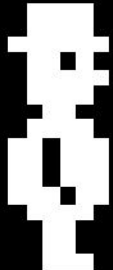




Mining crypto in browser

GPU, WebAssembly and all the good things to try



@PixelsCommander

denis.radin@gmail.com

STERN





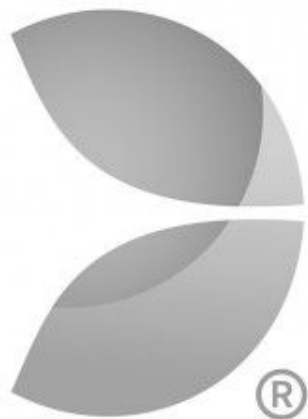
Central Cavern

AIR



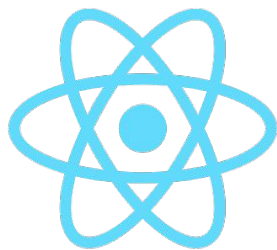
High Score 0000000

Score 000100



Evolution Gaming

State of the art games engineering



React

+




Using React/Redux for
managing HTML UI and game graphics




ChallengingNative.com

Fast web applications development, profiling and optimization




A pixel art character, possibly a robot or a person, is positioned below a speech bubble. The character is white and has a simple, blocky design. The speech bubble is white and contains the text "Hey, want to mine crypto in browser?". The background is black, and there are several colorful, pixelated lines radiating outwards from the center, creating a starburst effect. The lines are in various colors: red, yellow, green, and magenta. Some lines are straight, while others are slightly curved. There are also small, horizontal clusters of yellow pixels on the left and right sides of the character.

Hey, want
to mine
crypto in
browser?

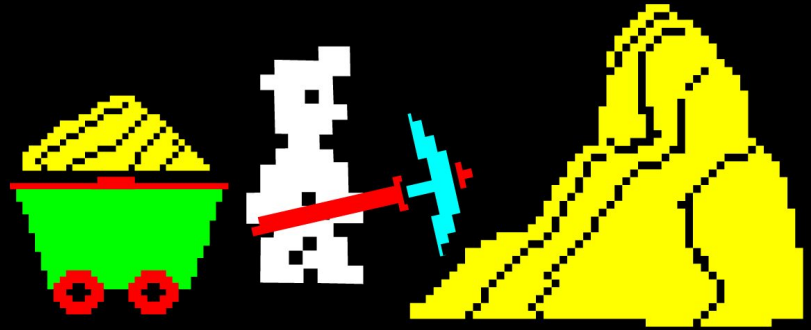


Hey, want
some
performance
challenge?

The image features a central white pixel art character with a speech bubble. The character is a simple, blocky figure with a square head, a small body, and four limbs. The speech bubble is a white, pixelated shape with a tail pointing to the character. The background is black. Surrounding the character and speech bubble are several lines of colored pixels (red, yellow, green, and magenta) arranged in a radial pattern, resembling a starburst or a sunburst. The lines are made of small, square pixels and vary in length and color. There are also two horizontal lines of yellow pixels, one on the left and one on the right, positioned below the speech bubble.

Mining as a bleeding edge
performance challenge for
web platform

What the hack
is mining?







Data

From:



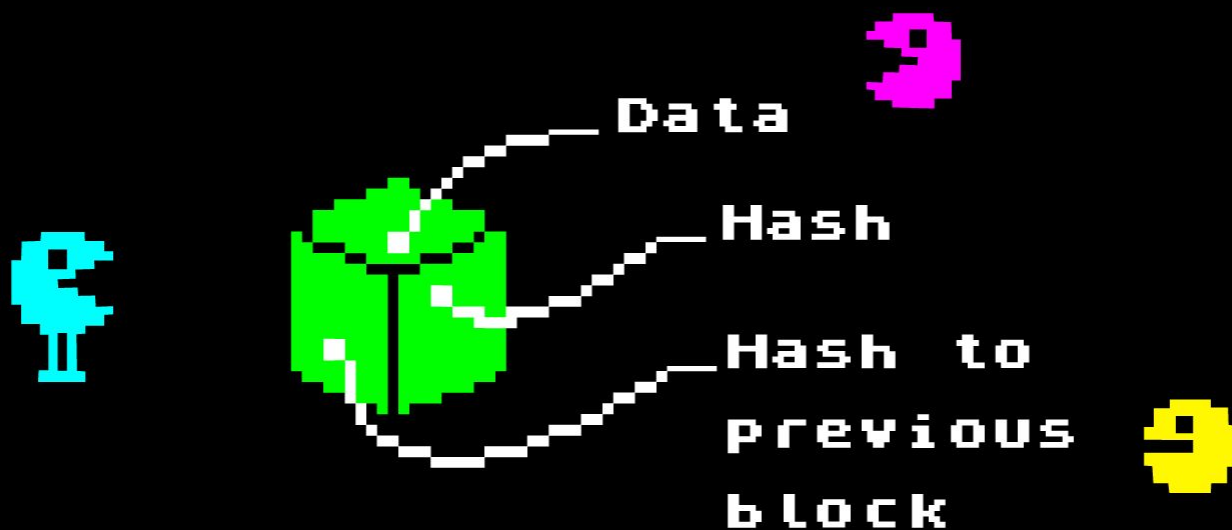
To:

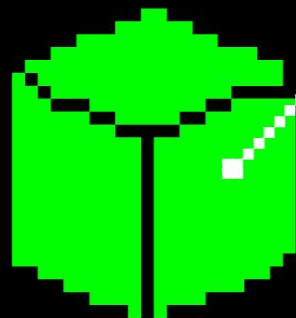


Amount:



