Draw

powered by

Blockchain

DRAW since 2014

- FILA develops a “Draw device” to separate the draw (random numbers) from the software (just displaying the result).
- The machine has a pre-shuffled table (from 1 to 99) and loops in the table around 200 times per second. Every number is pulled out until the next restart from the device.
- Some teams were also doubting about the outcome from them as they have no way of knowing if any electronical hack could have been performed on the device.
- Devices start to be old and a reset in the middle of a draw may lead to some numbers being picked again.

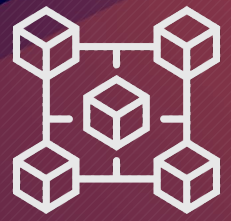
PROBLEMATICS to solve

- Trust in UWW or OG's isn't strong enough and can lead to doubts when some countries get a good draw
- Impossibility of proving that the draw is clean and hasn't been manipulated
- Draw process is slow (coaches coming one by one to the desk), not interesting for public and quite messy
- Performed at the last moment (1 day prior event) to show transparency, which makes promotion difficult.

IDEALLY

- Create trust by outsourcing the Draw 
- Proving that nobody (including UWW or OG) has control of the outcome 
- Giving the possibility to everybody to go online and check by themselves how the bracket has been built 
- Generate the bracket in one shot and display it in an engaging way (with head to head design) 

BLOCKCHAIN Technology



A Blockchain is by design DECENTRELIZED (no one has full control of it), it's UNCHANGABLE (what is written in it will never change), and TRANSPARENT (everybody can read what is inside).

A blockchain is a list of blocks filled with transactions that holds together using cryptography. Until today, the technology has proven itself unbelievably secure and has never been hacked. People around the world use it 24/7 to exchange cryptocurrencies and we are using their actions to build our brackets.

As nobody is in control of what is happening in the blockchain the outcome of it is **UNPREDICTABLE**

UWW has designed a system to get random numbers from the last(s) block(s) of a blockchain.

Why using blockchain for the draw ?

- Blockchain technology is 100% transparent, everything that happens in the blockchain can be checked online
- Blockchain technology doubled with Last Name sorting will make the draws very random
- The technology can be implemented in every Arena across the world, no need for federations to purchase draw devices to offer fair draws
- The bracket will be generated in a second

What is a Block

- A block is a piece of the blockchain
- A block contains from 1 to ~200 transactions
- Nobody can predict which transaction will be in which block as everybody in the world can make a transaction anytime
- A semi-randomized process defines who (validator) can add a new block to the blockchain, this happens every 12 seconds in average
- You can see what the content of a block look like by clicking here (block 9429167)

Which block will be used for the bracket ?

- The blockchain is adding a block to itself every 12 seconds. The goal is to get the last block available at the draw.
- If there is many weight categories, we will always select the most recent block in the order weight (From light to heavy).

Example 1 with one style :

- Categories to draw GR 55, 60, 63 & 67
- Last blocks available : 9929 9928 9927 9926
- GR 55 = 9929 / GR 60 = 9928 / GR 63 = 9927 / GR 67 = 9926

Example 2 with 2 styles :

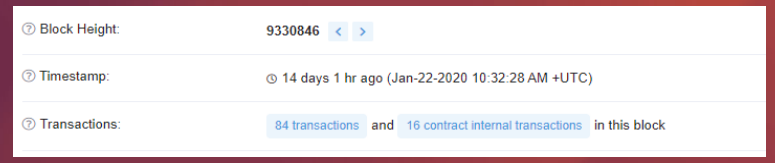
- Categories to draw GR 55, 60 and FW 50 & 55
- Last blocks available : 9929 9928 9927 9926
- GR 55 = 9929 / GR 60 = 9928
- At this point a new block is committed into the chain: 9930
- FW 50 = 9930 / FW 55 = 9927

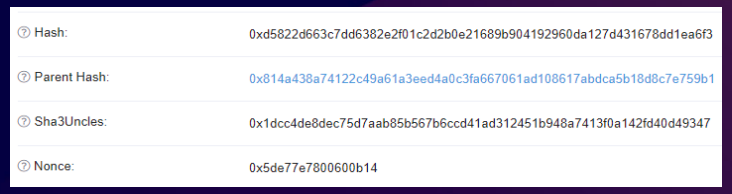
How a block can become to a Draw ?

