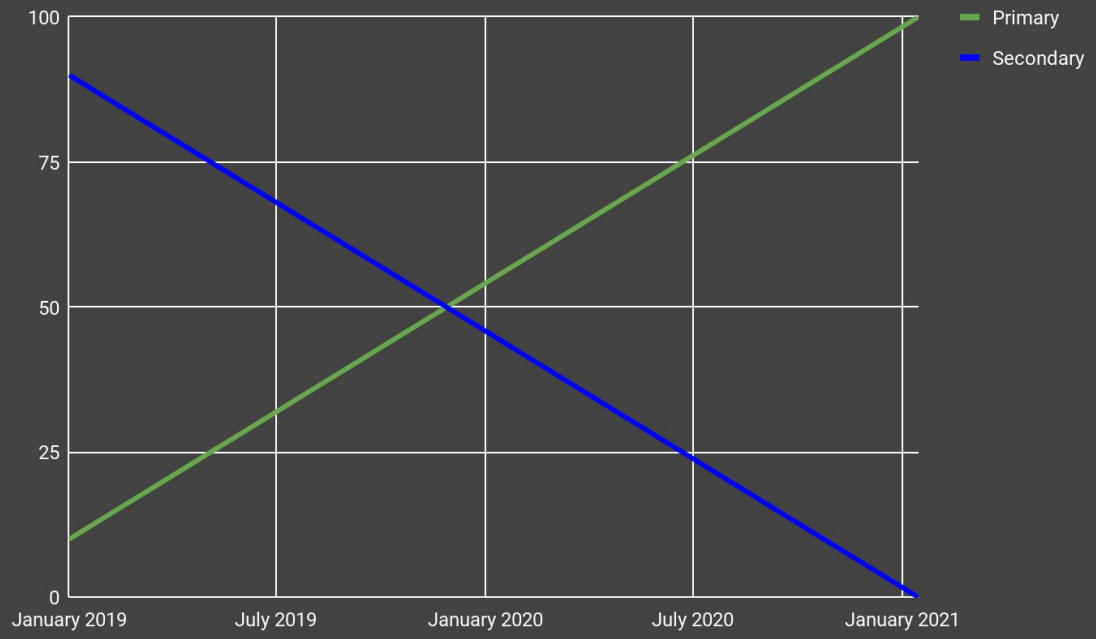
- To guarantee fair and distributed mining
- To encourage ASIC development



A Dual-PoWs Cryptocurrency

- For ASICs: **Cuckatoo31+** - 2^31 edges or more
  - Variant of Cuckoo PoW that simplifies ASIC design
  - Takes 512 MB of memory
  - Can be mined on 11GB GPU initially
  - 10% of rewards at launch, linearly increasing to 100% in 2 years
- For GPUs: **Cuckaroo29** - 2^29 edges
  - Variant of Cuckoo that enforces Mean mining
  - Mining 4GB of memory
  - Tweaked to maintain asic resistance for 2 years
  - 90% of rewards at launch, linearly decreasing to 0 in 2 years