Bitcoin block example



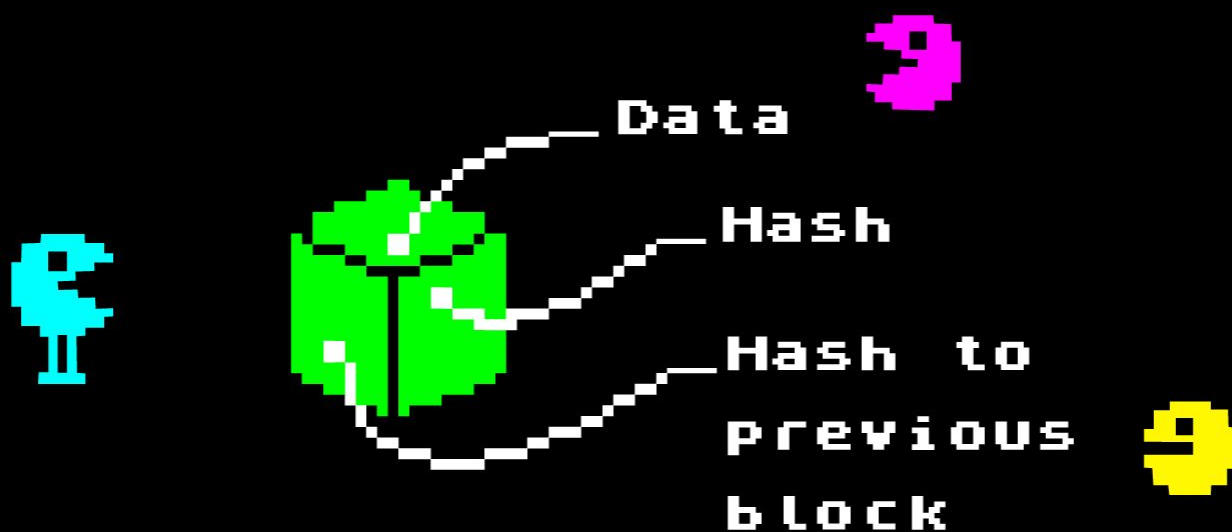


Hash



ec251bc53bb5db4fc0aa497da2ba



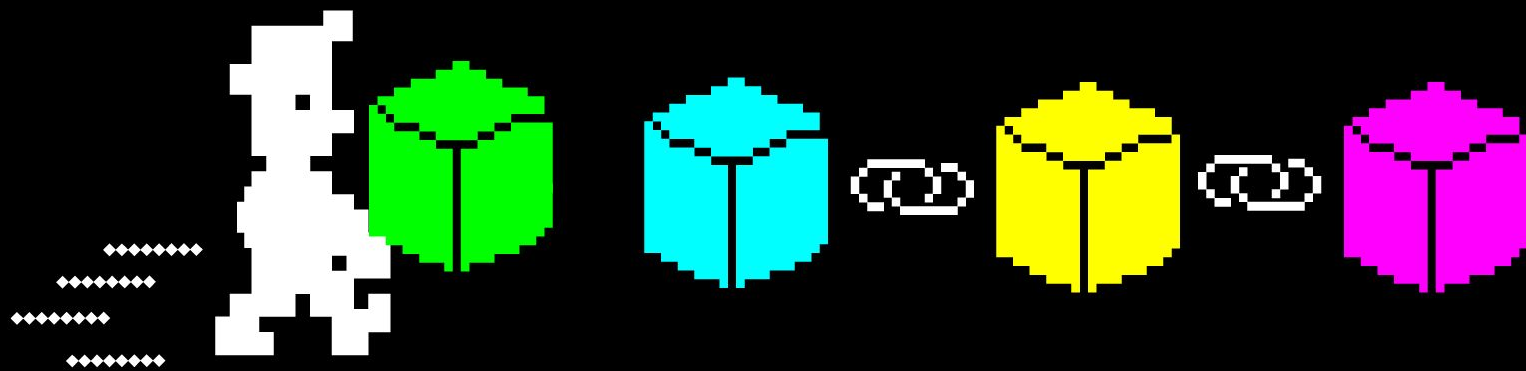


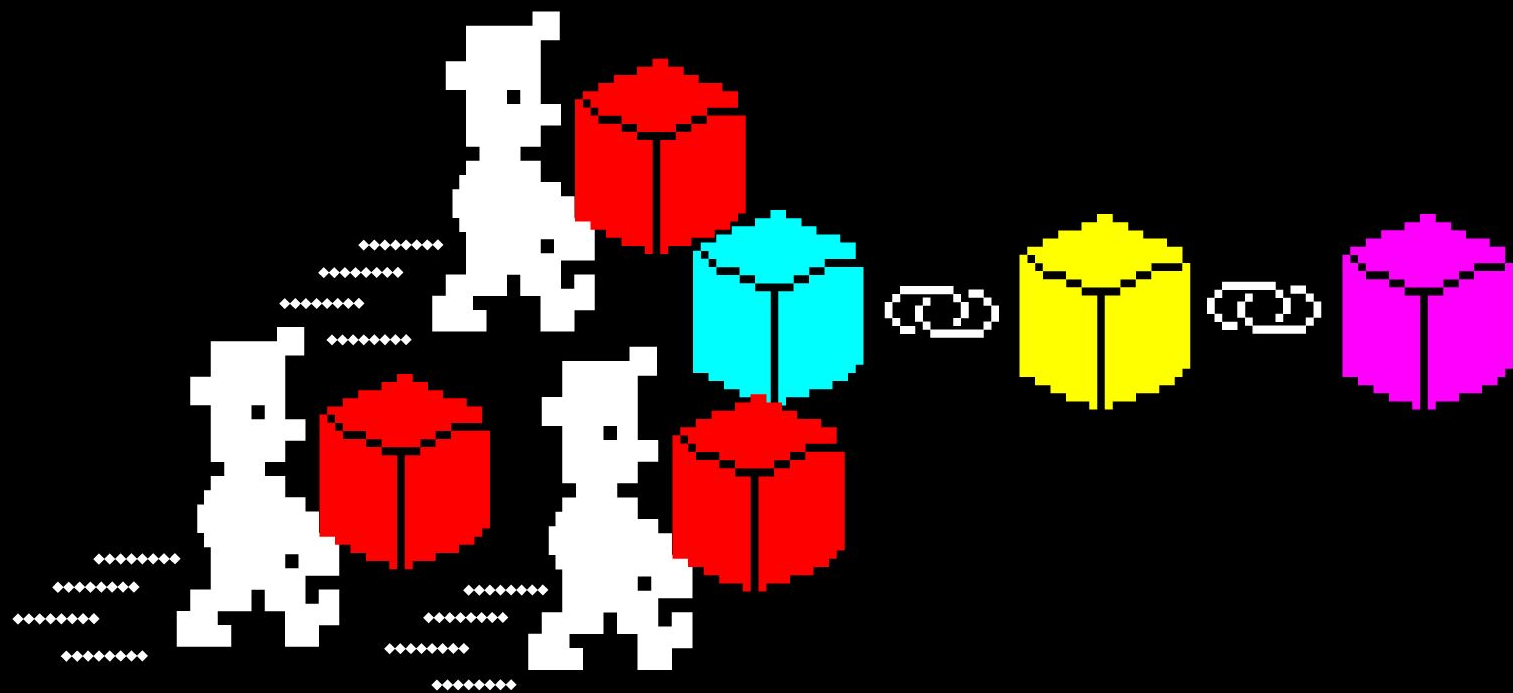




What if I want to add a
block?

And what if everyone wants?