- Every block has several attributes (ID, timestamp, miner, details of transactions), cryptographic details (checksums = hashes), link to previous block (parent)
- Hashes are just a sequence of numbers. A long sequence with "random" numbers in "random" order based on the content of a block
- Slicing these long strings to pieces provides a set of numbers which are viable to use during draw
- Again: not predictable, fraud proof and easy to verify its authenticity

DRAW USING ETHEREUM BLOCKCHAIN 1/3

1. Getting the last(s) block(s) available (ex : 9330846)
2. Getting the hash's from the block
   (we delete the 0x in front of each hash because it's related to the protocol and never changes)





Hash : ~~0x~~d5822d663c7dd6382e2f01c2d2b0e21689b904192960da127d431678dd1ea6f3

Parent Hash : ~~0x~~814a438a74122c49a61a3eed4a0c3fa667061ad108617abdca5b18d8c7e759b1

Not used because it doesn't change

Nonce : ~~0x~~5de77e7800600b14

3. We concatenate all of them (past them together)

d5822d663c7dd6382e2f01c2d2b0e21689b904192960da127d431678dd1ea6f3814a438a74122c49a61a3eed4a0c3fa667061ad108617abdca5b18d8c7e759b15de77e7800600b14

DRAW USING ETHEREUM BLOCKCHAIN 2/3

d5822d663c7dd6382e2f01c2d2b0e21689b904192960da127d431678dd1ea6f3814a438a74122c49a61a3eed4a0c3fa667061ad108617abdca5b18d8c7e759b15de77e7800600b14

4. Decomposition by 2 units

d5	82	2d	66	3c	7d	d6	38	2e	2f	1	c2	d2	b0	e2	16	89	b9	4	19	29	60	da	12	7d	43	16	78	dd	1e	a6	f3	81	4a	43	8a	74	12	2c	49	a6	1a	3e	ed	4a	0c	3f	a6	67	6	1a	d1	8	61	7a	bd	ca	5b	18	d8	c7	e7	59	b1	5d	e7	7e	78	0	60	0b	14

5. Hexadecimal conversion (to get numbers)*

d5	82	2d	66	3c	7d	d6	38	2e	2f	1	c2	d2	b0	e2	16	89	b9	4	19	29	60	da	12	7d	43	16	78	dd	1e	a6	f3	81	4a	43	8a	74	12	2c	49	a6	1a	3e	ed	4a	0c	3f	a6	67	6	1a	d1	8	61	7a	bd	ca	5b	18	d8	c7	e7	59	b1	5d	e7	7e	78	0	60	0b	14
213	130	45	102	60	125	214	56	46	47	1	194	210	176	226	22	137	185	4	25	41	96	218	18	125	67	22	120	221	30	166	243	129	74	67	138	116	18	44	73	166	26	62	237	74	12	63	166	103	6	26	209	8	97	122	189	202	91	24	216	199	231	89	177	93	231	126	120	0	96	11	20

In this step we also identify duplicates (in red) and delete them

6. **Get a list of numbers that will be used for the draw**

213	130	45	102	60	125	214	56	46	47	1	194	210	176	226	22	137	185	4	25	41	96	218	18		67		120	221	30	166	243	129	74		138	116		44	73		26	62	237		12	63		103	6		209	8	97	122	189	202	91	24	216	199	231	89	177	93			126	0		11	20

* Hexadecimal conversion in a very standard method in IT, many online generators might help you checking a conversion, for example : https://www.rapidtables.com/convert/number/hex-to-decimal.html

DRAW USING ETHEREUM BLOCKCHAIN 3/3

Last Step, Applying the list to our Athletes entries, ordered by Last Name

213 130 45 102 60 125 214 56 46 47 1 194 210 176 226 22 137 185 4 25 41 96 218 18 67 120 221 30 166 243 129 74 138 116 44 73 26 62 237 12 63 103 6 209 8 97 122 189 202 91 24 216 199 231 89 177 93 126 0 11 20