Evolution of PoW



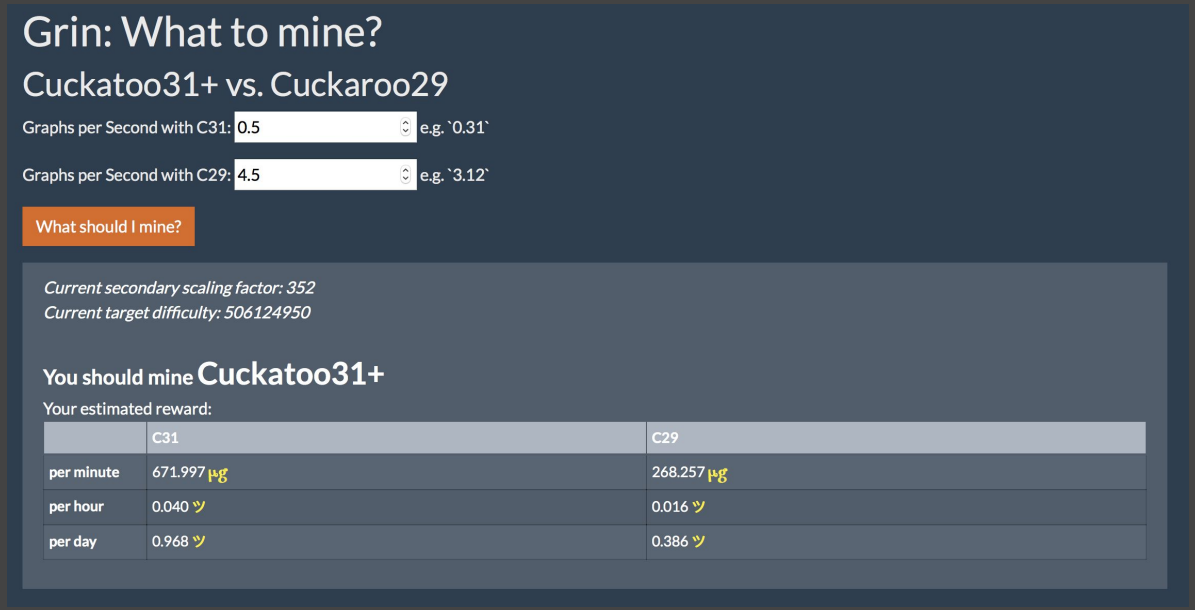
PoW Choice:

$$\frac{GPS_{31} * F_{31}}{42} * weight(31) > \frac{GPS_{29} * F_{29}}{42} * scale$$

$$\begin{aligned}
U_0(T,B) &= \langle H_0 \rangle - U_{\rm B}(T) \\
&= \frac{\hbar}{\pi}\int_0^\infty {\rm d}\omega \coth\left[\frac{\hbar\omega}{2k_{\rm B}T}\right]\left[\frac{1}{2}m(\omega^2+\omega_0^2)G(\omega){\rm Im}[\alpha_{\rho\rho}(\omega)]\right. \\
&\quad + \sum_{j=1}^{N}\frac{mg_j\omega^2}{2}\left({\rm Im}\left[\frac{g_j m_{\rm r}\omega^2}{m_j(\omega_j^2-\omega^2)}\alpha_{\rho\rho}(\omega)\right]\right. \\
&\quad \left.\left. + {\rm Im}\left[\frac{g_j m G(\omega)\omega_0^2}{m_j(\omega_j^2-\omega^2)}\alpha_{\rho\rho}(\omega) - \frac{2g_j(G(\omega))^2\lambda(\omega)\omega^2 e^2 B^2}{m_j(\omega_j^2-\omega^2)c^2\,{\rm Det}\,D(\omega)} - \frac{3g_j}{m_j(\omega_j^2-\omega^2)}\right]\right) \\
&\quad + \sum_{j,k=1}^{N}\frac{mg_jg_k\omega^2}{2}{\rm Im}\left[\frac{g_jg_k m m_{\rm r}\omega^2\omega_0^2}{m_jm_k(\omega_j^2-\omega^2)(\omega_k^2-\omega^2)}\alpha_{\rho\rho}(\omega)\right. \\
&\quad \left. - \frac{2g_jg_k m_{\rm r}\omega^4\lambda(\omega)e^2G(\omega)B^2}{m_jm_k(\omega_j^2-\omega^2)(\omega_k^2-\omega^2)c^2\,{\rm Det}\,D(\omega)} + \frac{3\delta_{jk}}{m_k(\omega_k^2-\omega^2)}\right] \\
&\quad \left. + \sum_{j=1}^{N}\frac{1}{2}m_j(\omega_j^2+\omega^2){\rm Im}\left[\frac{(g_j)^2 m m_{\rm r}\omega^2\omega_0^2}{(m_j)^2(\omega_j^2-\omega^2)^2}\alpha_{\rho\rho}(\omega) - \frac{2(g_j)^2 m_{\rm r}\omega^4\lambda(\omega)B^2e^2G(\omega)}{(m_j)^2(\omega_j^2-\omega^2)^2c^2\,{\rm Det}\,D(\omega)}\right]\right].
\end{aligned} \tag{63}$$

PoW Choice:

Use a calculator:
grin-pool.org/what-to-mine by Hendrik Richter



Hardware Choice

CPU

GPU

GPU Choice

- AMD and NVidia GPU are compatible
- At least 4GB of memory available
- NVidia are much more performant

Known compatibles GPUs

- AMD:
  R9 390 8GB/RX570 8GB/RX580 8GB/Vega 56 8GB/Vega 64 8GB
- NVidia:
  P104/P106/1070/1070Ti/1080/1080Ti/2070/2080/2080Ti/Tesla V100

GPU Choice

- Depends if you want to mine Cuckatoo31+
- Safe bet Nvidia RTX 2080 TI

Pros:

- Can mine both PoWs
- Higher resale value
- Can play Crysis in 4k

Cons:

- Expensive
- Once ASICs are out, Cuckatoo mining will not be profitable

ASIC

ASIC

One ASIC develops by Obelisk

- October 2019
- 100 GPS on Cuckatoo31
- Equivalent to 50 2080Ti
- A percentage of the profit goes to the Grin development fund.

ASIC: InnoSilicon

- Announced on January 25

- No details for now

Software Choice

The Fair Mining License

“Any derived miner that charges a developer fee for mining a fair coin
---one with no premine or other form of developer compensation---
shall offer to share half the fee revenue with the coin developers.”

- John Tromp

Software Choice: The Good

Mining softwares that are open source or give back to the community:

- Grin-Miner https://github.com/mimblewimble/grin-miner

- GrinGoldMiner https://github.com/mozkomor/GrinGoldMiner

Software Choice: The Good Too

Mining software that gives back to the community:

- GrinPro https://grinpro.io

- KBminer (included in Minerbabe) https://www.minerbabe.com

- BMiner https://www.bminer.me

Software Choice: The Bad

Mining software that takes a fee and does not give back anything:

- GMiner

Software Performances: Cuckaroo29

	P104	P106	1060	1070	1070Ti	1080	1080TI	2070	2080	2080TI	R9 390	RX 570	RX 580	Vega 56	Vega 64
Grin-Miner/GGM	NA	1.94	1.85	2.55	2.7	3	4.1	3.7	5	6.1	1.6	1.42	1.52	2.94	3
GMiner	NA	NA	NA	3.6	4.1	4.4	6.4	5.3	7.5	9	NA	NA	NA	NA	NA
Bminer	3.75	2.95	2.8	4.1	4.27	4.9	6.9	X	6.7	9.2	NA	NA	NA	NA	NA
GrinPro	X	2.2	X	3.2	X	X	5.4	X	6	X	NA	NA	2.1	NA	NA
Watt	137	77	77	110	120	165	220	175	225	240	275	190	230	230	230
GPS/Watt	0.0274	0.0383	0.0364	0.0373	0.0356	0.0297	0.0314	0.0303	0.0333	0.0383	0.0058	0.0075	0.0091	0.0128	0.0130

Software Performances: Cuckatoo31

	1080	1080TI	2080TI	Tesla V100	RX 580
Grin-Miner	0.0623	0.52	1.7	1.325	0.0653
Watt	165	220	240	300	230
GPS/Watt	0.0004	0.0024	0.0071	0.0044	0.0003

Software Performances: Do the Math!