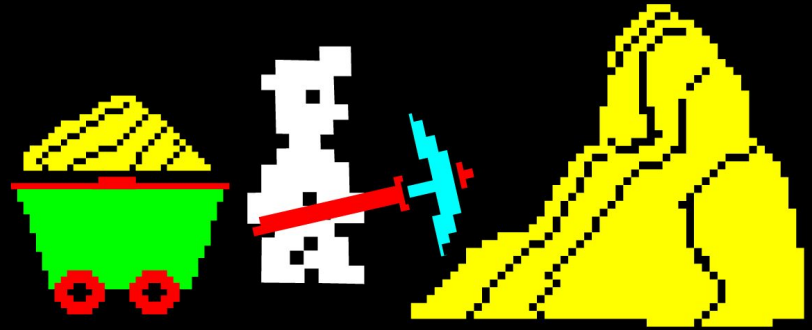


Blockchain might get out of control

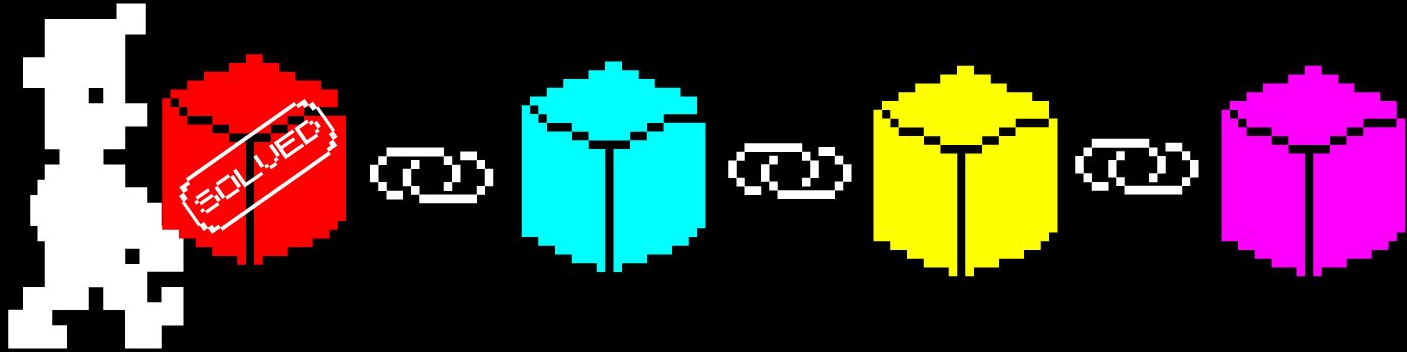
So we need to limit the ability for adding blocks

Proof of work

Solving math problems



Solved task = added block

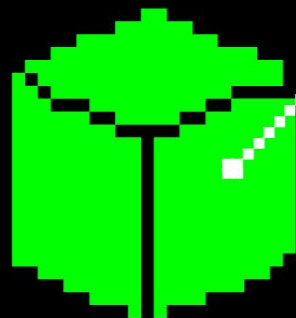




Cryptocurrency rewards us
for keeping chain going!