Step 2 - Sort by FAMILY name and Given name		
Draw	Country	Name
213	GUM	Mia Lahnee Ramos AQUINO
130	BRA	Kamila BARBOSA VITO DA SILVA
45	COL	Carolina CASTILLO HIDALGO
102	CAN	Jade Marie DUFOUR
60	CUB	Yusneylys GUZMAN LOPEZ
125	GER	Ellen RIESTERER
214	FRA	Julie Martine SABATIE
56	BUL	Miglena Georgieva SELISHKA
46	AZE	Mariya STADNIK
47	BLR	Kseniya STANKEVICH
1	CHN	Yanan SUN

*In case of Seeds, the number will be assigned to the next wrestler

How to check on a bracket ?

On a bracket you should be able to see what was the block used to generate it, and therefore you can check online if it matches the draw.

By using the steps in previous slides which are :

1) Go on any Ethereum blockchain explorer, look for block no 9332049
2) Get the hash, parent hash and the nonce
3) Past them together
4) Decompose by 2 unit
5) Hexadecimal conversion of each 2 units (to get numbers) - delete doubles
6) Apply the numbers to the entries, sorted by Last Name (not country)

BENEFITS

- Block information is public and available easily access on many websites (https://etherscan.io/ / https://ethplorer.io/)
- The bracket is going to be built using always the same procedure (easy to check)
- Manipulating the blocks in order to get a good draw would require unrealistic amounts of efforts and money and would be publicly displayed on the blockchain.
- Every national federations will be able to use the technology with Arena for free.
- In case of a doubt on the legitimacy of a draw, everybody will be able to check the block and investigate.
- No organization, company or government is owner of the solution, it’s is truly decentralized and autonomous.

FAQ

- Why is it so complicated ?

The draw has been a sensitive subject for years and we can fear that in the past, some draws has been manipulated. The first step to ensure fairness has been for FILA, to take back control of the draws by providing electronical devices. But even so, there is no 100% guarantee that the devices were fair. UWW decided now to move to a 100% transparent method, based on the transactions made by the entire world on the biggest public blockchain, Ethereum. In order to get a random list of numbers big enough for one category, we had to make a list of standard operations that would be accessible to everybody without specific tools. Even it the bracket construction is quite complicated yet, we know the trust on the process will be strong enough that It will dismiss the need of systematic check in short time.

- How can I be sure a block has been used for the bracket ?

On every bracket page, the block used for the draw should be written at the bottom with a link to its full details. UWW will soon provide an online tool to allow everybody to enter a block number and check the outcome.

- I’ve checked the block for a draw and the bracket, they don’t match, what should I do ?

In this case please contact us so we can check what happened. In theory this should be impossible. The bracket might have been manipulated.

- Can it be used without internet ?

Yes and No. To avoid any random number prediction extracted from blocks, Arena only keep blocks for 15 minutes. For every draw Arena caches +10 most recent blocks for further draws. Therefore if there is a temporary network outage, but Arena has enough blocks for the remaining draws (not used and not expired blocks), it is possible to utilize the blockchain framework for those weight categories. Otherwise the Internet connectivity must be restored in order to continue drawing with blocks

- During the draw, why sorting athlete’s list by “Last Name” and not Country anymore

This makes the participants mixed already and avoid to have always the same countries getting the first numbers of the table. Also it would prevent somebody to try to manipulate the blockchain as they won’t know anyway the name of each participant.

FAQ

- When this method will be used ?

Starting from now, on every next events.

- The category I want to draw has more that 80 athletes, is a block enough for 100 numbers ?

No but Arena has been developed to use more blocks if needed. So at the end one category could have 1, 2 or 3 blocks.

We invite our federations to ask their IT responsible or companies who are providing IT services to review this document so you can have an inside opinion on this new Draw Method. We are very confident that the level of transparency and fairness can't be match with any other technic and we are looking forward to get your feedbacks. Here is a detailed version of this presentation.

For any remarks, comments or questions you can contact the IT department at :

it@unitedworldwrestling.org

If you want more details about how blockchain technology works, a more detailed version of this document is available at this address : Detailed version