Verify that the software delivers the displayed graphrate

$$GPS = \frac{D * N * 42}{T}$$

D: pool difficulty

N: number of solutions found in time period T

T: time period in seconds

Software Performances: Fidelity

The probability for a solver to find a 42-cycle

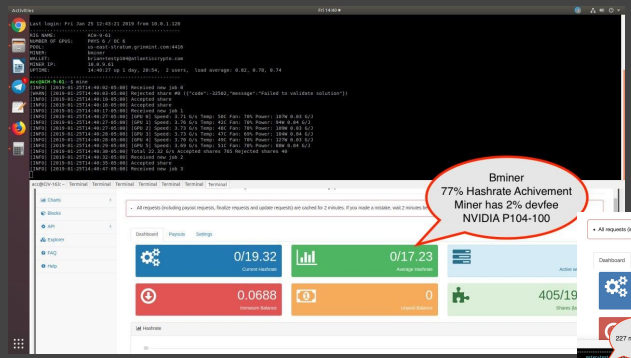
$$S = GPS * fidelity$$

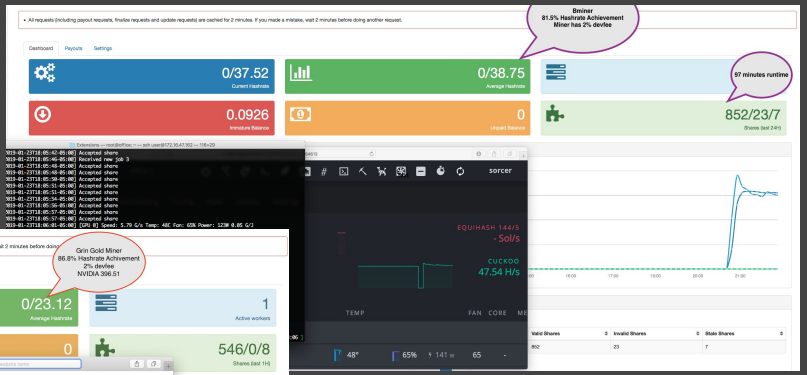
~1 for Cuckaroo29 solvers

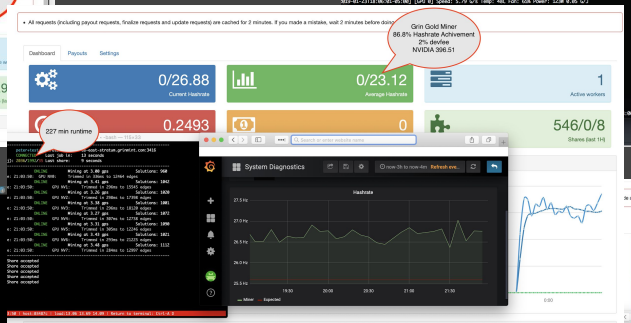
~.9 for Cuckatoo31 on GTX

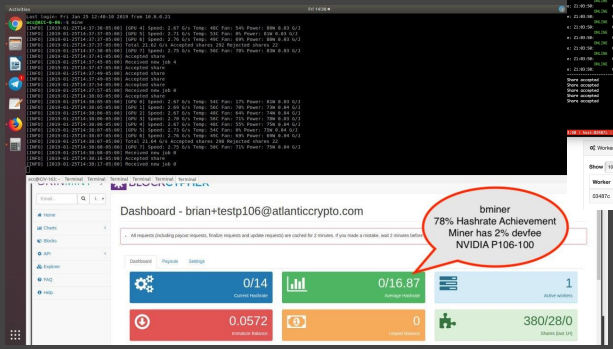
~.7 for Cuckatoo31 on RTX

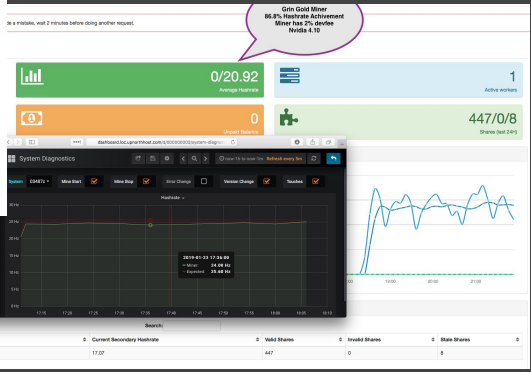
Software Performances: Some Experiments











Pool Choice

Which Pool?