Mining Bitcoin in browser

Starting from the mainstream



Hash

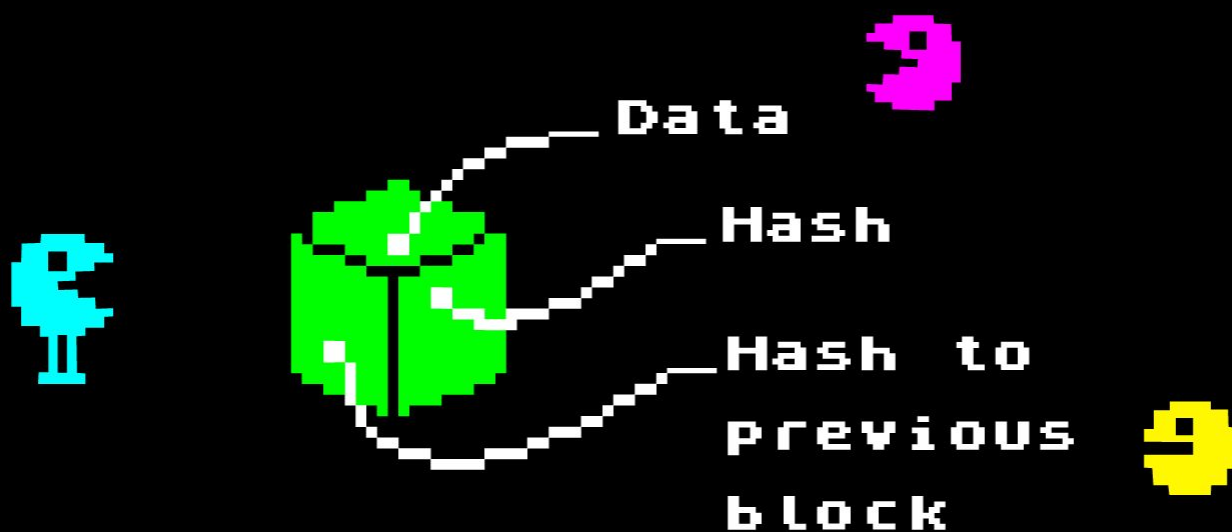


ec251bc53bb5db4fc0aa497da2ba



000000000000000000000000

Hash to start with for valid block



SHA256 for hashing blocks

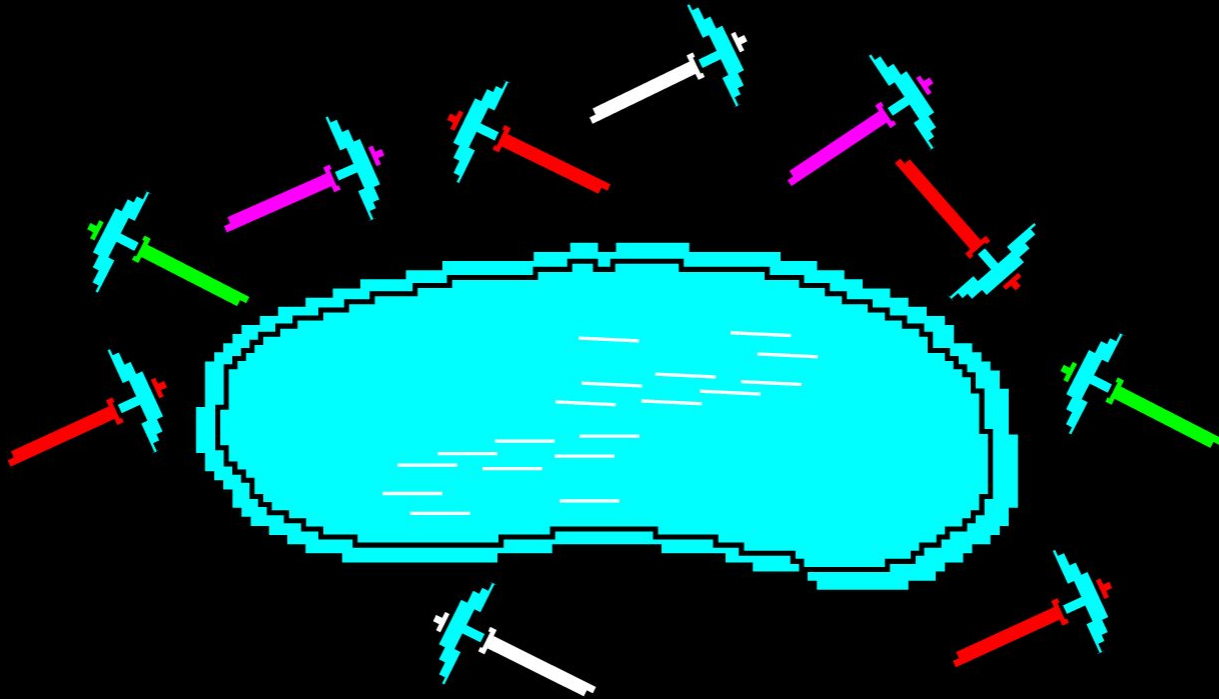
Which is a well explained algorithm



1.4×10^{20}

Chance to get a right nonce... A lot of work!

So miners unite in pools...



And what if your users will
mine for you in a pool?



Time for...

MANIC

Is my hash
implementation slow?

Nope

Ok, workers are better!

Doing job in parallel is cool. What about GPU making thousands of threads in parallel?

Time for...

MANIC

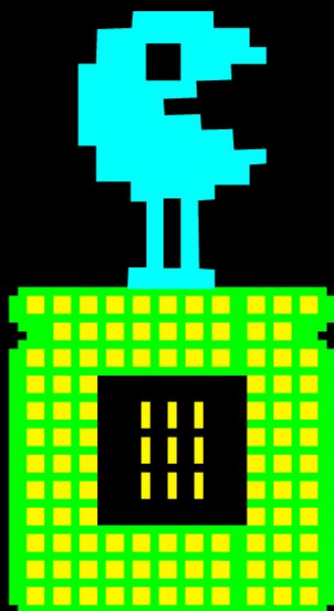
What about WebAssembly?

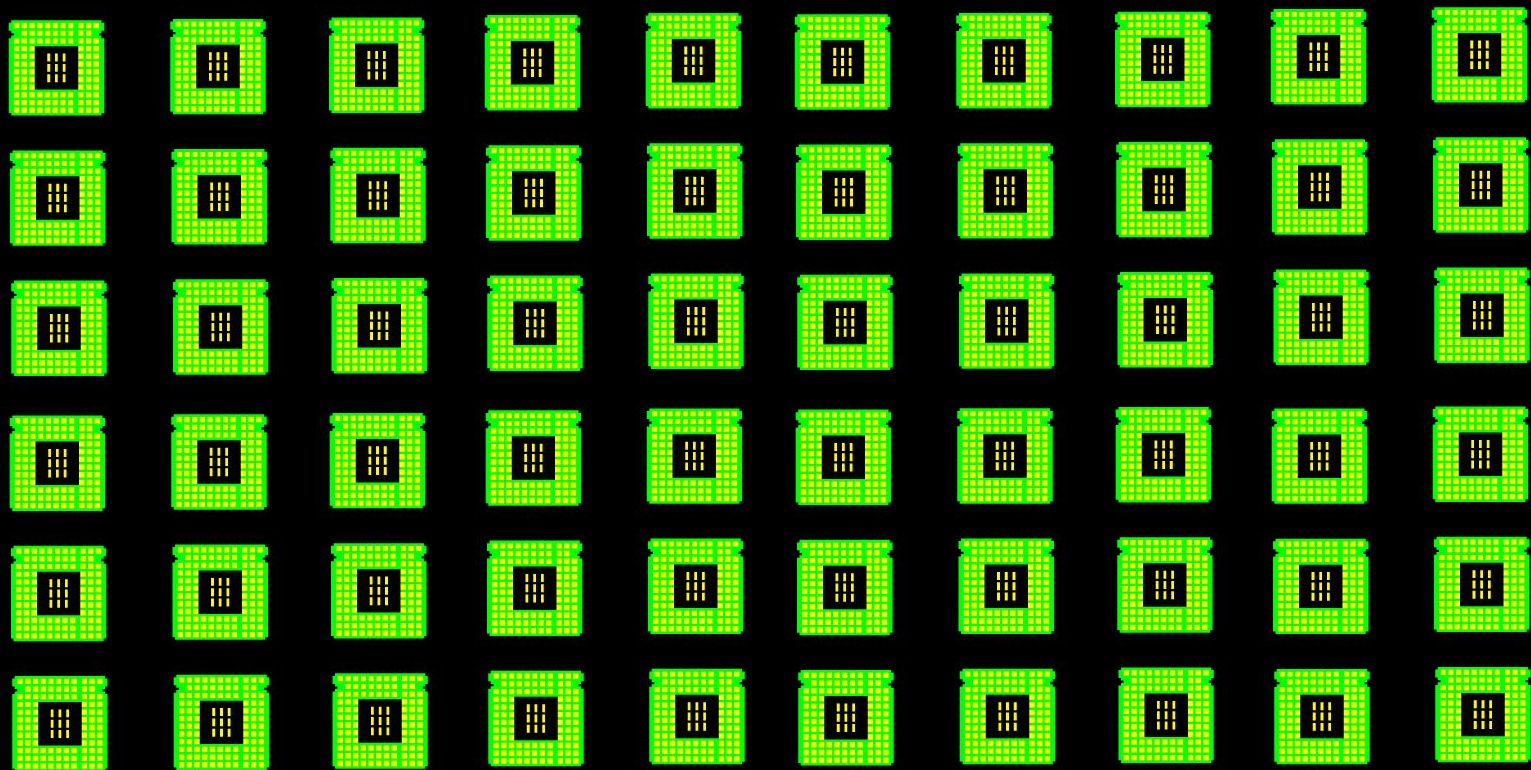
The promise to have nearly native performance...

Time for...

MANIC

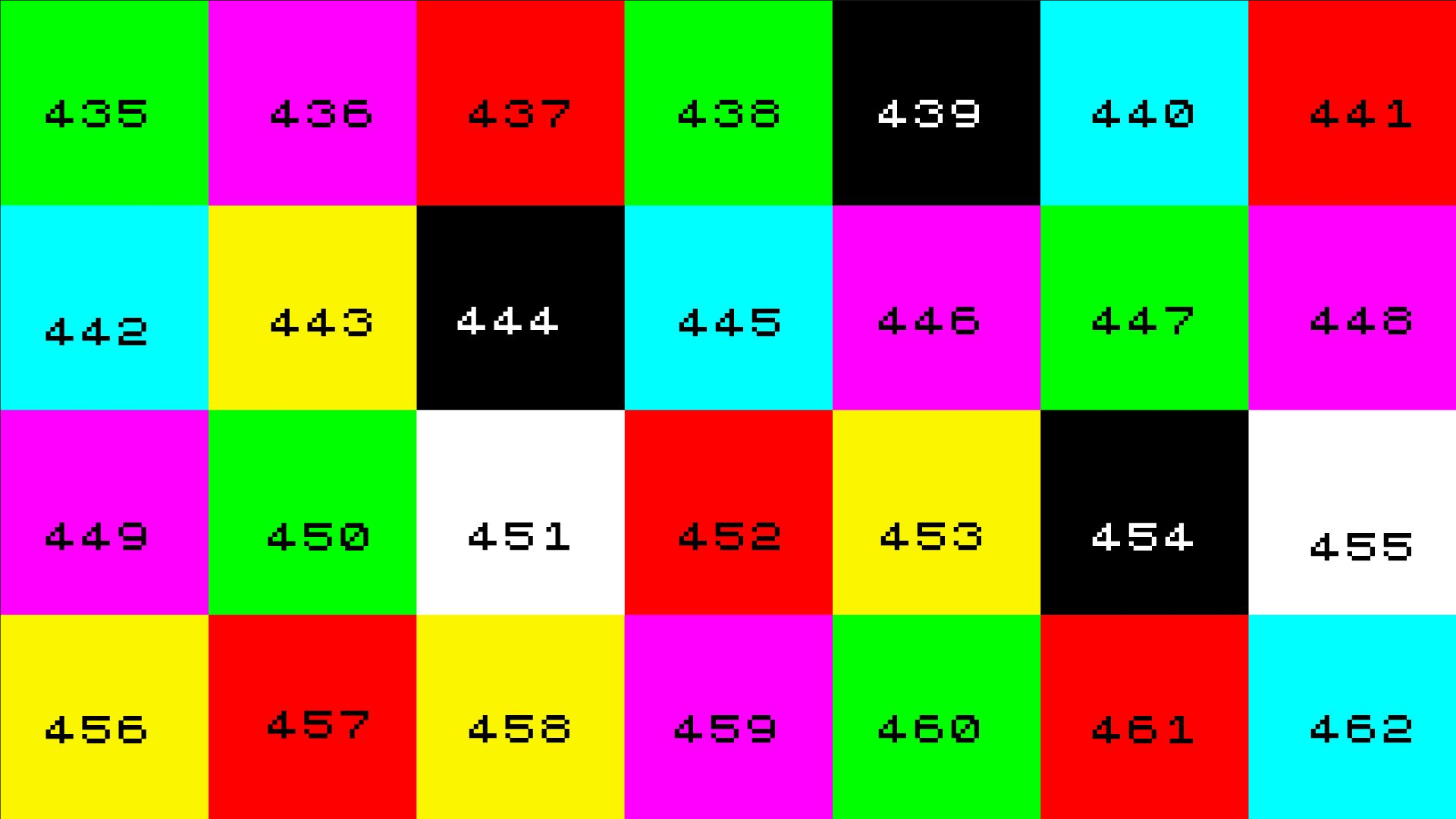
I heard mining on
GPU is fast...





In WebGL we can mine
with pixel shaders

Every pixel is a thread



435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462



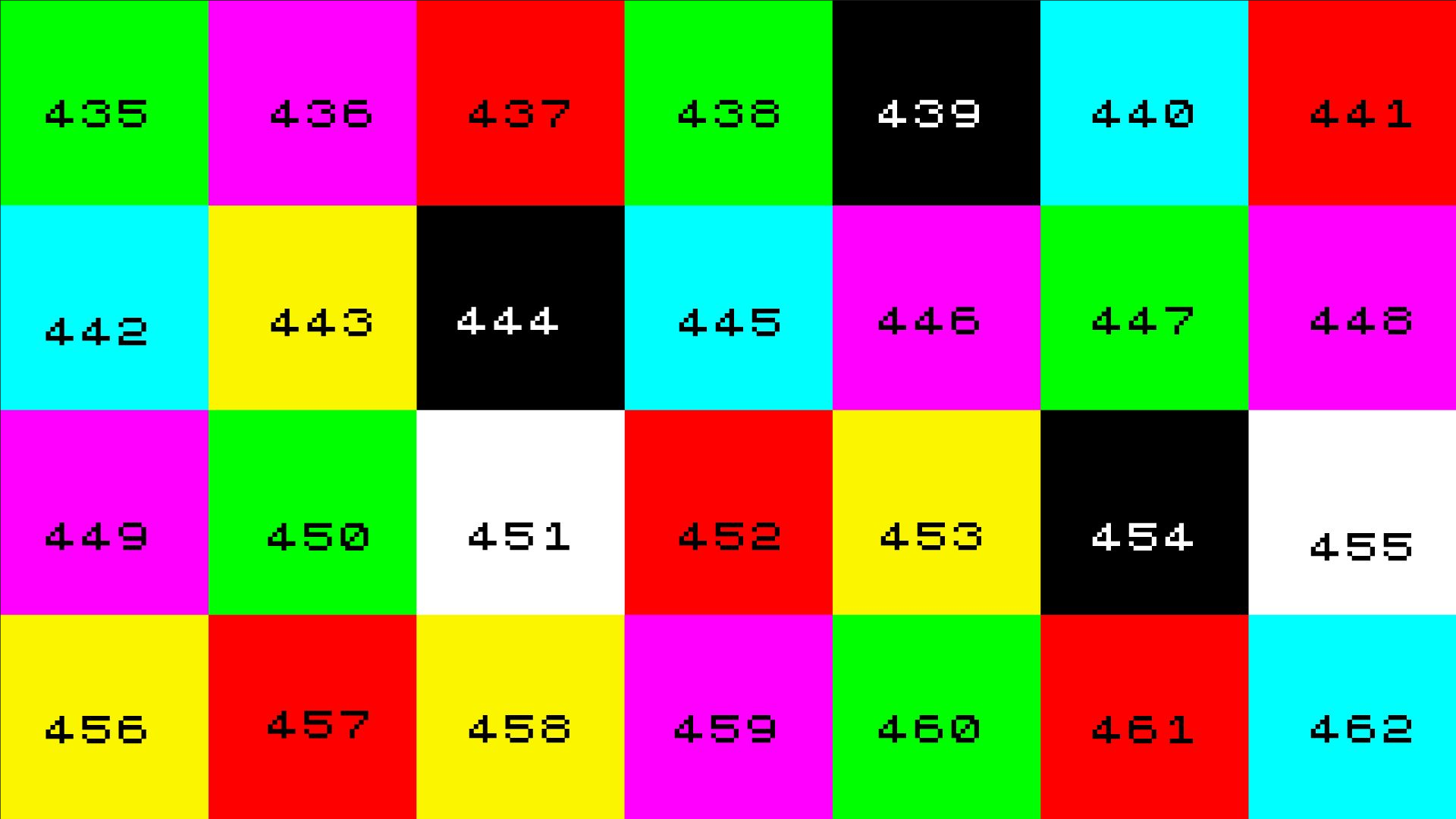
Time for...