f2pool


Pool


MWGrinPool


GRINMINT

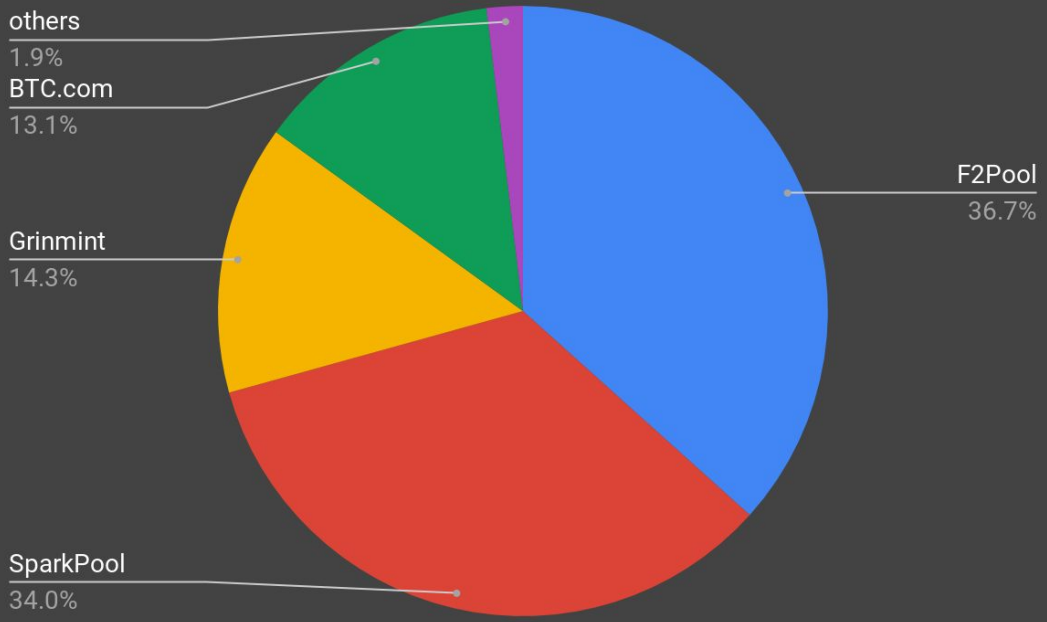

Grin-Pool.org


BTC
.com


SPARK POOL

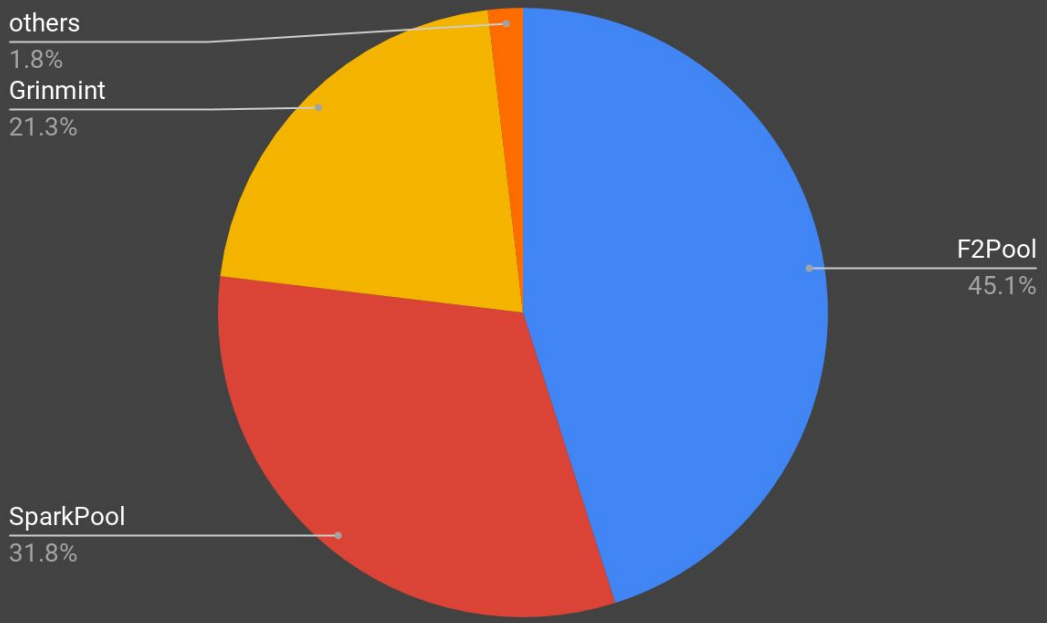
Which Pool?

Current situation: Cuckaroo29



19/01/28

Current situation: Cuckatoo31



19/01/28

Choose a Fair Pool™

Choose a pool that commit to give back to the Grin Development Fund:

- *MWGrinpool*
- Grinmint
- Grin-pool.org

Choose a pool with less than 50% of the hashrate.

How to get those Grins?