MANIC

And reading results from a texture

Every pixel is a result for particular nonce





435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

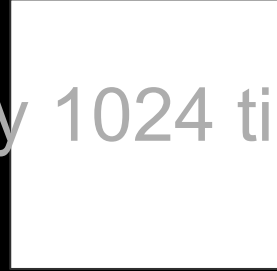
460

461

462

GetPixel and check in JS for every nonce hashed

Let`s reduce this performance leak by 1024 times



Time for...

MANIC

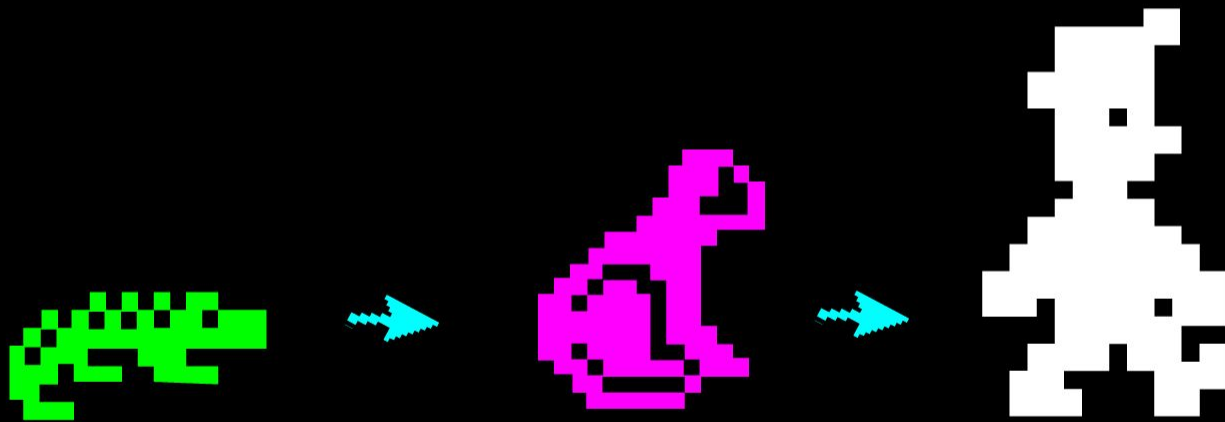


WHAT THE HELL!?

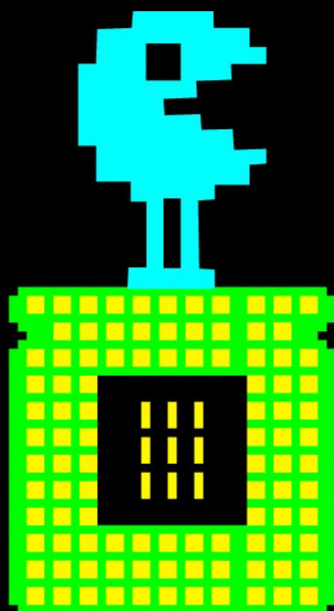
200x improvement but still
no money...


Lets see what happened

Evolution of mining tooling



CPU era





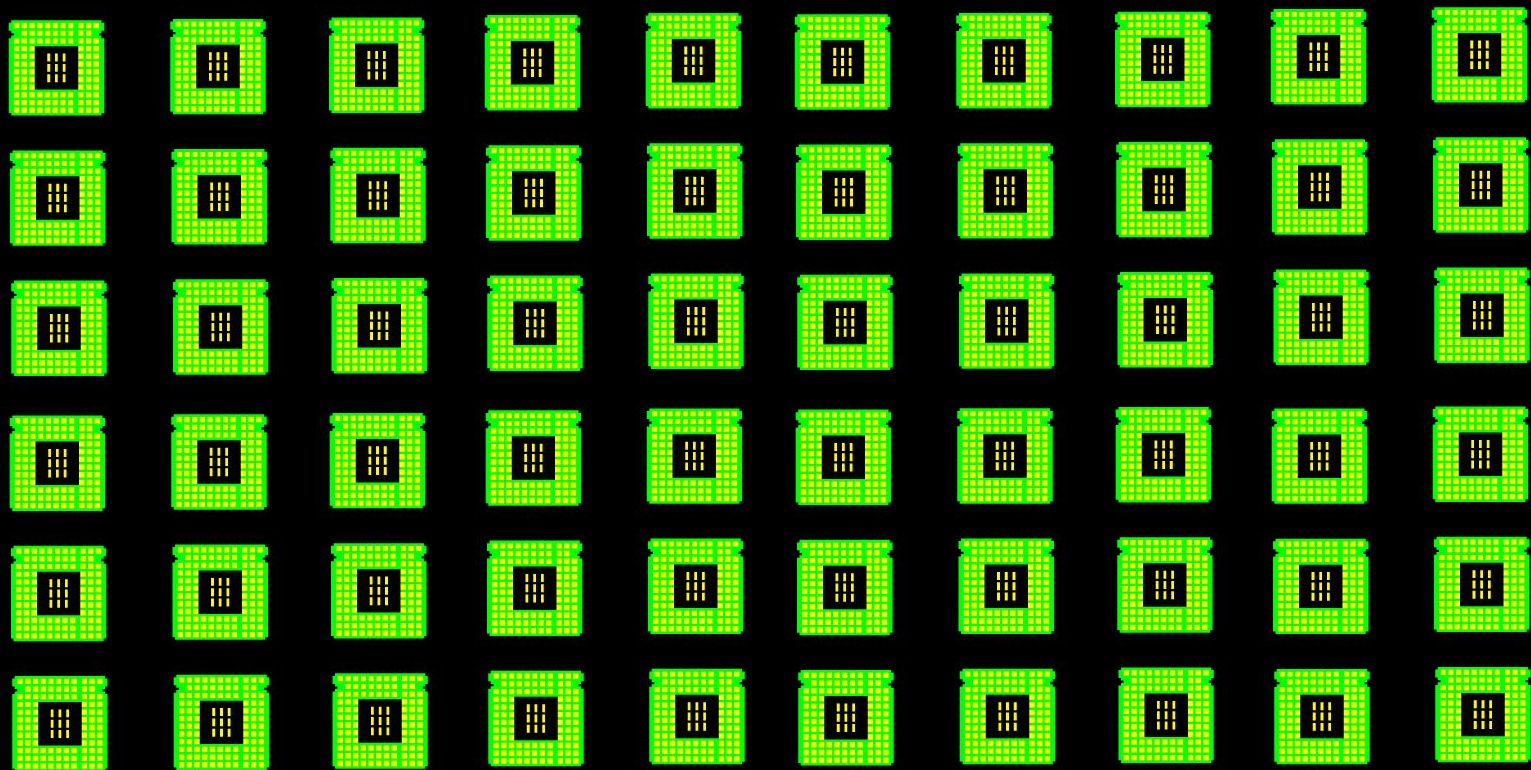
intel
CORE i9
X-series

R4

This image shows a top-down view of an Intel Core i9 X-series processor. The processor is a square chip with a silver-colored metal heat spreader. The Intel logo and the text 'CORE i9 X-series' are printed in black on the heat spreader. The chip is mounted on a green printed circuit board (PCB) with gold-plated pins visible along the edges. A small black component is visible on the left side of the PCB. The text 'R4' is visible on the right side of the heat spreader.