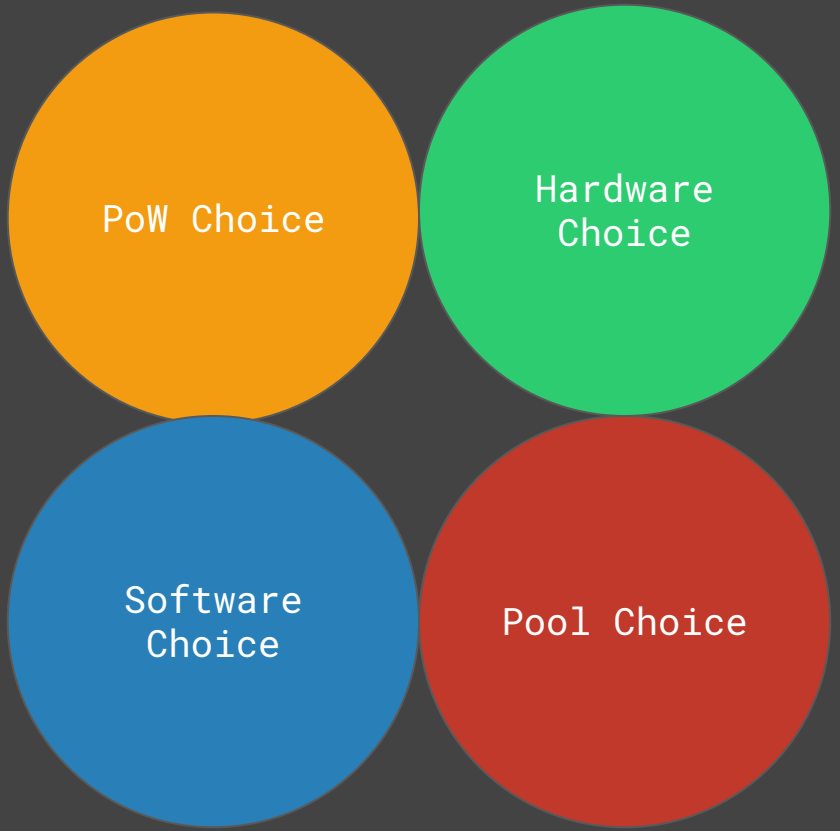
But no addresses…

Various way to move your grins from pool to wallet/exchange

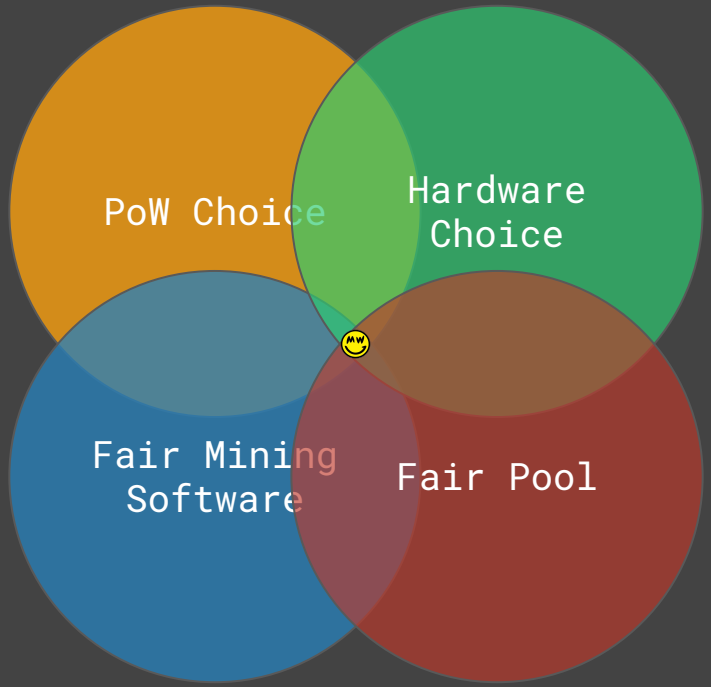
- Direct file/Email with a file
- Keybase
- HTTP/HTTPS
- Wallet713

Conclusion

Conclusion



Conclusion



For more presentations
like this and updates on
Grin, sign up here