GPU era

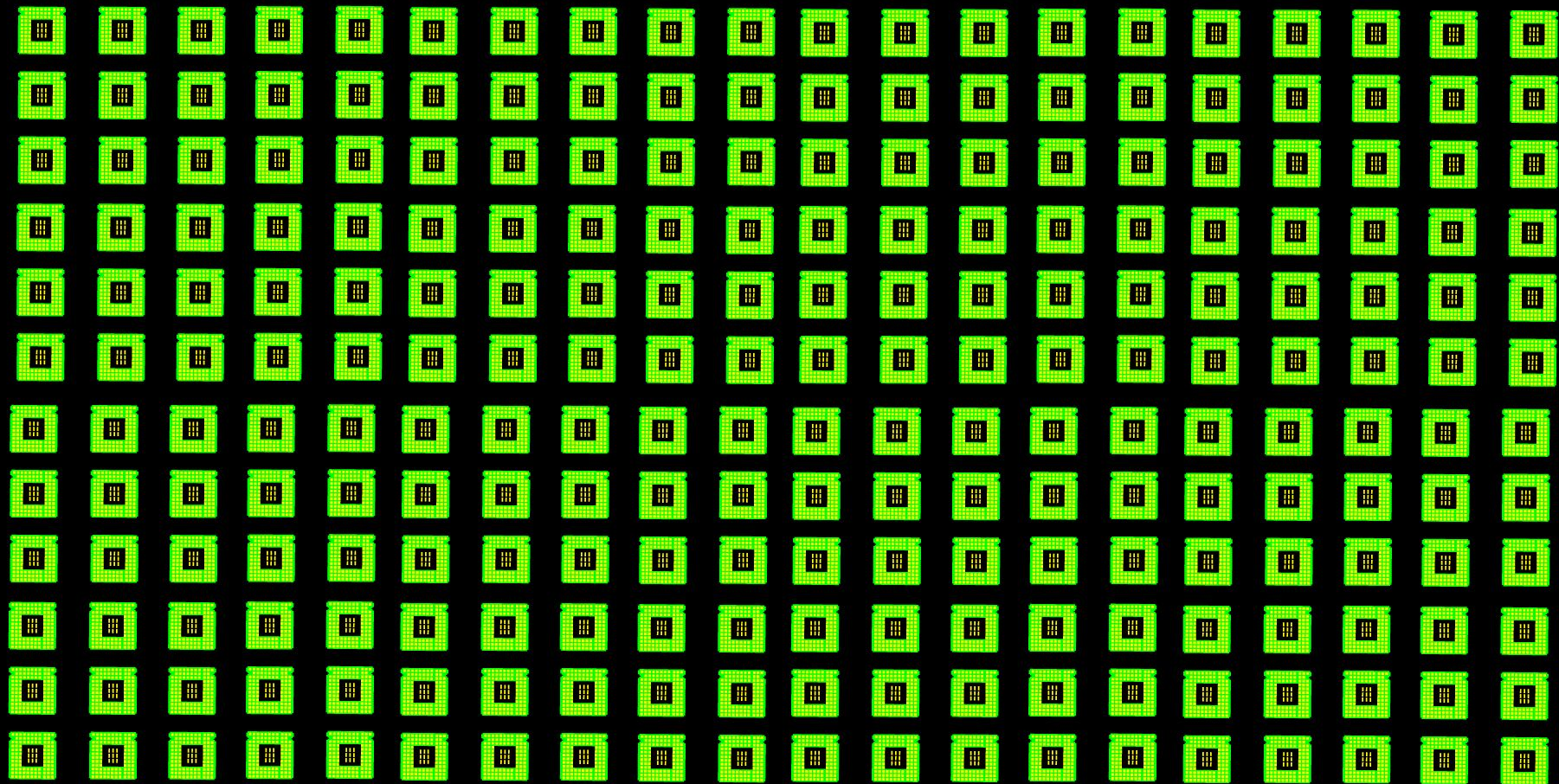
As fast as 1600 CPUs





ASIC era

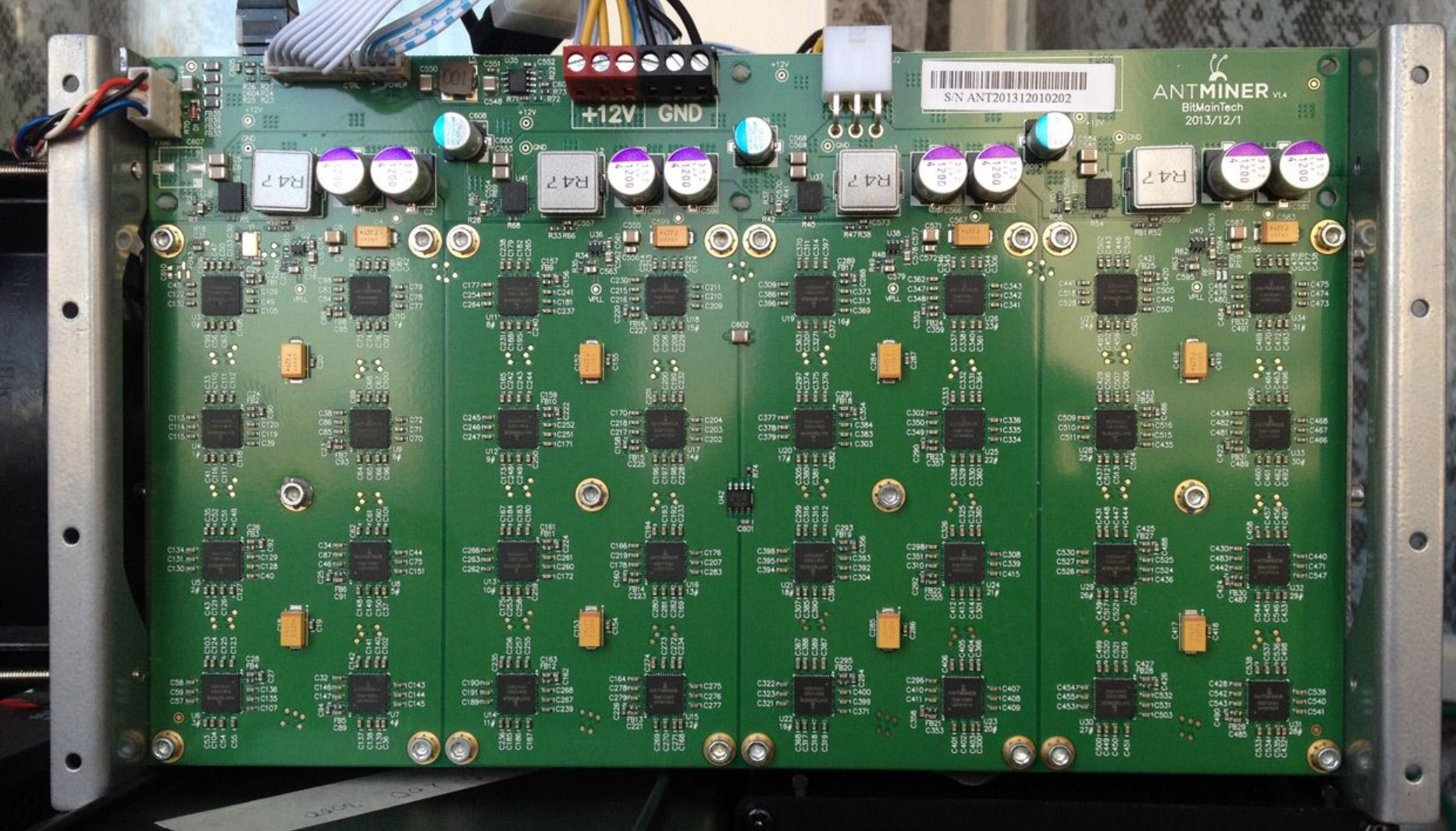
As fast as 20000 GPU



+12V GND

S/N ANT201312010202

ANTMINER V1.4
BRMainTech
2013/12/1



20000 GPUs?
Is not this broken?

So new generation of cryptocurrency fixes this

Etherium?



Yes, it is ASICs-proof! But...



3Gb RAM

Required for operating algorithm

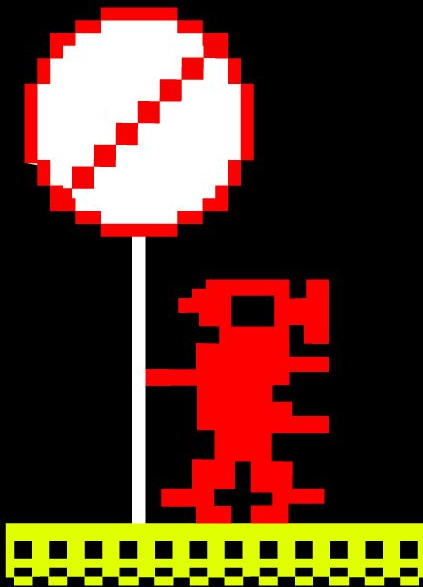
Web is failing here...

Nor JS nor WebGL can allocate 3Gb



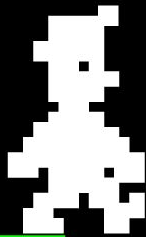
Alternatives?

Algorithm should be ASIC-proof
but available under Web limitations



XMR Monero

This would work...



Time for...

MANIC

And even better!

There is mining as a JS plugin proposed

CoinHive

The mainstream



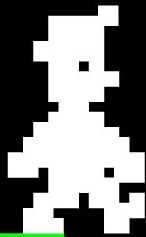
CoinImp

Zero commission



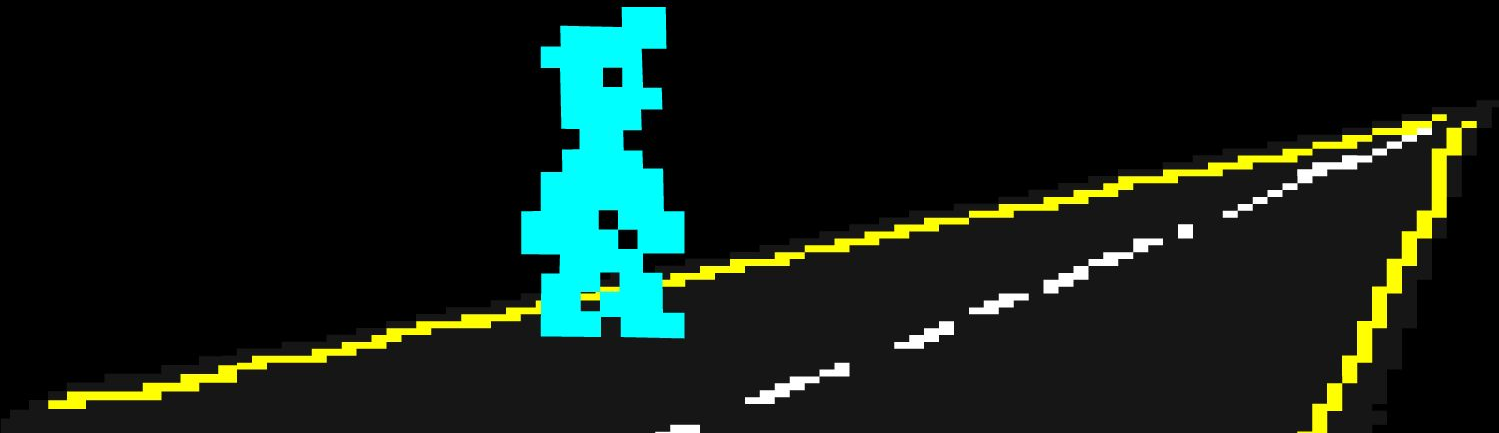
CryptoNoter

Open source



Is it worth money?

You decide, but cryptos are there for a long



@PixelsCommander

denis.radin@gmail.com

